

BỘ GIAO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HÀI PHÒNG
-----000-----

TÌM HIỂU CHUẨN IEEE 802.15.4 VÀ CÁC ỨNG DỤNG
ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH CÔNG NGHỆ THÔNG TIN

Sinh viên thực hiện: BÙI THỊ BÍCH THU
Giáo viên hướng dẫn: Ths. Nguyễn Trọng
Mã số sinh viên: Thể 110856

LỜI CẢM ƠN

Để hoàn thành đồ án này, trước hết em xin gửi lời cảm ơn và biết ơn sâu sắc tới các thầy giáo, cô giáo Khoa công nghệ thông tin trường Đại Học dân lập Hải Phòng, những người đã giảng dạy và tạo điều kiện cho em trong quá trình học tập và nghiên cứu tại trường. Những kiến thức mà em đã nhận được sẽ là hành trang giúp chúng em vững bối rối trong tương lai.

Em xin bày tỏ lòng biết ơn sâu sắc nhất tới thầy giáo Nguyễn Trọng Thể, người đã tận tình hướng dẫn, chỉ bảo, giúp đỡ em trong suốt thời gian em nghiên cứu và hoàn thành đồ án này. Em cũng xin cảm ơn gia đình và bạn bè đã hết lòng hướng dẫn, chỉ bảo và luôn tạo mọi điều kiện tốt nhất cho em trong suốt thời gian vừa qua.

Mặc dù em đã cố gắng hoàn thành đồ án này trong phạm vi khả năng có thể. Tuy nhiên không tránh khỏi những điều thiếu sót. Em rất mong nhận được sự cảm thông và tận tình chỉ bảo của quý thầy cô và toàn thể các bạn

Hải Phòng, ngày.... tháng năm 2011

MỤC LỤC

MỤC LỤC	3
DANH MỤC HÌNH VẼ	5
DANH MỤC CÁC TỪ VIẾT TẮT	6
LỜI NÓI ĐẦU	7
CHƯƠNG 1: MẠNG CẢM NHẬN KHÔNG DÂY	8
1.1. Tổng quan về mạng cảm nhận không dây	8
1.1.1. Khái niệm	8
1.1.2. Node cảm biến	8
1.1.3. Đặc điểm của cấu trúc mạng cảm biến	8
1.2. Ứng dụng	9
1.2.1. Ứng dụng	9
1.2.2. Nhược điểm	9
1.2.3. Ứng dụng	10
1.2.4. Sự khác nhau giữa WSN và mạng truyền thống	10
*** Kết luận	11
CHƯƠNG 2: KHÁI QUÁT VỀ ZIGBEE/IEEE 802.15.4	12
2.1. Khái niệm	12
2.2. Đặc điểm	12
2.3. Ứng dụng	13
2.4. Mạng ZigBee/ IEEE 802.15.4 LR-WPAN	14
2.4.1. Thành phần của mạng LR-WPAN	14
2.4.2. Kiến trúc liên kết mạng	14
2.4.3. Cấu trúc liên kết mạng hình sao (Star)	15
2.4.4. Cấu trúc liên kết mạng mắt lợn (mesh)	16
2.4.5. Cấu trúc liên kết mạng hình cây (cluster-tree)	17
CHƯƠNG 3: CHUẨN ZIGBEE/IEEE 802.15.4	19
3.1. Mô hình giao thức	19
3.2 Tầng vật lý ZigBee/IEEE 802.15.4	20
3.2.1 Mô hình điều chế tín hiệu	21
3.2.1.1 Điều chế tín hiệu của tầng PHY tại dải số 2.4 GHz	21
3.2.1.2 Điều chế tín hiệu của tầng PHY tại dải tần 868/915MHz	24
3.2.2 Các thông số kỹ thuật trọng tầng vật lý của IEEE 802.15.4	26
3.2.2.1 Chỉ số ED (energy detection)	26
3.2.2.2 Chỉ số chất lượng đường truyền (LQI)	27
3.2.2.3 Chỉ số đánh giá kênh truyền (CCA)	27
3.2.3 Định dạng khung tin PPDU	27
3.3 Tầng điều khiển dữ liệu ZigBee/IEEE 802.15.4 MAC	28
3.3.1 Cấu trúc siêu khung	28
3.3.1.1 Khung CAP	30
3.3.1.2 Khung CFP	30

3.3.1.3 Khoảng cách giữa hai khung (IFS)	31
3.3.2 Thuật toán tránh xung đột đa truy cập sử dụng cảm biến sóng mang CSMA-CA.	31
3.3.3 Các mô hình truyền dữ liệu.	34
3.3.4 Phát thông tin báo hiệu beacon	37
3.3.5 Quản lý và phân phối khe thời gian đảm bảo GTS.	37
3.3.6 Định dạng khung tin MAC.	39
3.4 Tầng mạng của ZigBee/IEEE802.15.4	40
3.4.1 Dịch vụ mạng.....	40
3.4.2 Dịch vụ bảo mật	41
3.5 Tầng ứng dụng của ZigBee/IEEE 802.15.4	43
CHƯƠNG 4: CÁC THUẬT TOÁN ĐỊNH TUYỀN CỦA ZigBee/IEEE 802.15.4 ..	44
4.1 Thuật toán định tuyến theo yêu cầu AODV (Ad hoc On Demand Distance Vector)	44
4.2 Thuật toán hình cây	47
4.2.1 Thuật toán hình cây đơn nhánh	47
4.2.2 Thuật toán hình cây đa nhánh.	50
4.3 Giới thiệu về chương trình mô phỏng OPNET	56
KẾT LUẬN.....	61
TÀI LIỆU THAM KHẢO	62

DANH MỤC HÌNH VẼ

Hình 2.1 Cấu trúc liên kết mạng	15
Hình 2.2 Cấu trúc mạng hình sao	15
Hình 2.3 Cấu trúc mạng mesh.....	16
Hình 2.4 Cấu trúc mạng hình cây.....	17
Hình 3.1 Mô hình giao thức của ZigBee	19
Hình 3.2 Băng tần hệ thống của ZigBee	21
Hình 3.3 Sơ đồ điều chế	22
Hình 3.4 Pha của sóng mang	24
Hình 3.5 Sơ đồ điều chế	25
Hình 3.6 Cấu trúc siêu khung.....	32
Hình 3.7 Sơ đồ khoảng cách hai khung IFS	32
Hình 3.8 Quy đước thuật toán.....	32
Hình 3.9 Liên lạc trong mạng không hỗ trợ beacon	34
Hình 3.10 liên lạc trong mạng có hỗ trợ beacon.....	35
Hình 3.11 Kết nối trong mạng hỗ trợ beacon	36
Hình 3.12 Kết nối trong mạng không hỗ trợ phát beacon	36
Hình 3.13 Khung tin mã hóa tầng MAC	41
Hình 3.14 Khung tin mã hóa tầng mạng	42
Hình 4.1 Định dạng tuyến đường trong giao thức AODV	46
Hình 4.3 Thiết lập kết nối giữa CH và nốt thành viên	49
Hình 4.4 Quá trình hình thành nhánh nhiều bậc	49
Hình 4.5 Gán địa chỉ nhóm trực tiếp.....	51
Hình 4.6 Gán địa chỉ nhóm qua nốt trung gian	52
Hình 4.10 Mô phỏng Zigbee với thợ viễn tử OPNET	57
Hình 4.11 Mô tả giao thức trong Zigbee	58
Hình 4.12 Mô phỏng Zigbee với thợ viễn tử OPNET	59

DANH MỤC CÁC TỪ VIẾT TẮT

PHY	Physical <i>Tầng vật lý</i>
MAC	Medial Access control <i>Tầng điều khiển dữ liệu</i>
PPDU	PHY protocol data unit <i>Khối thu phát dữ liệu tầng vật lý</i>
PAN coordinator	<i>Điều phối mạng</i>
RFD	Reduced function device <i>Thiết bị chức năng giảm</i>
FFD	Full function device <i>Thiết bị có chức năng đầy đủ</i>
O – QPSK	Offset – Quadrature Phrase Shift Keying <i>Khóa dịch pha góc 1/4</i>
CSMA/CA	Carrier Senre Multiple Access Collision A voidance <i>Thuật toán tránh xung đột đa truy cập sử dụng cảm biến sóng mang.</i>
AODV	Ad hoc On Demand Distance Vector <i>Thuật toán tìm đường theo yêu cầu trong mạng</i>

LỜI NÓI ĐẦU

Hàng ngày chúng ta đều thấy những ví dụ mới về cách thức mà công nghệ thông tin và viễn thông (ICT) tác động làm thay đổi cuộc sống của con người trên thế giới. Từ mức độ này hay mức độ khác, cuộc cách mạng kỹ thuật số đã lan rộng đến mọi ngõ ngách trên toàn cầu.

Trong mạng viễn thông ngày nay, con người đang quản lý, trao đổi, giao tiếp tranh luận, “làm chính trị”, mua bán và thử nghiệm – nghĩa là thực hiện tất cả các loại hình hoạt động bằng cách thức mà chỉ có ICT mới có thể làm được. Mạng viễn thông đã tạo ra một cầu nối liên kết loài người trên khắp hành tinh của chúng ta, và đang mở rộng không ngừng, đầy hứa hẹn, hy vọng và không một chút bí ẩn. Tuy vậy, trong một dải băng tần eo hẹp vẫn còn tồn đọng nhiều thách thức nếu muốn đạt được đầy đủ tiềm năng đó. Các nhà khoa học trên thế giới đã nghĩ đến việc sử dụng các băng tần cao hơn, nhưng việc này đang vấp phải nhiều trở ngại vì công nghệ điện tử và chế tạo chưa theo kịp. Vì vậy một giải pháp cấp bách được đưa ra là sử dụng chung kênh tần số, mặc dù vẫn còn nhiều vấn đề phát sinh, ví dụ như là can nhiễu lẫn nhau giữa các thiết bị cùng tần số, hay là vấn đề xung đột giữa các thiết bị... Một trong những công nghệ mới hiện đang được ứng dụng trong các mạng liên lạc đã đạt được hiệu quả là công nghệ ZigBee.

Công nghệ ZigBee là công nghệ được áp dụng cho các hệ thống điều khiển và cảm biến có tốc độ truyền tin thấp nhưng chu kỳ hoạt động dài. Công nghệ ZigBee hoạt động ở dải tần 868/915 MHz và 2,4 GHz, với các ưu điểm là độ trễ truyền tin thấp, tiêu hao ít năng lượng, giá thành thấp, ít lỗi, dễ mở rộng, khả năng toạ độ thích cao. Trong luận văn này, em muốn trình bày các khao cầu của em về công nghệ ZigBee và mô phỏng thuật toán định tuyến của ZigBee để có thể hiểu rõ hơn về công nghệ này.

Hy vọng thông qua các vấn đề được đề cập trong bản đồ án này, bạn đọc sẽ có được sự đánh giá và hiểu biết sâu sắc hơn về công nghệ ZigBee/IEEE 802.15.4 và vai trò cũng như tiềm năng của nó trong cuộc sống.

CHAPTER 1: MẠNG CẢM NHẬN KHÔNG DÂY

1.1. Tổng quan về mạng cảm nhận không dây

1.1.1. Khái niệm

Mạng cảm nhận không dây(WSN) có thể hiểu đơn giản là mạng liên kết các node với nhau bằng kết nối sóng vô tuyến (RF connection) trong đó các node mạng thường là các thiết bị đơn giản, nhỏ gọn, giá thành thấp... và có số lượng lớn, được phân bố một cách không có hệ thống (non-topology) trên một diện tích rộng (phạm vi hoạt động rộng), sử dụng nguồn năng lượng hạn chế (pin), có thời gian hoạt động lâu dài(vài tháng đến vài năm) và có thể hoạt động trong môi trường khắc nghiệt (chất độc, ô nhiễm, nhiệt độ...).

1.1.2. Node cảm biến

Một node cảm biến được cấu tạo bởi 3 thành phần cơ bản sau: vi điều khiển, sensor, bộ phát radio. Ngoài ra, còn có các cổng kết nối máy tính.

- Vi điều khiển: Bao gồm CPU, bộ nhớ ROM, RAM, bộ phận chuyển đổi tín hiệu từ analog sang digital và ngược lại.
- Sensor: Chức năng cảm nhận thế giới bên ngoài, sau đó chuyển dữ liệu qua bộ phận chuyển đổi để xử lý.
- Bộ phát radio: Bởi vì node cảm biến là thành phần quan trọng nhất trong WSN, do vậy việc thiết kế các node cảm biến sao cho có thể tiết kiệm được tối đa nguồn năng lượng là vẫn đề quan trọng hàng đầu.

1.1.3. Đặc điểm của cấu trúc mạng cảm biến

Đặc điểm của mạng cảm biến là bao gồm một số lượng lớn các node cảm biến, các node cảm biến có giới hạn và giảng buộc về tài nguyên đặc biệt là năng lượng rất khắt khe. Do đó, cấu trúc mạng mới có đặc điểm rất khác với các mạng truyền thống. Sau đây ta sẽ phân tích một số đặc điểm nổi bật trong các mạng cảm biến như sau:

- Không có lỗ hổng

- Khả năng mở rộng
- Ràng buộc phản ứng
- Môi trường hoạt động
- Phổ quát tiện truyền dẫn
- Cấu hình mạng cảm biến

1.2. Ưu, nhược điểm và ứng dụng của mạng cảm nhận không dây

1.2.1. Ưu điểm

Mạng không dây không dùng cáp cho các kết nối, thay vào đó, chúng sử dụng sóng radio, cũng tương tự như điện thoại không dây. Ưu thế của mạng không dây là khả năng di động và sự tự do, người dùng không bị hạn chế về không gian và vị trí kết nối. Những ưu điểm của mạng không dây bao gồm:

- Khả năng di động và sự tự do – cho phép kết nối từ bất kỳ đâu.
- Không bị hạn chế về không gian và vị trí kết nối.
- Dễ lắp đặt và triển khai.
- Không cần mua cáp.
- Tiết kiệm thời gian lắp đặt cáp.
- Dễ dàng mở rộng

1.2.2. Những thách thức, trở ngại

Để WSNs thực sự trở nên rộng khắp trong các ứng dụng, một số thách thức và trở ngại cần phải vượt qua

- Lưu trữ dữ liệu
- Vấn đề về năng lượng
- Khả năng chịu nỗi
- Định vị
- Khả năng mở rộng

- An ninh

1.2.3. Ứng dụng của mạng cảm nhận không dây

WSN bao gồm các node cảm biến nhỏ gọn, thích ứng được môi trường khắc nghiệt. Những node cảm biến này, cảm nhận môi trường xung quanh, sau đó gửi những thông tin thu được đến trung tâm xử lý theo ứng dụng. Các node không những có thể liên lạc với các node xung quanh nó, mà còn có thể xử lý dữ liệu trước khi gửi đến các node khác. WSN cung cấp rất nhiều những ứng dụng hữu ích ở nhiều lĩnh vực trong cuộc sống.

