ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC BÁCH KHOA

KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

----------o0o----------

LUẬN VĂN TỐT NGHIỆP ĐẠI HỌC

XÂY DỰNG GIẢI PHÁP TÍNH TIỀN NHANHTRONG SIÊU THỊ DỰA TRÊN MẠNG ZIGBEE

HỘI ĐỒNG: **KỸ THUẬT MÁY TÍNH**

GVHD: Vũ Tuấn Thanh

GVPB: Bùi Văn Hiếu

SVTH:

1. Nguyễn Quang Vinh 50702974
2. Nguyễn Văn Hải 50700680
3. Phạm Hoàng Phúc 50701839

TP. HỒ CHÍ MINH, Tháng 12/2011

LỜI CAM ĐOAN

Chúng tôi xin cam đoan luận văn **"Xây dựng giải pháp tính tiền nhanh trong siêu thị Queue Busting dựa trên mạng Zigbee"** là phần nghiên cứu và thể hiện của riêng chúng tôi, không sao chép từ bất kì luận văn nào khác. Các kết quả đạt được trong luận văn là trung thực, chưa từng được ai công bố trong bất kỳ công trình nào khác.

LỜI CẢM ƠN

Sau 4 năm học tập chuyên ngành Khoa Học và Kỹ Thuật Máy Tính tại trường Đại Học Bách Khoa thành phố Hồ Chí Minh, được sự cho phép của nhà trường, nhóm em thực hiện báo cáo luận văn hoàn thành khóa học.

Nhóm em xin chân thành cảm ơn các thầy cô trong bộ môn Khoa Học và Kỹ Thuật Máy Tính, các anh chị hướng dẫn đã tận tình giúp đỡ và truyền đạt kiến thức để nhóm em có thể hoàn thành luận văn này.Đặc biệt, nhóm em xin gửi lời cảm ơn sâu sắc nhất đến thầy Vũ Tuấn Thanh đã nhiệt tình hướng dẫn nhóm em trong suốt quá trình thực hiện luận văn.

Cảm ơn tất cả các bạn cùng khóa đã nhiệt tình chia sẻ kinh nghiệm và những kiến thức quý báo giúp nhóm em hoàn thành tốt luận văn tốt nghiệp của mình.

Mặc dù nhóm em đã cố gắng hoàn thành luận văn với tất cả sự nỗ lực của nhóm, nhưng luận văn chắc chắn không tránh khỏi những thiếu sót. Nhóm em kính mong quý thầy cô tận tình chỉ bảo.

Cuối cùng nhóm em xin gửi đến quý thầy cô lời chúc sức khỏe và lời cảm ơn chân thành nhất!

TP.HCM, tháng 1 năm 2012

Nhóm sinh viên thực hiện đề tài

TÓM TẮT ĐỀ TÀI

Toàn bộ đề tài được nhóm ba người chúng tôi hoàn thành trong bốn tháng. Thời gian đầu, chúng tôi tập trung tìm hiểu các kiến thức cơ bản về mô hình Queue – Busting và chuẩn giao tiếp mạng Zigbee. Sau đó, để đảm bảo tiến độ, chúng tôi chia toàn bộ hệ thống làm ba phần riêng lẻ. Khi các phần riêng lẻ của hệ thống đã hoạt động đúng chức năng, chúng tôi liên kết lại thành một hệ thống hoàn chỉnh và tiến hành các phép thử nghiệm trên hệ thống này nhằm tìm và khắc phục các lỗi có thể xảy ra trong quá trình hoạt động.

Sau bốn tháng nghiên cứu và hiện thực, chúng tôi đã hoàn thành một hệ thống thanh toán mới giúp cải thiện tốc độ thanh toán trong các siêu thị. Hệ thống thử nghiệm này mô phỏng toàn bộ quá trình từ lúc khách hàng mua hàng đến lúc thanh toán. Đáp ứng các yêu cầu cơ bản như: cải thiện tốc độ thanh toán khá tốt so với hệ thống cũ, đảm bảo độ tin cậy của dữ liệu, có thể hoạt động song song với hệ thống cũ, không tốn quá nhiều chi phí để đầu tư…

Hệ thống được thiết kế để thay thế cho hệ thống thanh toán hiện tại của các siêu thị, tuy nhiên, hệ thống có thể được áp dụng tại các điểm bán lẻ khác có ít không gian nhưng cần một hệ thống thanh toán nhanh và tiện lợi. Ngoài ra, hệ thống mới này có thể hoạt đông song song và tận dụng được hệ thống cũ, cần không quá nhiều chi phí để đầu tư,có nguyên tắc hoạt động khá đơn giản và dễ bảo trì nên không đòi hỏi nhân viên phải có kĩ thuật cũng như trình độ cao.

MỤC LỤC

LỜI CẢM ƠN ..... **ii**
TÓM TẮT ĐỀ TÀI ..... **iii**
MỤC LỤC ..... **iv**
MỤC LỤC HÌNH ..... **vii**
MỤC LỤC BẢNG ..... **viii**
DANH SÁCH CÁC TỪ VIẾT TẮT ..... **ix**
Chương 1. GIỚI THIỆU ĐỀ TÀI **1**
1.1 Giới thiệu chung về đề tài 1
1.2 Phân tích đề tài 2
1.2.1 Vấn đề thực tế và bài toán 2
1.2.2 Giải pháp đề nghị 2
1.2.3 Nhiệm vụ của đề tài 3
1.3 Mô hình Queue-Busting on Zigbee 4
1.3.1 Mô hình 4
1.3.2 Nguyên tắc hoạt động 4
1.3.3 Khả năng ứng dụng 5
1.4 Kế hoạch 5
1.5 Công cụ hỗ trợ 6
Chương 2. KIẾN THỨC NỀN TẢNG **7**
2.1 Tổng quan về mạng ZigBee 7
2.1.1 Thị trường mà mạng ZigBee hướng tới. 7
2.1.2 ZigBee là gì? 8
2.1.3 Kiến trúc mạng cơ bản của ZigBee 12
2.2 Application Layer 14
2.2.1 Những chú ý trong gửi và nhận dữ liệu 15
2.2.2 Zigbee PANs (Personal Area Network) 15
2.2.3 Application Framework 16
2.3 Application Support Sublayer (APS) 16
2.3.1 APS ACKs 17
2.3.2 APS Binding 18
2.3.3 APS Groups 18
2.3.4 Address Map 18

2.3.5 AES-128 bit Security 19
2.4 Zigbee Device Object (ZDO) 21
2.4.1 Device Descriptor 22
2.4.2 Service Discovery và Matching Endpoint 22
2.4.3 Low Power 22
2.5 Network Layer 23
2.5.1 ZigBee và IEEE 802.15.4 23
2.5.2 Thiết lập, tham gia và tái tham gia trong mạng ZigBee 24
2.5.3 Gán địa chỉ ZigBee 29
2.5.4 Tìm đường cho packet trong ZigBee 32
2.6 MAC và PHY Layer 33
2.6.1 PHY Layer 33
2.6.2 MAC Layer 33
2.7 Giới thiệu Z-stack của Texas Instrument 33
Chương 3. HIỆN THỰC ĐỀ TÀI 34
3.1 Kiến trúc hệ thống Queue – Busting on ZigBee 34
3.1.1 Hệ thống phần cứng 34
3.1.2 Hệ thống phần mềm 34
3.1.3 Giới thiệu bộ phần cứng DK CC2530 của TI 36
3.1.4 Một số thành phần khác của hệ thống 41
3.1.5 Cấu hình mạng ZigBee cho Z-stack 42
3.2 Thiết bị cashier 43
3.2.1 Nguyên tắc hoạt động 43
3.2.2 Hardware 43
3.2.3 Software 44
3.3 Thiết bị handheld 48
3.3.1 Nguyên tắc hoạt động 48
3.3.2 Hardware 49
3.3.3 Software 50
3.4 Ứng dụng trên PC (personal computer) 53
3.4.1 Nguyên tắc hoạt động 53
3.4.2 Hiện thực 55
3.4.3 Giới thiệu ứng dụng PC 56

Chương 4. KẾT QUẢ VÀ ĐÁNH GIÁ 60
4.1 Kết quả đạt được..... 60
4.2 Hạn chế 60
4.3 Hướng phát triển..... 60
TÀI LIỆU THAM KHẢO..... 62

MỤC LỤC HÌNH

Hình 1-1: Khái niệm hệ thống Queue – Busting on ZigBee 4
Hình 2-1: So sánh các kĩ thuật không giây [3] 8
Hình 2-2 Kết nối mạng mesh trong ZigBee [3] 9
Hình 2-3: Việc tìm lại đường đi trong mạng mesh ZigBee [3] 10
Hình 2-4: Thời gian sử dụng Pin của ZigBee [3] 11
Hình 2-5: Các mảng thị trường của ZigBee [3] 12
Hình 2-6: Kiến trúc của ZigBee [1] 13
Hình 2-7: Sơ đồ stack của lớp ứng dụng. [4] 14
Hình 2-8: Cơ chế tự động gửi lại của lớp APS [4] 17
Hình 2-9: APS Address map [3] 19
Hình 2-10: Mã hóa dùng khóa đối xứng trong mạng Zigbee [4] 20
Hình 2-11: Vị trí của ZDO [4] 21
Hình 2-12: Quá trình ZigBee tạo mạng [3] 26
Hình 2-13: Quá trình ZigBee tham gia mạng [3] 28
Hình 2-14: Gán địa chỉ Cskip trong cây đối xứng [3] 31
Hình 3-1: Sơ đồ kết nối thiết bị của hệ thống 34
Hình 3-2: Sơ đồ phân lớp kiến trúc phần mềm 35
Hình 3-3:SmartRF05 Evaluation Board [2] 37
Hình 3-4:SmartRF05 Battery Board [2] 38
Hình 3-5:CC2530 Evaluation Modules 38
Hình 3-6: CC2531 USB Dongle [2] 39
Hình 3-7: CC2530 Antenna [2] 39
Hình 3-8: Kiến trúc CC2530 [5] 41
Hình 3-9: Sơ đồ khối các chức năng 44
Hình 3-10: Sơ đồ tổng quát các sựkiện chính trong chương trình 45
Hình 3-11: Sự kiện của timer trong cashier 45
Hình 3-12: Sự kiện của scanner trong cashier 46
Hình 3-13: Sự kiện của pc trong cashier 47
Hình 3-14: Sự kiện của radio trong cashier 48
Hình 3-15: Các phần cứng cho hiện thực 49
Hình 3-16: Sơ đồ mô tả tổng quát task ứng dụng trong Handheld 50
Hình 3-17: Sơ đồ xử lý dữ liệu từ Scanner trong Handheld 51
Hình 3-18: Sơ đồ xử lý dữ liệu từ mạng ZigBee trong Handheld 52
Hình 3-19: Sơ đồ hiện thực ứng dụng trên PC 55
Hình 3-20: Giao diện chính của chương trình demo 56
Hình 3-21: Giao diện khi thanh toán. 57
Hình 3-22: Định dạng file excel thể hiện hóa đơn tính tiền 58

MỤC LỤC BẢNG

Bảng 1-1: Bảng kế hoạch công việc chi tiết 5
Bảng 2-1: So sánh xu hướng ứng dụng giữa các giao thức wireless khác và ZigBee. 7
Bảng 2-2: Zigbee Binding table [3] 18
Bảng 2-3: Cskip được tính toán cho stack profile 0x01[3] 30
Bảng 2-4: So sánh các phương tìm đường trong ZigBee [3] 32
Bảng 3-1: Định dạng của giaothức Queue – Busting on ZigBee 36
Bảng 3-2: Các thông số cấu hình cho mạng ZigBee 42
Bảng 3-3: Các thông số cho Simple Description 42
Bảng 3-4: Thông tin về các thiết bị handheld trong mạng ZigBee 58

DANH SÁCH CÁC TỪ VIẾT TẮT

ZC	ZigBee Coordinator
ZR	ZiBee Router
ZED	ZigBee End Device
EB	Evaluation Board
BB	Battery Board
PC	Personal Computer
CSMA-CA	Carrier Sense Multiple Access Collision Avoidance
O-QPSK	Offset-Quadrature Phase-Shift Keying
DSSS	Direct Sequence Spread Spectrum
ACK	Acknowledgement
SAP	Service Access Point
API	Application Programming Interface
NLDE-SAP	Network Layer Data Entity Service Access Point
CRC	Cyclic Redundancy Check
PAN	Personal Area Network
PHY	Physical Layer
NWK	Network Layer
APS	Application Support Sublayer
APSME	APS Management Entity
APSDE	APS Data Entity
SAP	Service Access Point
AF	Application Framework
ZDO	ZigBee Device Object
ZDP	ZigBee Device Profile
PIB	PAN Information Base
NIB	NWK Information Base
AIB	APS Information Base
OSAL	Operating System Abstract Layer
DMA	Direct Memory Access

Chương 1.GIỚI THIỆU ĐỀ TÀI

1.1 Giới thiệu chung về đề tài

Ngày nay, khi nền kinh tế phát triển, đời sống con người ngày càng được nâng cao thì nhu cầu mua sắm, tiêu dùng của con người cũng tăng lên đáng kể. Để đáp ứng nhu cầu đó, một hình thức mua sắm mới và tiện dụng ra đời. Đó là siêu thị, thay cho các chợ truyền thống. Các hệ thống siêu thị hiện nay mọc lên ngày càng nhiều, trở thành một địa điểm thường xuyên lui tới của người tiêu dùng. Với đầy đủcác mặt hàng được trưng bày, người tiêu dùng thỏa thích chọn lựa những gì mình cần.

Khi mà siêu thị trở thành địa điểm mua sắm yêu thích của mọi người thì sẽ nhanh chóng trở nên đông đúc.Thêm vào đó, hệ thống tính tiền truyền thống tại các siêu thị đã trở thành "nỗi ám ảnh" đối với những người tiêu dùng, khi họ phải đợi rất lâu mặc dù chỉ mua một vài thứ.Điều này làm cho người tiêu dùng tốn rất nhiều thời gian để mua sắm, đồng thời làm giảm lợi nhuận của siêu thị, tăng áp lực cho các nhân viên tính tiền, đặc biệt là vào dịp cuối tuần, các ngày nghỉ lễ, các đợt khuyến mãi khi mà nhu cầu mua sắm ngày càng tăng.

Do đó, đề tài "**Xây dựng hệ thống tín tiền nhanh trong siêu thị sử dụng mạng ZigBee**" gọi tắt là "Queue – Busting" được đưa ra nhằm xây dựng hệ thống tính tiền mới trong siêu thị để giảm thiểu thời gian chờ của khách hàng tại các quầy tính tiền. Để giải pháp có thể trở nên cơ động hơn, chúng tôi đưa mạng không dây vào mô hình. Đây là yêu cầu thiết thực, giảm không gian, tăng sự linh động trong siêu thị.

Để thực hiện đề tài thì chúng tôi đưa ra mục tiêunhư sau:

- Hiểu được các kiến thức vềmạng ZigBee.
- Phân tích và thiết kế hệ thống mới đáp ứng yêu cầu thực tế đưa ra.
- Hiện thựchệ thốngthử nghiệm hoàn chỉnh.

Đề tài của chúng tôi là xây dựng giải pháp Queue – busting trên mạng không dây Zigbee nên việc tìm hiểu về mạng không dây Zigbee là ưu tiên hàng đầu. Tuy nhiên, mô hình Queue – Bustingđã được áp dụng vào thực tế nên việc tìm hiểu nguyên tắc hoạt động của mô hình này cũng rất cần thiết. Chúng ta có thể tóm tắt lại những vấn đề chúng ta cần giải quyết như sau:

- Tìm hiểu mô hình Queue – Busting thực tế.
- Nắm vững các kiến thức về mạng Zigbee
- Hiện thực giải pháp trên theo chuẩn mạng Zigbee
- Kiểm tra hoạt động và khắc phục các lỗi có thể xảy ra trong quá trình hoạt động.
- Thực hiện thêm các phương thức bảo mật cho hệ thống.

1.2 Phân tích đề tài

1.2.1 Vấn đề thực tế và bài toán

Từ tìm hiểu thực tế của hệ thống siêu thị hiện nay, chúng tôi đưa ra một số nhược điểm và hiện trạng như sau:

Về phía người tiêu dùng, họ cảm thấy khó chịu, mất kiên nhẫn khi phải đợi rất lâu để thanh toán hàng hóa mà mình chi trả. Do đó, mong muốn to lớn nhất của khách hàng là việc chi trả, thanh toán hàng hóa phải diễn ra nhanh chóng, thuận tiện và chính xác.

Về phía nhân viên thu ngân của siêu thị, họ phải chịu áp lực công việc rất lớn vừa quét và gói hàng hóa vừa tính tiền cho khách hàng. Thêm vào đó là sự cáu gắt của khách hàng khi phải chờ đợi lâu. Việc tính toán tiền bạc rất dễ bị sai lệch, quản lý khách hàng, hàng hóa không được tốt. Một số nhân viên giám sát, túc trực trong siêu thị, có thời gian rảnh rỗi nhiều.

Về phía siêu thị, khi số lượng khách hàng tăng lên cũng đồng nghĩa với doanh thu của họ tăng lên. Tuy nhiên, sự phục vụ chậm trễ trong việc thanh toán, áp lực đối với nhân viên và làm tăng nguy cơ mất lòng tin của khách hàng, giảm doanh thu.

Do đó, một hệ thống thanh toán mới rất cần được thiết kế và xây dựng. Và thỏa mãn các yêu cầu sau:

- Thanh toán nhanh chóng, đơn giản và dễ bảo trì.
- Chuyên môn hóa , bộ phận nào làm chức năng đó.
- Vận hành chính xác trong mọi điều kiện.
- Chi phí đầu tư thấp, có thể tận dụng được hệ thống hiện đang sử dụng.

1.2.2 Giải pháp đề nghị

Hiện nay, có một số mô hình Queue – busting thực tế được áp dụng như giải pháp PreScan của Datalogic. Nhưng yếu điểm của hệ thống này là được thiết kế theo mạng hình sao, tức chỉ kết nối một hop nên chỉ hoạt động gần quầy tính tiền, không linh động.

Nắm bắt được vấn đề thực tế này, chúng tôi đã đưa ra một giải pháp tính tiền nhanh bằng việc ứng dụng mạng ZigBee vào mô hình Queue – Busting. Tất cả các thiết bị được kết nối thành mạng, có thể giao tiếp với nhau. Hệ thống gồm hai phần: di động và cố định. Phần di động sẽ được phân bố bất kì đâu trong siêu thị, nhằm quét và đóng gói hàng hóa cho người tiêu dùng. Phần cố định sẽ nằm ở khu vực quầy tính tiền, chỉ việc yêu cầu dữ liệu người tiêu dùng ở phần di động.

Việc chúng tôi chọn mạng ZigBee để áp dụng vào việc cải thiện hệ thống thanh toán trong siêu thị, bởi vì mạng Zigbee có nhiều ưu điểm, đáp ứng được các yêu cầu về chi phí và độ tin cậy:

- Khác với các hệ thống không dây khác, ZigBee yêu cầu phần cứng thấp nên giảm tối thiểu chi phí đầu tư so với mạng không dây khác.
- Hệ thống phần cứng (chip) và firmware (ZigBee stack) được hỗ trợ nhiều từ nhà cung cấp. Và với giá thành rẻ.

- Dễ dàng mở rộng, có thể hỗ trợ tới hơn 60 ngàn thiết bị.
- Dữ liệu để truyền tải trong siêu thị không nhiều dễ dàng thực hiện bởi tốc độ của mạng ZigBee mà không gặp vấn đề lớn về thời gian và băng thông.
- ZigBee truyền tin cậy, bảo mật tốt.
- Ít tiêu hao năng lượng.

Ưu điểm của mô hình Queue – Busting so với các mô hình khác:

- Tầm hoạt động rộng, có thể mở rộng một cách dễ dàng.
- Tận dụng thời gian rỗi của khách hàng trong quá trình chờ đợi, giảm tình trạng chen lấn.
- Tận dụng lực lượng nhân viên giám sát, túc trực rảnh rỗi trong siêu thị, giảm áp lực lên quầy tính tiền.
- Không cần tốn chi phí đâu tư thêm các quầy thanh toán.
- Có thể hoạt động song song với hệ thống cũ.
- Đã được thử nghiệm thực tế và chứng minh được hiệu quả mang lại.

Từ tất cả những ưu điểm kể trên, chúng tôi đưa ra yêu cầu của hệ thống Queue – Busting sử dụng mạng Zigbee (Queue – Busting on Zigbee) như sau :

- Vận hành đúng, không gây mất mát thông tin về hàng hóa của khách hàng khi thanh toán.
- Hệ thống phải vận hành tốt trong điều kiện môi trường nhiễu, nhiệt độ cao, không gây ảnh hưởng đến các hoạt động của mạng không dây khác.
- Giảm thời gian đáng kể so với hệ thống thanh toán hiện nay.
- Thuận lợi cho nhân viên điều hành và quản lý.
- Chi phí đầu tư thấp, dễ dàng bảo trì và vận hành.
- Có khả năng bảo mật thông tin, phòng chống các sự cố mất dữ liệu khi có kẻ cố tình phá hoại hoặc lấy trộm thông tin.
- Có khả năng mở rộng theo nhu cầu.
- Có thể hoạt động song song với hệ thống cũ.