- Ứng dụng quân sự an ninh và thiên nhiên
- Ứng dụng trong giám sát xe cộ và các thông tin liên quan
- Ứng dụng cho việc điều khiển các thiết bị trong nhà
- Ứng dụng các tòa nhà tự động
- Ứng dụng trong quá trình quản lý tự động trong công nghiệp
- Ứng dụng trong y học

1.2.4 Sự khác nhau giữa WSN và mạng truyền thống

Qua phân tích và tìm hiểu ta có thể thấy được sự khác biệt cơ bản của WSN và mạng truyền thống như sau.

- Số lượng các nút cảm biến trong một mạng cảm biến lớn hơn nhiều lần so với những nút cảm biến ad-hoc
- Các nút cảm biến thường được triển khai với mật độ dày hơn
- Những nút cảm biến dễ hỏng, ngừng hoạt động.
- Topology mạng cảm biến thay đổi rất thường xuyên.
- Mạng cảm biến chủ yếu sử dụng truyền thông quảng bá (broadcast) trong khi mà đa số các mạng ad hoc là điểm - điểm (point- to- point)
- Những nút cảm biến có giới hạn về năng lượng, khả năng tính toán và bộ nhớ.

- Những nút cảm biến có thể định danh toàn cầu(global ID).
- Truyền năng lượng qua các phơơng tiện không dây.
- Chia sẻ nhiệm vụ giữa các node lân cận

**** Kết luận

Trong chương này chúng ta đã tìm hiểu tổng quan về mạng cảm nhận không dây, cấu trúc và các ứng dụng của nó đã cho thấy sự phát triển của mạng cảm biến và tầm quan trọng đối với cuộc sống của chúng ta. Với sự phát triển nhoi vũ bão của khoa học công nghệ thì lĩnh vực mạng cảm biến sẽ có nhiều ứng dụng mới.

CHAPTER 2: KHÁI QUÁT VỀ ZIGBEE/IEEE 802.15.4

2.1. Khái niệm

Cái tên ZigBee được xuất phát từ cách mà các con ong mật truyền những thông tin quan trọng với các thành viên khác trong tổ ong. Đó là kiểu liên lạc “Zig-Zag” của loài ong “honeyBee”. Và nguyên lý ZigBee được hình thành từ việc ghép hai chữ cái đầu với nhau. Việc công nghệ này ra đời chính là sự giải quyết cho vấn đề các thiết bị tách rời có thể làm việc cùng nhau để giải quyết một vấn đề nào đó.

2.2. Đặc điểm

Đặc điểm của công nghệ ZigBee là tốc độ truyền tin thấp, tiêu hao ít năng lượng, chi phí thấp, và là giao thức mạng không dây hướng tới các ứng dụng điều khiển từ xa và tự động hóa. Tổ chức IEEE 802.15.4 bắt đầu làm việc với chuẩn tốc độ thấp được một thời gian ngắn thi tiêu ban về ZigBee và tổ chức IEEE quyết định sát nhập và lấy tên ZigBee đặt cho công nghệ mới này. Mục tiêu của công nghệ ZigBee là nhắm tới việc truyền tin với mức tiêu hao năng lượng nhỏ và công suất thấp cho những thiết bị chỉ có thời gian sống từ vài tháng đến vài năm mà không yêu cầu cao về tốc độ truyền tin như Bluetooth. Một điều nổi bật là ZigBee có thể dùng được trong các mạng mây lõi (mesh network) rộng hơn là sử dụng công nghệ Bluetooth. Các thiết bị không dây sử dụng công nghệ ZigBee có thể dễ dàng truyền tin trong khoảng cách 10-75m tùy thuộc và môi trường truyền và mức công suất phát được yêu cầu với mỗi ứng dụng. Tốc độ dữ liệu là 250kbps ở dải tần 2.4GHz (tổng cầu), 40kbps ở dải tần 915MHz (Mỹ+Nhật) và 20kbps ở dải tần 868MHz (Châu Âu).

Các nhóm nghiên cứu Zigbee và tổ chức IEEE đã làm việc cùng nhau để chi rõ toàn bộ các khía cạnh giao thức của công nghệ này. IEEE 802.15.4 tập trung nghiên cứu vào 2 tầng thấp của giao thức (tầng vật lý và tầng liên kết dữ liệu). Zigbee còn 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 nhau nhưng vẫn theo một chuẩn riêng để làm việc cùng nhau được mà không tương tác lẫn nhau.

Hiện nay thì IEEE 802.15.4 tập trung vào các chi tiết kỹ thuật của tầng vật lý PHY và tầng điều khiển truy cập MAC ứng với mỗi loại mạng khác nhau (mạng hình sao, mạng hình cây, mạng mắt lợn). Các phong pháp định tuyến được thiết kế sao cho năng lượng được bảo toàn và độ trễ trong truyền tin là ở mức thấp nhất có thể bằng cách dùng các khe thời gian bảo đảm (GTSs_guaranteed time slots). Tính năng nổi bật chỉ có ở tầng mạng Zigbee là giảm thiểu được sự hỏng hóc dẫn đến gián đoạn kết nối tại một nút mạng trong mạng mesh. Nhiệm vụ đặc trưng của tầng PHY gồm có phát hiện chất lượng của đường truyền (LQI) và năng lượng truyền (ED), đánh giá kênh truyền (CCA), giúp nâng cao khả năng chung sống với các loại mạng không dây khác.

2.3. Ưu điểm của ZigBee/IEEE 802.15.4 với Bluetooth/IEEE 802.15.1

- Zigbee cũng tương tự như Bluetooth nhưng đơn giản hơn, Zigbee có tốc độ truyền dữ liệu thấp hơn, tiết kiệm năng lượng hơn. Một nút mạng trong mạng Zigbee có khả năng hoạt động từ 6 tháng đến 2 năm chỉ với nguồn là hai ác quy AA.
- Phạm vi hoạt động của Zigbee là 10-75m trong khi của Bluetooth chỉ là 10m (trong trường hợp không có khuếch đại).
- Zigbee xếp sau Bluetooth về tốc độ truyền dữ liệu. Tốc độ truyền của Zigbee là 250kbps tại 2.4GHz, 40kbps tại 915MHz và 20kbps tại 868MHz trong khi tốc độ này của Bluetooth là 1Mbps.
- Zigbee sử dụng cấu hình chủ-tớ cơ bản phù hợp với mạng hình sao tĩnh trong đó các thiết bị giao tiếp với nhau thông qua các gói tin nhỏ. Loại mạng này cho phép tối đa tới 254 nút mạng. Giao thức Bluetooth phức tạp hơn bởi loại giao thức này hướng tới truyền file, hình ảnh, thoại trong các mạng ad hoc (ad hoc là một loại mạng đặc trưng cho việc tổ chức tự do, tính chất của nó là bị hạn chế về không gian và thời gian). Các thiết bị Bluetooth có thể hỗ trợ mạng scatternet là tập hợp của nhiều mạng piconet không đồng bộ. Nó chỉ cho phép tối đa là 8 nút slave trong một mạng chủ-tớ cơ bản.

- Nút mạng sử dụng Zigbee vận hành tốn ít năng lượng, nó có thể gửi và nhận các gói tin trong khoảng 15msec trong khi thiết bị Bluetooth chỉ có thể làm việc này trong 3sec.

2.4. Mạng ZigBee/ IEEE 802.15.4 LR-WPAN

Đặc điểm chính của chuẩn này là tính mềm dẻo, tiêu hao ít năng lượng, chi phí nhỏ, và tốc độ truyền dữ liệu thấp trong khoảng không gian nhỏ, thuận tiện khi áp dụng trong các khu vực nhỏ nhà riêng, văn phòng....

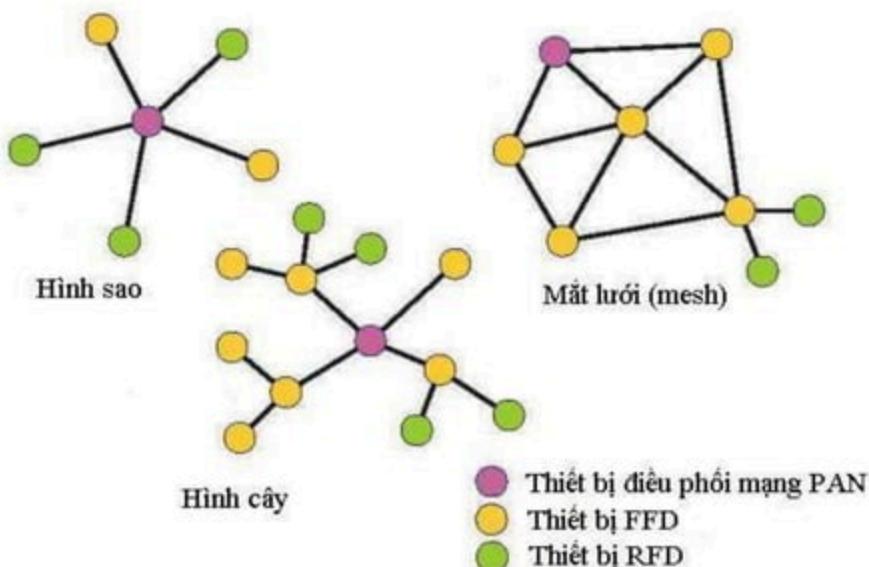
2.4.1. Thành phần của mạng LR-WPAN

Một hệ thống ZigBee/IEEE802.15.4 gồm nhiều phần tạo nên. Phần cơ bản nhất tạo nên một mạng là thiết bị có tên là FFD (full-function device), thiết bị này đảm nhận tất cả các chức năng trong mạng và hoạt động như một bộ điều phối mạng PAN, ngoài ra còn có một số thiết bị đảm nhận một số chức năng hạn chế có tên là RFD (reduced-function device). Một mạng tối thiểu phải có 1 thiết bị FFD, thiết bị này hoạt động như một bộ điều phối mạng PAN.

FFD có thể hoạt động trong ba trạng thái : là điều phối viên của toàn mạng PAN (personal area network), hay là điều phối viên của một mạng con, hoặc đơn giản chỉ là một thành viên trong mạng. RFD được dùng cho các ứng dụng đơn giản, không yêu cầu gửi lượng lớn dữ liệu. Một FFD có thể làm việc với nhiều RFD hay nhiều FFD, trong khi một RFD chỉ có thể làm việc với một FFD.

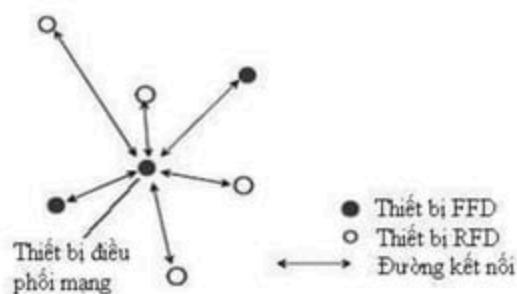
2.4.2. Kiến trúc liên kết mạng

Hiện nay Zigbee và tổ chức chuẩn IEEE đã đưa ra một số cấu trúc liên kết mạng cho công nghệ Zigbee. Các node mạng trong một mạng Zigbee có thể liên kết với nhau theo cấu trúc mạng hình sao (star) cấu trúc mạng hình lưới(Mesh) cấu trúc bô cụm hình cây. Sự đa dạng về cấu trúc mạng này cho phép công nghệ Zigbee được ứng dụng một cách rộng rãi. Hình 1 cho ta thấy ba loại mạng mà ZigBee cung cấp: tópô sao, tópô mắt lưới, tópô cây.



Hình 2.1 Cấu trúc liên kết mạng

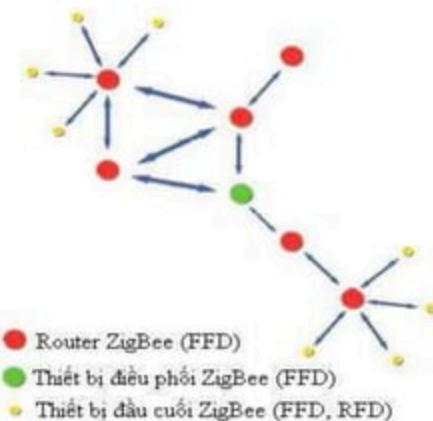
2.4.3. Cấu trúc liên kết mạng hình sao (Star)



Hình 2.2 Cấu trúc mạng hình sao

Đối với loại mạng này, một kết nối được thành lập bởi các thiết bị với một thiết bị 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 chi số nhận dạng cá nhân của riêng mình được gọi là PAN ID(PAN identifier), nó cho phép mạng này có thể hoạt động một cách độc lập. Khi đó cả FFD và RFD đều có thể kết nối tới bộ điều phối mạng PAN. Tất cả mạng nằm trong tầm phủ sóng đều phải có một PAN duy nhất, các nút trong mạng PAN phải kết nối với (PAN coordinator) bộ điều phối mạng PAN.

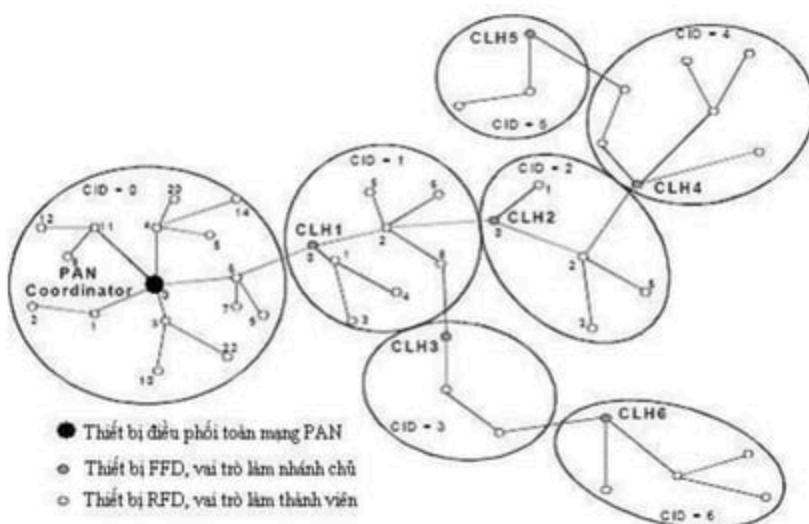
2.4.4. Cấu trúc liên kết mạng mắt lợn (mesh)



Hình 2.3 Cấu trúc mạng mesh

Kiểu cấu trúc mạng này cũng có một bộ điều phối mạng PAN (PAN coordinator). Thực chất đây là kết hợp của 2 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 miễn là thiết bị đó nằm trong phạm vi phủ sóng của thiết bị A. Các ứng dụng của cấu trúc này có thể áp dụng trong đo lường và điều khiển, mạng cảm biến không dây, theo dõi cảnh báo và kiểm kê (cảnh báo cháy rừng....).

2.4.5. Cấu trúc liên kết mạng hình cây (cluster-tree)



Hình 2.4 Cấu trúc mạng hình cây

Cấu trúc này là một dạng đặc biệt của cấu trúc mảng lõi, trong đó đa số thiết bị là FFD và một RFD có thể kết nối vào mạng hình cây như một nốt 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 qui mô phủ sóng và khả năng 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 (PAN coordinator).