1.2.3 Nhiệm vụ của đề tài

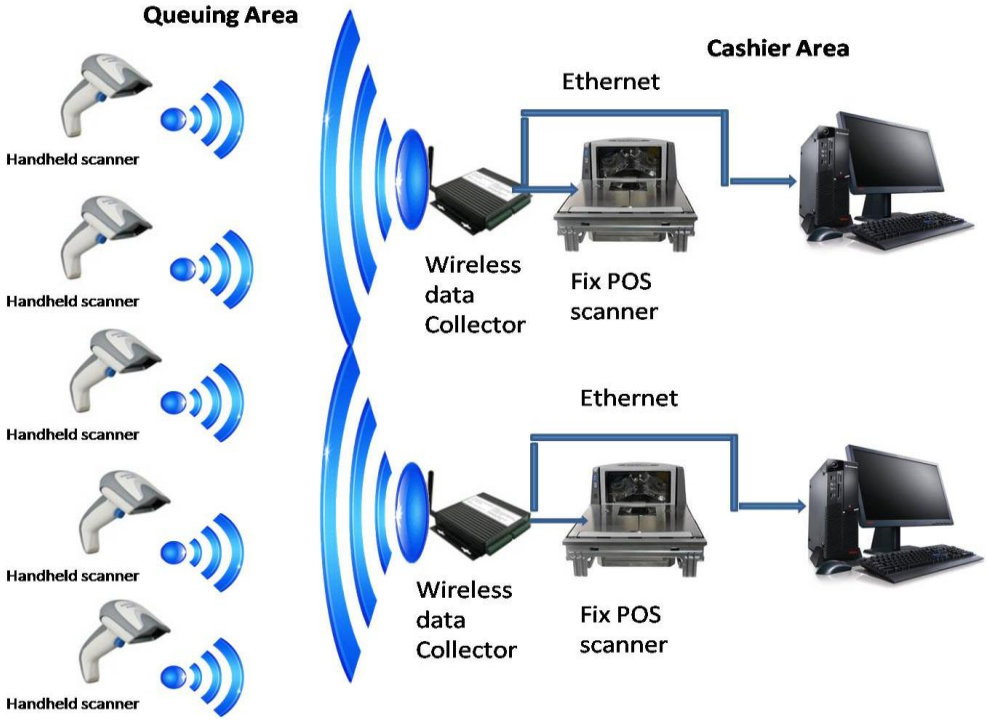
- Hiểu rõ nguyên tắc hoạt động cũng như cấu trúc của mô hình Queue – Busting.
- Hiểu và nắm vững kiến thức về mạng ZigBee.
- Phân tích và thiết kế một hệ thống Queue – Busting on ZigBee hoàn chỉnh.
- Hiện thực hệ thống và đảm bảo hệ thống hoạt động đúng chức năng cơ bản từ lúc mua hàng đến lúc thanh toán.
- Xử lý các tình huống có thể xảy ra trong quá trình hoạt động như: không tìm thấy thông tin khách hàng, thông tin khác hàng bị trùng…
- Bổ sung thêm một số tính năng cần thiết khác cho việc bảo trì cũng như kiểm tra hệ thống.
- Phát triển thêm các phương thức bảo mật cho hệ thống.
- Đánh giá hệ thống Queue – Busting on ZigBee vừa thực hiện được.

1.3 Mô hình Queue-Busting on Zigbee

1.3.1 Mô hình

Queue – Busting giải quyết vấn đề xếp hàng dựa trên nguyên tắc quét (mã vạch) hàng hóa của khách hàng trước khi họ đến quầy tính tiền. Do đó, giảm thời gian quét hàng hóa đối với nhân viên thu ngân, giúp cho việc thanh toán được diễn ra nhanh hơn.

Để việc quét hàng hóa trở nên nhanh hơn, hệ thống Queue – Busting cần phải làm việc được với các thiết bị quét mã vạch cầm tay và cố định đặt ở quầy thu ngân. Các thiết bị này phảigiao tiếp với được với nhau thông qua mạng không dây, để thiết bị cầm tay có thể hoạt động ở phạm vi rộng. Hệ thống Queue – Busting on Zigbee được mô tả như hình sau :



Hình 1-1: Khái niệm hệ thống Queue – Busting on ZigBee

1.3.2 Nguyên tắc hoạt động

Khi có rất nhiều khách hàng đứng xếp hàng, một vào nhân viên sẽ cầm máy quét mã vạch cầm tay, quét hàng hóa của từng khách hàng. Sau khi quét cho một khách hàng xong, nhân viên sẽ quét tiếp một mã số định danh dành riêng cho khách hàng đó. Tất cả thông tin về hàng hóa sẽ được lưu trữ trong máy quét mã vạch cầm tay này.

Khi đến quầy tính tiền, khách hàng chỉ phải đưa cho nhân viên thu ngân mã số định danh trên. Tất cả thông tin về hàng hóa của khách hàng sẽ được truyền về cho máy tính của nhân viên thu ngân. Việc thanh toán sẽ được diễn ra rất nhanh chóng.

1.3.3 Khả năng ứng dụng

Hiện tại, hệ thống Queue – Busting đã được triển khai trên một số của hàng, siêu thị trên thế giới. Tuy nhiên, hệ thống chỉ dừng lại ở mức 1-1, tức là một thiết bị quét mã vạch cầm tay kết nối với một thiết bị quét mã vạch cố định ở quầy thu ngân. Do nhu cầu mở rộng, tất cả các thiết bị quét mã vạch cầm tay (handheld scanner) có thể kết nối với tất cả thiết bị quét mã vạch cố định ở quầy thu ngân (point of sale – POS), và tiết kiệm chi phí, nên giải pháp Queue – Busting dựa trên mạng không dây Zigbee được đưa ra.

1.4 Kế hoạch

Do yêu cầu của đề tài là ứng dụng một chuẩn giao tiếp lên một mô hình đã có nên việc tìm hiểu chiếm khá nhiều thời gian (2 tháng) trong toàn bộ thời gian hiện thực đề tài (4 tháng). Khi hệ thống đã hoạt động được thì việc kiểm tra sửa lỗi cũng rất cần được quan tâm. Sau đây là bảng kế hoạch làm việc chi tiết của cả nhóm chúng tôi :

Bảng 1-1: Bảng kế hoạch công việc chi tiết

STT	DETAILS	DEADLINE	ASSIGN
1	Tìm hiểu mạng Zigbee và hardware sẽ hiện thực hệ thống : - Application layer và Network layer của mạng Zigbee - Datasheet và các cấu hình cho 2 board EB và BB	01/11	Team
2	Làm bộ chuyển đổi điện áp RS232	01/11	Hải
3	Xây dựng trên Evaluation Board (EB): - 1 module để nhận data từ barcode scanner. - 1 module truyền nhận data với PC. - 1 databases mã khách hàng	11/11	Vinh
4	Xây dựng trên Battery Board (BB): - 1 module đọc, ghi, xóa datacho Flash. - 1 module nhận data từ barcode scanner	11/11	Hải
5	Xây dựng trên PC : - 1 chương trình thanh toán hóa đơn. - 1 databases mã hàng hóa và đơn giá.	11/11	Phúc
6	Alpha release : - Kết hợp các module trên EB và BB lại để tạo thành 1 bộ code hoàn chỉnh. - Hoàn thành chức năng cơ bản nhất của hệ thống	18/11	Team
7	Alpha test : - Kiểm tra chức năng cơ bản của toàn bộ hệ thống từ quét hàng hóa đến lúc thanh toán - Sửa chữa các lỗi xảy ra nếu có	25/11	Team
8	Beta release : - Thêm các tính năng cần thiết khác : báo lỗi, xử lý lỗi có thể xảy ra trong quá trình hoạt động … - Thêm tính năng bảo mật cho hệ thống	05/12	Team
9	Beta test : - Kiểm tra tất cả cách tính năng của hệ thống	10/12	Team

	- Sửa chữa các lỗi xảy ra nếu có		

1.5 Công cụ hỗ trợ

- IAR Embedded Workbech for 8051 8.10 : công cụ lập trình và kiểm tra lỗi của toàn bộ luận văn.
- Barcode studio : hỗ trợ việc tạo ra các barcode cho việc kiểm tra hoạt động của hệ thống
- ComTestSerial 3.0.0.103 : hỗ trợ việc kiểm tra hoạt động truyền nhận dữ liệu giữa các thiết bị thông qua cổng COM
- Eclipse (Java) : hiện thực chương trình thanh toán trên PC

Chương 2.KIẾN THỨC NỀN TẢNG

2.1 Tổng quan về mạng ZigBee

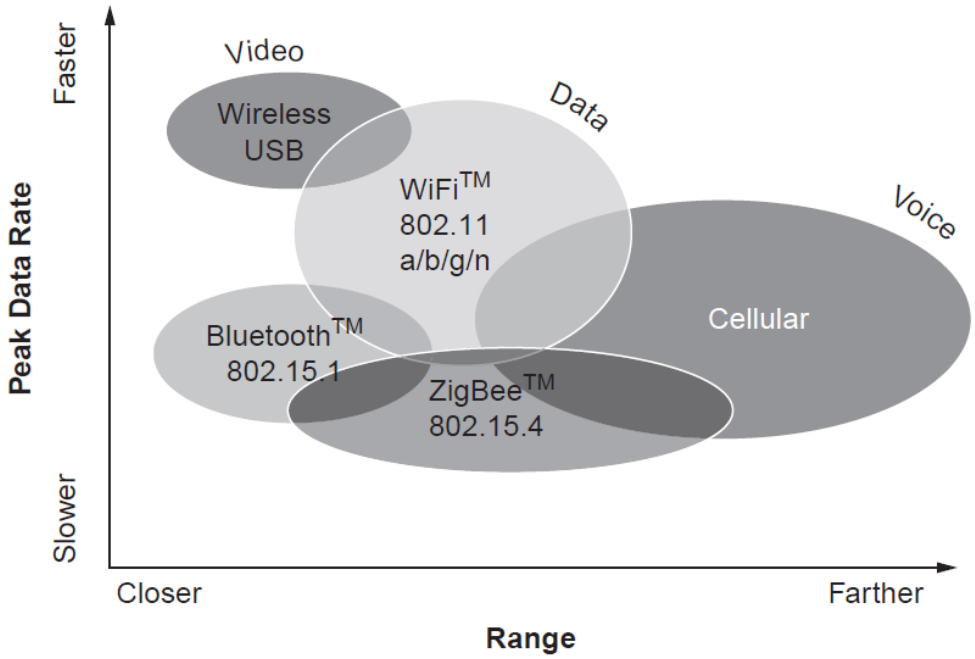
2.1.1 Thị trường mà mạng ZigBee hướng tới.

Hiện nay, mạng không dây được ứng dụng rộng rãi và phát triển mạnh mẽ trên thế giới. Nhiều chuẩn mạng ra đời nhằm đáp ứng những yêu cầu khác nhau của đời sống như wifi cho mạng Internet, Bluetooth cho việc kết nối các thiết bị không dây, các chuẩn mạng điện thoại… Vậy, khi mà các mạng không dây khác đang trở nên phổ biến và ưa chuộng thì mục đích của việc mạng không dây ZigBee ra đời là gì? Chuẩn mạng không dây ZigBee phù hợp với nhu cầu thị trường mà các kĩ thuật không dây khác không thể đáp ứng (xemBảng 2-1).

Bảng 2-1: So sánh xu hướng ứng dụng giữa các giao thức wireless khác và ZigBee.

	Các giao thức wireless khác	ZigBee
Tốc độ	Tốc độ truyền dữ liệu cao	Tốc độ truyền dữ liệu thấp
Tính năng	Nhiều tính năng	Nhắm tới một stack nhỏ
Nhu cầu	Media độ nét cáo	Điều khiển thiết bị
Thời gian sử dụng Pin	Vài giờ, vài ngày	Hàng năm
Vòng đời sản phẩm	1 đến 2 năm	Hàng thập kỉ

Trong khi hầu hết các chuẩn không dây khác hướng tới tốc độ nhanh hơn thì ZigBee nhắm tới tốc độ truyền dữ liệu thấp. Trong khi các giao thức không dây khác thêm càng nhiều tính năng thì ZigBee nhắm tới một stack nhỏ mà phù hợp với các vi điều khiển 8-bit. Trong khi các kĩ thuật không dây khác hướng tới cung cấp truyền data tới Internet hay phân phối dòng media độ nét cao (high-definition) thì ZigBee hướng tới điều khiển đèn hoặc gửi dữ liệu nhiệt độ từ các cảm biến… Trong khi các kĩ thuật không dây khác được thiết kế để chạy trong vài giờ hoặc có thể vài ngày bằng pin thì ZigBee chạy tới hàng năm. Trong khi các kĩ thuật không dây khác cung cấp 12 đến 24 tháng vòng đời cho một sản phẩm thì các sản phẩm ZigBee có thể dùng trong hàng thập kỉ hoặc hơn trong các ứng dụng đặc trưng. Do đó, các dịch vụ mà ZigBee hướng tới là việc kết nối cảm biến không dây và điều khiển hay đơn giản là điều khiển không dây.Màmục tiêucủa ZigBee là “Wireless Control That Simply Works”.



Hình 2-1: So sánh các kĩ thuật không giây [3]

Tóm lại, thị trường điều khiển không dây có nhiều yêu cầu mà chỉ có ZigBee mới phù hợp. Đó là:

- Tin cậy cao
- Chi phí thấp
- Năng lượng cần rất thấp
- Bảo mật cao
- Một chuẩn mở

Và để có được năng lượng tiêu thụ thấp và chi phí thấp, ZigBee đã chấp nhận một ràng buộc kĩ thuật là tốc độ truyền thấp.

Như vậy, mạng ZigBee ra đời nhằm đáp ứng nhu cầu điều khiển là chính, không đòi hỏi tốc độ truyền cao, phù hợp với mảng thị trường mà các mạng không dây khác không thể đáp ứng.

2.1.2 ZigBee là gì?

Để hiểu rõ hơn về mạng ZigBee so với các mạng không dây khác, chúng tôi phân tích chi tiết về các đặc điểm của mạng như sau.

ZigBee có độ tin cậy cao.

Thực tế, sự truyền thông không dây là không tin cậy. Chứng minh điều này bằng việc đi lòng vòng với một chiếc điện thoại di động, sau đó bước vào thang máy. Bất cứ ai sử dụng điện thoại đều gặp sự cố cuộc gọi bị ngắt hoặc đường truyền yếu. Tất cả bởi vì sóng radio cũng chỉ là các sóng. Chúng chạy qua các vật cản, có thể bị chặn bởi kim loại, nước hoặc khối bê tông và phụ thuộc vào nhiều yếu tố phức tạp gồm thiết kế ăng-ten, sự khuếch đại năng lượng, và thậm chí các điều kiện thời tiết.

Tuy nhiên, điều khiển không dây thường không có cùng vấn đềnhư trong một cuộc điện thoại, di chuyển để tìm điểm nhận sóng tốt hơn hay đợi đểthử lại sau. Hiệp hội ZigBee hiểu điều này, được thể hiện trong sự đặc tảZigBee để giành khả năng tin cậy cao trong nhiều cách:

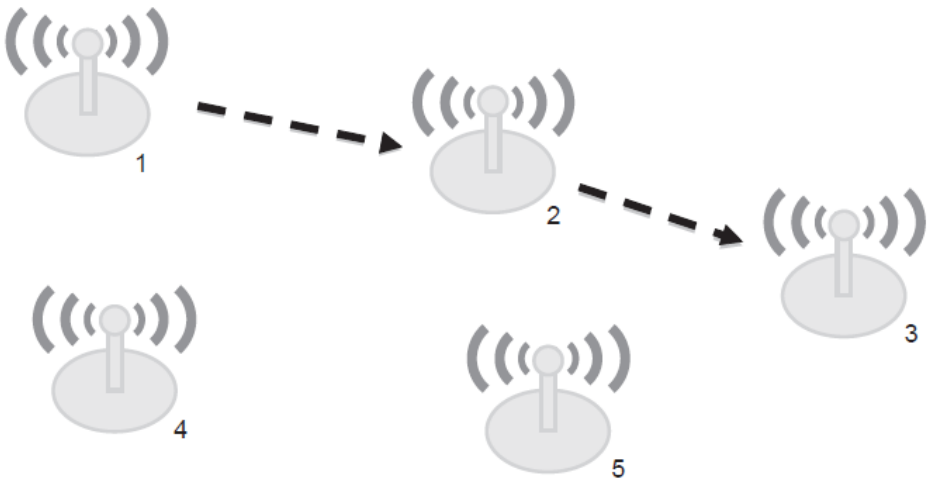
- IEEE 802.15.4 với O-QPSK và DSSS
- CSMA-CA
- 16-bit CRCs
- ACK tại mỗi hop (chặng)
- Việc nối mạng lưới (mesh) để tìm ra đường đi tin cậy
- End-to-end ACK để kiểm tra dữ liệu đến đích

Điều đầu tiên là dựa vào một kĩ thuật không dây rất tin cậy, khoảng cách thấp và dùng sự đặc tả IEEE 802.15.4. Đặc tả này là một kĩ thuật radio mạnh, rất hiện đại được xây dựng trên 40 năm kinh nghiệm của IEEE. Nó dùng những gì được gọi là Offset-Quadrature Phase-Shift Keying (O-QPSK) và Direct Sequence Spread Spectrum (DSSS), một sự kết hợp của các kĩ thuật mà cung cấp hiệu suất tuyệt vời trong các môi trường có tỉ lệ tín hiệu trên nhiễu thấp.

Thứ hai, ZigBee dùng cái gọi là "Carrier Sense Multiple Access Collision Avoidance" (CSMA-CA) để tăng khả năng tin cậy. Trước khi truyền, ZigBee lắng nghe kênh truyền. Khi kênh truyền trống, ZigBee bắt đầu truyền. Điều này ngăn các radio khỏi việc gây ra xung đột dữ liệu. CSMA-CA tương tự những gì con người làm trong các hội thoại. Chúng ta chờ người khác nói xong mới nói.

Thứ ba, ZigBee dùng 16-bit CRC trên mỗi gói (packet), được gọi là một Fame Checksum (FCS). Điều này đảm bảo các bit dữ liệu chính xác.

Thứ tư, mỗi packet được thử lại 3 lần (trong toàn bộ 4 lần truyền). Nếu packet không thể truyền qua sau lần truyền thứ tư, thì ZigBee thông báo với node gửi về việc truyền thất bại này.

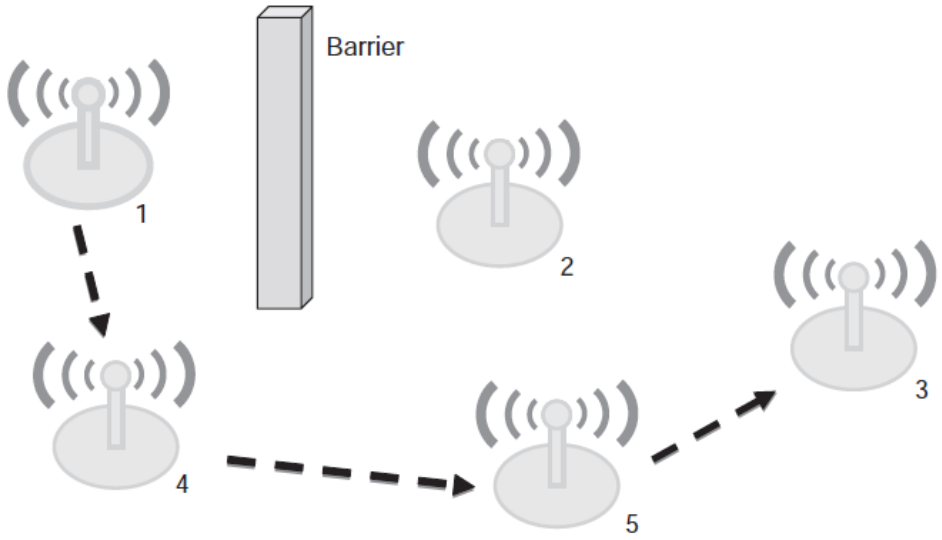


Hình 2-2 Kết nối mạng mesh trong ZigBee [3]

Thứ năm, một cách khác mà ZigBee có được khả năng tin cậy là kết nối mạng lưới (mesh). Mạng lưới một cách cơ bản cung cấp ba khả năng tăng cường cho một mạng wireless: mở rộng khoảng cách bằng multi-hop, việc tạo mạng ad-hoc, và quan trọng hầu hết là tìm đường đi tự

động và tự phục hồi.Với mạng lưới, dữ liệu từ node đầu tiên có thể đến bất cứ node nào khác trong mạng ZigBee, đánh giá khoảng cách bằng các radio để gửi message (xem Hình 2-2).

Node 1 muốn giao tiếp với node 3, nhưng nó ra khỏi vùng phủ song của node 3. ZigBee tự động tìm ra đường tốt nhất và node 1 sẽ gửi thông tin cho node 2, rồi truyền tiếp đến node 3.Bây giờ giả sử rằng, có vài thứ xảy ra trên đường đi này. Có thể node 2 hoàn toàn bị loại bỏ hoặc chết hay vài vật cản như một bức tường bê-tông hoặc gặp một thùng nước lớn. Điều này không hề gì với ZigBee. ZigBee sẽ tự động phát hiện sự thất bại của đường đi và đi vòng (xem Hình 2-3).



Hình 2-3: Việc tìm lại đường đi trong mạng mesh ZigBee [3]

Thêm vào đó, ZigBee cung cấp việc broadcast tin cậy, một kĩ thuật cho việc phân phối một message đến nhiều node trong mạng. ZigBee cũng cung cấp multicasting có thể gửi một message đến bất kì group các node. Và như một kĩ thuật tìm đường back-up, ZigBee cung cấp tìm đường cây (tree routing) đểtăng mạng lưới ZigBee trong các hệ thống giới hạn RAM.

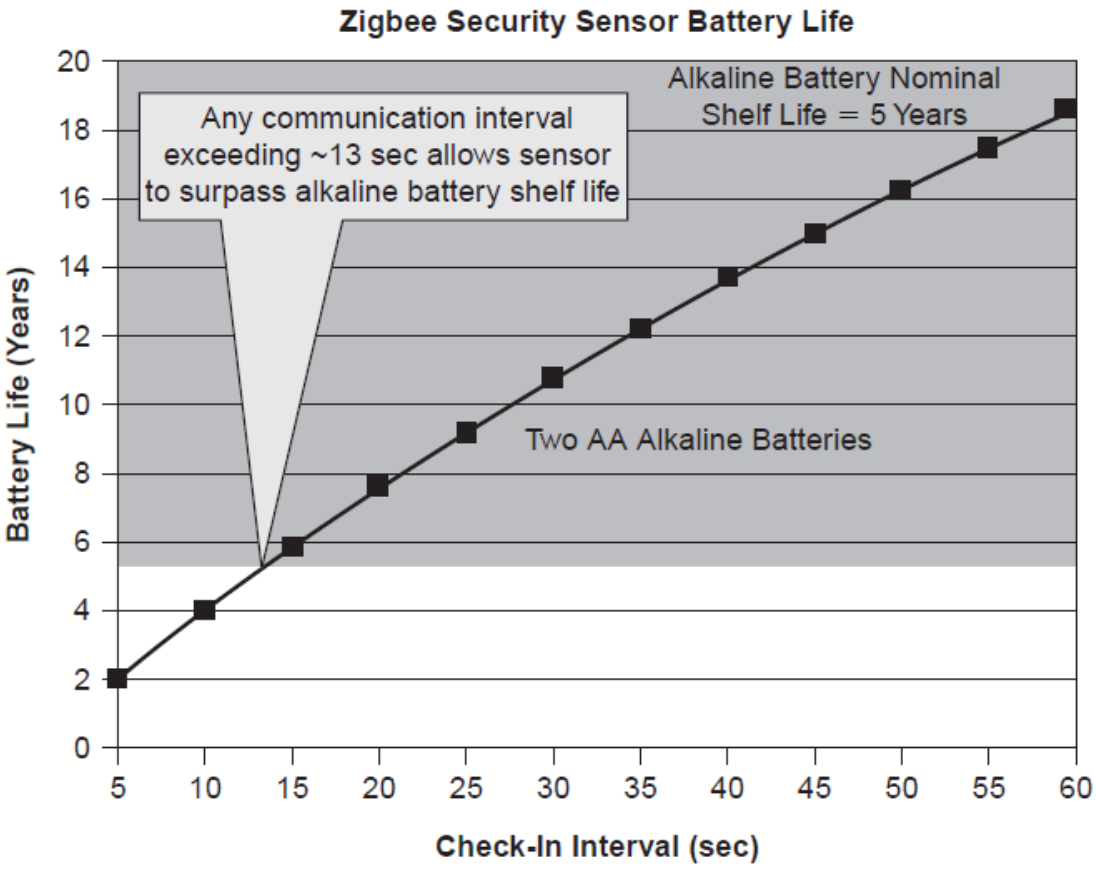
Cuối cùng, ZigBee cung cấp tự động ACK end-to-end. Ứng dụng có thể biết một gói cụ thể được nhận bởi node khác hay không. Với tất cả các truyền, ZigBee lọc ra các gói trùng, nên ứng dụng không cần bận tâm.

ZigBee có chi phí thấp

Nhiều nhà cung cấp stack và chip, các module ZigBee và nhiều tài nguyên phân phối với chi phí phát triển thấp cho các thiết bị ZigBee như Texas Instrument, Microchip, Atmel, ST …

ZigBee sử dụng năng lương thấp

Các thiết bị trong một mạng ZigBee có thể chạy trong nhiều năm chỉvới một cặp pin AA, phụ thuộc ứng dụng (xem Hình 2-4).



Hình 2-4: Thời gian sử dụng Pin của ZigBee [3]

ZigBee bảo mật cao

Cho việc bảo mật mạng, ZigBee dùng National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES). Chuẩn AES – 128 là một mã hóa khối (block cipher) mà mã hóa và giải mã các packets trong một phương thức khó có thể để bẻ khóa. Đây là một trong những chuẩn nổi tiếng. Nguyên nhân mà nó được dùng bởi ZigBee là:

- Chuẩn được xác thực quốc tế.
- Miến phí
- Có thể hiện thực trên một vi điều khiển 8-bit

ZigBee là một chuẩn mở toàn bộ

Nhiều nhà cung cấp ZigBee stack, chip và các giải pháp ứng dụng.Đặc tả ZigBee có thể được tải miễn phí từ websitehttp://www.zigbee.org

ZigBee có tốc độ dữ liệu thấp

Để có được chi phí thấp và năng lượng tiêu hao thấp và việc xem xét không gian và thị trường ứng dụng mà ZigBee nhắm tới, hiệp hội ZigBee đã quyết định giữ giao thức trong một môi trường tốc độ truyền dữ liệu thấp.

ZigBee nằm trên các IEEE 802.15.4 transceivers, trong không gian 2.4GHz truyền thông tại 250kbps, nhưng do số lần truyền lại, sự mã hóa và giải mã, và giao thức lưới đầy đủ được dùng

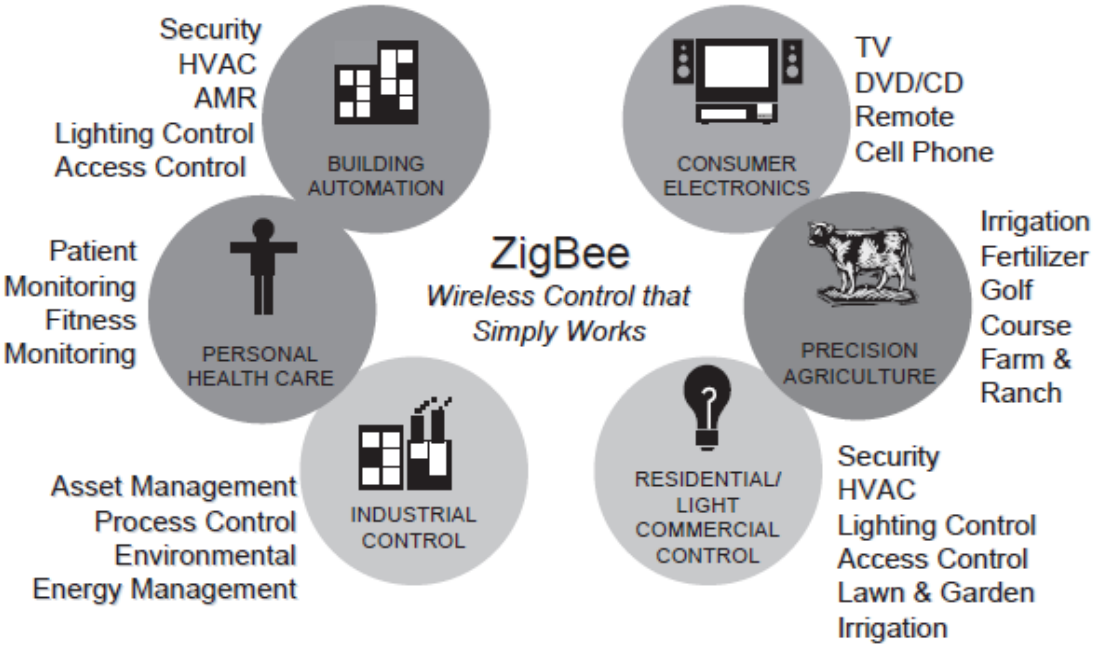
nên through-put thực sự khoảng 25kbps.Transceivers là half-duplex, đây cũng là một yếu tố giảm through-put từ 250 tới 25kbps.

Các ứng dụng sử dụng ZigBee

Mạng ZigBee được sử dụng trong các ứng dụng thực tế sau:

- Home Automation
- Commercial Building Automation
- Industrial Plant Monitoring
- Telecommunication Applications
- Automatic Metering Initiative
- Personal Home and Health Care

ZigBee xuất hiện ở nhiều thị trường gồm nhà, thương mại, công nghiệp tự động, y tế và các dịch vụ dựa trên cục bộ (local-based).



Hình 2-5: Các mảng thị trường của ZigBee [3]

2.1.3 Kiến trúc mạng cơ bản của ZigBee

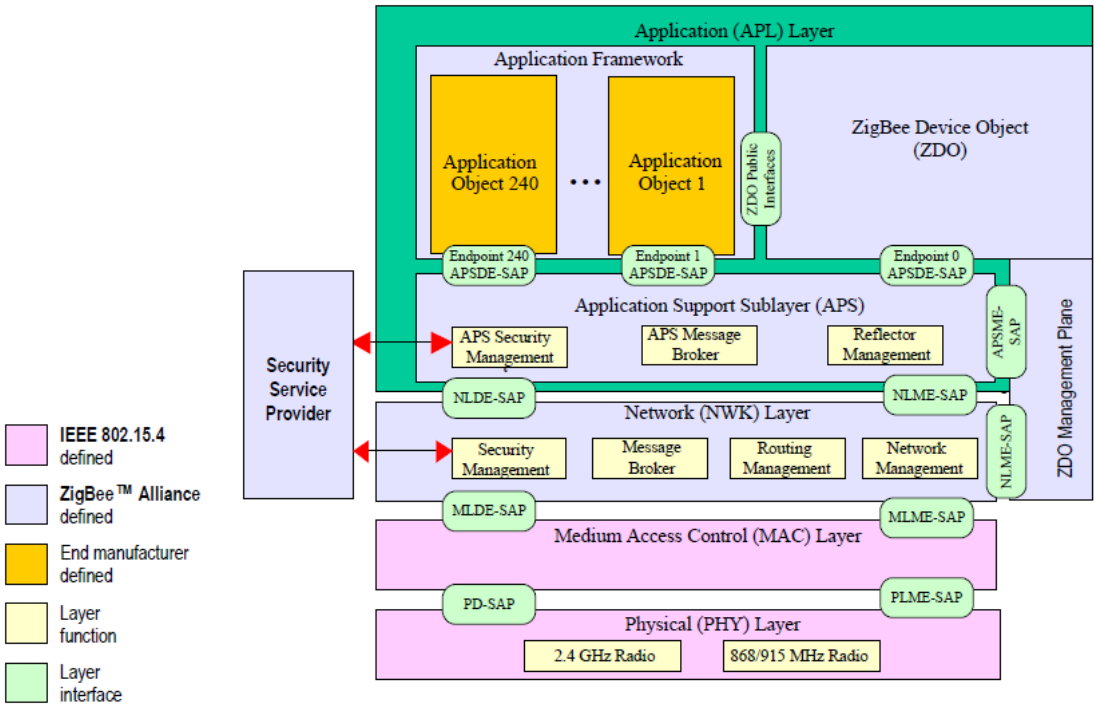
Kiến trúc mạng ZigBee chia làm 3 phần chính:

- Ứng dụng
- ZigBee stack
- Radio

Và được chia thành các lớp, mỗi lớp không biết gì về lớp trên nó. Lớp trên được xem như một "master" mà gửi yêu cầu cho "slave" bên dưới làm.

ZigBee không giống mô hình mạng OSI 7-layer, nhưng nó có vài thành phần giống gồm PHY (physical), MAC (link layer), NWK (network). Các lớp 4-7 (transport, session ,

presentation và application) được chuyển qua các lớp APS (APplication support) và ZDO (ZigBee Device Object) trong mô hình ZigBee.



Hình 2-6: Kiến trúc của ZigBee [1]

Giữa các lớp là "Service Access Points"(SAPs). SAPs cung cấp API tách biệt bên trong lớp khỏi các lớp trên và bên dưới. Giống như đặc tả IEEE 802.15.4, ZigBee dùng 2 SAPs cho mỗi lớp, một cho dữ liệu và một cho sự quản lý.Ví dụ, tất cả các sự truyền thông dữ liệu đến và từ lớp mạng đi qua "Network Layer Data Entity Service Access Point" (NLDE-SAP). Các yêu cầu trong đặc tả ZigBee giống như APSDE-DATA.request. Một yêu cầu gửi dữ liệu ra radio nhưng chỉ được khởi tạo ở lớp APS.

Hai lớp thấp nhất, MAC và PHY được định nghĩa bởi đặc tả IEEE 802.15.4. Lớp PHY đơn giản dịch các packet thành các over-the-air bits và ngược lại. Lớp MAC cung cấp khái niệm của một network, gồm một PAN ID, và kết nối thông qua các beacon requests và reponses. Nó cũng cung cấp các ACK trên hop và một vài lệnh cho việc tham gia và tạo một mạng. Lớp MAC không có multi-hop hay mesh.

Lớp NWK có trách nhiệm cho hình thành mạng mesh, gồm broadcasting các packets qua mạng, xác định các đường đi cho các unicasting packets, và đảm bảo các packets được gửi một cách tin cậy từ một node đến node khác. Lớp network cũng có một tập các lệnh cho mục đích bảo mật, gồm bảo mật tham gia và tái tham gia mạng. Tất cả các mạng ZigBee được bảo mật ở lớp NWK, và toàn bộ payload của NWK frame được mã hóa.

Lớp APS có trách nhiệm cho ứng dụng. Nó hoạt động như một bộ lọc cho ứng dụng chạy phía trên nó là các endpoints, đơn giản là logic trong các ứng dụng này. Nó hiểu những gì các Clusters và Endpoints đưa ra, và kiểm tra xem endpoint là một thành viên của Application Profile và Group trước khi gửi message lên trên. Lớp APS cũng lọc các message trùng mà hoàn

toàn được gửi lên bởi lớp NWK. Lớp APS giữ một bảng Local Binding, một bảng chỉ các nodes hoặc các groups trong mạng mà node muốn giao tiếp đến.

Lớp ZDO (bao gồm ZigBee Device Profile, ZDP) có trách nhiệm cho quản lý cục bộ và over-the-air của mạng. Nó cung cấp các dịch vụ để khám phá các nodes khác và các dịch vụ trong mạng, và có trách nhiệm trực tiếp cho trạng thái hiện tại của node trên mạng.

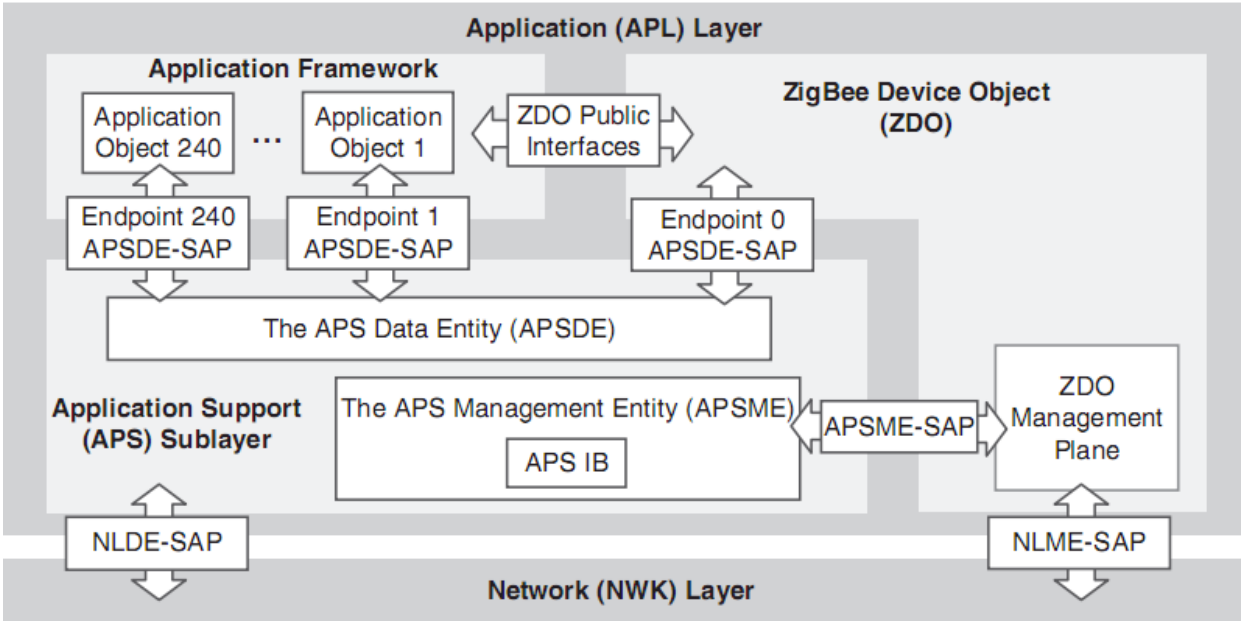
Application Framework chứa ZigBee Cluster Library và cung cấp một framework mà các ứng dụng chạy bên trong. Các endpoints là cơ chế được sử dụng tách biệt một ứng dụng khỏi các ứng dụng khác.

Tất cả các lớp có một thành phần được gọi là"information base" (thông tin cơ bản). Tại lớp MAC, được gọi là một PAN Information Base (PIB). Tại lớp NWK được gọi là Network Information Base (NIB), và tất nhiên AIB cho lớp APS. Tất cả "information base" nghĩa là các cài đặt của lớp đó. Bao nhiêu sự truyền lại được yêu cầu? PAN ID hay địa chỉ network hiện giờ của một node cụ thể là gì? Các trường này trong "information base" nhìn chung được cài đặt bởi các lớp cao hơn hoặc thông qua việc dùng các câu lệnh quản lý thông qua các sự quản lý SAPs.

Chú ý rằng trong đặc tả không đề cập về sự tương tác với bất kì phần cứng trong một thiết bị ZigBee hơn là radio. Không đề cập về giao tiếp LEDs, LCD, speaker, GPIO ports, bộ nhớ non-volatile hoặc flash. ZigBee chỉ quan tâm tới giao thức mạng và hành vi over-the-air. ZigBee kiểm tra phù hợp yếu tố này. Khi tất cả các message over-the-air có thể được hiểu một cách chính xác bởi bất kì node ZigBee khác, cho phép các nhà cung cấp cải tiến trong khi vẫn cung cấp khả năng tương thích hoàn toàn giữa các nhà cung cấp.

2.2 Application Layer

Đây là lớp cao nhất trong các lớp giao thức của mạng Zigbee. APL layer bao gồm 3 phần như hình dưới đây: APS, ZigBee Device Objects (ZDO), và các framework.



Hình 2-7: Sơ đồ stack của lớp ứng dụng. [4]

The application support sublayer (APS): cung cấp interface giao tiếp giữa lớp network layer (NWK) và lớp APL. APS là lớp con của APL. Cũng như những lớp thấp khác, APS hỗ trợ 2 dịch vụ: dữ liệu và quản lý. Dịch vụ dữ liệu được cung cấp bởi APS Data Entity (APSDE) và được tiến hành thông qua APSDE Service Access Point (SAP). Dịch vụ quản lí được cung cấp bởi APS Management Entity (APSME) và được tiến hành thông qua APSME-SAP.

Framework trong Zigbee là môi trường để Application objects điều khiển và quản lý . Application objects được phát triển bởi nhà sản xuất thiết bị. có thể có đến 240 Application objects trong 1 thiết bị đơn.

Application objects sử dụng APSDE-SAP để gửi và nhận dữ liệu giữa các application objects (như Hình 2-7). Mỗi Application object có 1 địa chỉ endpoint (endpoint 1 đến endpoint 240). Địa chỉ 0 dùng cho ZDO. Để broadcast 1 tin nhắn đến tất cả các application objects, người ta thiết lập địa chỉ endpoint là 255.

The ZigBee Device Objects (ZDO) cung cấp 1 giao diện để giao tiếp giữa APS và application framework.

2.2.1 Những chú ý trong gửi và nhận dữ liệu

Zigbee hỗ trợ một cách tốt nhất để truyền dữ liệu giữa các node trong hệ thống mạng. Zigbee sử dụng chuẩn truyền dự liệu được định nghĩa bởi IEEE. Hỗ trợ: unicast, broadcast and groupcast:

- Sử dụng unicast: khi việc gửi nhận dữ liệu giữa 2 node với tần số thấp, giúp tiết kiệm băng thông.
- Sử dụng acknowledged unicasts nếu việc gửi nhận cần có sự xác thực, đảm bảo là có gửi hay nhận được chưa.
- Sử dụng broadcast không nên hơn 1 lần trong 1 phút, nếu khoảng cách xa. Đôi lúc gửi broadcast giữa những node gần nhau lại rất hữu ít. Broadcast không có acknowledged.
- Sử dụng groupcast để điều khiển 1 nhóm lớn hơn 5 node. Groupcast sẽ giúp quá trình truyền nhận nhanh hơn là sử dụng unicast trong 1 nhóm nhiều node. Giống như broadcast, groupcast hữu ít với những node ở gần nhau và không có acknowledged.