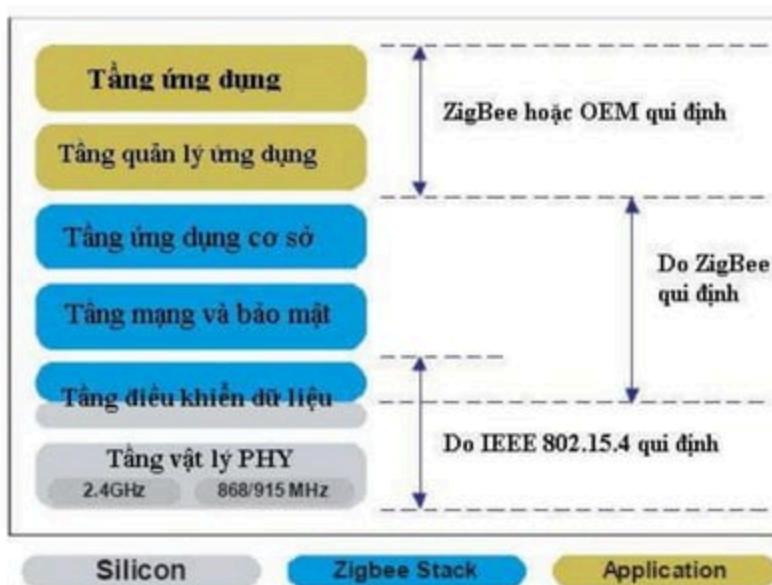
Bộ điều phối mạng PAN coordinator này tạo ra nhóm đầu tiên cách tự baura ngoài lãnh đạo cho mạng của mình, và gán cho người lãnh đạo đó một chỉ số nhận dạng cá nhân đặc biệt gọi là CLH (cluster head) bằng CID-0 (cluster identifier), nó chọn một PAN identifier rồi và phát khung tin quảng bá nhận dạng tới các thiết bị lân cận. Thiết bị nào nhận được khung tin này có thể yêu cầu kết nối vào mạng với CLH. Nếu bộ điều phối mạng PAN (PAN coordinator) 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 có thể hình thành được các CLH1,CLH2,...(như hình 1.4).

CHAPTER 3: CHUẨN ZIGBEE/IEEE 802.15.4

3.1. Mô hình giao thức của ZigBee/IEEE 802.15.4

ZigBee/IEEE 802.15.4 là công nghệ mới phát triển do được khoắng gần một năm trở lại đây. Công nghệ này xây dựng và phát triển các tầng ứng dụng và tầng mạng trên nền tảng là hai tầng PHY và MAC theo chuẩn IEEE 802.15.4, chính vì thế nên nó thừa hưởng được ưu điểm của chuẩn IEEE802.15.4. Đó là tinh tin cậy, đơn giản, tiêu hao ít năng lượng và khả năng thích ứng cao với các môi trường mạng. Dựa vào mô hình như hình 2.1, các nhà sản xuất khác nhau có thể chế tạo ra các sản phẩm khác nhau mà vẫn có thể làm việc tương thích cùng với nhau.



Hình 3.1 Mô hình giao thức của ZigBee

3.2 Tầng vật lý ZigBee/IEEE 802.15.4

Tầng vật lý (PHY) cung cấp hai dịch vụ là dịch vụ dữ liệu PHY và dịch vụ quản lý PHY, hai dịch vụ này có giao diện với dịch vụ quản lý tầng vật lý PLME (physical layer management). Dịch vụ dữ liệu PHY điều khiển việc thu và phát của khối dữ liệu PPDU (PHY protocol data unit) thông qua kênh sóng vô tuyến vật lý.

Các tính năng của tầng PHY là sự kích hoạt hoặc giảm kích hoạt của bộ phận nhận sóng, phát hiện năng lượng, chọn kênh, chỉ số độ rộng truyền, giải phóng kênh truyền, thu và phát các gói dữ liệu qua môi trường truyền.

Chuẩn IEEE 802.15.4 định nghĩa ba dải tần số khác nhau theo khuyến nghị của Châu Âu, Nhật Bản, Mỹ.

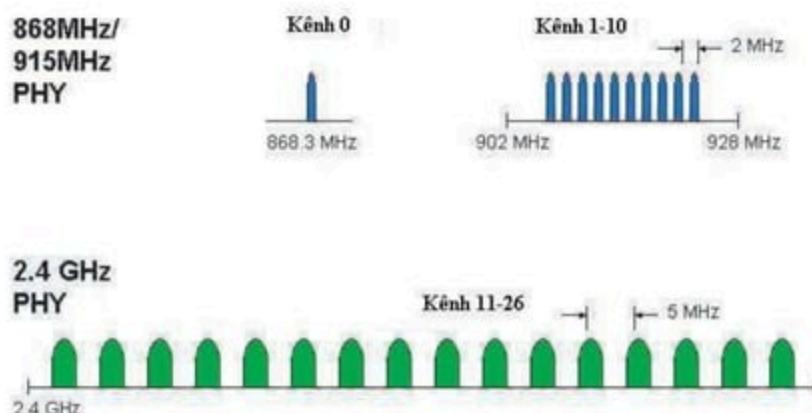
PHY(MHz)	Băng Tần(MHz)	Tốc Độ Chip(kchips/s)	Điều Chế	Tốc Độ Bit(kb/s)	Tốc Độ Ký Tự(ksymbol/s)	Ký Tự
868	868-868.6	300	BPSK	20	20	Nhị Phân
915	902-928	600	BPSK	40	40	Nhị Phân
2450	2400-2486.5	2000	O-QPSK	250	62.5	Hệ 16

Bảng 3.1 Băng tần và tốc độ dữ liệu.

Có tất cả 27 kênh truyền trên các dải tần số khác nhau được mô tả nhoé bảng dưới đây.

Tần số trung tâm (MHz)	Số lượng kênh (N)	Kênh	Tần số kênh trung tâm (MHz)
868	1	0	868.3
915	10	1-10	906+2(k-1)
2405	16	11-16	2405+5(k-11)

Bảng 3.2 Kênh truyền và tần số



Hình 3.2 Bảng tần số của ZigBee

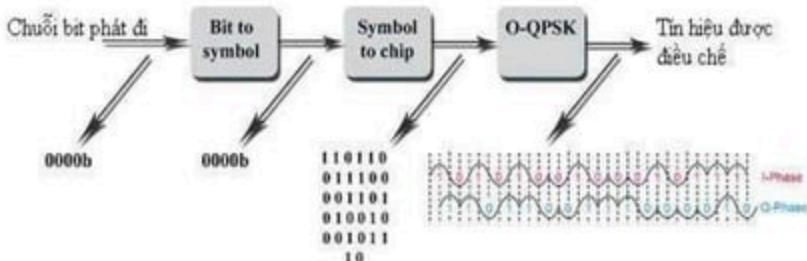
3.2.1 Mô hình điều chế tín hiệu của tầng vật lý.

3.2.1.1 Điều chế tín hiệu của tầng PHY tại dải số 2.4 GHz

Tốc độ truyền dữ liệu của PHY 2405MHz có thể đạt tới 250 kb/s

➤ **Sơ đồ điều chế**

Việc điều chế từ bit dữ liệu nhị phân sang dạng tín hiệu trong dài tần 2,4GHz được mô tả theo sơ đồ dưới đây. Một chuỗi số nhị phân “0000b” được biến đổi sang chuỗi dài tần cơ sở với định dạng xung.



Hình 3.3 Sơ đồ điều chế

➤ **Bộ chuyển bit thành ký tự :**

Theo như sơ đồ trên thì đây là bước đầu tiên để mã hóa tất cả dữ liệu trong PPDU từ mã nhị phân sang dạng ký tự. Mỗi byte được chia thành ký tự và ký tự có nghĩa nhỏ nhất được phát đầu tiên. Đối với trường hợp trường hợp byte đó liên quan đến bảo mật thì trong trường đó byte có nghĩa lớn nhất sẽ được phát trước.

➤ **Bộ chuyển ký tự thành chip:**

Theo như sơ đồ thì đây là bước thứ hai trong quá trình mã hóa. Mỗi ký tự dữ liệu được sắp xếp trong một chuỗi giả ngẫu nhiên (Pseudo-random) 32-chip. Chuỗi chip này được truyền đi với tốc độ 2Mchip/s với chip có nghĩa nhỏ nhất (c_0) được truyền trước mọi ký tự.

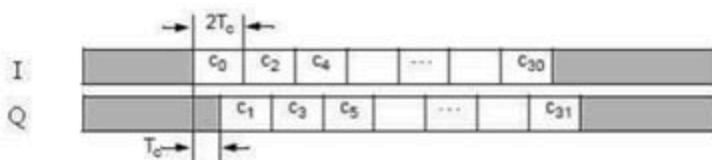
Ký Tự Dữ Liệu (Hệ Thập Phân)	Giá Trị Chip (c0 c1 ... c30 c31)
0	11011001110000110101001000101110
1	11101101100111000011010100100010
2	00101110110110011100001101010010
3	00100010111011011001110000110101
4	01010010001011101101100111000011
5	00110101001000101110110110011100
6	11000011010100100010111011011001
7	10011100001101010010001011101101
8	1000110010010110000001110111101
9	10111000110010010110000001110111
10	01111011100011001001011000000111
11	01110111101110001100100101100000
12	000001110111000111000110010010110
13	0110000001110111011100011001001001
14	1001011000000111011101110001100
15	1100100101100000011101110111000

Bảng 3.3 Sơ đồ biến đổi symbol to chip



Bộ điều chế O-QPSK :

Phương pháp điều chế được dùng ở đây là phương pháp điều chế khóa dịch pha góc $\frac{1}{4}$ có chọn góc dịch pha ban đầu O-QPSK (Offset-Quadrature Phase Shift Keying) tương đương với phương pháp điều chế khóa dịch pha tối thiểu MSK (Minimum Shift Keying). QPSK là phương pháp hiệu quả đối với dài tần số ché. Mỗi phần tử tin hiệu biểu diễn cho 2 bit. Bằng việc sử dụng độ dịch offset trong O-QPSK, thay đổi pha trong tín hiệu tổng hợp tối đa là 90° , cũng trong trường hợp này mà dùng QPSK thì độ lệch pha tối đa là 180° .



Hình 3.4 Pha của sóng mang

Như vậy O-QPSK cung cấp một phương pháp tốt hơn QPSK khi kênh truyền có các thành phần không tuyến tính.

Biểu thức sau đây chỉ ra cách mà O-QPSK có thể diễn đạt:

$$s(t) = \frac{1}{\sqrt{2}} I(t) \cos 2\pi f_c t + \frac{1}{\sqrt{2}} Q(t-T_c) \sin 2\pi f_c t \quad (1)$$

f_c : là tần số trung tâm.

T_c : là thời gian mà Q trễ đạt tới thay đổi pha 90°

Q : sóng mang vuông pha.

I : sóng mang cùng pha.

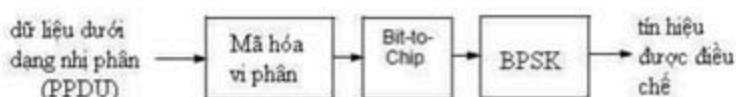
Việc sử dụng dạng xung nửa sin để khử đi những biến thiên biên độ. Công thức sau mô tả dạng xung nửa sin.

$$p(t) = \begin{cases} \sin(\frac{\pi t}{2T_c}), & 0 \leq t \leq 2T_c \\ 0, & \text{ngoài ra} \end{cases} \quad (2)$$

3.2.1.2 Điều chế tín hiệu của tầng PHY tại dải tần 868/915MHz

Tốc độ truyền dữ liệu của ZigBee/IEEE802.15.4 PHY tại băng tần 868 MHz có thể đạt tới 20kb/s, và có thể đạt tới 40 kb/s ở băng tần 915MHz.

➤ **Sơ đồ điều chế**



Hình 3.5 Sơ đồ điều chế

➤ **Bộ mã hóa vi phân**

Mã hóa vi phân hay còn gọi là mã hóa trojóc. Khi cho tín hiệu nhị phân vào bộ mã hóa này thì bit có giá trị 0 sẽ được chuyển tiếp, có nghĩa là số được tách là số 1 nếu số liền trojóc nó là số 0 và ngược lại. Nếu một số được tách xung sai, lỗi này sẽ có xu hướng lan truyền đi, và để loại trừ việc này thi Lender đã đề nghị việc mã hóa trojóc số các dữ liệu. Có nghĩ là nếu chuỗi số dữ liệu thô là R_n thì ta sẽ phát đi chuỗi số E_n theo qui tắc:

$$E_n = R_n \oplus E_{n-1} \quad (3)$$

Trong đó:

$$1 \oplus 1 = 0 \oplus 0 = 0$$

$$0 \oplus 1 = 1 \oplus 0 = 1$$

E_n là chuỗi bit sau khi mã hóa

R_n là chuỗi bit thô

E_{n-1} là chuỗi bit mã hóa liền trước

➤ **Bộ ánh xạ bit thành chip.**

Mỗi bit đầu vào có thể ánh xạ sang chuỗi giá ngẫu nhiên (PN) 15-chip theo như bảng dưới đây. Trong khoảng thời gian mỗi symbol thì ký tự có được truyền đầu tiên, ký tự 14c được chuyển sau cùng.

Bit Đầu Vào	Giá Trị Chip (c ₀ c ₁c ₁₄)
0	111101011001000
1	000010100110111

Bảng 3.4 Biến đổi bit to chip



Bộ điều chế khóa dịch pha nhị phân BPSK

Chuỗi chip được điều chế trên sóng mang sử dụng phương pháp điều chế BPSK có dạng xung là xung cosin nâng (raised cosine). Tốc độ chip là 300kchip/s trong dải tần 868 MHz và đạt được 600 kchip/s trong dải tần 915MHz. Công Thức sau mô tả dạng xung này :

$$p(t) = \frac{\sin\left(\frac{\pi t}{T_c}\right) \cdot \cos\left(\frac{\pi t}{T_c}\right)}{\pi t/T_c \cdot (1 - (4t^2/T_c^2))} \quad (4)$$

3.2.2 Các thông số kỹ thuật trọng tầng vật lý của IEEE 802.15.4

3.2.2.1 Chỉ số ED (energy detection)

Chi số ED đo đặc được bởi bộ thu ED. Chi số này sẽ được tầng mạng sử dụng như là một bộ lọc trong thuật toán chọn kênh. ED là kết quả của sự lọc lượng công suất

năng lượng của tín hiệu nhận được trong băng thông của kênh trong IEEE 802.15.4. 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 ED thường đợt khoảng thời gian 8 symbol. Kết quả phát hiện năng lượng sẽ được thông báo bằng 8 bit số nguyên trong khoảng từ 0x00 tới 0xff. Giá trị nhỏ nhất của ED (=0) khi mà công suất nhận được ít hơn mức +10dB so với lý thuyết. Độ lớn của khoảng công suất nhận được để hiển thị chỉ số ED tối thiểu là 40dB và sai số là ± 6dB.

3.2.2.2 Chỉ số chất lượng đợt truyền (LQI)

Chi số chất lượng đường truyền LQI là đặc trưng chất lượng gói tin nhận được. Số đo này có thể bổ sung vào ED thu được, đánh giá tỷ số tin trên tạp SNR, hoặc một sự kết hợp của những phương pháp này. Giá trị kết quả LQI được giao cho tầng mạng và tầng ứng dụng xử lý.