2.2.2 Zigbee PANs (Personal Area Network)

Những node trong mạng zigbee chỉ có thể gửi dữ liệu cho node khác trong cùng mạng của nó. Mạng đó được gọi là PAN.

- Các Zigbee PAN được được thành bởi Zigbee Coordinators (ZCs),và chỉ có ZCs mới tạo ra PAN. Những dạng node khác, như Zigbee Routers (ZRs) và Zigbee End-Devices (ZEDs) có thể tham gia vào mạng nhưng không thể tạo mạng.
- Để định danh các PAN người ta sử dụng PAN IDs. Zigbee PAN IDs là 1 số 16 bit trong khoảng từ 0x0000 đến 0x3fff (chú ý là vùng số này khác trong định nghĩa của 802.15.4 0x0000- 0xfffe).

- Extended PAN IDs là 1 số 64 bit để định danh PAN, được sử dụng khi 1 node muốn tham gia vào mạng.

2.2.3 Application Framework

Zigbee cung cấp lựa chọn sử dụng các application profiles trong việc phát triển ứng dụng. việc sử dụng này giúp các nhà sản xuất có khả năng tương tác, các sản phẩm tương thích với nhau.Mỗi application profile được định danh bởi 1 số 16 bit gọi làprofile identifier. Kiến trúc cơ bản của application profiles như hình :

Application profiles gồm 2 thành phần chính : clusters và device descriptions. Cluster là 1 nhóm các thuộc tính được gom chung thành nhóm với nhau. Mỗi cluster được định danh bởi duy nhất 1 số 16 bit gọi là cluster identifier. Mỗi thuộc tính trong cluster cũng được định danh duy nhất bởi 1 số 16 bit gọi là attribute identifier. Những thuộc tính này được sử dụng để lưu trữ dữ liệu hoặc các trạng thái. Mỗi application profile có 1 list các cluster identifiers, mỗi cluster identifiers chỉ đến 1 cluster đúng nhất.

Một phần khác của application profile là device descriptions, cung cấp những thông tin về thiết bị. Mỗi device description được định danh bởi 1 số 16 bit.

2.3 Application Support Sublayer (APS)

APS nằm trên lớp Network trong mô hình kiến trúc của Zigbee, cung cấp một giao diện cho 2 lớp network và application. Có khả năng hiểu được các frame ở lớp ứng dụng. APS frame bao gồm các thành phần : endpoint, clusters, profile ID và groups. APS hỗ trợ 2 loại dịch vụ là data (dữ liệu) và management (quản lý). Dịch vụ APS data được cung cấp bởi APSDE và được truy cập thông qua APSDE-SAP. Dịch vụ APS management được cung cấp bởi APSME và được truy cập thông qua APSME-SAP.

APS cung cấp dịch vụ về dữ liệu cho lớp application và Zigbee Device Object (ZDO) thông qua APSDE. APSDE nhận dữ liệu cần truyền dưới dạng các Protocol Data Unit (PDU), thêm vào header để tạo thành APS data frame, frame này sẽ được truyền xuống cho lớp network bên dưới.

APSME chịu trách nhiệm chính cho các tác vụ sau :

- Lọc ra các gói tin không phù hợp với endpoints và profiles.
- Tạo ra các gói ACK end-to-end.
- Duy trì bảng tên nhóm(group table), bảng kết nối (binding table), bản dịchđịa chỉ (address map) cục bộ.

APSME có nhiệm vụ lọc ra các gói tin có endpoints không phù hợp với các endpoint hiện có. Lọc ra các gói tin không phù hợp với profiles ID. Lọc ra các gói tin có cùng nội dung (trùng), xảy ra do cơ chế tự động truyền lại của mạng.

Nếu bên gửi yêu cầu 1 gói tin ACK thì APSME chịu trách nhiệm tự động gửi lại gói tin nhằm tăng khả năng gửi thành công, và sẽ thông báo cho bên gửi biết gói tin đã được truyền thành công hay chưa.

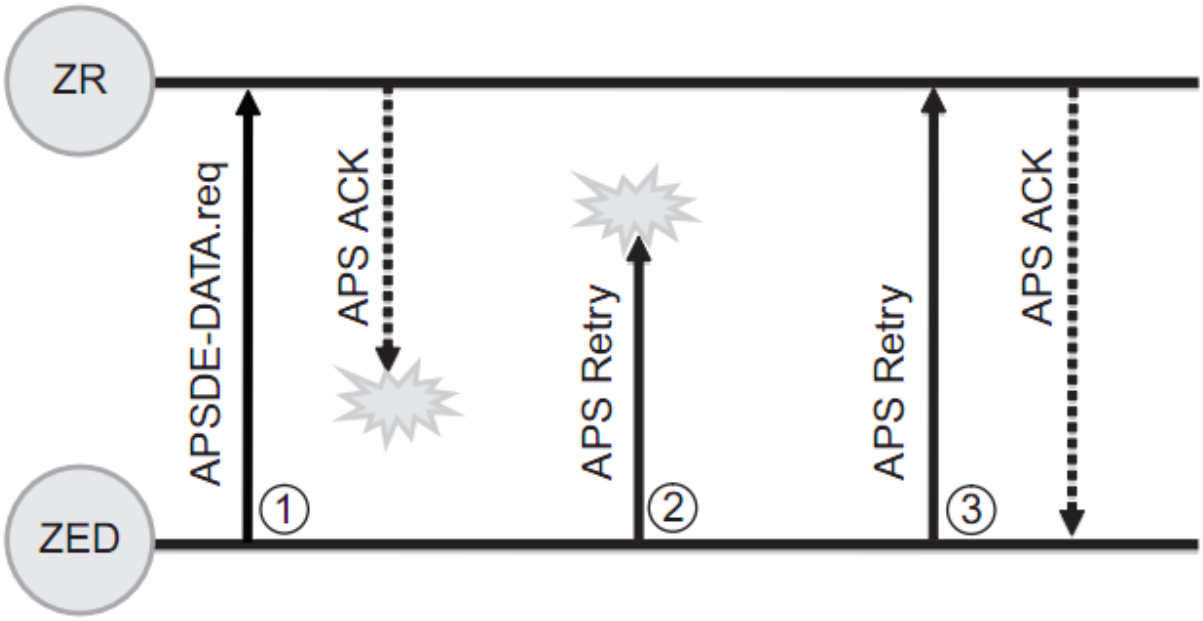
APSME duy trì các bảng của lớp ứng dụng :

- Binding table : tất cả thông tin về việc kết nối từ một endpoint của nút này với endpoint của nút khác.
- Group table : tất cả thông tin về tập hợp các ứng dụng trên một tập hợp các nút.
- Address map : tất cả thông tin về việc dịch địa chỉ MAC 64-bit sang địa chỉ Network 16-bit.

2.3.1 APS ACKs

Lớp MAC cung cấp ACK trên từng nút (giữa 2 nút kề nhau), APS cung cấp ACK end-to-end (giữa bên gửi và bên nhận)

Hình 2.3-1 giải thích thế nào là APS ACK. Giả sử ZED muốn gửi 1 thông điệp cho ZR với tùy chọn có ACK trả về. Khoảng cách giữa chúng là bất kỳ, có thể là hai nút kề nhau, nhưng cũng có thể cách nhau một vài nút. Giả sử thông điệp đã được gửi đến ZR.



Hình 2-8: Cơ chế tự động gửi lại của lớp APS [4]

Nhưng gói APS ACK gửi về cho ZED không thành công, lúc này APS sẽ tự động gửi lại thông điệp đó sau 1 khoảng thời gian (thông thường là 1.5 giây). Chỉ sau khi gửi lại lần 3 thì ASP mới thông báo cho bên gửi biết là việc gửi thông điệp đã thành công.

Tuy nhiên, APS ACK ít khi được sử dụng, vì Zigbee sử dụng đến 3 MAC ACK. Chỉ khi kênh truyền quá kém, hoặc việc liên lạc với nhau quá khó, hoặc đường truyền bị hỏng do 1 số thiết bị ngưng hoạt động hay do môi trường vậy lý thay đổi thì APS ACK mới được sử dụng để đảm bảo thông tin liên lạc.

APS có khả năng nhận biết 1 gói tin có bị trùng hay không để không gửi lên lớp ứng dụng 2 lần. ỞHình 2-8, gói tin chỉ được gửi lên lớp ứng dụng ở lần đầu tiên, các lần sau APS sẽ tự động loại bỏ. Nên khi viết ứng dụng, không cần phải xử lý việc gói tin sẽ bị trùng.

2.3.2 APS Binding

Binding cho phép một endpoint trên một nút kết nối với một hoặc nhiều endpoint trên nút khác (giống như một công tắt, có thể kết nối với một hoặc nhiều bóng đèn). Binding được lưu trên nút cần gửi, bao gồm các thông tin sau :

- Endpoint nguồn.
- Địa chỉ mạng hoặc endpoint hoặc nhóm đích.
- Cluster ID

Bảng 2-2: Zigbee Binding table [3]

Src EP	Destination Addr	Addr/Grp	Dst EP	Cluster ID
5	0x1234	A	12	0x0006
6	0x796F	A	240	0x0006
5	0x9999	G	-	0x0006
5	0x5678	A	44	0x0006

Nếu có nhiều địa chỉ endpoint nguồn trong bảng, thì sẽ gửi cho tất cả các endpoint đích tương ứng. Như trên**Error! Reference source not found.** thì từ endpoint 5 sẽ có 2 gói tin gửi ho endpoint 12, 44 nhóm A và 1 gói tin boardcast cho nhóm G.

Việc lưu trữ bảng binding này không phải là một yêu cầu bắt buộc, vì có thể dùng cơ chế broadcast để xác định địa chỉ đích. Tuy nhiên, việc lưu trữ này sẽ giúp cho các nút trong mạng kết nối với nhau nhanh chóng, dễ dàng và linh hoạt hơn. Do đó, nếu như không gặp vấn đề về bộ nhớ thì việc đưa bảng binding này vào là một sự lựa chọn khôn ngoan.

2.3.3 APS Groups

Groups cung cấp thêm một chỉ dẫn cho việc lọc ra các gói tin không cần thiết. Nếu một endpoint không nằm trong group thì nó sẽ không nhận được thông điệp.

Để một thông điệp được gửi xuống cho endpoint, thì phải trùng cả hai profile ID và group ID. Nếu không, gói tin sẽ bị loại bỏ.

2.3.4 Address Map

Lớp APS có chứa một bảng gọi là bảng dịch địa chỉ, bảng này chứa địa chỉ Network 16-bit và địa chỉ MAC 64-bit tương ứng với nó (xem Hình 2-9).

NwkAddr	IEEE Addr
0x0000	0x0050c237b0040102
0x0001	0x0050c237b0045ae3
0x796f	0x0050c237b004c290

Hình 2-9: APS Address map [3]

Một vài lệnh trong Zigbee chỉ dùng địa chỉ MAC, nhưng Zigbee cần địa chỉ 16-bit để trao đổi thông tin, vì vậy cần một cách thức để chuyển đổi hai địa chỉ này. Khi một thiết bị trong mạng thay đổi chịa chỉ 16-bit, thiết bị đó sẽ thông báo bằng lệnh Device Announce. Khi đó, các nút sẽ cập nhật lại bảng này và bảng binding.

2.3.5 AES-128 bit Security

Bảo mật của Zigbee được xây dựng dựa trên chuẩn mã hóa AES 128-bit, một giải thuật mã hóa khối được công bố bởi National Institue of Standards and Technology.

Zigbee hiện thực cả mã hóa và xác thực gói tin :

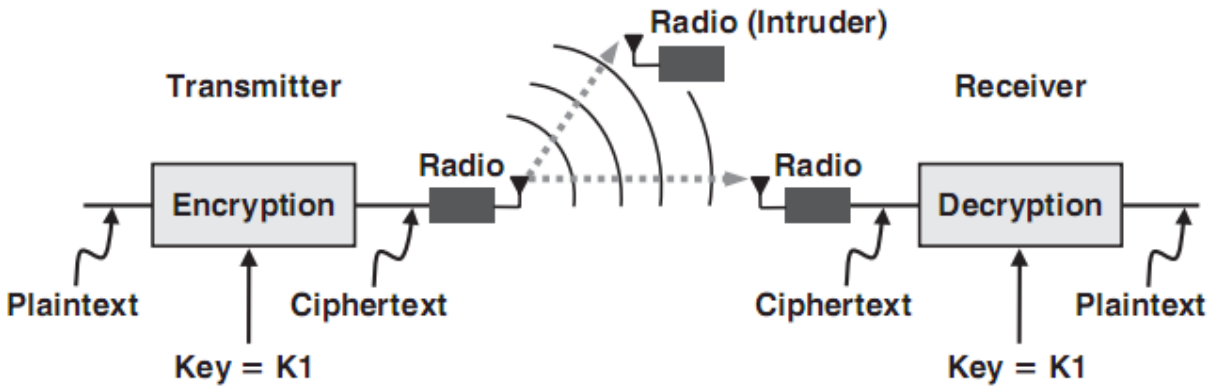
- Zigbee mã hóa nội dung của gói tin, cluster, profile và endpoint được sử dụng. Cho dù cho kẻ trộm có lấy cắp được gói tin thì cũng không thể hiểu được nội dung của nó.
- Zigbee xác thực toàn bộ frame, để ngăn chặn replay attack, thay đổi frame từ bất kỳ nút mạng nào.

Mã hóa trong mạng Zigbee

Đối với AES, mỗi giải thuật mã hóa đều có liên quan đến một khóa (key), giải thuật được công bố cho tất cả mọi người biết nhưng giá trị của khóa được giữ bí mật. Khóa là một dãy các số nhị phân. Có rất nhiều cách để đưa khóa này vào sử dụng : nhúng vào trong thiết bị, lấy từ thiết bị được chỉ định khi tham gia vào mạng…

Có hai khóa được sử dụng trong suốt quá trình giao tiếp giữa các thiết bị : link key và network key. Link key được chia sẻ giữa hai thiết bị, và được dùng trong trường hợp unicast. Network key được chia sẻ cho toàn mạng, dùng trong trường hợp broadcast. Trong mạng Zigbee, có một thiết bị được chọn để phân phối link key và network key cho các thiết bị khác, thiết bị đó gọi là trust center. Chỉ có duy nhất một trust center trong mạng. ZC sẽ gán địa chỉ cho trust center trong mạng.

Zigbee sử dụng khóa có chiều dài 128-bit, có nghĩa là có 2^{128} (tương đương $3.4x10^{38}$) khóa. Do đó kẻ đột nhập cần phải thử đến gần $3.4x10^{38}$ lần mới có thể đọc được nội dung của thông điệp. ỞHình 2-10, người nhận dùng một khóa giống như của người gửi để giải mã thông điệp, nên được gọi là phương pháp khóa đối xứng.



Hình 2-10: Mã hóa dùng khóa đối xứng trong mạng Zigbee [4]

Có 3 cách để một thiết bị trong mạng lấy được link key :

- Preinstallation : nhà sản xuất nhúng khóa vào bản thân thiết bị.
- Key transport : thiết bị sẽ hỏi trust center. Yêu cầu khóa sẽ được gửi tới trust center dùng APS command. Trust center sẽ gửi khóa tới thiết bị yêu cầu. Tuy nhiên, phương pháp này vẫn chưa được an toàn vì kẻ xâm nhập có thể tìm cách lấy trôm khóa từ trust center. Giải pháp đề xuất là dùng thêm một khóa để mã hóa khóa gửi từ trust center.
- Key establishment : tạo một khóa ngẫu nhiên giữa hai thiết bị mà không cần phải liên lạc với nhau. Phương pháp này dựa trên giao thức Symmetric-Key Key Establishment (SKKE). Các thiết bị tạo khóa đều có chung một khóa, gọi là khóa chính (master key). Khóa chính này có thể tạo bởi hai phương pháp trên hay cũng có thể do người dùng nhập vào. Trong giao thức SKKE, có hai thiết bị, một thiết bị gọi là người khởi xướng (initiator) và một thiết bị gọi là người đáp ứng (responder). Initiator tạo một link key dựa trên master key và truyền nó cho responder. Responder sử dụng dữ liệu đó để tạo ra một link key khác. Initiator cũng tạo ra một link key từ dữ liệu đó. Nếu quá trình tạo khóa hoạt động chính xác thì lúc này hai thiết bị sẽ có cùng một link key có thể sử dụng để mã hóa và giải mã dữ liệu.

Xác thực trong mạng Zigbee

Ziggbee hỗ trợ hai dạng xác thực là xác thực thiết bị và xác thực dữ liệu. Xác thực thiết bị là hoạt động xác nhận một thiết bị mới được quyền tham gia vào mạng. Đối với xác thực dữ liệu, người nhận kiểm tra xem dữ liệu có bị thay đổi trên đường truyền hay không.

Xác thực thiết bị được thực hiện bởi trust center. Khi một thiết bị mới tham gia vào mạng, nó sẽ có trạng thái là "joined but unauthenticated". Nếu thiết bị không được trust center xác thực là an toàn, nó sẽ bị yêu cầu thiết bị rời khỏi mạng ngay lập tức. Có 2 chế độ xác thực trong Zigbee :

- Chế độ Residential : nếu một thiết bị mới gia nhập mạng không có network key, thiết bị đó sẽ được trust center gửi network key (không được bảo vệ). Nếu thiết bị

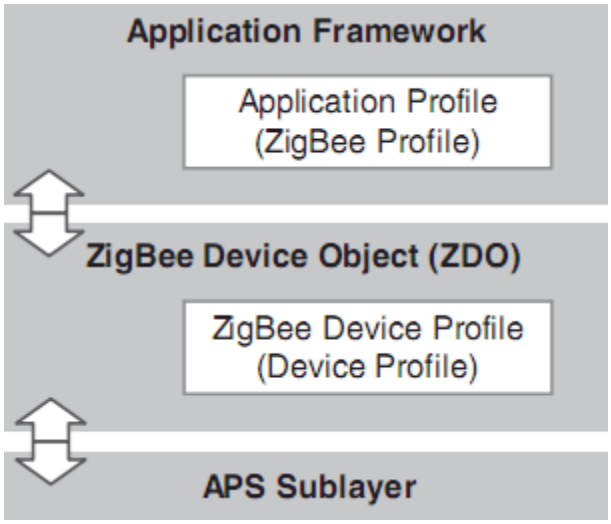
đã có network key, nó sẽ đợi trust center gửi network key (tất cả khóa đều bằng 0) và thiết bị lúc này được xem như là đã được xác thực.

- Chế độ Commercial : trust center không bao giờ gửi network key, mà thay vào đó sẽ gửi master key. Sau khi thiết bị mới nhận được master key, trust center và thiết bị sẽ bắt đầu giao thức tạo khóa "key establishment". Nếu thiết bị tạo đúng link key trong khoảng thời gian xác định, thiết bị sẽ nhận được network key từ trust center. Nếu không tạo được link key trong thời gian xác định, thiết bị sẽ được yêu cầu rời khỏi mạng.

Xác thực dữ liệu đảm bảo dữ liệu không bị thay đổi trong quá trình truyền. Để làm được điều này, bên truyền sẽ chèn vào frame một đoạn mã đặc biệt gọi là Message Integrity Code (MIC).MIC được tạo bởi một phương thức mà cả bên gửi và nhận đều biết. Bên nhận sẽ lặp lại quá trình tạo MIC và so sánh MIC đó với MIC nhận được. Nếu cả 2 MIC trùng nhau, dữ liệu được xem là an toàn. Khả năng an toàn của việc xác thực này tăng lên khi độ dài của MIC tăng lên (tăng số bit). Chuẩn Zigbee và IEEE 802.15.4 hỗ trợ 32-bit, 64-bit và 128-bit MIC

2.4 Zigbee Device Object (ZDO)

ZDO là một giao diện giữa APS và Application Framework. ZDO chịu trách nhiệm cài đặt APS, Network và Security Service Provider (SSP). Có một số profile được định nghĩa trước dành cho ZDO và gọi là ZigBee Device Profile (ZDP). ZDP chứa mô tả về thiết bị (device dscritor), cluster, khả năng hỗ trợ của thiết bị. ZDP chỉ có duy nhất một device descriptor.



Hình 2-11: Vị trí của ZDO [4]

ZDP hỗ trợ các dịch vụ như khám phá thiết bị (device discovery), khám phá dịch vụ (service discovery)…

- Device discovery : xác định xem có những thiết bị nào khác trong mạng.
- Service discovery : yêu cầu các thiết bị khác trong mạng cung cấp thông tin về profile, descriptor, các cluster in và cluster out.