3.2.2.3 Chỉ số đánh giá kênh truyền (CCA)

CCA được sử dụng để xem xét khi nào một kênh truyền được coi là rỗng hay bận. Có ba phương pháp để thực hiện việc kiểm tra này:

- CCA 1 : “Năng lượng vượt ngưỡng”. CCA sẽ thông báo kênh truyền bận trong khi dò ra bất kỳ năng lượng nào vượt ngưỡng ED.
- CCA 2 : “Cảm biến sóng mang”. CCA thông báo kênh truyền bận chỉ khi nhận ra tín hiệu có đặc tính trái phổ và điều chế của IEEE802.15.4. Tin hiệu này có thể thấp hoặc cao hơn ngưỡng ED.
- CCA 3 : “Cảm biến sóng mang kết hợp với năng lượng vượt ngưỡng”. CCA sẽ báo kênh truyền bận chỉ khi dò ra tín hiệu có đặc tính trái phổ và điều chế của IEEE 802.15.4 với năng lượng vượt ngưỡng ED.

3.2.3 Định dạng khung tin PPDU.

Mỗi khung tin PPDU bao gồm các trường thông tin.

- SHR (synchronization header) : đồng bộ thiết bị thu và chốt chuỗi bit
- PHR (PHY header): chứa thông tin độ dài khung
- PHY payload: chứa khung tin của tầng MAC

Octets: 4	1	1	variable
Đầu khung	SFD (bắt đầu phân định khung)	Độ dài khung (7 bits)	Phần giành riêng (1 bit)
SHR		PHR	PHY payload

Bảng 2.5 Định dạng khung PPDU

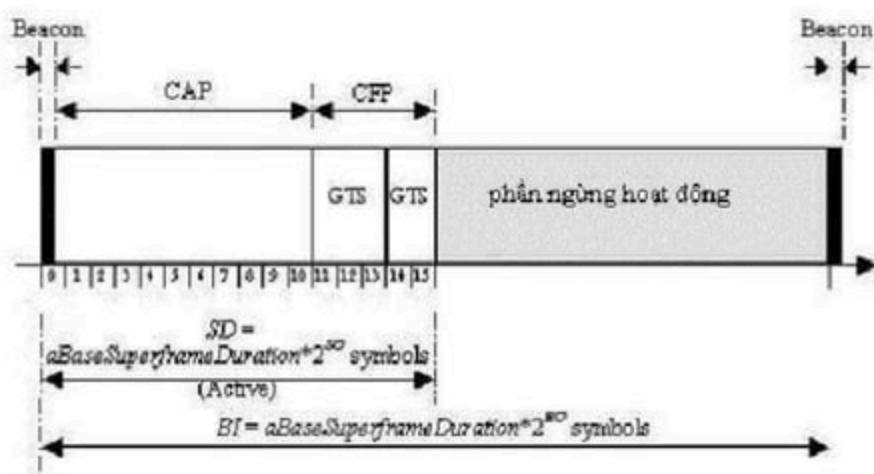
3.3 Tầng điều khiển dữ liệu ZigBee/IEEE 802.15.4 MAC

Tầng điều khiển môi trường truy cập MAC (media access control) cung cấp 2 dịch vụ là dịch vụ dữ liệu MAC và quản lý MAC, nó có giao diện với điểm truy cập dịch vụ của thực thể quản lý tầng MAC (MLMESAP). 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.

3.3.1 Cấu trúc siêu khung.

LR-WPAN cho phép sử dụng theo nhu cầu cấu trúc siêu khung. Định dạng của siêu khung được định rõ bởi PAN coordinator. Mỗi siêu khung được giới hạn bởi từng mạng và được chia thành 16 khe nhợt nhau. Cột mốc báo hiệu dò đòng beacon được gửi đi trong khe đầu tiên của mỗi siêu khung. Nếu một PAN coordinator không muốn sử dụng siêu khung thì nó phải dừng việc phát mốc beacon. Mốc này có nhiệm đồng bộ các thiết bị định kèm, nhận dạng PAN và chứa nội dung mô tả cấu trúc của siêu khung.



Hình 2.6 Cấu trúc siêu khung

Siêu khung có 2 phần “hoạt động” và “nghi”. Trong trạng thái “nghi” thì PAN coordinator không giao tiếp với các thiết bị trong mạng PAN, và làm việc ở mode công suất thấp. Phần “hoạt động” gồm 2 giai đoạn: 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 một kênh truyền hoặc tài nguyên trên mạng). Bất kỳ 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 CFP gồm có các GTSs, các khe thời gian GTS này thường xuất hiện ở cuối của siêu khung tích cực mà siêu khung này được bắt đầu ở khe sát ngay sau CAP. PAN coordinator có thể định vị được bảy trong số các GTSs, và mỗi một GTS chiếm nhiều hơn một khe thời gian.

Khoảng thời gian tồn tại của các phần khác nhau của siêu khung được định nghĩa bởi giá trị của macBeaconOrder và macSuperFrameOrder. macBeaconOrder mô tả khoảng thời gian mà bộ điều phối coordinator truyền khung báo hiệu tìm đường. Khoảng thời gian giữa hai mốc beacon BI(beacon interval) có quan hệ tới

macBeaconOrder (BO) theo biểu thức sau: $BI = aBaseSuperFrameDuration^* 2 BOsymbol$, với $0 \leq BO \leq 14$. Lưu ý rằng siêu khung được bỏ qua nếu $BO=15$.

Giá trị của macSuperFrameOrder cho biết độ dài của phần tích cực của siêu khung. Khoảng thời gian siêu khung_SD (superframe duration) có quan hệ macSuperFrameOrder_SO theo biểu thức sau: $SD=aBaseSuperFrameDuration^* 2 SOsymbol$. Nếu $SO=15$ thì siêu khung vẫn có thể ở phần “nghi” sau mốc beacon của khung.

Phần tích cực của mỗi siêu khung được chia thành 3 phần CAP, CFP và beacon. Mốc beacon được phát vào đầu ở khe số 0 mà không cần sử dụng CSMA.

3.3.1.1 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. CAP sẽ có tối thiểu aMinCAPLength symbols trừ trường hợp phần không gian thêm vào được dùng để điều chỉnh việc tăng độ dài của khung beacon để vẫn có thể duy trì được GTS và điều chỉnh linh động tăng hay giảm kích thước của CFP.

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 sử dụng thuật toán CSMA-CA để truy nhập kênh. Một thiết bị phát trong khoảng thời gian phần CAP kết thúc sẽ khoảng thời gian IFS trước khi hết phần CAP. Nếu không thể kết thúc được thì thiết bị này sẽ trì hoãn việc phát cho đến khi CAP của khung tiếp theo được phát. Khung chứa lệnh điều khiển MAC sẽ được phát trong phần CAP.

3.3.1.2 Khung CFP

Phần CFP sẽ được phát ngay sau phần CAP và kết thúc trước khi phát beacon của khung kế tiếp. Nếu bắt kỳ một GTS nào được cấp phát bởi bộ điều phối mạng PAN, chúng sẽ được đặt bên trong phần CFP và lắp đầy một loạt các khe liền nhau. Bởi vậy kích thước của phần CFP sẽ do tổng độ dài các khe GTSs này quyết định. CFP không sử dụng thuật toán CSMA-CA để truy nhập kênh. Một thiết bị phát trong CFP sẽ kết thúc trong khoảng một IFS trước khi kết thúc GTS.

3.3.1.3 Khoảng cách giữa hai khung (IFS)

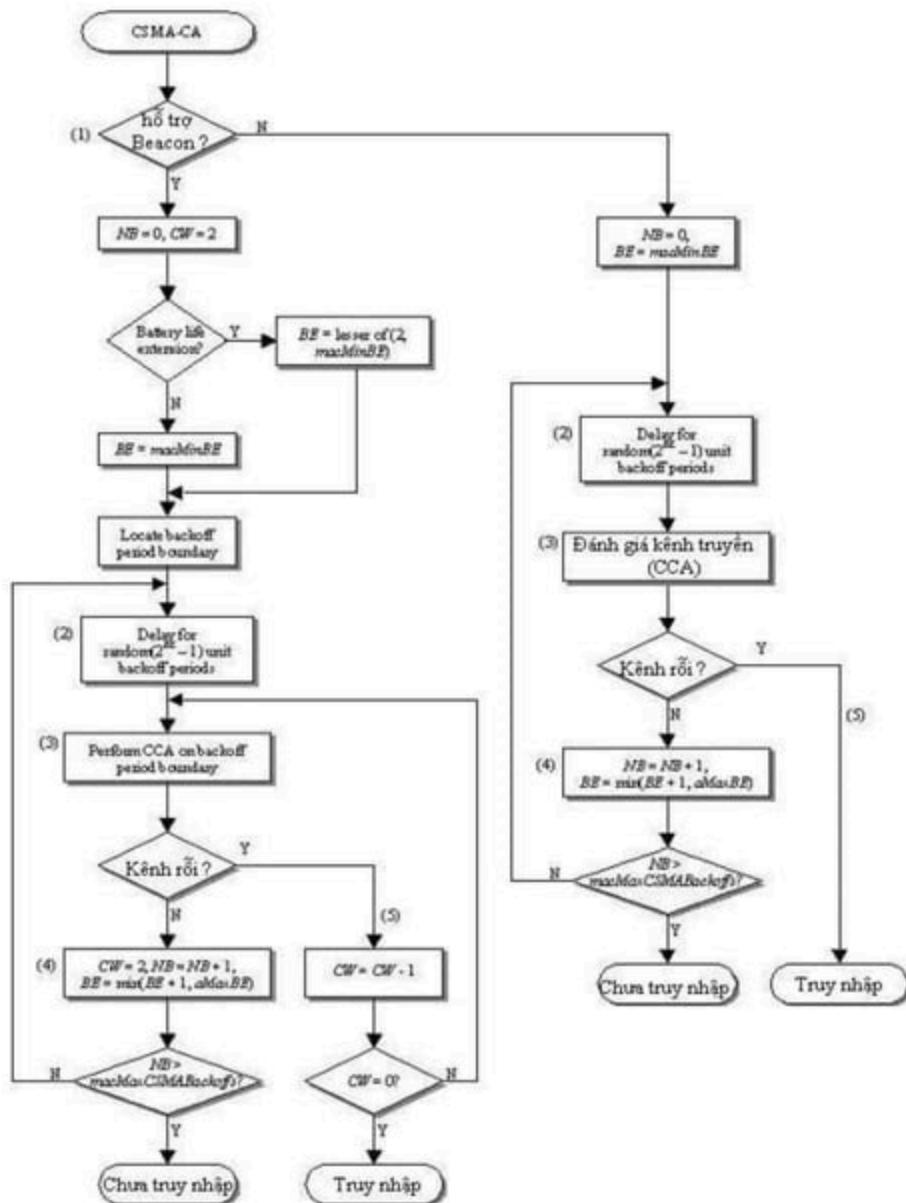
Khoảng thời gian IFS là thời gian cần thiết để tầng PHY xử lý một gói tin nhận được. Khung tin được truyền theo chu kỳ IFS, trong đó độ dài của chu kỳ IFS phụ thuộc vào kích thước của khung vừa được truyền đi. Khung có độ dài phụ thuộc vào aMaxSIFSFrameSize sẽ tuân theo chu kỳ SIFS (là khoảng thời gian tối thiểu aMinSIFSPeriod symbols), và các khung có độ dài lớn hơn aMaxSIFSFrameSize sẽ tuân theo chu kỳ LIFS (là khoảng thời gian tối thiểu aMinLIFSPeriod symbols).



Hình 3.7 Khoảng cách giữa hai khung IFS

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

CSMA/CA (Carrier Sense Multiple Access-Collision Avoidance). Phương pháp tránh xung đột đa truy cập nhờ vào cảm biến sóng. Thực chất đây là phương pháp truy cập mạng dùng cho chuẩn mạng không dây IEEE 802.11. Các thiết bị trong mạng (các nút mạng) sẽ liên tục lắng nghe tín hiệu thông báo trước khi truyền. Đa truy cập (multiple access) chỉ ra rằng nhiều thiết bị có thể cùng kết nối và chia sẻ tài nguyên của một mạng (ở đây là mạng không dây). Tất cả các thiết bị đều có quyền truy cập nhau khi đó đang truyền rồi. Ngay cả khi thiết bị tìm cách nhận biết mạng đang sử dụng hay không, vẫn có khả năng là có hai trạm tìm cách truy cập mạng đồng thời. Trên các mạng lớn, thời gian truyền từ đầu cáp này đến đầu kia là đủ để một trạm có thể truy cập đến cáp đó ngay cả khi có một trạm khác vừa truy cập đến. Nó tránh xung đột bằng cách là mỗi nút sẽ phát tín hiệu về yêu cầu truyền trước rồi mới truyền thật sự.



Hình 3.8 Lưu đồ thuật toán

Thuật toán truy nhập kênh CSMA-CA được sử dụng trước khi phát dữ liệu hoặc trước khi phát khung tin MAC trong phần CAP. Thuật toán này sẽ không sử dụng để phát khung tin thông báo beacon, khung tin Ack, hoặc là khung tin dữ liệu trong phần CFP. Nếu bản tin báo hiệu được sử dụng trong mạng PAN thì thuật toán CSMA-CA gán khe thời gian được dùng, ngược lại thuật toán CSMA-CA không gán khe thời gian sẽ được sử dụng. Tuy nhiên trong cả hai trường hợp thuật toán đều được bù xung bằng cách sử dụng khối thời gian backoff bằng với thời gian của tham số aUnitBackoffPeriod. Trong thuật toán truy nhập kênh CSMA-CA gán khe thời gian, biên của khoảng thời gian backoff của mỗi thiết bị trong mạng PAN được sắp thẳng hàng với biên của khe siêu khung của thiết bị điều phối mạng PAN. Trong thuật toán này, mỗi lần thiết bị muốn truyền dữ liệu trong CAP thì nó phải xác định biên thời gian backoff kế tiếp. Trong thuật toán CSMA-CA không gán khe thời gian thì khoảng thời gian backoff của một thiết bị trong mạng không cần phải đồng bộ với khoảng thời gian backoff của thiết bị khác.

Mỗi thiết bị chứa 3 biến số: NB, BW, BE. Trong đó NB là số lần mà thuật toán này bị yêu cầu rút lại trong khi đang cố gắng truyền. Giá trị ban đầu của nó là 0 trước khi truyền. Biến CW là độ dài cửa sổ tranh chấp, nó cho biết khoảng thời gian cần thiết để làm sạch kênh truyền trước khi phát, giá trị ban đầu của nó là 2 trước khi cố gắng phát và quay trở lại 2 khi kênh truy nhập bị bận. Biến số CW chỉ sử dụng cho thuật toán gán khe thời gian CSMA-CA. Biến số BE (backoff_exponent) cho biết một thiết bị phải chờ bao lâu để có thể truy nhập vào một kênh. Cho dù bộ thu của thiết bị làm việc trong suốt khoảng thời gian CAP của thuật toán nhưng nó vẫn bỏ qua bất kỳ khung tin nào nhận được trong khoảng thời gian này.