2.4.1 Device Descriptor

Zigbee dùng descriptor để mô tả một nút mạng và thuộc tính của nút đó, cho phép các ứng dụng khác trong mạng có thể biết được thuộc tính này khi cần. Một descriptor đầy đủ bao gồm :

- Node descriptor : bao gồm rất nhiều trường khác nhau như loại thiết bị (ZC, ZR hay ZED), mã nhà sản xuất, có dùng complex descriptors, user descriptor hay không, có hỗ trợ phân mảnh hay không…
- Power descriptor : chế độ năng lượng đang sử dụng.
- Complex descriptor : tên nhà sản xuất, số serial, tên model…
- User descriptor : một chuỗi xác định địa điểm (phòng khách, phòng làm việc…) do người dùng định nghĩa

2.4.2 Service Discovery và Matching Endpoint

Khám phá endpoint mà ứng dụng sử dụng và dịch vụ mà nó hỗ trợ là hoạt động cơ bản của một thiết bị mạng Zigbee. Những nhà sản xuất khác nhau dùng endpoint khác nhau cho ứng dụng của họ.

ZDP có thể xác định những endpoint đang hoạt động thông qua Active_EP_req. Ứng dụng sẽ trả về thông tin của một endpoint đang hoạt động.Match_Desc_req có thể được sử dụng để tìm một dịch vụ nào đó trong mạng. Kết quả trả về sẽ là một danh sách các endpoint phù hợp từ một nút bất kì nào đó. Cần phải giống nhau về cả profile ID và có ít nhất mội input cluster phù hợp với một output cluster hoặc ngược lại, thì một dịch vụ được xem là tồn tại. Match_Desc_req có thể được gửi theo broadcast hay unicast.

2.4.3 Low Power

Một đặc trưng của Zigbee là một nút có khả năng hoạt động trong nhiều năm chỉ với nguồn cung cấp từ pin (từ 5 đến 7 năm đối với 2 cục pin AA). Các ZED, để tiết kiệm năng lượng sẽ rơi vào trạng thái sleep nếu không có dữ liệu cần xử lý. Tuy nhiên, ZC và ZR không được rơi vào trạng thái sleep và phải được cung cấp nguồn xuyên suốt.

ZED có thể vào trạng thái sleep vì nó không định tuyến. Đó là lý do nó được gọi là end device. Nếu gửi một gói tin đến ZED (child) khi nó đang ở trạng thái sleep thì parent (ZR hay ZC) sẽ lưu lại gói tin đó và truyền lại khi child thoát khỏi trạng thái sleep. Quan hệ parent-child sẽ được nói rõ hơn trong phần Network Layer. Tuy nhiên, gói tin không được lưu lại mãi mãi, mà chỉ tồn tại trong khoảng thời gian mặc định là 7 giây (có thể điều chỉnh được) . Nếu một parent mà có nhiều child đang ở trạng thái ngủ, và có quá nhiều thông điệp cần gửi đi, thì một số thông điệp có thể không được lưu lại/bị xóa trước khi nó được gửi đi.

Về tổng quan, một thiết bị khi rơi vào trạng thái sleep, nên thoát khỏi trạng thái đó và giao tiếp định kỳ với các nút xung quanh. Hoặc nên cấu hình cho thiết bị đó như một thiết bị truyền dữ liệu : chỉ thoát khỏi trạng thái sleep khi cần, truyền data và sau đó đi vào trạng thái sleep.

2.5 Network Layer

2.5.1 ZigBee và IEEE 802.15.4

Nhìn chung, cái tên "ZigBee" và 802.15.4 thường được dùng qua lại lẫn nhau nhưng nó không giống nhau. Về đặc tả 802.15.4 được tạo và hỗ trợ bởi IEEE. Đặc tả này định nghĩ các lớp vật lý và MAC cho một mạng không dây, cá nhân, low-power.

IEEE 802.15.4 định nghĩa:

- Các cơ chế cho việc tìm mạng
- Các cơ chế cho việc thiết lập và kết nối vào mạng
- Các các cơ chế cho thay đổi kênh truyền
- Các cơ chế việc phát hiện vật cản và nhiễu trên một kênh
- Phương pháp phấn phối data-packet, single-hop, ACK, việc dung CSMA-CA để tránh đụng độ
- Phương pháp data-broadcast, single-hop, không có ACK

IEEE 802.15.4 không định nghĩa về truyền thông multi-hop, gán địa chỉ, hay khả năng tương tác với mức ứng dụng.Nếu mạng xây dựng chỉ với một hop, thì 802.15.4 MAC/PHY có thể làm tất cả những gì cần. Các nhà cung cấp hỗ trợ một môi trường ứng dụng 802.15.4 mà không yêu cầu ZigBee.

Ngoài ZigBee, các nhiều protocol network hoàn toàn được xây dựng trên tiêu chuẩn 802.15.4, một số là dạng mesh hay multi-hop, một số là single-hop hay mạng star.Nhưng ZigBee là giao thức chính mà được xây dựng trên tiêu chuẩn 802.15.4, thêm vào đó là một lớp mạng có khả năng tạo mạng mesh, peer-to-peer, multi-hop; một lớp bảo mật có khả năng xử lý các trường hợp bảo mật phức tạp, và một lớp ứng dụng cho các profile ứng dụng có thể tương thích với nhau.

Trong sơ đồ kiến trúc ZigBee chuẩn, các lớp MAC và PHY thể hiện dưới IEEE, trong khi phần còn lại thể hiện dưới ZigBee.

Công việc của lớp MAC là chuyển các packet từ chuỗi byte thành phổ RF và ngược lại. Lớp MAC cho phép một mạng được thiết lập, các kênh được chia sẽ, và dữ liệu được truyền trong một hop đơn (single-hop) trong một cách thức tinh cậy, hợp lý.

ZigBee đặc tả tất cả các lớp trên MAC và PHY, gồm NWK, APS, ZDO và các lớp bảo mật. ZigBee cung cấp mạng mesh và các khả năng multi-hop, tang cường khả năng tin cậy của phân phối packet dữ liệu, và đặc tả tương thích giữa các ứng dụng.

ZigBee không dung tất cả sự đặc tả 802.15.4 MAC/PHY; chỉ một phần nhỏ. Điều này cho phép các nhà cung cấp stack có các giải pháp nhỏ hơn (dùng ít RAM và flash) bằng cách cung cấp một lớp MAC giới hạn cho ZigBee stack của họ. Ví dụ, ZigBee không dùng các phương pháp 802.15.4 beaconing, hay khe thời gian được đảm bảo. ZigBee là bất đồng bộ. Bất kỳ node nào có thể truyền tại bất cứ lúc nào. Chỉ dùng CSMA-CA, một cơ chế mức MAC, để ngăn các node khỏi truyền đè lên nhau.

ZigBee cũng có một số điều chỉnh trong chuẩn 802.15.4. Một trong số đó là mô hình bảo mật. MAC định nghĩa một thứ gọi mà CCM, được viết tắt từ "Counter-mode Cipher-block chaining-Message authentication code". CCM yêu cầu bảo mật khác nhau cho mỗi lớp. Do ràng buộc hiệu suất trên các vi xử lý nhỏ, ZigBee không làm vậy. Mô hình bảo mật ZigBee cũng được gọi là CCM (một điều chỉnh nhỏ của bảo mật MAC CCM).

Một trong các phần thú vị hơn mà ở đó ZigBee khác với sự đặc tả 802.15.4 là time-out cho các beacon response. Với cách này, các beacon request và các beacon response không làm gì khi network là một beaconing network hay không (tham khảo [1]).

Một beacon đơn giản là một packet chứa thông tin về node và network. Được dùng trong ZigBee để tìm các network. Trong các mạng với hơn 30 nodes trong cùng vùng phủ sóng, các timeout 802.15.4 mặc định cho các phản hồi các beacon request không cho phép đủ thời gian cho tất cả các node phản hồi. Đặc tả 802.15.4 đã không được xây dựng với các mạng lớn, nhưng ZigBee thì có thể.

Đặc tả 802.15.4 MAC hoàn toàn ổn định từ tháng 11 năm 2003. Một số nhà cung cấp chip thậm chí cung cấp 802.15.4 MAC trong ROM. Nhưng IEEE vẫn chưa dừng tại đó. Năm 2006, IEEE ra một đặc tả 802.15.4 khác được gọi là 802.15.4-2006.

Thay đổi lớn nhất trong IEEE 802.15.4-2006 là một PHY tốt hơn cho các radio dưới 1GHz. Trong đặc tả 802.15.4-2003, 868MHz và 900 MHz bị giới hạn 20kbps và 40kbps. Tốc độ truyền dữ liệu tại tần số dưới 1GHz quá chậm cho ZigBee; radio cho ZigBee là 2.4GHz, hoạt động với 250kbps. IEEE 802.15.4-2006 đã thay đổi tất cả. Đặc tả này đã thêm 2 PHY tùy chọn mới cho tần số dưới 1GHz cho phép truyền lên tới 250kbps.

2.5.2 Thiết lập, tham gia và tái tham gia trong mạng ZigBee.

Trước khi bất kì các node ZigBee có thể giao tiếp trên một mạng, nó phải thiết lập một mạng mới hay kết nối vào một mạng đang tồn tại. Chỉ ZigBee Coordinator có thể thiết lập một mạng. Chỉ ZigBee Routers và ZigBee End-Devices có thể kết nối vào mạng. Nhiều nhà cung cấp stack cung cấp khả năng để một node được chỉ định như một ZC, ZRm ZED tại lúc biên dịch (tiết kiệm code và RAM) hay tại lúc chạy (giảm các phần OEM-manufactured)

Mỗi node bắt đầu với một địa chỉ 64-bit IEEE (MAC), được gán bởi OEM trong sản xuất. Trong quá trình kết nối mạng, mỗi node được gán một địa chỉ 16-bit short duy nhất (NwkAddr) để dùng khi giao tiếp với các node khác qua mạng. Địa chỉ 16-bit thường dùng cho các giao tiếp gần, để giảm overhead trong over-the-air protocol.

Quá trình thiết lập mạng

ZigBee Coordinator thiết lập mạng. Quá trình thiết lập một mạng là xác định một định danh duy nhất cho mạng, được gọi là PAN ID, và chọn một trong 16 kênh 802.15.4 (11-16) để điều hành mạng. Trong suốt quá trình thiết lập mạng, một gói đơn được gửi over-the-air trên mỗi kênh: một MAC active scan (hay beacon request).

Một ZigBee Coordinator có nhiệm vụ sau:

- Thiết lập mạng

- Thiết lập kênh 802.15.4 trên mạng sẽ hoạt động
- Thiết lập extended và short PAN ID cho mạng
- Quyết định stack profile để dùng
- Hoạt động như Trust Center cho các ứng dụng bảo mật và mạng
- Hoạt động như người đứng giữa cho việc End-Device-Bind
- Hoạt động như một router trong mesh routing
- Hoạt động như là gốc của tree, nếu tree routing được sử dụng

ZigBee Coordinator thực sự chỉ là một router nếu network không được ủy thác. Và có nhiều cách để thay thế ZigBee Coordinator sau khi một network chạy nếu thiết bị ZC trục trặc do một số nguyên nhân.

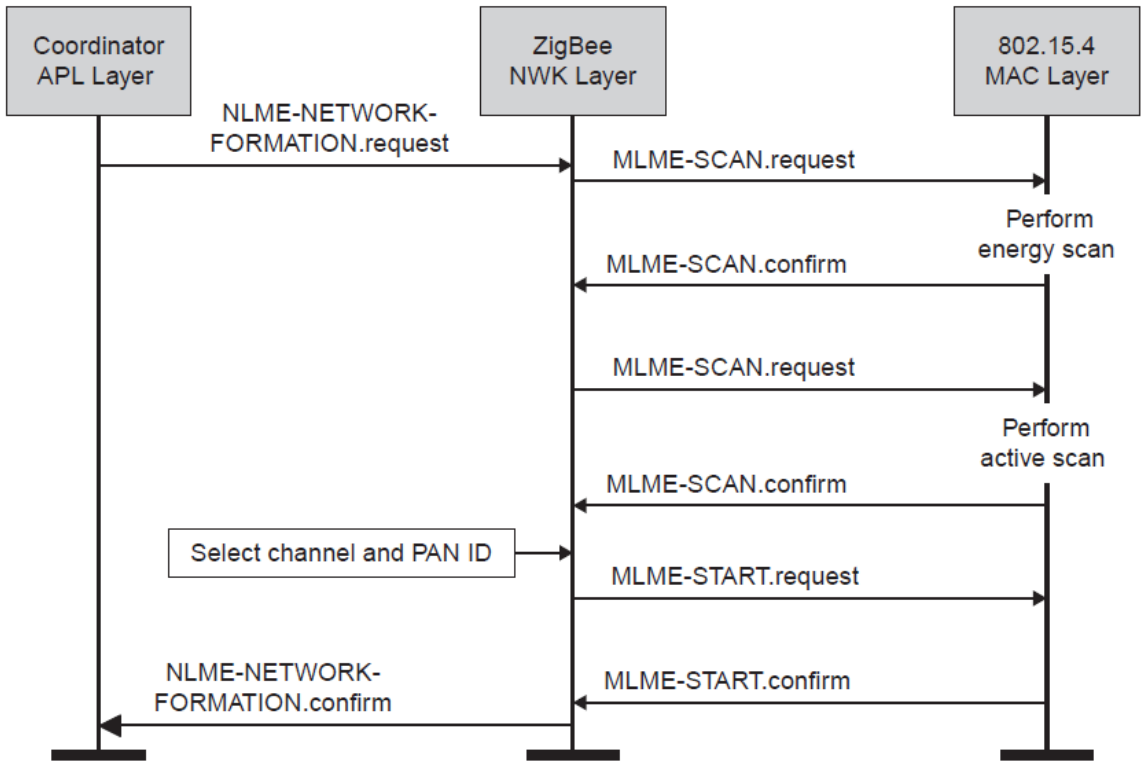
Ứng dụng chạy trên một node ZigBee Coordinator thực sự quyết định khi nào để thiết lập một network, từ một tập các kênh và từ tập các PAN ID. Ứng dụng trên ZC có thể là bất cứ thứ gì: một gateway được kết nối với Internet, một hộp điều khiển, một bộ ổn nhiệt, đèn, hay công tơ điện. Khi năng lượng được cấp đến thiết bị mà chứa ZigBee Coordinator, nó có thể tức khắc hình thành một network, hay có thể đợi một vài sự kiện trước khi tạo mạng. Nó thậm chí kiểm tra để xem những mạng nào sẵn sang ở đó, và quyết định trở thành ZigBee Router hơn là một Coordinator, nếu một node khác đã hoàn toàn tạo mạng mong muốn. Tuy nhiên ứng dụng đã được lập trình, một ZigBee Coordinator sẽ tạo một mạng.

NLME-NETWORK-FORMATION.request được khởi tạo bởi ZDO để tạo một mạng bởi ứng dụng. Trong Z-stack:

NLME_NetworkFormationRequest();

Tiếp theo ZigBee gọi lớp MAC để thể hiện hai scan: energy scan và active scan. Energy scan được dùng để xác định kênh nào là kênh yên tĩnh nhất từ tập các kênh được cụ thể trong biến thông tin cơ bản APS, apsChannelMask. Energy scan mất 0.5 giây cho mỗi kênh và chỉ là một kiểm tra “moment-in-time”. Kênh có thể thực sự nhiễu trong 1 giờ trước đó và quá trình này không phát hiện ra điều này. Việc quét tất cả 16 kênh mất khoảng 8 giây.

Tiếp theo là active scan, đơn giản một MAC beacon request được trả về không hoặc hơn các beacon response, được dùng để tìm mạng khác trong vùng. Active scan đảm bảo ZigBee không tạo một mạng có cùng PAN ID. Active scan có thể mất thời gian.



Hình 2-12: Quá trình ZigBee tạo mạng [3]

Quá trình tham gia mạng

ZigBee Router và ZigBee End-Device tham gia mạng. ZigBee Router thường được cấp nguồn chính, luôn bật, lắng nghe các packet để tìm đường. ZED thường dùng nguồn Pin và sleeping, chỉ waking up để giao tiếp một cách ngắn trước khi trở về sleep.

ZigBee Router có nhiệm vụ:

- Tìm và tham gia mạng
- Duy trì các broadcast thông qua mạng
- Tham gia việc tìm đường, gồm khám phá và duy trì đường đi
- Cho phép các thiết bị khác tham gia mạng
- Lưu các packet thay cho các children đang sleep

ZigBee End-Device có nhiệm vụ:

- Tìm và tham gia mạng
- Polling parent của nó để xem có bất kỳ các messages đã được gửi tới chúng khi chúng sleep hay không
- Tìm một parent mới nếu kết nối tới parent cũ bị mất (NWK rejoin)
- Sleep hầu hết thời gian để tiết kiệm Pin

Việc tham gia mạng là một quá trình của tìm mạng và node nào trong vùng và sau đó chọn một trong chúng để tham gia. Sự kết hợp được cung cấp có thể chấp nhận bởi network, việc tham gia hoàn thành và node tham gia sẽ có 1 địa chỉ trên mạng.

Quá trình tham gia sử dụng beacon request. Bất kì ZCs và ZRs trong vùng trả lời bằng beacon response. Các ZCs và ZRs có cùng kênh với node muốn tham gia, và không phân biệt PAN ID.

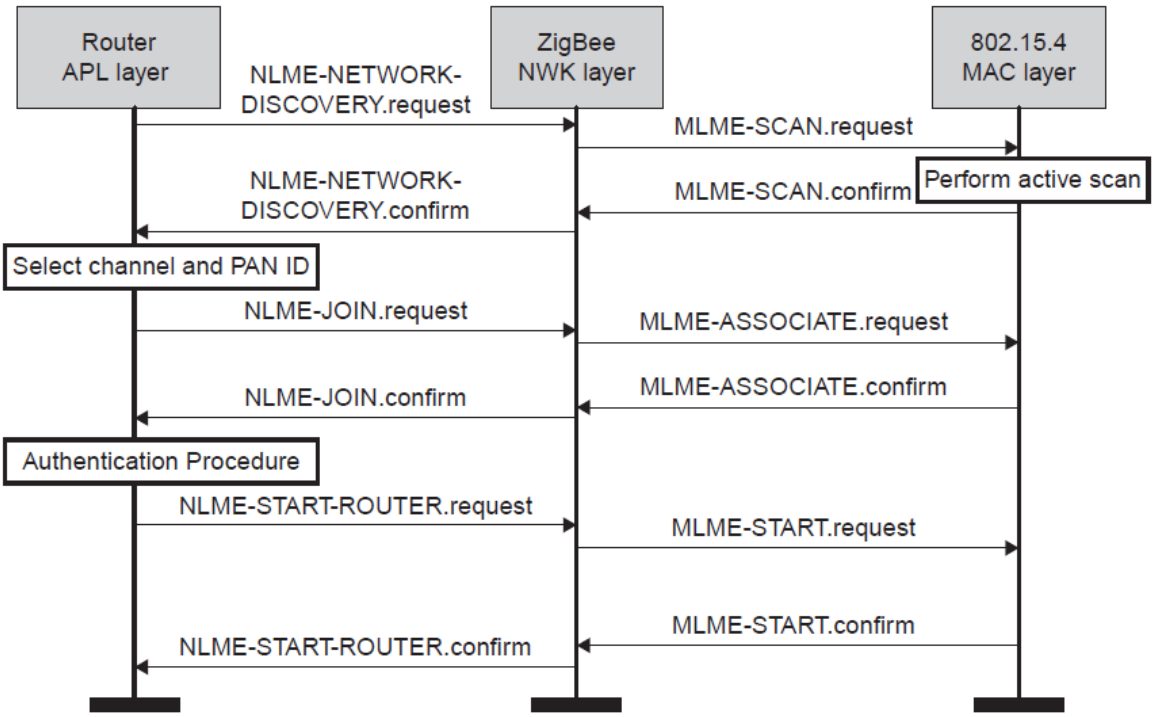
Các beacon response chứa khá nhiều thông tin về mạng ZigBee, gồm PAN ID, extended PAN ID, sự cho phép tham gia và node có đủ khả năng cho router hay end-device để tham gia hay không. Những gì beacon thiếu là thông tin về mức ứng dụng (application). Cho điều này, một node đang tìm kiếm đầu tiên phải tham gia mạng, tìm kiếm ứng dụng phù hợp, nếu không thấy thì rời mạng và thử các mạng khác.

ZR và ZED tham gia một node cụ thể, không phải một mạng, dùng 64-bit MAC cho địa chỉ đích và nguồn của MAC association request. Node thực hiện việc tham gia được gọi là child. Node nhận association request được gọi là parent.

ZR và ZC có thể là parent của node khác nhưng ZED luôn là child. Mối quan hệ parent/child không là gì trong mạng kiểu mesh. Bất kì các routers nào cũng có thể tìm đường qua bất kì router khác trong vùng nghe trên cùng mạng. Tất cả các routers là ngang hang. Nếu một parent hay child của router ra khỏi vùng nghe (thậm chí rời mạng) không tác động tới các đường đi, đường đi khác sẽ tới các thiết bị cụ thể này. ZigBee Router không tìm đường thông qua các mạng khác, chỉ trong cùng PAN ID và kênh.