Trong thuật toán CSMA-CA gán khe thời gian, NB, CW, BE được thiết lập trước, biên của khoảng thời gian backoff kế tiếp cũng được xác định trước. Trong thuật toán CSMA-CA không gán khe thời gian thì NB và BE được thiết lập trước (bước 1). Tầng MAC sẽ trả ngẫu nhiên trong phạm vi 0 đến $2^{\text{BE}} - 1$ (bước 2) sau đó yêu cầu tầng PHY thực hiện đánh giá truy kênh truy nhập xem là rỗng hay bận. (bước 3). Nếu kênh truyền bận (bước 4), tầng MAC sẽ tăng NB và BE lên 1, nhưng cũng luôn đảm bảo rằng giá trị này nhỏ hơn aMaxBE. Trong CSMA-CA gán khe thời gian thì việc truyền khung tin, Ack phải được thực hiện trước khi kết thúc phần CAP trong siêu khung, nếu không sẽ phải chờ đến CAP của siêu khung kế tiếp, trong thuật toán

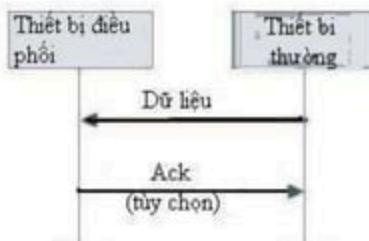
này thì CW có thể cũng reset lại thành giá trị 2. Nếu giá trị của NB nhỏ hơn hoặc bằng giá trị tham số macMaxCSMABackoffs, thì sẽ quay lại bước 2 đồng thời thông báo lỗi truy nhập kênh.

Nếu kênh truyền là rỗng (bojorc5), trong CSMA-CA gán khe thời gian, tầng MAC phải giảm CW đi 1. nếu CW ≠ 0 quay trở lại bojorc 3. Nếu CW=0 thì thông báo truy nhập kênh thành công. Còn trong CSMA-CA không gán khe thời gian thì tầng MAC bắt đầu phát ngay nếu kênh truyền rỗng.

3.3.3 Các mô hình truyền dữ liệu.

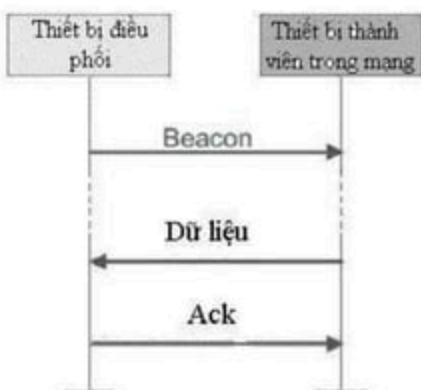
Dựa trên cấu trúc mạng WPAN thì ta có thể phân ra làm ba kiểu, ba mô hình truyền dữ liệu: từ thiết bị điều phối mạng PAN coordinator tới thiết bị thường, từ thiết bị thường tới thiết bị điều phối mạng PAN coordinator, và giữa các thiết bị cùng loại. Nhìn chung thì mỗi cơ chế truyền đều phụ thuộc vào việc là kiểu mạng đó có hỗ trợ việc phát thông tin thông báo beacon hay không.

Khi một thiết bị muốn truyền dữ liệu trong một mạng không hỗ trợ việc phát beacon, khi đó chỉ đơn giản là truyền khung dữ liệu tới thiết bị điều phối bằng cách sử dụng thuật toán không gán khe thời gian. Thiết bị điều phối Coordinator trả lời bằng khung Ack như hình 3.9



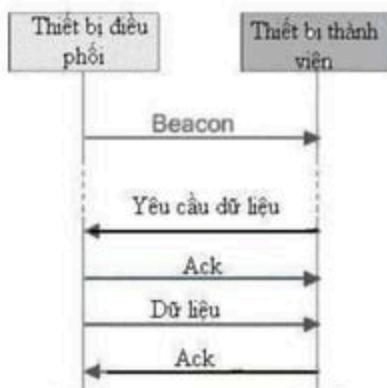
Hình 3.9 Liên lạc trong mạng không hỗ trợ beacon

Khi một thiết bị muốn truyền dữ liệu tới thiết bị điều phối trong mạng có hỗ trợ beacon. Lúc đầu nó sẽ chờ báo hiệu beacon của mạng. Khi thiết bị nhận được báo hiệu beacon, nó sẽ sử dụng tin hiệu này để đồng bộ các siêu khung. Đồng thời, nó cũng phát dữ liệu sử dụng phojong pháp CSMA-CA gán khe thời gian và kết thúc quá trình truyền tin bằng khung tin xác nhận Ack.



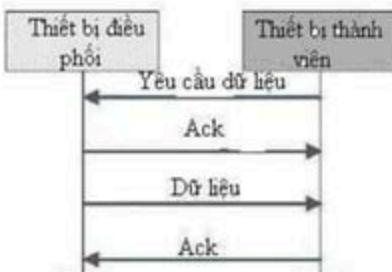
Hình 3.10 liên lạc trong mạng có hỗ trợ beacon.

Các ứng dụng truyền dữ liệu được điều khiển hoàn toàn bởi các thiết bị trong mạng PAN hơn là được điều khiển bởi thiết bị điều phối mạng. Chính khả năng này cung cấp tính năng bảo toàn năng lượng trong mạng ZigBee. Khi thiết bị điều phối muốn truyền dữ liệu đến một thiết bị khác trong loại mạng có hỗ trợ phát beacon, khi đó nó sẽ chỉ thị trong thông tin báo hiệu beacon là đang truyền dữ liệu. Các thiết bị trong mạng luôn luôn lắng nghe các thông tin báo hiệu beacon một cách định kỳ, khi phát hiện ra có dữ liệu liên quan tới nó đang được truyền, nó sẽ phát lệnh yêu cầu dữ liệu này, công việc này sử dụng slotted CSMA-CA. Công việc này được mô tả bằng hình2.11 , trong hình này khung tin Ack của thiết bị điều phối cho biết rằng gói tin đã được truyền thành công, việc truyền gói tin sử dụng kỹ thuật gán khe thời gian CSMA-CA, khung Ack thiết bị thợòng trả lời là nhận gói tin thành công. Vào lúc nhận khung tin Ack từ thiết bị thợòng thì bản tin sẽ được xóa khỏi danh sách bản tin trong thông tin báo hiệu beacon.



Hình 3.11 Kết nối trong mạng hỗ trợ beacon

Trong trường hợp mạng không hỗ trợ phát beacon (hình 2.8) thiết bị điều phối muốn truyền dữ liệu tới các thiết bị khác, nó sẽ phải lож trữ dữ liệu để chờ thiết bị liên quan có thể yêu cầu và tiếp xúc với dữ liệu đó. Thiết bị có thể tiếp xúc đợt với dữ liệu liên quan đến nó bằng cách phát đi lệnh yêu cầu dữ liệu tới thiết bị điều phối, sử dụng thuật toán không gán khe thời CSMA-CA. Nếu dữ liệu đang đợt truyền, thì thiết bị điều phối sẽ phát khung tin bằng cách sử dụng thuật toán không gán khe thời gian CSMA-CA, nếu dữ liệu không đợt truyền thì thiết bị điều phối sẽ phát đi khung tin không có nội dung để chỉ ra rằng dữ liệu không đợt phát.



Hình 3.12 kết nối trong mạng không hỗ trợ phát beacon

Nói chung trong mạng mắt lợn, tất cả các thiết bị đều bình đẳng và có khả năng kết nối đến bất kỳ thiết bị nào trong mạng miễn là thiết bị đó nằm trong bán kính phủ sóng của nó. Có hai cách để thực hiện việc kết nối. Cách thứ nhất là nốt trong mạng liên tục lắng nghe và phát dữ liệu của nó đi bằng cách sử dụng thuật toán không gán khe thời gian CSMA-CA. Cách thứ hai là các nốt tự đồng bộ với các nốt khác để có thể tiết kiệm được năng lượng.

3.3.4 Phát thông tin báo hiệu beacon

Một thiết bị FFD hoạt động trong chế độ không phát thông tin báo hiệu hoặc có thể phát thông tin báo hiệu giống nhau là thiết bị điều phối mạng. Một thiết bị FFD không phải là thiết bị điều phối mạng PAN có thể bắt đầu phát thông tin báo hiệu beacon chỉ khi nó kết nối với thiết bị điều phối PAN. Các tham số macBeaconOrder và macSuperFrameOrder cho biết khoảng thời gian giữa hai thông tin báo hiệu và khoảng thời gian của phần hoạt động và phần nghỉ. Thời gian phát báo hiệu liên tục được ghi lại trong tham số macBeaconTxTime và được tính toán để giá trị của tham số này giống nhau giá trị trong khung thông tin báo hiệu beacon.

3.3.5 Quản lý và phân phối khe thời gian đảm bảo GTS.

Khe thời gian đảm bảo GTS cho phép một thiết bị có thể hoạt động trong một kênh truyền bên trong một phần của siêu khung dành riêng cho thiết bị đó. Một thiết bị chỉ có thể chiếm và sử dụng một khe thời gian khi mà thiết bị đó liên quan đến thông tin báo hiệu beacon hiện thời lúc đó. Thiết bị điều phối mạng PAN có thể chiếm hữu khe thời gian GTS và sử dụng khe thời gian này để liên lạc với các thiết bị khác trong mạng. Một khe thời gian đơn có thể kéo dài hơn thời gian của siêu khung. Thiết bị điều phối mạng PAN có thể chiếm hữu tối đa khe thời gian GTS cùng một lúc miễn là nó có đủ thẩm quyền trong siêu khung.

Một khe thời gian có thể được chiếm hữu trước khi sử dụng nếu có sự yêu cầu của thiết bị điều phối mạng PAN. Tất cả các khe thời gian GTS đều được đặt liền nhau ở cuối của siêu khung sau phần CAP, và hoạt động theo cơ chế FCFS (first-come-first-serve) đến trước dùng trước. Mỗi khe thời gian GTS có thể được giải phóng nếu không có yêu cầu nào, và một khe thời gian GTS có thể được giải phóng vào bất kỳ lúc nào khi thiết bị chiếm hữu nó không dùng nữa. Chỉ duy nhất thiết bị điều phối PAN mới có quyền quản lý khe thời gian. Để quản lý mỗi khe thời gian đảm bảo, thiết bị

điều phối có thể loại trừ khe bắt đầu, độ dài, phong hoảng (thu hay phát) và địa chỉ thiết bị kết nối.

Chi duy nhất thiết bị điều phối PAN mới có quyền quản lý khe thời gian. Để quản lý mỗi khe thời gian đảm bảo, thiết bị điều phối có thể loại trừ khe bắt đầu, độ dài, phong hoảng (thu hay phát) và địa chỉ thiết bị kết nối.

Mỗi thiết bị trong mạng có thể yêu cầu một khe thời gian phát hay một khe thời gian thu. Để chiếm hữu được một khe thời gian thì thiết bị đó phải loại trừ thông tin khe bắt đầu, độ dài và phong hoảng. Nếu một thiết bị được cấp phát một khe thời gian GTS thu, nó sẽ có toàn quyền sử dụng trọn vẹn khe thời gian đó để nhận dữ liệu. Tuy nhiên, nếu vậy thiết bị điều phối mạng PAN cũng có thể có toàn quyền sử dụng trọn vẹn khe thời gian đó để nhận dữ liệu khi có một thiết bị khác chiếm khe thời gian phát. Một thiết bị yêu cầu chiếm hữu khe thời gian mới thông qua lệnh yêu cầu GTS với các tính chất (độ dài, thu hay phát,...) thiết lập theo yêu cầu ứng dụng. Để xác nhận lệnh này thì thiết bị điều phối sẽ gửi một khung tin Ack. Sau khi phát khung tin Ack thì thiết bị điều phối sẽ kiểm tra khả năng hiện thời của siêu khung dựa trên độ dài của phần CAP và độ dài khe thời gian GTS được yêu cầu. Siêu khung sẽ sẵn sàng nếu độ dài khe thời gian GTS không làm giảm độ dài của phần CAP đi quá độ dài nhỏ nhất của CAP được qui định trong tham số aMinCAPLength. Thiết bị điều phối mạng PAN thực hiện quyết định của nó bên trong siêu khung aGTSDescPersistenceTime. Trong khi xác nhận gói tin Ack từ thiết bị điều phối thì thiết bị này vẫn tiếp tục theo dõi thông tin báo hiệu và chờ siêu khung aGTSDescPersistenceTime. Khi thiết bị điều phối quyết định xem nó có sẵn sàng cho yêu cầu GTS không, nó sẽ phát đi mô tả về GTS với chi tiết yêu cầu và đoạn ngắn địa chỉ của thiết bị yêu cầu. Nó sẽ chỉ ra độ dài và khe GTS đầu tiên trong siêu khung rồi thông báo cho tầng trên về việc cấp phát khe GTS mới này. Nếu sau khi kiểm tra mà thấy khả năng của siêu khung là không đủ để cấp phát theo yêu cầu về GTS, thì khe đầu tiên sẽ được đánh số 0 tới độ dài khe GTS lớn nhất có thể cung cấp được hiện thời. Những mô tả về GTS sẽ được giữ trong khung tin báo hiệu beacon cho aGTSPersistenceTime. Trong khi xác nhận khung tin báo hiệu beacon, thiết bị sẽ xử lý và thông báo lên tầng trên.

Tuy nhiên, khi yêu cầu cấp phát GTS, một thiết bị cho biết nó yêu cầu được giải phóng sự chiếm hữu GTS thông qua lệnh yêu cầu giải phóng với các thông số của GTS đang tồn tại. Sau đó thì khe thời gian này sẽ được tự do. Thiết bị điều phối PAN

phải đảm bảo rằng không có khoảng trống nào xuất hiện trong CFP khi giải phóng khe thời gian GTS, độ dài maximum CAP nhờ thế mà được tăng lên (độ tăng đúng bằng độ dài của khe thời gian được giải phóng).

Thực thể quản lý tầng MAC (MLME) của thiết bị điều phối mạng PAN có nhiệm vụ phát hiện khi một thiết bị dừng sử dụng khe thời gian GTS. Công việc đó thực hiện bằng nguyên tắc sau. Đối với khe GTS phát, MLME sẽ công nhận một khe thời gian GTS được giải phóng nếu khung dữ liệu không được nhận trong tối thiểu 2^*n siêu khung. Đối với khe GTS thu, MLME sẽ công nhận thiết bị không còn sử dụng GTS nữa nếu khung tin xác nhận Ack không được nhận trong tối thiểu 2^*n siêu khung.

$$n = 2^{8 - macBeaconOrder}, \text{ nếu } 0 \leq macBeaconOrder \leq 8;$$

$$n = 1, \text{ nếu } 9 \leq macBeaconOrder \leq 14;$$

3.3.6 Định dạng khung tin MAC.

Mỗi khung bao gồm các thành phần sau:

- Đầu khung MHR(MAC header): gồm các trường thông tin về điều khiển khung tin, số chuỗi, và trường địa chỉ
- Tài trọng khung (MAC payload) : chứa các 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 (frame check sequence)

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	bien thiên	2
Điều khiển khung	Số chuỗi	ID mang PAN đích	Địa chỉ đích	ID PAN nguồn	Địa chỉ nguồn	Tài trọng khung	Chuỗi kiểm tra khung (FCS)
		Trường địa chỉ					
Phần đầu khung MHR					Tài trọng	Cuối khungMFR	

Bảng 3.6 Định dạng khung MAC

3.4 Tầng mạng của ZigBee/IEEE802.15.4

3.4.1 Dịch vụ mạng

Tầng vật lý trong mô hình của giao thức ZigBee được xây dựng trên nền của tầng điều khiển dữ liệu, nhờ những đặc điểm của tầng MAC mà tầng vật lý có thể kéo dài việc đón tin, có thể mở rộng được qui mô mạng dễ dàng, một mạng có thể hoạt động cùng các mạng khác hoặc riêng biệt. Tầng vật lý phải đảm nhận các chức năng như là:

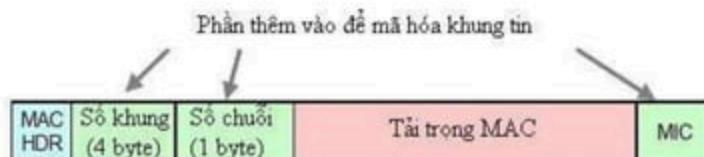
- Thiết lập một mạng mới.
- Tham gia làm thành viên của một mạng đang hoạt hoặc là tách ra khỏi mạng khi đang là thành viên của một mạng nào đó.
- Cấu hình thiết bị mới nhõi hệ thống yêu cầu, gán địa chỉ cho thiết bị mới tham gia vào mạng.
- Đồng bộ hóa các thiết bị trong mạng để có thể truyền tin mà 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 đón/tới
- Định tuyến, giúp gói tin có thể đến đón/tới đúng đích mong muốn. Có thể nói rằng thuật toán của ZigBee là thuật toán định tuyến phân cấp sử dụng bằng định tuyến phân cấp tối ưu đón/tới áp dụng từng trường hợp thích hợp.

3.4.2 Dịch vụ bảo mật

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. Nhược điểm 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 toán AES (chuẩn mã hóa cao cấp). Nói chung thì tầng MAC là một quá trình mã hóa, nhược 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 toán 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.



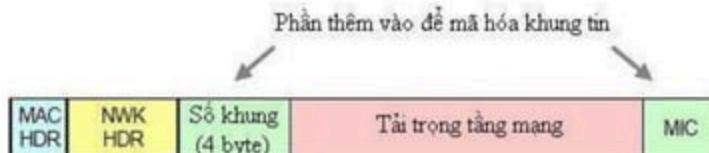
Hình 3.13 Khung tin mã hóa tầng MAC

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 cẩn thận 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. Bộ mã hóa của tầng MAC dựa trên ba trạng thái của hệ thống.

- Để bảo đảm tính nguyên vẹn: Mã hóa sử dụng AES với bộ đếm CTR
- Để bảo đảm tính tinh cậy: Mã hóa sử dụng AES với chuỗi khối mã CBC-MAC
- Để đảm bảo tính tinh cậy cũng như nguyên vẹn của bản tin thì kết hợp cả hai trạng thái CTR và CBC-MAC trên thành trạng thái CCM.

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 biến 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. Nhờ 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 định 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.



Hình 3.14 Khung tin mã hóa tầng mạng

3.5 Tầng ứng dụng của ZigBee/IEEE 802.15.4

Lớp ứng dụng của ZigBee/IEEE802.15.4 thực chất gồm các ba tầng nhô hình vẽ trên, các tầng này tương ứng với các tầng phiên, trình diễn và ứng dụng trong mô hình OSI 7 tầng.

Trong ZigBee/IEEE 802.15.4 thì chức năng của tầng Application Framework 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, chuyên tiếp thông tin giữa các nốt mạng. Chức năng của tầng Application Profiles là: Xác định vai trò của các thiết bị trong mạng. (thiết bị điều phối mạng, hay thiết bị đầu cuối, FFD hay RFD....)
- Thiết lập hoặc trả lời yêu cầu kết nối.
- Thành lập các mối quan hệ giữa các thiết bị mạng.

Chức năng của tầng Application là thực hiện các chức năng do nhà sản xuất qui trình định (giao diện...) để bổ sung thêm vào các chức năng do ZigBee qui định.

CHAPTER 4: CÁC THUẬT TOÁN ĐỊNH TUYỀN CỦA ZigBee/IEEE 802.15.4

Trong ZigBee/ IEEE802.15.4 sử dụng thuật toán chọn đường có phân cấp nhờ xét các phuong án tối ưu. Khởi điểm của thuật toán định tuyến này chính là thuật toán miền công cộng đã được nghiên cứu rất kỹ có tên là AODV (Ad hoc On Demand Distance Vector) dùng cho những mạng có tính chất tự tổ chức và thuật toán hình cây của Motorola.

4.1 Thuật toán định tuyến theo yêu cầu AODV (Ad hoc On Demand Distance Vector)

AODV (Ad hoc On Demand Distance Vector) đơn thuần chỉ là thuật toán tìm đường theo yêu cầu trong mạng ad hoc (một mạng tự tổ chức). Có thể hiểu như sau, những nút trong mạng khi mà không nằm trong tuyến đường truyền tin thì không duy trì thông tin nào về tuyến đường truyền và cũng không tham gia vào quá trình định tuyến theo chu kỳ. Nói kỹ hơn nữa, một nút mạng không có chức năng tự định tuyến và luôn trữ tuyến đường tới một nút mạng khác cho đến khi cả hai nút mạng trên liên lạc với nhau, trừ trường hợp những nút mạng cũ để nghị dịch vụ nhỡ là một trạm chuyển tiếp để giữ liên lạc giữa hai nút mạng khác.

Mục đích đầu tiên của thuật toán là chỉ phát quảng bá các gói tin dò đường khi cần thiết hoặc khi có yêu cầu, việc làm này để phân biệt giữa việc quản lý liên lạc cục bộ với việc bảo quản giao thức liên lạc chung và để phát quảng bá thông tin về sự thay đổi trong liên kết cục bộ tới những nút di động lân cận (là những nút cần thông tin để cập nhật). Khi một nút nguồn cần để kết nối tới nút khác, mà nút nguồn không chứa thông tin về thông tin tuyến đường tới nút đó, nhỡ vậy một quá trình tìm đường được thiết lập.

Để thiết lập quá trình tìm đường này thì mỗi nút mạng đều lưu hai bộ đếm độc lập: sequence number và broadcast id. Để bắt đầu quá trình tìm đường, nút nguồn sẽ khởi tạo một gói tin tìm đường (RREQ) và phát quảng bá gói tin này tới tất cả các nút mạng lân cận, gói tin RREQ này chứa các thông tin về địa chỉ nguồn (source addr), số chuỗi nguồn (source sequence number), số id quảng bá (broadcast id), địa chỉ đích (dest addr), số chuỗi đích (dest sequence number), số đếm bước truyền (hop cnt).

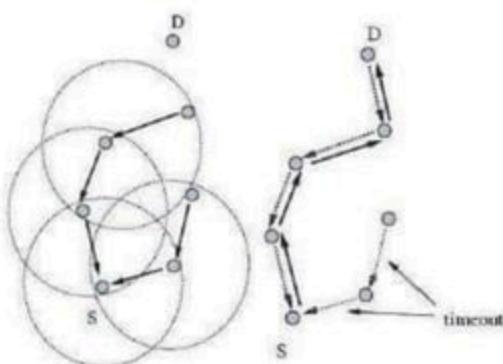
Bởi mỗi khi nốt mạng nguồn phát ra một gói tin RREQ mới thì số id quảng bá sẽ tăng lên, nên trong mỗi gói tin RREQ thì cặp địa chỉ nguồn và số id quảng bá luôn luôn là duy nhất. Khi nốt mạng trung gian nhận được một gói tin RREQ mới, nó sẽ đem so sánh địa chỉ nguồn và số id quảng bá với gói tin RREQ trước đó, nếu giống nhau nốt mạng trung gian này sẽ tự động xóa RREQ do thừa này và dừng việc phát gói tin này lại. Nhoáng nếu so sánh thấy khác nhau thì nốt mạng này sẽ tự động tăng số đếm bộ nhớ truyền (hop cnt) lệnh và tiếp tục phát quảng bá gói tin RREQ này tới các nốt lân cận để tiếp tục quá trình tìm đường. Trong mỗi một nốt mạng đều lưu trữ các thông tin về địa chỉ IP đích, địa chỉ IP nguồn, số id quảng bá, số chuỗi nốt nguồn, và thời gian thời gian hạn định cho phép gói tin mang thông tin xác nhận được gửi trả lại nơi phát

Khi gói tin RREQ được truyền trên mạng từ nguồn tới đích, nó sẽ tự động thiết lập con đường ngược lại từ các nốt mạng này quay trở lại nốt nguồn. Để thiết lập tuyến đường ngược chiều, mỗi nốt phải lưu giữ bảng địa chỉ của các nốt bên cạnh mà nó sao chép được trong gói tin RREQ đầu tiên. Truyền đường ngược chiều được lưu giữ trong thời gian tối thiểu để gói tin RREQ này vượt qua mạng và trở về nơi xuất phát ban đầu. Khi RREQ tới một nốt nào đấy mà có thể nốt mạng này là đích đến của nó, hoặc

nốt này nằm trên tuyến đường truyền từ nguồn tới đích, nốt nhận tin này đầu tiên sẽ kiểm tra xem gói tin RREQ vừa nhận qua kết nối hai chiều. Nếu nốt mạng này chưa phải là nốt mạng đích nhoáng có lưu giữ tuyến đường tới nốt đích, khi đó nó sẽ quyết định xem xem tuyến đường này có chính xác không bằng cách so sánh số chuỗi nguồn chứa bên trong gói tin RREQ này với số chuỗi nguồn trong bảng định tuyến của nốt mạng đó. Nếu số chuỗi đích của RREQ lớn hơn số chuỗi đích trong các nốt trung gian, thì nốt trung gian đó không nằm trên tuyến đường truyền ứng với gói tin RREQ này.

Nếu tuyến đường này có số chuỗi đích lớn hơn hoặc bằng với số chuỗi đích trong RREQ nhoáng có số bộ nhớ truyền nhỏ hơn, thì nó có thể phát một gói tin RREP (route reply packet) trả lại nốt mạng đã phát RREQ cho nó. Một gói tin RREP gồm có các thông tin sau: đường địa chỉ nguồn, đường địa chỉ đích, số chuỗi đích, số đếm bộ nhớ truyền và thời gian sống. Khi mà gói tin RREP quay trở lại được nốt nguồn, các nốt mạng đọc theo tuyến đường của RREP sẽ thiết lập con chò hoảng tới nốt mạng RREP vừa đến, cập nhật thông tin timeout (timeout là khoảng thời gian mà một

nốt không còn hoạt động nữa và nằm trong trạng thái chờ) của nó cho bảng định tuyến đường tới nguồn và đích, đồng thời sao lưu lại số chuỗi đích cuối của nốt đích cần tới. Những nốt mạng nằm dọc theo tuyến đường xác định bởi RREP sẽ “chết” sau khi hết thời gian yêu cầu định tuyến và con chó đáo bị xóa khi chúng không còn nằm trên tuyến đường truyền từ nguồn tới đích. Thời gian “chết” này phụ thuộc vào kích cỡ của mạng.



Hình 4.1 Định dạng tuyến đường trong giao thức AODV

Nốt nguồn có thể phát dữ liệu ngay khi nó nhận được gói tin RREP đầu tiên, đồng thời cũng luôn cập nhật thông tin về tuyến đường nếu phát hiện ra tuyến đường tối ưu hơn.

Mỗi bảng định tuyến gồm các trường thông tin sau: trường thông tin về đích đến, bộ lọc truyền kế tiếp, số bộ lọc truyền, số chuỗi đích, nút lân cận tích cực thuộc tuỳn đường, thời gian chết cho nhập liệu vào bảng định tuyến.

Để duy trì đường truyền, mỗi nốt mạng luôn phải có địa chỉ của các nốt mạng tích cực lân cận (một nốt mạng được coi là tích cực nếu nó có chức năng khởi phát hoặc chuyển tiếp tối thiểu một gói tin đến đích trong thời gian cho phép). Khi mà bộ lọc truyền kế tiếp nằm trong tuyến đường từ nguồn tới đích này không thực hiện được (tức là thông tin yêu cầu không được nhận trong một khoảng thời gian nào đó, thông tin yêu cầu này đảm bảo rằng chỉ có những nốt mạng nào liên lạc hai chiều mới được coi là nốt mạng lân cận). Quá trình này cứ tiếp diễn đến khi tất cả các nốt nguồn tích cực được thông báo. Nhờ vào việc nhận những thông báo về gián đoạn đường truyền,

mà các nút nguồn có thể khởi động lại quá trình tìm đường nếu chúng vẫn cần một tuyến đường tới đích cũ. Nếu nút nguồn lựa chọn việc xây dựng lại tuyến đường mới từ nguồn tới đích, nó cần phải phân phát một gói tin RREQ mới với số chuỗi đích mới lớn hơn số chuỗi đích cũ.

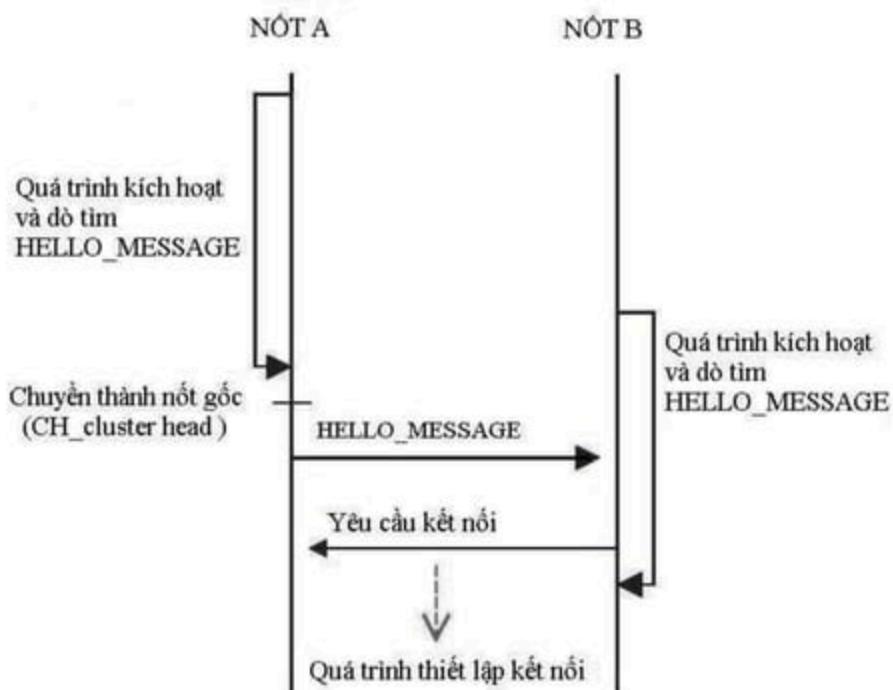
4.2 Thuật toán hình cây

Giao thức hình cây là giao thức của tầng mạng và tầng datalink, giao thức này sử dụng gói tin “trạng thái kết nối” để định dạng một mạng hình cây đơn, cũng như một mạng hình cây mở rộng. Loại mạng này cơ bản là một loại mạng có tính chất tự tổ chức và tự hỗ trợ để hạn chế lỗi mạng một mức độ lỗi cho phép, đặc biệt hơn do đây là một loại mạng có tính chất tự tổ chức nên nó cũng có thể tự sửa chữa khi gặp sự cố ở một nút mạng nào đó. Các nút mạng chọn một nút làm gốc cây và tạo các nhánh cây một cách tự do. Sau đó cách nhánh cây tự phát triển kết nối tới những nhánh cây khác nhờ vào thiết bị gốc (DD- Designated Deviece).