Tuy nhiên, đối với ZEDs, mối quan hệ parent/child rất đặc biệt. ZEDs trong khi chúng có thể giao tiếp với các node khác trong mạng, chúng chỉ giao tiếp trực tiếp với parent. Hop kế tiếp của ZED luôn là parent của nó. Nếu một ZED mất kết nối với parent, nó phải tìm parent khác để giữ liên lạc với mạng, được gọi là tham gia lai (rejoin).

Không thường xuyên ZED mất liên lạc với parent. Sự giao tiếp 2.4GHz bị ảnh hưởng bởi nước và lien kết bị mất. Trong vài giây, ZED sẽ tìm parent mới, thông báo đến mạng rằng nó hoàn toàn di chuyển và các giao tiếp tiếp tục.



Hình 2-13: Quá trình ZigBee tham gia mạng [3]

Quá trình tham gia của ZR và ZED được mô tả trong đặc tả ZigBee. Đầu tiên một active scan (beacon request) gửi ra trên mỗi kênh. ZC hoặc ZED chờ một thời gian cho beacon response. Thời gian được cài bởi ứng dụng, nhưng mặc định là 0.5 giây trên kênh. Khi các beacon được thu thập, chúng được phân tích kênh và PAN ID. Ngoài ra còn có permit-join để ngăn các node tham gia vào và cũng có thể được dùng để bắt buộc các node có một parent cụ thể.

Sau khi active scan hoàn thành và một parent phù hợp được chọn, quá trình xác thực bắt đầu. Chú ý rằng node có một địa chỉ trên mạng trước thời gian xác thực bắt đầu. Sự xác thực chỉ có ở mạng bảo mật, và đưa trust center quyền từ chối/cho phép node tham gia. Một node giả mạo mà chỉ giả mạo một địa chỉ trên PAN sẽ không nhận key mạng và nên không thể giao tiếp với các node khác. Nếu xác thực không hoàn thành thành công, parent sẽ thông báo với child chưa được xác thực rời và đánh dấu địa chỉ đó có thể dùng bởi node khác muốn tham gia.

Khi một node hoàn toàn tham gia một mạng, nó có thể giao tiếp với bất kì node khác trong toàn bộ mạng. Không có yêu cầu cho việc binding hoặc các cơ chế khác. Đơn giản gửi dữ liệu từ node này đến node khác, miễn là biết địa chỉ short của node đó. Tất nhiên, ứng dụng muốn thấy packet thì Application Profile phải giống nhau ở hai phía và endpoint nguồn trên node gửi và endpoint đích trên node nhận phải được đăng kí vơi ZDO.

Quá trình tái tham gia mạng

Việc tái tham gia giả sử node sẵn sang tham gia mạng, có một PAN ID, extended PAN ID, security key, và short address. Có nhiều nguyên nhân một node cần phải tái tham gia mạng:

- Một ZED mất lien lạc với parent của nó
- Năng lượng bị thay thế và nhiều hay tất cả các node trong mạng tái tham gia « silently«
- Tham gia một mạng bảo mật nếu permit-joining tắt.

ZED luôn giao tiếp trực tiếp với parent của nó. Nếu parent không trả lời, child phải tìm parent mới để giữ giao tiếp trên mạng. Child tự quyết khi nào nó mất parent. ZigBee không cụ thể số lần poll hay message trước khi ZED cho rằng nó không thể giao tiếp với parent; ứng dụng quyết định.

Quá trình tái tham gia bắt đầu với một beacon request để tìm parent phù hợp. Nó không lien quan tới node parent tiềm năng có thể có permit-joining hay không. Chỉ một thứ là chúng có khả năng chứa thiết bị hay không. Sauk hi beacon request, ZED lấy một node (cùng PAN) làm parent, thực hiện tái tham gia, nhận một short address mới (chỉ trong stack profile 0x01), và cuối cùng phát một device-annouce để nói cho mạng rằng node hoàn toàn di chuyển. Bước cuối rất quan trọng để bảo vệ binding trong mạng.

Một loại khác của việc tái tham gia là "silent rejoin". Silent rejoin không được đặc tả trong ZigBee, nhưng tất cả các nhà cung cấp stack có vì nó cần thiết trong một mạng hiện thực với bất kì kích thước nào. Ví dụ, tưởng tượng rằng năng lượng bị tái cung cấp đến tất cả các router trong một mạng 1000 node. Khi năng lượng có trở lại, nếu tất cả các node đều cố gắng tham gia (tái tham gia) mạng cùng một lúc, mạng sẽ thất bại : đơn giản quá nhiều lưu lượng trong mạng. Nhưng khi các routers biết thông tin mạng của nó (PAN ID, extended PAN ID, NwkAddr, security key), chúng đơn giản bắt đầu một cách thầm lặng, không nói bất cứ gì. Các node ZigBee không cần nói chuyện để duy trì trạng thái mạng. Khi mất điện có thể xem như mạng không nói chuyện trong một lúc. Khi điện có trở lại, mỗi router nhận chế độ trên PAN ID, extended PAN ID, NwkAddr, security key chính xác như thể mạng không bao giờ tắt. Điều này gọi là "silent rejion "

Silent Rejion cũng được dùng khi mạng chuyển đến kênh mới, một đặc tính mới trong ZigBee 2007 và Pro. Silent rejoin chỉ làm việc nếu các node có một vài loại lưu trữ vĩnh viễn (non-volatile memory).

Một cách dùng khác của tái tham gia là dùng NWK-Rejoin để tham gia một mạng mà có permit-joining tắt. Điều này thình thoảng được dùng nếu quá trình ủy nhiệm có network key, PAN ID,… sẵn sàng lập trình trong node. Quá trình NWK-Rejoin sẽ đưa thiết bị đó và địa chỉ trên mạng, và ZDP : DeviceAnnce sẽ cho phép tất cả các node trong mạng biết nó hoàn toàn tham gia.

2.5.3 Gán địa chỉ ZigBee

Định địa chỉ là quan trọng trong một mạng. Địa chỉ mỗi node phải duy nhất trong ZigBee. ZigBee dùng hai địa chỉ duy nhất trên một node : long address (IEEE hay MAC address) và short address (NwkAddr).Long address (64-bit), cũng được gọi là IEEE hay MAC address, được gán bởi nhà sản xuất thiết bị dùng 802.15.4 radio (không phải nhà sản xuất chip), và không thay đổi trong đời thiết bị. Long address định nghĩa một cách duy nhất thiết bị với tất cả các thiết bị khác trên thế giới.Short address (16-bit) được gán tới một node tại thời điểm node tham gia mạng.

Chú ý rằng cả MAC layer header và NWK layer header có cả một địa chỉ nguồn và một địa chỉ đích. Nếu địa chỉ MAC 8-byte được dùng, thì sẽ dùng tới 32 byte của 127byte over-the-air packet. Do đó, ZigBee dùng một địa chỉ mạng 2-byte, giảm các trường này đến 8 bytes, cho phép hơn 24 bytes cho ứng dụng dùng.

Tại sao phải dùng các trường địa chỉ này trong cả MAC header và NWK header? Nếu việc gửi packet từ node "A" đến node "Z", hop đầu tiên từ "A" tới "B", hop tiếp theo từ "B" tới "C", … cho đến hop cuối cùng từ "Y" tới "Z". NwkSrc và NwkDst luôn chỉ từ "A" tới "Z", trong khi MacSrc và MacDst là địa chỉ tại mỗi hop.

Khi nói về việc gán địa chỉ ZigBee, thì là liên quan tới địa chỉ short address. Short address được mạng ZigBee gán tại thời điểm một node tham gia mạng hoặc thiết lập mạng, và không liên quan tới IEEE address. ZigBee dùng hai mô hình để gán short address:

- Cskip
- Stochastic (random)

Gán địa chỉ Stochastic, một node tham gia vào một mạng chọn riêng cho mình một địa chỉ. Sau đó nó gửi một thông báo broadcast đến mạng để xem có node nào khác có địa chỉ đó hay không. Nếu có, node chọn một địa chỉ khác. Nếu không node giữ địa chỉ đó. Việc định địa chỉ theo tochastic có trong stack profile 0x02 (còn được gọi là ZigBee Pro).

Trong stack profile 0x01, các địa chỉ được gán với một mối quan hệ parent-child tạo một tree đối xứng. Mô hình gán địa chỉ trong stack profile 0x01 dùng một số được tính toán cho mỗi "depth" (số hop từ ZC), được gọi là Cskip (Child skip).

Trong Cskip, ZC là node 0 (0x0000). Node tiếp theo tham gia mạng sẽ nhận một địa chỉ từ node parent. Địa chỉ mà node này được gán phụ thuộc vào child là một router, mà có thể có các children của riêng nó hay một thiết bị, mà không có child.

Bảng 2-3: Cskip được tính toán cho stack profile 0x01[3]

Cskip level 0	0×143d
Cskip level 1	0×035d
Cskip level 2	0×008d
Cskip level 3	0×0015
Cskip level 4	0×0001
Cskip level 5	0×0000

maxDepth	5
maxChildren	20
maxRouters	6

Cskip dùng ba thông số để xác định việc địa chỉ : maxDepth, maxChildren và maxRouter. Việc dùng các thông số này, Cskip có thể xác định một cách toán học những địa chỉ child mới

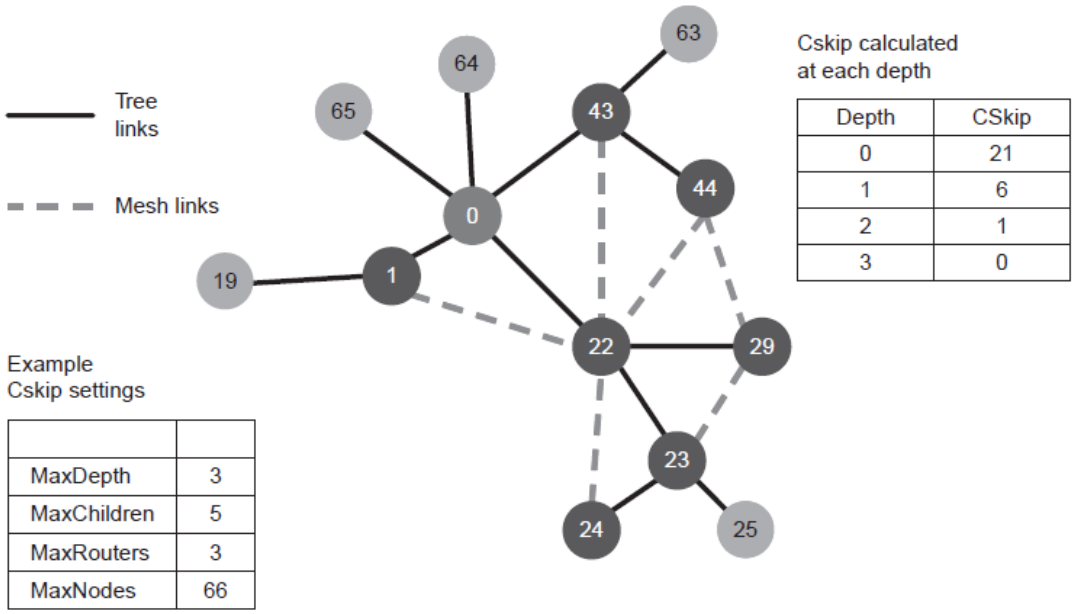
tham gia, và như thế nào để tìm đường một packet theo tree đối xứng. Stack profile 0x01 dùng giá trị maxDepth(5), maxChildren(20), và maxRouter(6), mà giới hạn tổng số node trong mạng tới 31,101 nodes.

Khái niệm cơ bản là : Tree chia thành " level", level 0 là ZC, level 1 là children của nó, level 2 là children của children của nó … Router đầu tiên tham gia mạng ZC nhận địa chỉ 0x0001. Router tiếp theo tham gia ZC nhận địa chỉ (0x0001 + Cskip tại level đó), như vậy là 0x143e, bởi vì Cskip tại level 0 là 0x143d. Số này, 0x143d, đủ lớn cho router này và tất cả các children và grandchildren của nó phủ hết tree đối xứng.

ZED đầu tiên tham gia tại level 0 nhận một địa chỉ sau tất cả các router, đó là 0x796f. Công thức:

1[ZC nhận 1 địa chỉ]+6[maxRouter]x0x143d[Cskip tại level 0]=0x796f

Khái niệm của Cskip được giải thích dễ hơn với một mạng dùng các thông số Cskip nhỏ, mặc dù nó không tương thích với stack profile 0x01. Xem Hình 7.11. Các thông số là maxDepth(3), maxChildren(5) và maxRouter(3). Điều này chỉ cho phép 66 node trong mạng. Chú ý các thông số này chỉ để giải thích tree đối xứng cho dễ hiểu.



Hình 2-14: Gán địa chỉ Cskip trong cây đối xứng [3]

Để hiểu tree định địa chỉ, dễ nhất để bắt đầu tại đáy của tree (maxDepth). Xét node 24. Bởi vì nó nằm ở maxDepth, có ba hop từ ZC, nó không thể bất kì children, nên Cskip tại mức này là 0. Parent của nó là node 23. Node này tại mức 3, có hai hop từ ZC, nên nó có Cskip là 1. Mỗi children của nó sẽ dùng một địa chỉ. Node 23 có năm children, nên địa chỉ của nó (23) cộng với năm children của nó (24-28) dùng hết sáu địa chỉ. Do đó, Cskip của parent (node 22) của nó là 6. Node 22 và tất cả các children và grandchildren dùng tổng cộng 21 địa chỉ: 1+3x6+2=21. Ở đây 2 là số ZED có thể tham gia vào node:

2 = maxChildren(5) – maxRouter(3)= maxChildren(2)

Do đó, Cskip tại mức 0, cho ZC trong mạng này là 21. Mỗi router child tại mức 0 dùng 21 địa chỉ cho chính nó và tất cả các nhánh của nó. Các ZED không bao giờ có children, nên các ZED dùng hai địa chỉ. Công thức cho tổng các node cho phép trong mạng với các thông số ở trên là:

1 + 3x21 + 2 = 66

Bằng cách giả sử một tree đối xứng, ZigBee có thể biết, dùng các công thức toán học đơn giản, địa chỉ node là một child (bao gồm grandchildren) hay không. Nếu nó là một child, packet được gửi đến hop tiếp theo bên dưới, đến một router hoặc địa chỉ chính nó. Nếu địa chỉ không phải là một child, packet được gửi tới parent. Node 22 biết rằng bất kì địa chỉ từ 23 đến 42 là child. Còn lại là không phải nên nó gửi tới parent.

Vấn đề của Cskip, và nguyên nhân nó không được dùng trong ZigBee Pro (stack profile 0x02) là nó không thể co giản ngoài maxDepth(5), cho phép lớn nhất 10 hops trong mạng (2x maxDepth). Nếu muốn nhiều hop hownm chỉ thay đổi maxDepth đến 6 và maxChildren(20) và maxRouter(6) cho phép 186,621 node, một số không thể chứa trong 16-bit short address.

Trong hình Hình 2-14, bao gồm cả kết nối tree (đường đen) và mesh (đường đứt). ZigBee luôn luôn là một mạng mesh. Tree có thể được dùng như một mô hình tìm đường backup nếu mesh quá tải, nhưng không thay thế mesh.

2.5.4 Tìm đường cho packet trong ZigBee

ZigBee dùng nhiều phương pháp cho việc tìm đường cho các packet từ một node đến node khác:

- Broadcast (từ một node đến nhiều node)
- Mesh routing (unicast từ một node đến node khác)
- Tree routing (unicast từ một node đến node khác, chỉ trong stack profile 0x01)
- Source routing (unicast từ một node đến node khác, chỉ trong stack profile 0x02)

Mỗi phương pháp có ưu điểm và nhược điểm

Bảng 2-4: So sánh các phương tìm đường trong ZigBee [3]

	Broadcast	Mesh	Tree	Source Route
Multi-hop	Up to 30	Up to 30	Up to 10	Up to 5 hops
Multiple destinations	Yes	No	No	No
One-to-one	No	Yes	Yes	Yes
Bandwidth efficient	No	Yes	Yes	Yes
Payload efficient	Yes	Yes	Yes	No
Acknowledged	No	Yes	Yes	Yes

Broadcast cho phép một node vươn tới nhiều node khác với chỉ một request. Phương pháp này không cần ACK và cần nhiều tài nguyên.

Mesh routing là bảng điều khiển và rất hữu dụng (time, bandwidth, tài nguyên bộ nhớ), khi đường đi được thiết lập. Packet được gửi theo mesh có ACK, nên node gửi biết packet đã nhận hay chưa. Các đường đi mesh được phân phối, mà điều này giảm overhead trong over-the-air packet. ZigBee mesh có thể phân phối các packet đến 30 hop.

Tree routing, cũng có ACK, chỉ có trong stack profile 0x01. Nó được diễn tả ở Cskip. Tree có hiệu quả băng thông như mesh và hiệu quả hơn về bộ nhớ. Nhưng khi liên kết giữa parent và child đứt thì nó không thể phục hồi. Vậy nên ZigBee dùng mesh như mặc định.

Source routing, như mesh và tree, có ACK, chỉ có trong stack profile 0x02. Được sử dụng chính khi một data concentrator (hoặc gateway) cần giao tiếp với nhiều node. Với mesh routing, mỗi đường đi cần một table entry, và các node ZigBee không đủ RAM cho một ngàn đường đi. Trong source routing, một node đơn (đắt hơn) có nhiều RAM để lưu tất cả các đường đi. Đường đi cho bất kì giao tiếp cụ thể nào được gửi như một over-the-air packet. Hạn chế lớn nhất là nó giới hạn lớn nhất 5 hop.

2.6 MAC và PHY Layer

Lớp MAC và PHY được đặc tả trong IEEE 802.15.4, nhưng ZigBee không hiện thực đầy đủ các đặc điểm mà IEEE đưa ra, bởi ZigBee muốn tối thiểu kích thước bộ nhớ để phù hợp với các ứng dụng trong một vi điều khiển 8-bit và giảm tiêu hao năng lượng không cần thiết.

2.6.1 PHY Layer

Trong mạng ZigBee, lớp giao thức thấp nhất là lớp vật lý IEEE 802.15.4, hay PHY. Lớp này là gần nhất với phần cứng và điều khiển và giao tiếp trực tiếp với radio transceiver. Lớp PHY chịu trách nhiệm cho việc kích hoạt radio truyền và nhận packet. PHY cũng lựa chọn tần số kênh và đảm bảo kênh hiện không được dùng bởi các thiết bị khác trên mạng khác.

2.6.2 MAC Layer

Medium Access Control (MAC) layer cung cấp giao diện giữa PHY layer và NWK layer. MAC có trách nhiệm sinh ra các beacon và đồng bộ thiết bị với các beacon (trong mạng beacon-enabled). MAC layer cũng cung cấp dịch vụ kết hợp và không kết hợp.

2.7 Giới thiệu Z-stack của Texas Instrument

Z-Stack™ là một stack giao thức phù hợp với ZigBee của TI cho các sản phẩm và platform IEEE 802.15.4. Z-Stack™phù hợp với đặc tả ZigBee® 2007 (ZigBee và ZigBee PRO), hỗ trợ tính chất cả ZigBee và ZigBee PRO trên CC2530 System-on-chip, MSP430+CC2520 và Stellaris LM3S9B96+CC2520. Z-Stack™ hỗ trợ Smart Energy và Home Automation profiles.