4.2.1 Thuật toán hình cây đơn nhánh

Quá trình hình thành nhánh cây bắt đầu bằng việc chọn gốc cây. Sau khi một nút gốc được chọn, nó sẽ mở rộng kết nối với các nút khác để tạo thành một nhóm.

Sau khi một nút được kích hoạt nó sẽ dò tìm HELLO message từ các nút khác (HELLO message thường tự như beacon trong tầng MAC theo chuẩn IEEE 802.15.4). Nếu trong một thời gian nhất định nào đó nó không nhận được bất kỳ một HELLO message nào, thì nút này sẽ tự trở thành nút gốc và lại gửi HELLO message tới các nút lân cận. Nút gốc mới này sẽ chờ gói tin yêu cầu kết nối từ các nút lân cận trong một khoảng thời gian nào đó, nếu nó vẫn không nhận được bất kỳ yêu cầu kết nối nào từ các nút lân cận thì nó sẽ trở lại thành một nút bình thường và lại tiếp tục dò tìm HELLO_MESSAGE. Nút gốc cũng có thể được chọn lựa dựa trên tham số của mỗi nút mạng (ví dụ như phạm vi truyền, công suất, vị trí, khả năng tính toán).



Hình 4.2 Quá trình chọn nốt gốc (CH)

Sau khi trở thành nốt gốc, nó sẽ phát quảng bá gói tin HELLO_MESSAGE theo chu kỳ, gói tin HELLO_MESSAGE này gồm một phần địa chỉ MAC và địa chỉ ID của nốt gốc. Những nốt mạng nhận được gói tin này sẽ gửi trả lời lại bằng gói tin yêu cầu kết nối (REQ) tới nốt gốc (nó vừa phát đi). Khi nốt gốc nhận được gói tin yêu cầu kết nối, nó sẽ ngay lập tức gửi trả lại gói tin vừa đưa ra yêu cầu bằng một gói tin khác CONNECTION_RESPONSE., gói tin này chứa địa chỉ ID cho nốt thành viên (nốt B), địa chỉ ID này do nốt gốc qui định. Để xác nhận thông tin thì nốt thành viên B này sẽ gửi lại nốt gốc gói tin Ack. Quá trình trao đổi tin này được mô tả qua hình3.3



Hình 4.3 Thiết lập kết nối giữa CH và nốt thành viên

Nếu tất cả các nốt đều ở trong phạm vi phủ sóng của nốt gốc thì kiến trúc mạng là kiến trúc hình sao, tất cả các nốt thành viên sẽ liên lạc trực tiếp với nốt gốc qua một bơm truyền (onehop). Một nhánh có thể phát triển thành cấu trúc mạng liên lạc qua nhiều bơm truyền (multihop).



Hình 4.4 Quá trình hình thành nhánh nhiều bậc

Tất nhiên nốt gốc chỉ có thể quản lý được một số hữu hạn các nốt, và các nhánh của mạng cũng chỉ có thể vojon tới những khoảng cách hạn chế... chính vị thế mà có lúc nốt mạng cũng cần phải từ chối kết nối của những nốt mới. Việc từ chối này được thực hiện nhờ vào việc chỉ định một ID đặc biệt cho nốt này. Bảng danh sách các nốt lân cận và tuyên đường luôn luôn được cập nhật mới thông qua gói tin HELLO_MESSAGE. Trong một thời gian nhất định, nếu vì một lý do nào đó mà một nốt không được cập nhật các thông tin trên thì nó sẽ bị loại bỏ.

Tất nhiên trong một mạng có tính chất tự do, tự tổ chức nhợt loại mạng này thì không thể tránh khỏi việc một nốt mạng thuộc nhánh này lại nhận được gói tin HELLO_MESSAGE của nhánh khác. Vậy trong trường hợp này nốt mạng này sẽ tự động thêm địa chỉ ID của nhánh mới này (CID) vào danh sách các nốt lân cận và gửi nó tới nốt gốc (CH) thông qua gói tin báo cáo tình trạng đường truyền, để từ đó nốt gốc (CH) có thể biết được nhánh mạng nào tranh chấp để xử lý.

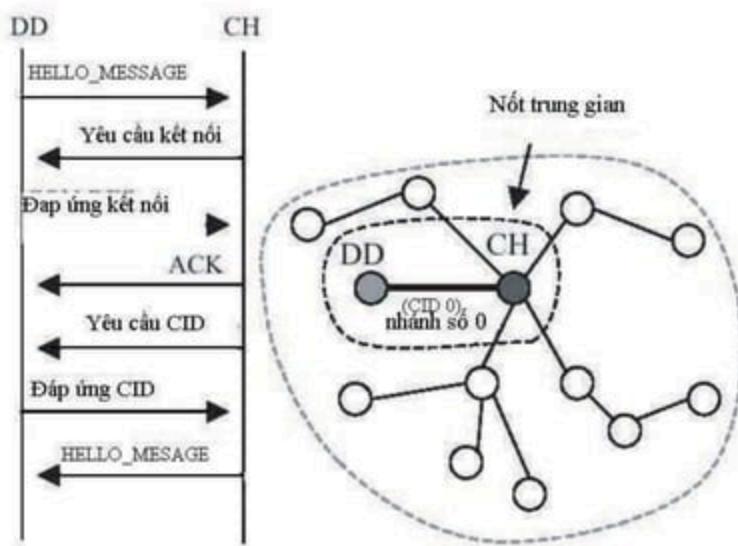
Bản tin báo cáo tình trạng kết nối cũng chứa danh sách ID nốt lân cận của nốt đó, điều này giúp cho nốt gốc biết được trọng vị cấu trúc mạng để có thể đưa ra cấu trúc tối ưu. Khi cấu trúc mạng cần thay đổi, nốt gốc (CH) sẽ phát đi bản tin cập nhật tới các nốt thành viên. Nốt thành viên nào nhận được bản tin cập nhật này lập tức thay đổi các thông tin về nốt gốc nhợt trong bản tin này, đồng thời cũng tiếp tục gửi đến các nốt ở cấp thấp hơn trong nhánh cây tại thời điểm đó.

Khi một nốt thành viên có vấn đề, không thể kết nối được thì nốt gốc phải định dạng lại tuyên đường. Thông qua bản tin báo cáo tình trạng đường truyền được gửi theo chu kỳ thì nốt gốc có thể biết vấn đề của nốt mạng đó. Nhợng khi nốt gốc gặp phải vấn đề trong liên lạc thì việc phát bản tin HELLO_MESSAGE theo chu kỳ sẽ bị gián đoạn, khi đó các nốt thành viên sẽ mất đi nốt gốc, và nhánh đó sẽ phải tự định dạng lại từ đầu theo cách tốn kém tự nhợt quá trình định dạng nhánh cây

4.2.2 Thuật toán hình cây đa nhánh.

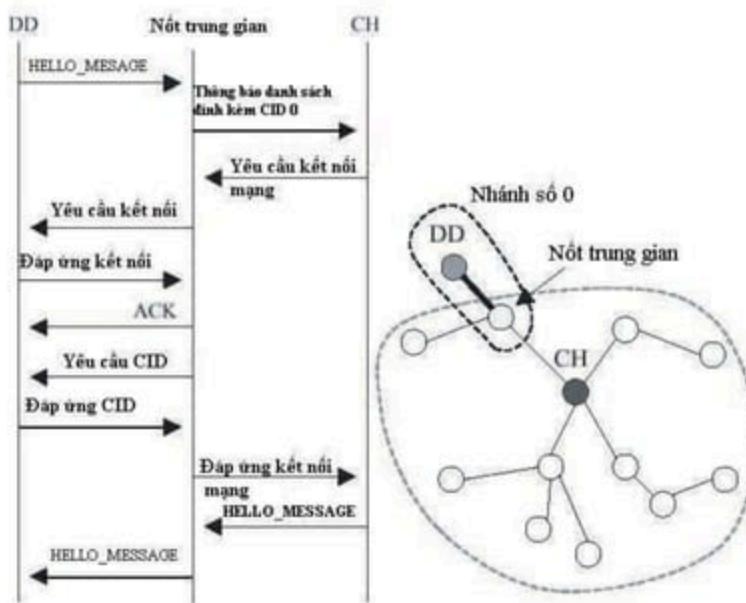
Để tạo định dạng lên loại mạng này thì cần phải sử dụng thiết bị gốc (DD). Thiết bị này có trách nhiệm gán địa chỉ ID nhóm (địa chỉ này là duy nhất) cho các nốt gốc (CH). Địa chỉ ID nhóm này kết hợp với địa chỉ ID nốt (là địa chỉ NID mà nốt gốc gán cho các nốt thành viên trong nhánh của mình) tạo ra địa chỉ logic và được sử dụng trong các gói tin tìm đường. Một vai trò quan trọng nữa của thiết bị gốc DD là tinh

toán quãng đường ngắn nhất từ nhánh mạng tới DD và thông báo nó tới tất cả các nốt mạng.



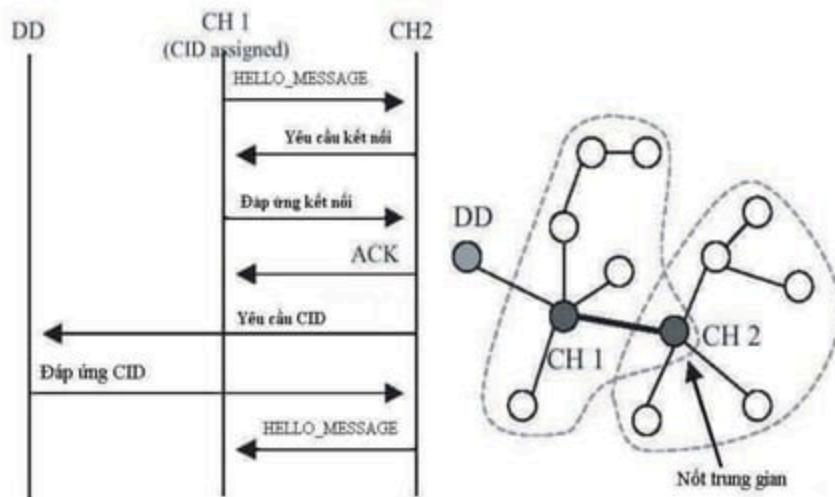
Hình 4.5 Gán địa chỉ nhóm trực tiếp

Khi thiết bị gốc DD tham gia vào mạng, nó sẽ hoạt động như một nốt gốc của nhánh số 0 (CID 0) và bắt đầu phát quang bá HELLO_MESSAGE tới các nốt lân cận. Nếu một nốt gốc (CH) nhận được bản tin này, nó sẽ gửi bản tin yêu cầu kết nối tới DD để tham gia vào CID 0, sau đó nốt gốc này sẽ yêu cầu DD gán cho nó một ID nhánh (CID). Nhờ vậy thì nốt gốc này có hai địa chỉ logic, một là thành viên của CID 0, thứ hai là địa chỉ của nốt gốc. Khi nốt gốc tạo ra một nhánh mới, (một CID mới), nó sẽ thông báo đến các nốt thành viên của nó bằng bản tin HELLO_MESSAGE.

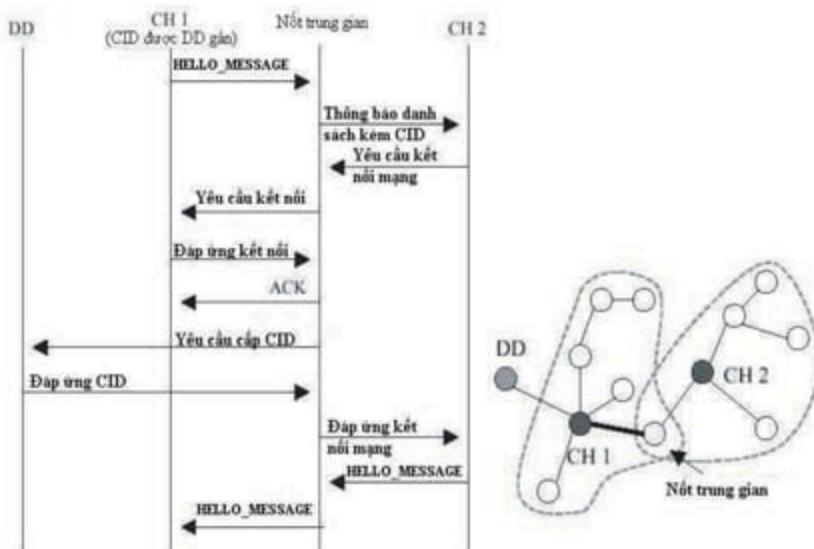


Hình 4.6 Gán địa chỉ nhóm qua nút trung gian

Khi một thành viên nhận được bản tin HELLO_MESSAGE từ thiết bị DD, nó sẽ thêm địa chỉ ID của CID 0 vào danh sách thành viên rồi thông báo cho nút gốc. Nút gốc được thông báo này sẽ chọn nút thành viên này như là một nút trung gian giữa nó với nút gốc của nó, rồi gửi bản tin yêu cầu kết nối mạng tới các nút thành viên để thiết lập kết nối với thiết bị DD. Nút trung gian này yêu cầu một kết nối và tham gia vào thành viên của nhánh số 0. Sau đó nó sẽ gửi bản tin yêu cầu CID tới thiết bị DD. Đến khi nhận được đáp ứng CID, nút trung gian này gửi bản tin đáp ứng liên kết mạng này tới nút CH, bản tin này chứa các thông tin về địa chỉ ID nhánh mới cho nút gốc CH. Sau khi nút gốc có được CID mới, thì cách thành viên trong nhánh của nút gốc cũng sẽ nhận được thông qua HELLO_MESSAGE



Hình 4.7 Gán địa chỉ nhóm qua nốt gốc



Hình 4.8 Gán địa chỉ nhóm qua nốt gốc và nốt trung gian

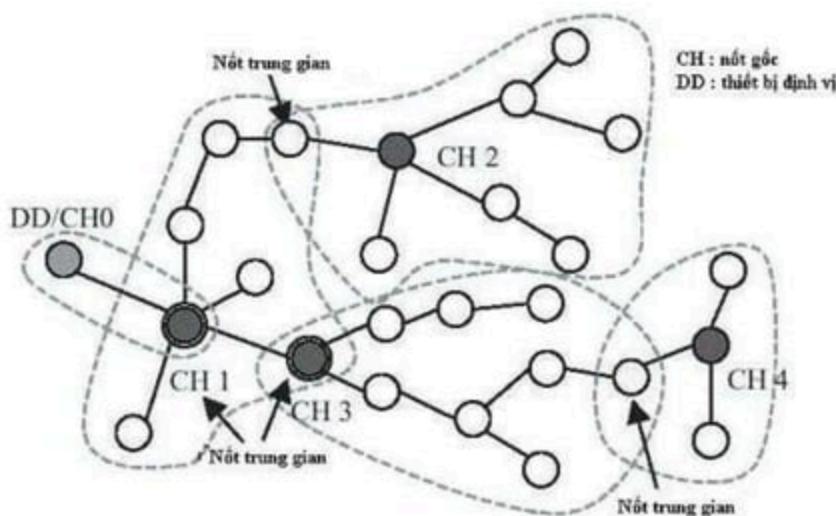
Trong mạng này thì việc tự tổ chức mạng là một tính chất khá mạnh mẽ, và mềm dẻo. Cứ nhánh mạng liền trước sẽ có nhiệm vụ gán CID cho nhánh mạng sau. Quá trình này được mô tả rõ nét hơn ở hình 4.5,4.6,4.7,4.8.