Toàn bộ Z-Stack™ download tại trang http://www.ti.com/tool/z-stack . Z-Stack™ đóng một phần source-code nên được biên dịch sẵn cho một số dòng chip mà Z-Stack™ hỗ trợ. Tài liệu liên quan đến Z-Stack™ cũng được hỗ trợ đầy đủ kèm theo gói stack được tải về

Chương 3.HIỆN THỰC ĐỀ TÀI

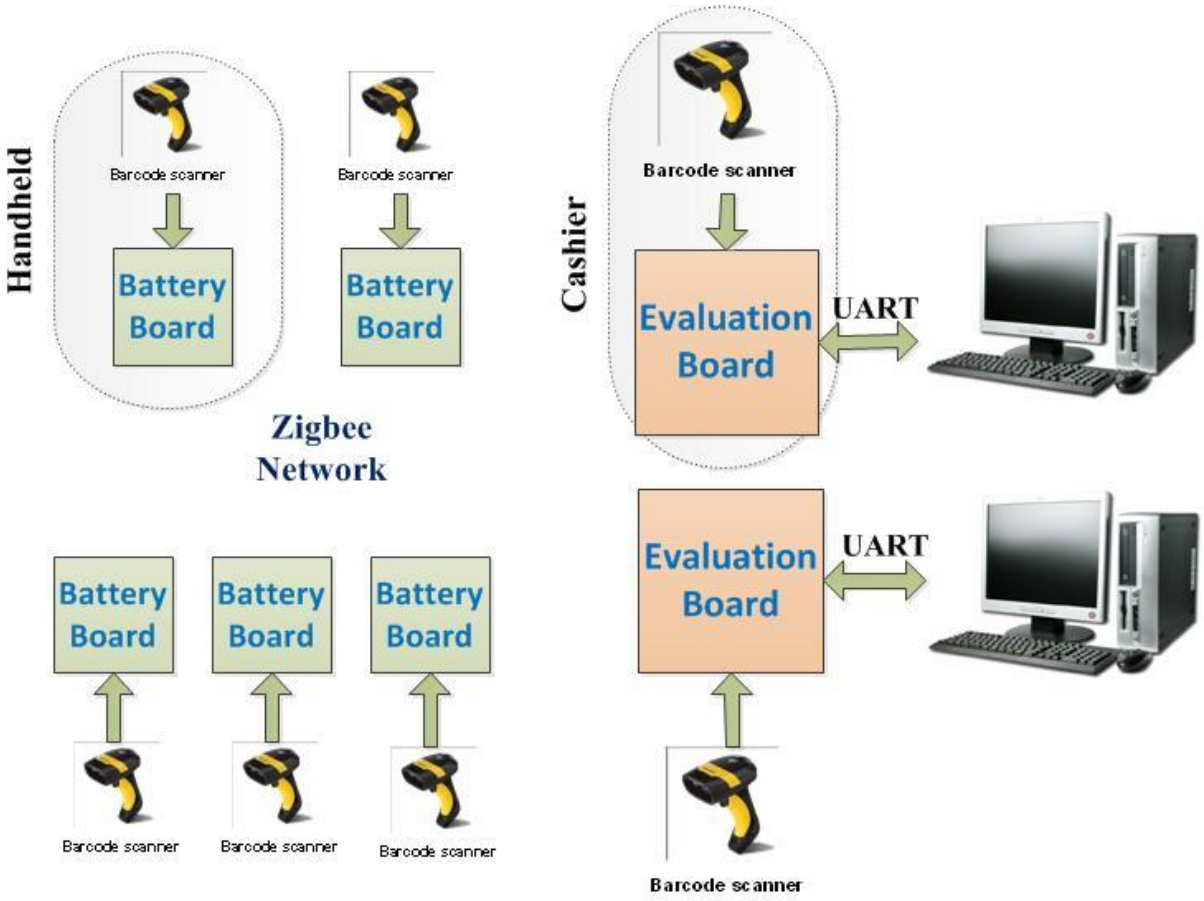
3.1 Kiến trúc hệ thống Queue – Busting on ZigBee

3.1.1 Hệ thống phần cứng

Toàn bộ hệ thống mạng ZigBee (xem Hình 3-1) gồm hai thiết bị chính:

- Cashier: thiết bị cố định tại quầy tính tiền nên cashier nên là ZC hoặc ZR trong mạng ZigBee. Cashier giao tiếp với PC để tính toán dữ liệu.
- Handheld: thiết bị di động, có thể là ZR hoặc ZED trong mạng ZigBee

Các thiết bị Handheld và Cashier được kết nối và giao tiếp với nhau thông qua mạng Zigbee.

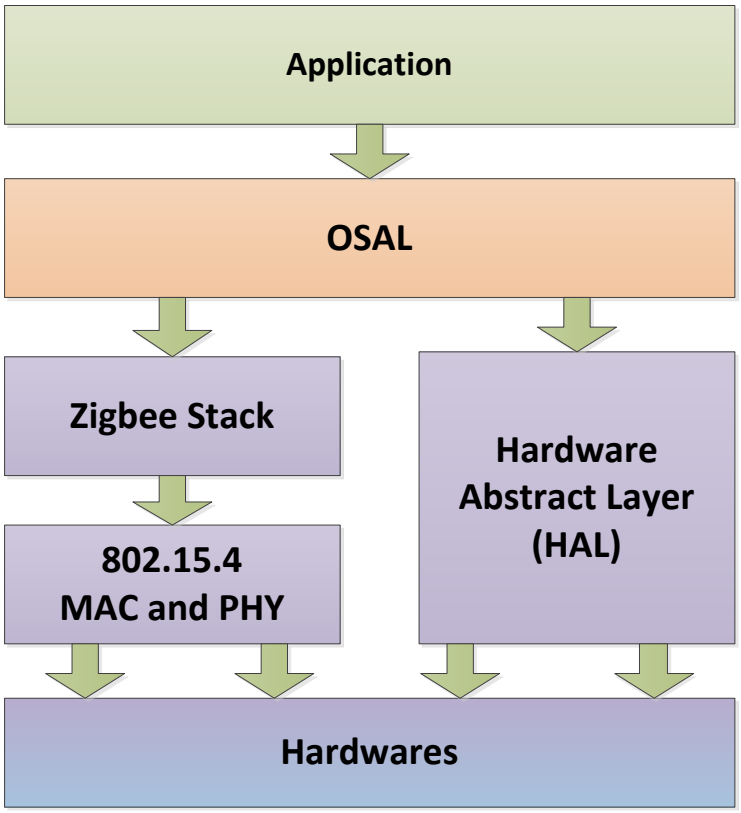


Hình 3-1: Sơ đồ kết nối thiết bị của hệ thống

3.1.2 Hệ thống phần mềm

Kiến trúc software của mỗi thiết bị được phân ra theo lớp. Ứng dụng thể hiện hành vi của thiết bị được hiện thực trên lớp Application dưới một task của mộthệ điều hànhtrừu tượng (OSAL) để điều khiển các thiết bị phần cứng bên dưới. Tất cả các sự kiện (events) xảy ra trong

suốt quá trình hoạt động (về radio, interrupt…) đều được lớp OSAL điều khiển. Lớp trừu tượng phần cứng (HAL) cung cấp việc điều khiển các thiết bị ngoài vi của lớp Application thông qua các hàm APIs. Và phần quan trọng của hệ thống là ZigBee stack, ở đây Z – stack của Texas Instrument được sử dụng để điều khiển quá trình giao tiếp với các thiết bị khác trên mạng ZigBee.



Hình 3-2: Sơ đồ phân lớp kiến trúc phần mềm

Giao thức giao tiếp giữa các thiết bị được thực hiện dựa trên mạng ZigBee, được đóng gói dưới dạng phần dữ liệu của các gói từ Z – stack. Giao thức này được định nghĩa và hiện thực riêng cho đề tài nhằm đơn giản việc xử lý của lớp Application.

Giao thức này có định dạng nhưBảng 3-1, gồm phần header xác định loại frame có chiều dài một byte và phần dữ liệu kèm theo frame đó có chiều dài thay đổi theo loại frame.

Các định dạng của frame:

- Basket frame : các thông tin liên quan đến giỏ hàng.
  + Basket request frame : yêu cầu một basket
  + Basket respond frame :gửi một basket tới thiết bị yêu cầu
- Status frame :các thông tin liên quan đến trạng thái hiện tại của mạng.
  + Status request frame : yêu cầu thông tin thiết bị.
  + Status respond frame : trả lời yêu cầu thông tin thiết bị gồm địa chỉ MAC, Short Address, địa chỉ của parent.
- Delete frame : lệnh xóa dữ liệu mà cashier hay PC cần handheld xử lý.

+ Delete all basket frame: Xóa toàn bộ các basket lưu trong thiết bị.
+ Delete baskets frame : Xóa các basket chứa trong frame.

Bảng 3-1: Định dạng của giao thức Queue – Busting on ZigBee

1 byte	N bytes
Header	Data

Basket request

'%'	Basket ID: 8Bytes

Basket respond

'H'	ShortAddr: 2bytes	Basket ID length: 1byte	Product ID length: 1byte	Basket: variable length

Status request

'S'	No data

Status respond

'S'	MAC Addr: 6bytes	Short Addr: 2bytes	Parent Addr: 2bytes

Delete all basket

'^'	1byte: all zero

Delete baskets

'^'	Number: 1byte	Basket IDs: variable length

3.1.3 Giới thiệu bộ phần cứng DK CC2530 của TI

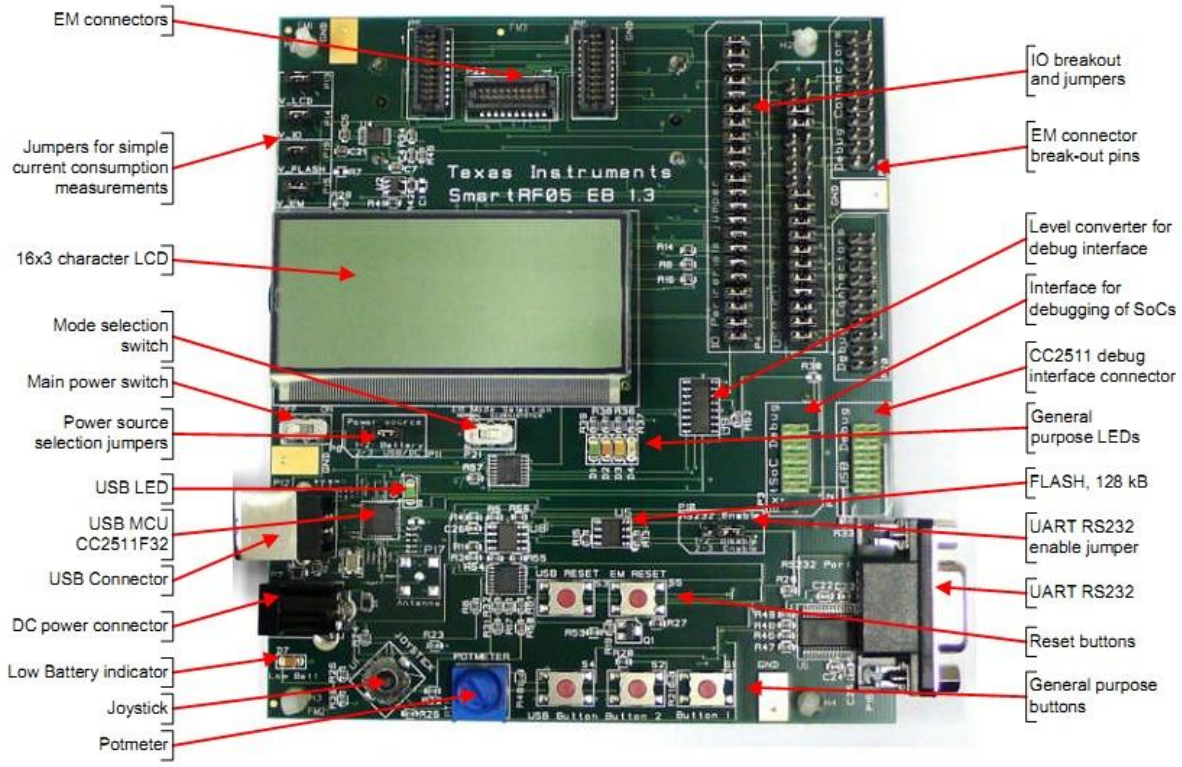
Bộ Kit phát triển CC2530DK hỗ trợ CC2530 System-on-chip phù hợp chuẩn 2.4GHz IEE 802.15.4 thế hệ thứ hai của TI và chứa tất cả phần cứng, phần mềm và các công cụ cần thiết để xây dựng sản phẩm phù hợp với 802.15.4.Có thể hoạt động ở 125°C và điện áp thấp, tiết kiệm năng lượng.

Bộ DK CC2530 bao gồm:

- 7 x CC2530EM Evaluation Modules
- 7 x 2.4 GHz Antennas
- 2 x SmartRF05EB Evaluation Boards
- 2 x SmartRF05BB Battery Boards
- 1 x CC2531 USB Dongle
- USB cables vàtàiliệu

3.1.3.1 SmartRF05 Evaluation Boards

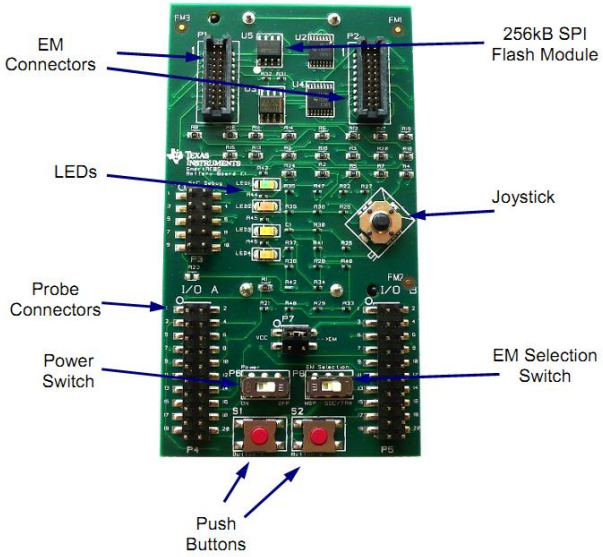
- Dùng để nạp code, kiểm tra lỗi cho CC2530 Evaluation Modules.
- Cung cấp nguồn cho CC2530 từ 2 pin AA, DC-in hoặc từ USB.
- Gắn các thiết bị ngoại vi kết nối với CC2530 Evaluation Modules như : LCD, Flash (128kB), 2 UART, Joystick, Switch…
- Trong hệ thống, board này đóng vai trò là cashier. Thực hiện việc thanh toán (checkout) các mã giỏ hàng (basket id) của khách hàng, kết nối với PC qua cổng COM để truy cập cơ sở dữ liệu và in hóa đơn thanh toán.



Hình 3-3:SmartRF05 Evaluation Board [2]

3.1.3.2 SmartRF05 Battery Boards

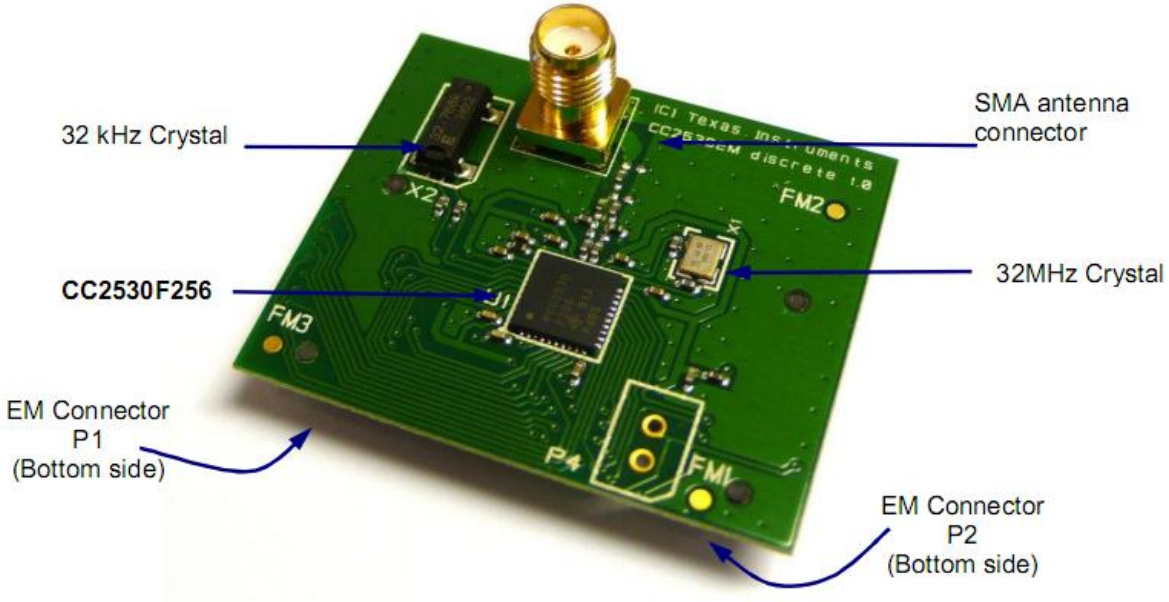
- Nhỏ hơn và đơn giản hơn SmartRF05 Evaluation Boards.
- Chỉ có các ngoại vi cần thiết.
- Trong hệ thống, đóng vai trò là handheld. Thực hiện nhiệm vụ kết nối với máy quét mã vạch (scanner) và lưu trữ vào flash nội dung giỏ hàng của khách hàng. Khi cashier có yêu cầu, handheld sẽ gửi trả nội dung giỏ hàng thông qua mạng zigbee.



Hình 3-4:SmartRF05 Battery Board [2]

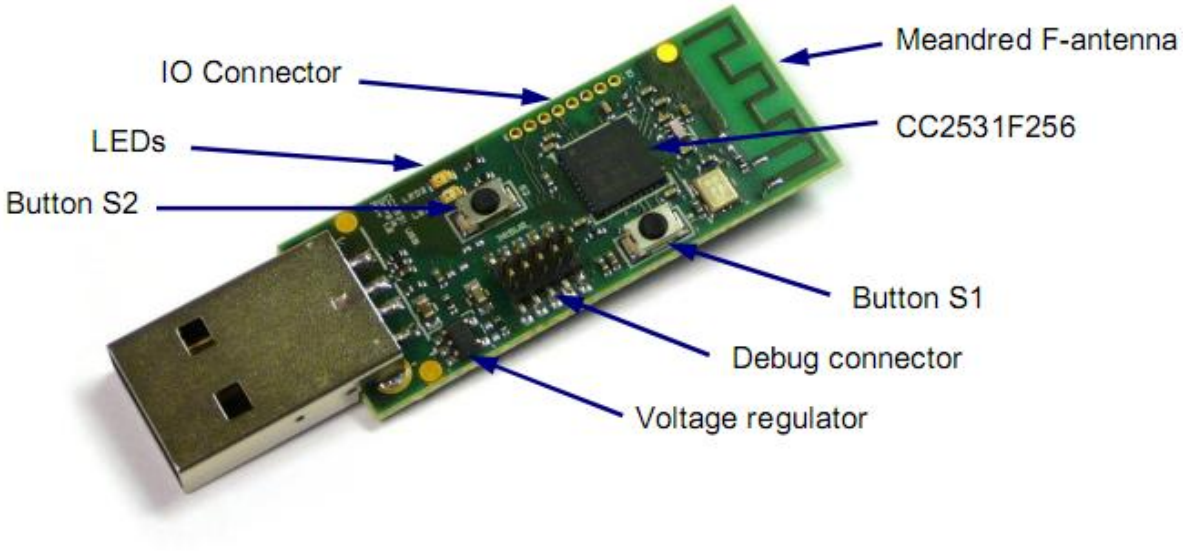
3.1.3.3 CC2530 Evaluation Modules

- Module chính thực hiệc các công việc liên quan đến mạng không dây.
- Cần kết nối với board SmartRF05 và antenna để hoạt động.



Hình 3-5:CC2530 Evaluation Modules

3.1.3.4 Một số các thiết bị khác



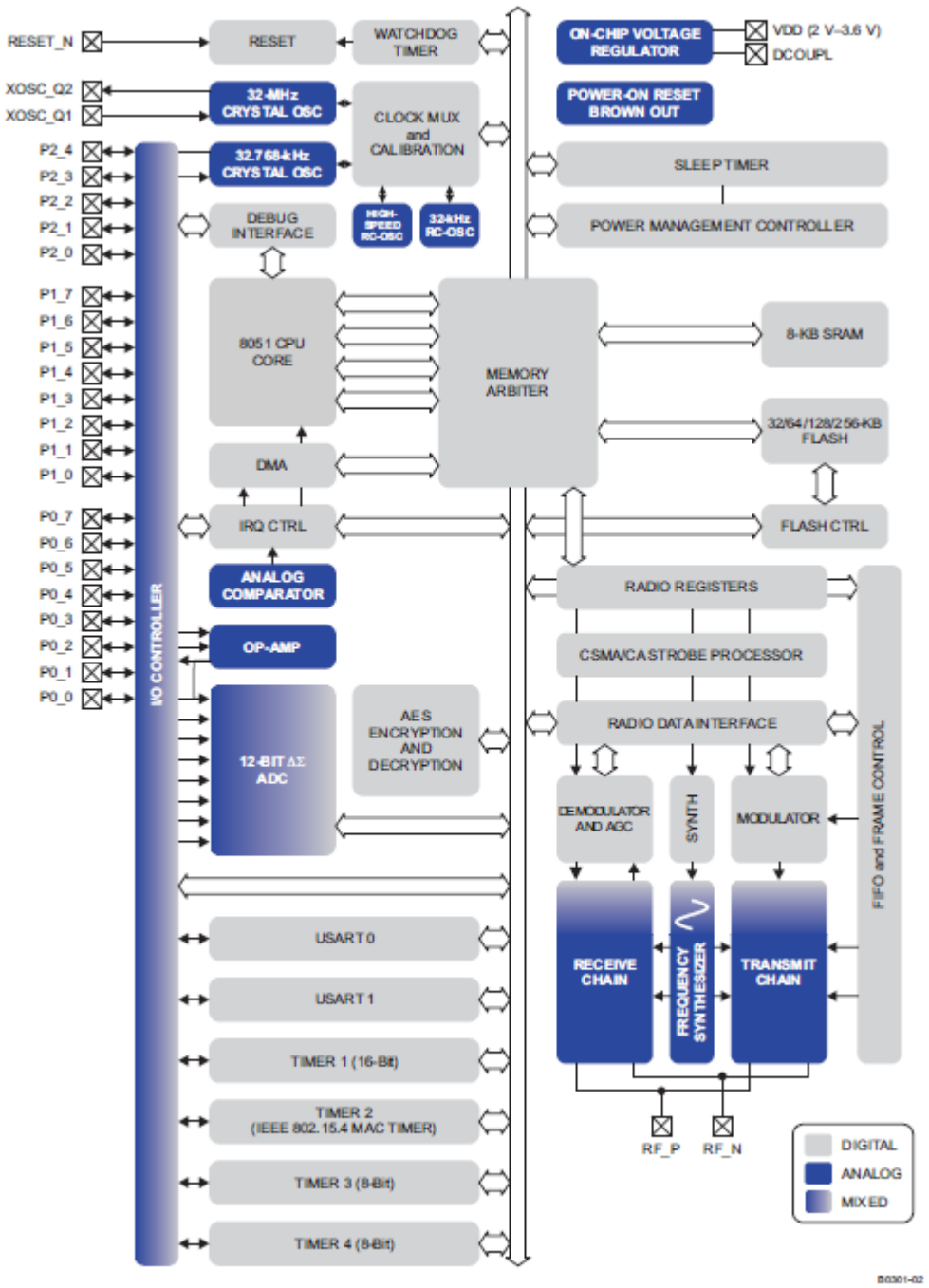
Hình 3-6: CC2531 USB Dongle [2]