Mỗi một nốt thành viên của nhánh phải ghi lại thông tin về nhánh gốc và các nhánh con của nó, hoặc cả ID của nốt trung gian nếu có. Thiết bị gốc phải có trách nhiệm lưu giữ toàn bộ thông tin về cấu trúc cây mạng của các nhánh.

Cũng giống như các nốt thành viên của nhánh thì các nốt gốc CH cũng là thành viên của thiết bị gốc và như vậy chúng cũng phải có trách nhiệm thông báo tình trạng đợt sóng truyền đến DD. Để thực hiện thì nốt gốc phải gửi định kỳ bản tin thông báo tình trạng đợt sóng truyền trong mạng tới DD, bản tin này chứa danh sách CID lân cận. DD sau khi xử lý thông tin sẽ tính toán, chọn lựa ra đợt sóng truyền tối ưu nhất rồi thông báo định kỳ tới các nhánh của nó thông qua bản tin cập nhật.

Như trên ta có thể thấy vai trò của thiết bị gốc này là rất quan trọng, chính vì thế luôn cần có những thiết bị gốc dự phòng (BDD) sẵn sàng thay thế thiết bị chính khi gặp sự cố.

Hình 4.9 mô tả việc liên lạc trong nhánh. Các nốt trung gian vừa liên kết các nhánh mạng, vừa chuyên tiếp các gói tin giữa các nhánh mạng. Khi nốt trung gian nhận được một gói tin, nó sẽ kiểm tra địa chỉ đích của gói tin đó, sau đó sẽ chuyển tới địa chỉ đích của nó nếu địa chỉ đích nằm trong nhánh này hoặc là chuyên tiếp tới nốt trung gian tiếp theo của nhánh liền kề nếu địa chỉ đích không nằm trong nhánh của nó.



Hình 4.9 Mạng cây đa nhánh và các nốt trung gian

Chi duy nhất thiết bị gốc mới có thể gửi bản tin tới tất cả các nốt trong mạng, bản tin này được chuyên dọc theo tuyến đường của các nhánh. Các nốt trung gian thì chuyên tiếp các gói tin quảng bá từ nhánh gốc đến các nhánh con.

4.3 Giới thiệu về chương trình mô phỏng OPNET

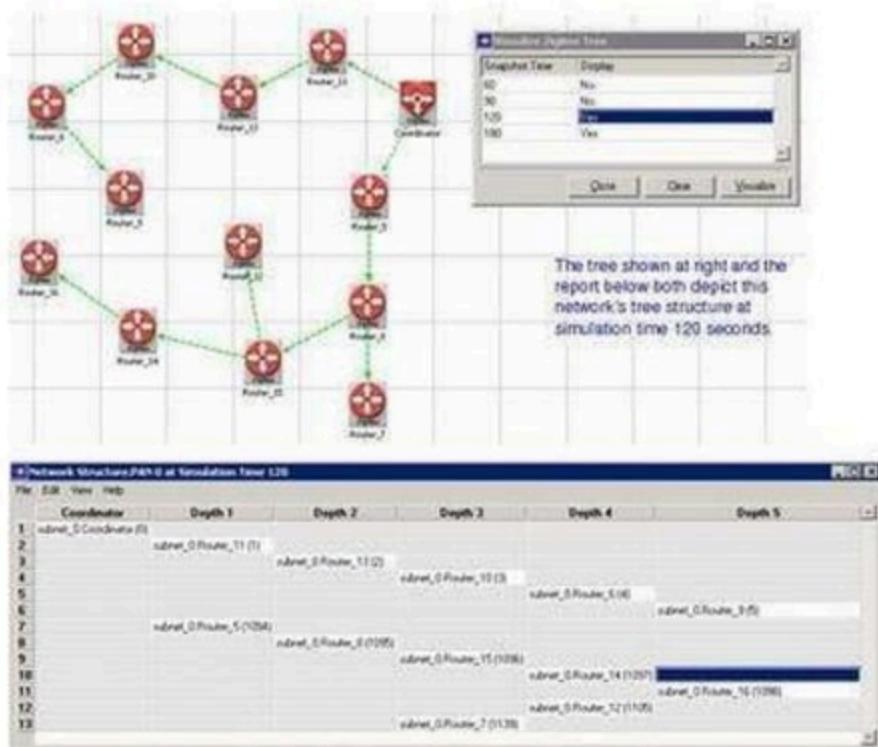
OPNET là chương trình mô phỏng mạng WSN tốt và kể từ phiên bản 14.5 trở đi thì OPNET có hỗ trợ thư viện ZigBee.

Kể từ phiên bản 14.5 trở đi, OPNET có sẵn thư viện cho giao tiếp mạng Zigbee (phiên bản trước đó không có thư viện này). Thư viện này viết cho **4 lớp**, gồm lớp vật lý – physical, lớp điều khiển truy cập kênh truyền – medium access control, lớp mạng – network, và lớp ứng dụng – application.

Đặc tính của thư viện này bao gồm liệt kê từ tài liệu của OPNET

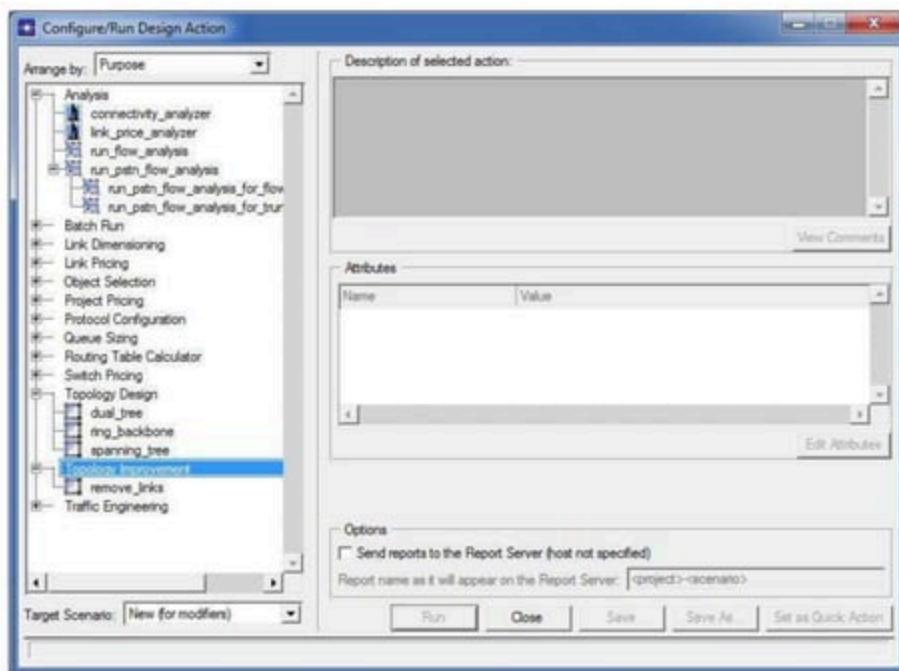
Hỗ trợ	<p><u>Application layer features</u></p> <ul style="list-style-type: none">• Generating and receiving application traffic• Initiating network discovery and network join• Falling and recovering ZigBee devices <p><u>Network layer features</u></p> <ul style="list-style-type: none">• Establishing a network• Joining a network and permitting network joins• Assigning an address• Maintaining a neighbor table• Mesh Routing Process• Network Broadcast• Tree routing process• Transmitting and receiving data• Mobility• Beacon scheduling <p><u>MAC layer features</u></p> <ul style="list-style-type: none">• Channel Scanning• CSMA/CA (Contention-based operation mode)
Chưa hỗ trợ	<ul style="list-style-type: none">• Multicast traffic• Indirect transmission• Security• Slotted mode• Contention-free operation mode• Support for other application models (such as HTTP, e-mail, and other standard network applications, custom applications, ACE and ACE Whiteboard applications)

Bảng 4.1 Các thuộc tính của thư viện Zigbee của OPNET.

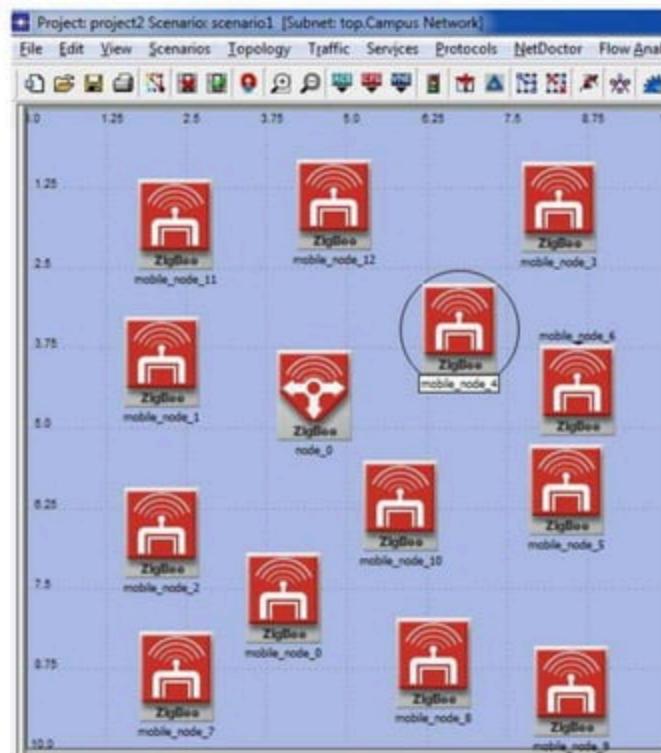


Hình 4.10 Mô phỏng Zigbee với thư viện từ OPNET.

Rất đáng tiếc là thư viện chỉ hỗ trợ chế độ hoạt động non – beacon – enable, có nghĩa là các điểm nút chỉ có thể truyền theo kiểu unslot – CSMA/CA. Tuy nhiên chương trình này cung cấp cái nhìn tốt về cơ chế vạch đường đi (routing) của Zigbee.

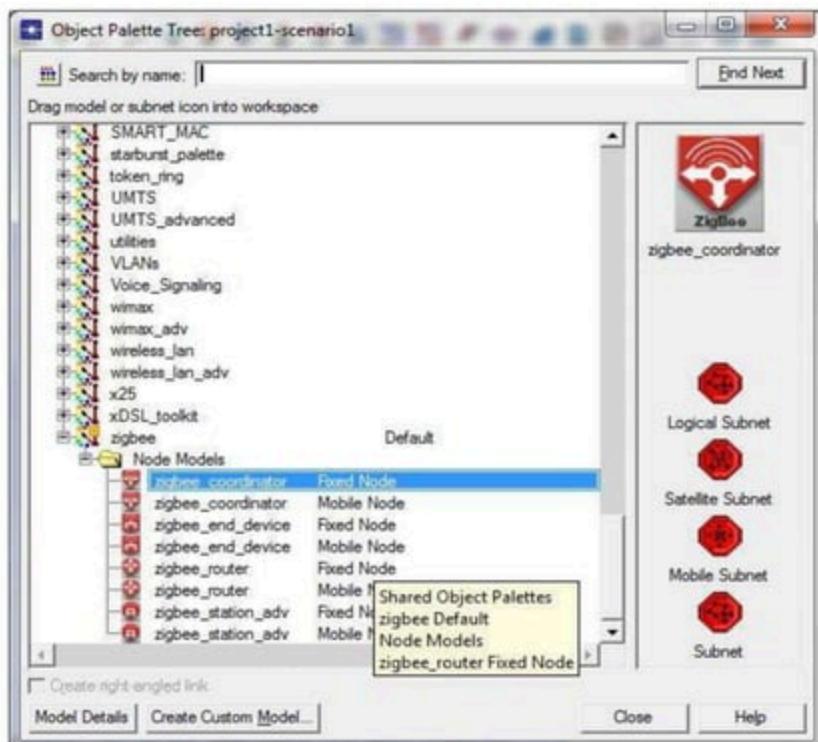


Hình 4.11 Mô tả giao thức trong Zigbee.



Hình 4.12 Mô phỏng Zigbee với thư viện từ OPNET.

Rất đáng tiếc là thư viện chỉ hỗ trợ chế độ hoạt động non – beacon – enable, có nghĩa là các điểm nút chỉ có thể truyền theo kiểu unslot – CSMA/CA. Tuy nhiên chương trình này cung cấp cái nhìn tốt về cơ chế vạch đường đi (routing) của Zigbee.



Hình 4.13 Mô tả nút mạng định tuyến của ZigBee trong OPNET.

Kết luận

Sau thời gian làm đồ án tốt nghiệp dojới sự hojóng dẫn tận tình của thầy giáo Th.s Nguyễn Trọng Thể, đến nay em đã hoàn thành đồ án của mình. Đồ án tìm hiểu chung về mạng máy tính, mạng cảm nhận không dây WSN, tìm hiểu chuẩn IEEE 802.15.4/ZigBee, tìm hiểu thuật toán định tuyến AODV. Bojorc đầu em đã cài đặt thành công chương trình mô phỏng OPNET.

Mạng cảm nhận không dây gồm số lượng lớn các thiết bị có khả năng cảm nhận và truyền thông không dây. Thông thường các nút mạng này hạn chế về tài nguyên phần cứng như khả năng xử lý thấp, giải thông bê, tín hiệu yếu và hoạt động dojới tần số chia sẻ. Việc xác định chuẩn 802.15.4 có ý nghĩa quan trọng trong việc xác định không gian ứng dụng, thiết kế mạng cảm nhận không dây. Thông qua đó ứng dụng cụ thể trong y tế cho mạng cảm nhận không dây.

Cuối cùng em xin chân thành cảm ơn thầy giáo Th.S Nguyễn Trọng Thể, người đã tận tình hojóng dẫn và giúp đỡ em trong cả quá trình làm đồ án.

Em xin chân thành cảm ơn !

TÀI LIỆU THAM KHẢO

1. Wireless Sensor Network design and implement.
2. Nael Abu-Ghazaleh, kyoung- Don Kang, and Ke Liu. “Towards resilient geographic orwarding in wireless sensor networks”.
3. <http://www.wsn.com>
4. Wireless Sensor Network Ian F and mehment C Vuran 2001