Hình 3-7: CC2530 Antenna [2]

3.1.3.5 Giới thiệu chip CC2530

- RF/Layout
  - Bộ truyền nhận RF phù hợp 2.4GHz IEEE 802.15.4
  - Độ nhạy nhận cao
  - Năng lượng đầu ra có thể lập trình tới 4.5 dBm
  - Cần rất it các thành phần bên ngoài
  - Chỉ một thạch anh đơn giản cho đồng bộ các mạng
- Năng lượng thấp
  - Active-Mode RX (CPU Idle): 24mA
  - Active-Mode TX tại 1dBm (CPU Idle): 29mA
  - Dãy điện áp cung cấp rộng (2V – 3.6V)

- Vi điều khiển
  - Nhân vi điều khiển 8051 năng lượng thấp và hiệu suất cao với Code Prefetch
  - Bộ nhớ Flash In-System-Programmable 32-, 64-, 128-, 2560Kbytes.
  - 8Kbytes RAM được duy trì trong tất cả các chế độ năng lượng
  - Hỗ trợ debug phần cứng
- Ngoại vi
  - Năm kênh DMA và bộ mã hóa, giải mã AES
  - Bộ so sánh năng lượng siêu thấp
  - IEEE 802.15.4 MAC timer và các timer mục đích chung (một 16-bit, hai 8-bit)
  - Hỗ trợ phần cứng CSMA/CD
  - Cảm biến nhiệt độ và theo dõi Pin
  - 12-bit ADC với 8 kênh và độ phân giải có thể cấu hình
  - Hai USART với hỗ trợ các giao thức nối tiếp
  - 21 I/O chân mục đích chung
  - Watchdog Timer
- Ứng dụng
  - Các hệ thống 2.4GHz IEEE 802.15.4
  - Các hệ thống điều khiển từ xa RF4CE
  - Hệ thống ZigBee
  - Home/Building Automation
  - Hệ thống ánh sáng
  - Giám sát và điều khiển công nghiệp
  - Mạng cảm biến không dây năng lượng thấp
  - Điện tử dân dụng và chăm sóc sức khỏe



Hình 3-8: Kiến trúc CC2530 [5]

3.1.4 Một số thành phần khác của hệ thống

Barcode Scanner là thiết bị đọc mã vạch, với giao tiếp chuẩn RS232 được cấu hình với9600 baud rate, none parity bit, stop bit là 1

Mạch chuyển đổi điện áp 3.3V dùng cho board sang điện áp của chuẩn RS232 để giao tiếp với máy tính và máy đọc mã vạch dùng MAX3232.

3.1.5 Cấu hình mạng ZigBee cho Z-stack

Các cài đặt cho Z-stack (xemBảng 3-2), đây là các thông số cần thiết cho Z-stack để trình biên dịch lựa chọn đúng cấu hình cho ứng dụng của hệ thống và mạng ZigBee sẽ hoạt động theo các giá trị cài đặt này (tham khảo thêm [2]).

Bảng 3-2: Các thông số cấu hình cho mạng ZigBee

ZIGBEEPRO	Mạng dùng ZigBee Pro Profile
DEFAULT_CHANLIST=0x00000800	Kênh mặc định là 11
ZDAPP_CONFIG_PAN_ID=0xFFFF	Sử dụng PAN ID tự động
BEACON_REQUEST_DELAY=100	Trì hoãn giữa các beacon-request (ms)
ROUTE_EXPIRY_TIME=30	Thời gian timeout cho tìm đường (s)
APSC_MAX_FRAME_RETRIES=3	Cho phép truyền lại 3 lần
NWK_MAX_DATA_RETRIES=2	Số lần tìm địa chỉ của hop kế tiếp
MAX_BCAST=9	Số thực thể trong bảng broadcast
MAX_RTG_ENTRIES=40	Số thực thể trong bảng tìm đường
NWK_MAX_BINDING_ENTRIES=4	Số thực thể trong bảng binding
MAX_BINDING_CLUSTER_IDS=4	Số cluster ID trong mỗi thực thể của bảng binding

Để các thiết bị trong mạng ZigBee có thể giao tiếp với nhau, thì các thiết bị này phải trùng Simple Description với nhau (xem

) và sử dụng hàm sau để cấu hình:

```
//Register an Application's EndPoint description.

afStatus_t afRegister( endPointDesc_t *epDesc );

ZStatus_t ZDO_RegisterForZDOMsg( uint8 taskID

                                 , uint16 clusterID );
```

Bảng 3-3: Các thông số cho Simple Description

Q_BUSTING_ENDPOINT	10
Q_BUSTING_PROFID	0x0F04
Q_BUSTING_DEVICEID	0x0001
Q_BUSTING_DEVICE_VERSION	0
Q_BUSTING_FLAGS	0
Q_BUSTING_MAX_CLUSTERS	1
Q_BUSTING_CLUSTERID	1

3.2 Thiết bị cashier

3.2.1 Nguyên tắc hoạt động

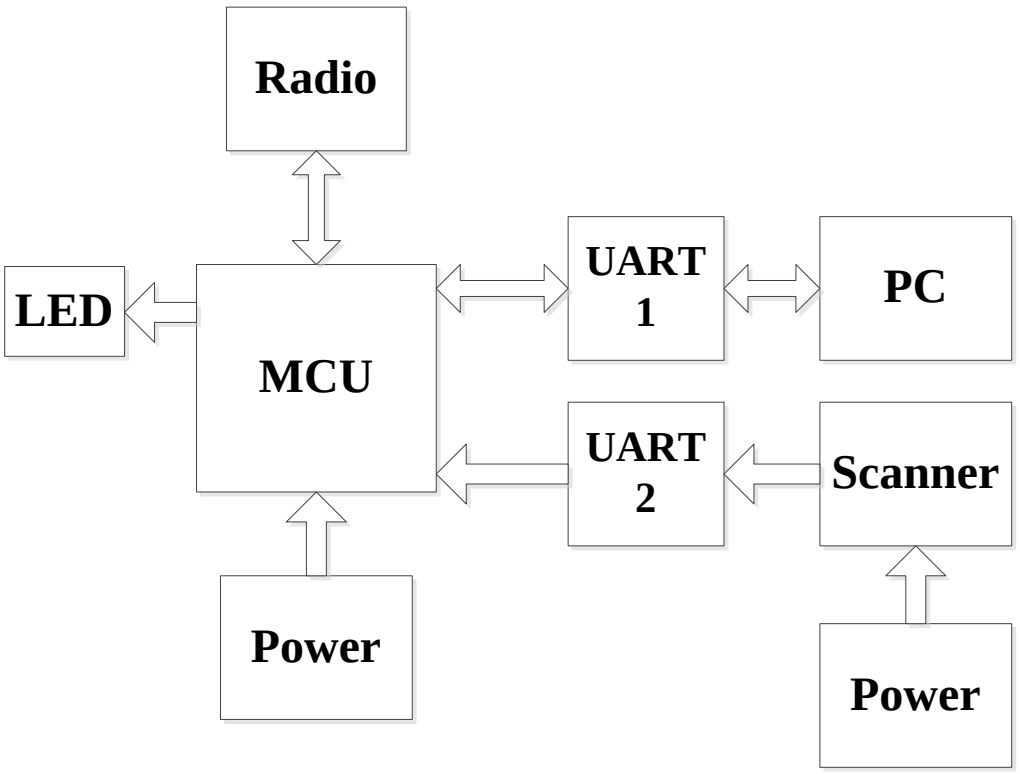
Cashier giao tiếp với 3 device chính :

- Giao tiếp với barcode scanner :
  + Nếudữliệunhậntừ scanner là '+'hay'-', thìchuyển sang mode "prod". Trong mode này, nếu dữ liệu nhận từ scanner là mã sản phẩm (products ID) thì hàng hóa đó sẽ được thêm/xóa khỏi giỏ hàng. Việc thêm/xóa hàng hóa này sẽ được gửi lên PC để tính tiền, và không ảnh hưởng đến handheld đang chứa giỏ hàng đó.
  + Nếudữliệunhậntừ scanner là *'%'*, thìchuyển sang mode "basket". Trong mode này, nếu dữ liệu nhận từ scanner là basket ID thì cashier sẽ broadcast basket request frame cho tất cả các handheld có trong mạng.
  + Nếudữliệunhậntừ scanner là *'@FlashReset'*, cashiersẽbroadcastchotấtcảcácthiếtbịhandheldđểxóatoànbộdữliệuđanglưutrongbộnhớ flash. Chỉdùngkhi siêuthịđãngừnghoạtđộng, cần reset lạicácthiếtbị.
  + Nếudữliệunhậntừ scanner là*'S'*,cashier sẽ broadcast chotấtcảcácthiếtbị handheld đểyêucầucác handheld báocáotrạngtháicủamình. Chỉdùngkhicầnkiểmtrathiếtbịcóhoạtđộngbìnhthường hay không.
- Giaotiếpvới PC :
  + Nếudữliệunhậnđượctừ PC códạng*'^'+[num:1byte]+[Basket IDs]*, cashier sẽ tìm trong dữ liệu của mình để gửi tới 1 handheld đang giữ giỏ hàng có Basket ID tương ứng. Khi handheld nhận được frame này, handheld sẽ xóa basket có Basket ID tương ứng trong flash của mình.
  + Nếu dữ liệu nhận được từ PC có dạng *'S'*,cashiersẽ broadcast chotấtcảcácthiếtbị handheld đểyêucầucác handheld báocáotrạngtháicủamình.
- GiaotiếpvớimạngZigbee :
  + Nếukhôngnhậnđượcgói ACK của handheld thìsẽgửimãlỗitươngứngcho PC.
  + Nếunhậnđược basket respond frame, cashier đọc qua 4 byte đầuđểlưulạiđịachỉvà basket ID tươngứngcủa handheld. Sauđósẽchuyểntoànbộ frame đócho PC.
  + Nếunhậnđược status respond frame, cashier sẽchuyểntoànbộ frame đócho PC.

3.2.2 Hardware

Phần cứng (hardware) của cashier bao gồm :

- 1 module scanner: giao tiếp với MCU thong qua UART
- 1 module radio: được tích hợp sẵn trên CC2530F256, 8k Bytes RAM, 256k Bytes Flash
- 1 module quản lý nguồn: sử dụng 2 Pin AA ~ 3.3V cho MCU và một mạch boost từ 3.3V lên 5V cho Scanner. Tuy nhiên, có thể sử dụng nguồi DC-in hay nguồn từ USB.
- 2 LED trạng thái

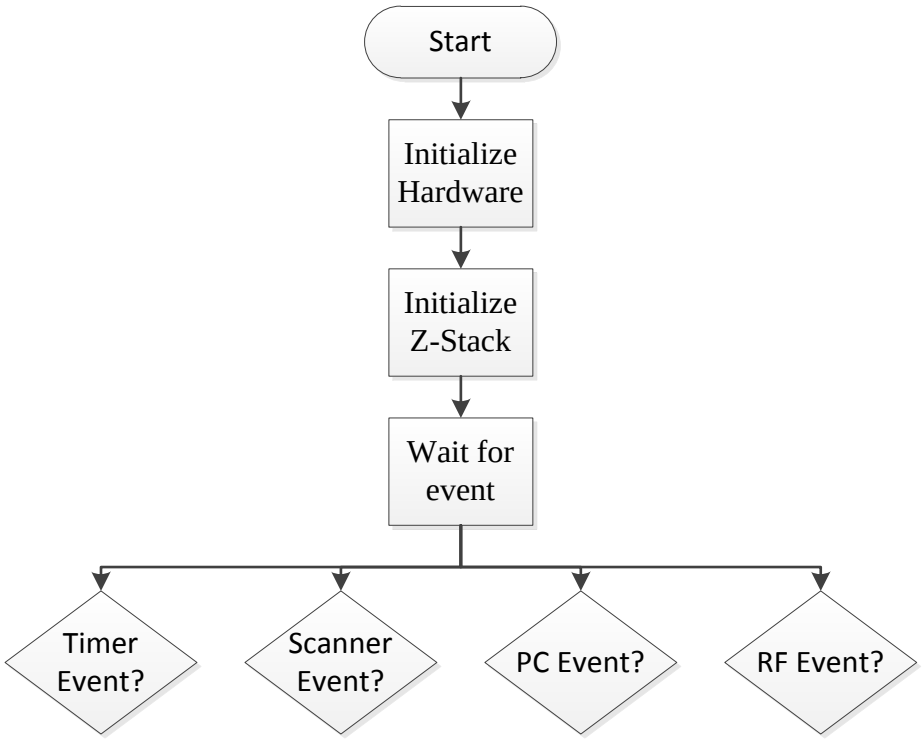


Hình 3-9: Sơ đồ khối các chức năng

3.2.3 Software

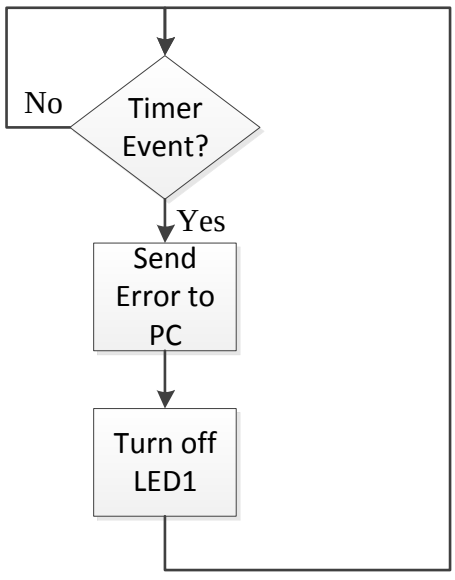
Chương trình (software) trên cashier :

- Chương trình dùng một hệ điều hành thời gian thực của Z-Stack (OSAL) để quản lý các thiết bị được tối ưu. OSAL quản lý các thiết bị thông qua các sự kiện (event), có 4 event chính như sau :
  + Timer : gây ra do timer đã đếm hết khoảng thời gian quy định trước, chủ yếu dùng để báo lỗi.
  + Scanner : gây ra do barcode scanner truyền dữ liệu thông qua UART 2.
  + PC : gây ra do PC dư liệu thông qua UART 1.
  + Radio Frequency : gây ra do có sự thay đổi trong mạng.



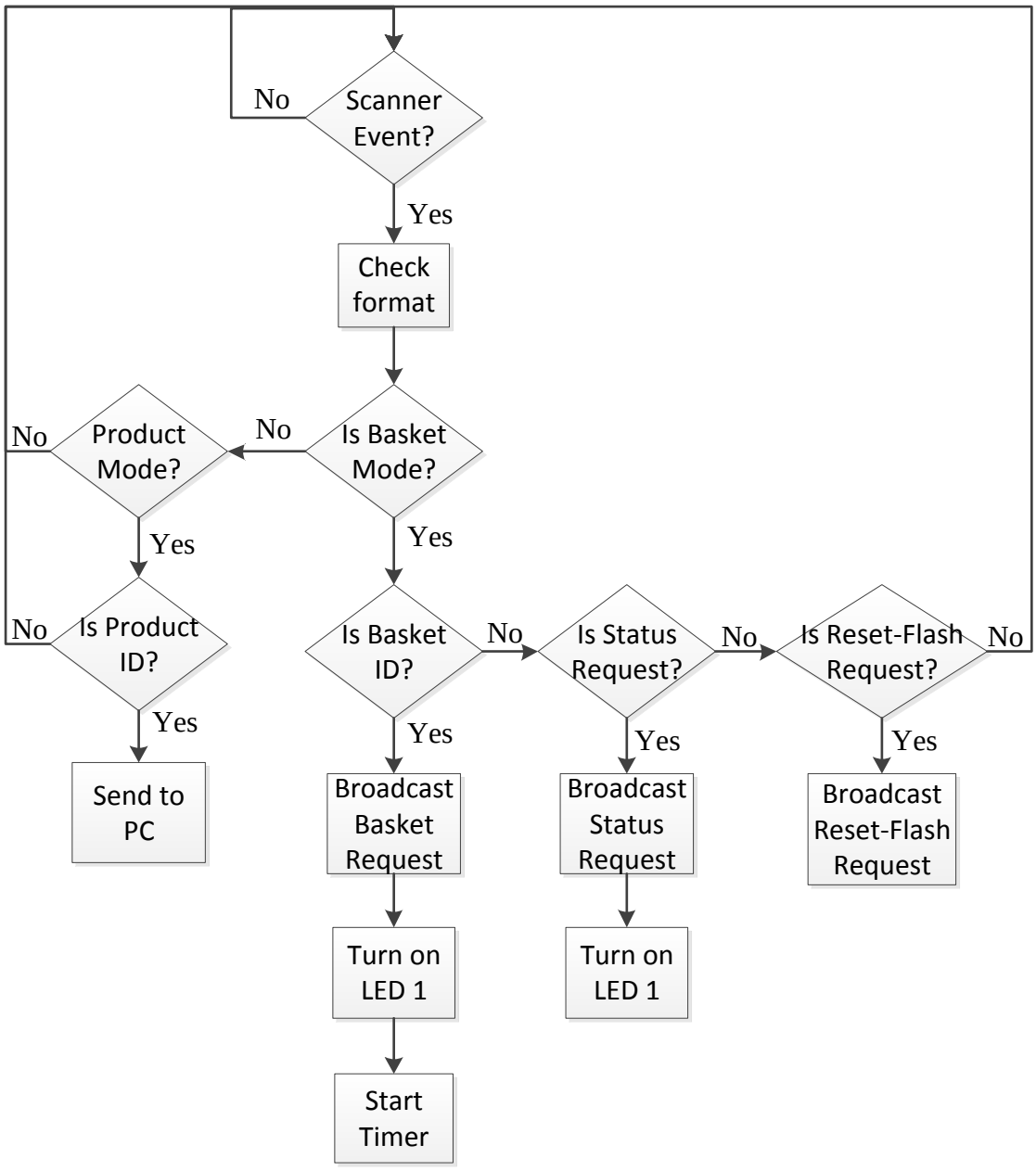
Hình 3-10: Sơ đồ tổng quát các sự kiện chính trong chương trình

- Timer Event : khi một quá trình xử lý cần tính toán thời gian để xuất ra các thông báo có liên quan, Timer sẽ được kích hoạt để bắt đầu đếm thời gian. Khi Timer đã đếm đến thời điểm xác định, Timer sẽ gây ra một event trong OSAL.



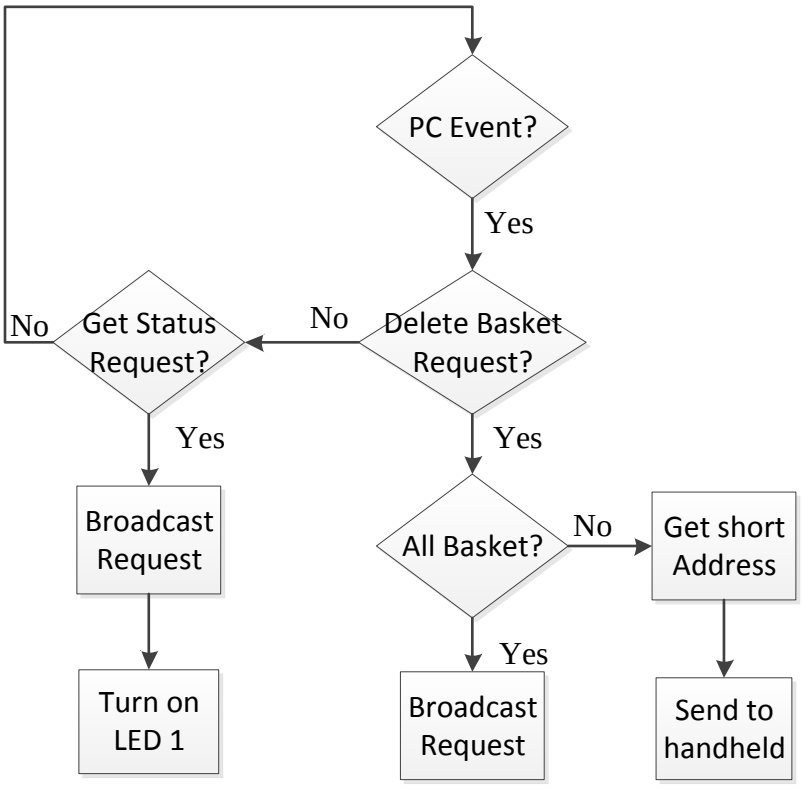
Hình 3-11: Sự kiện của timer trong cashier

- Scanner Event : khi barcode scanner đọc 1 mã vạch, dữ liệu sẽ được gửi đến thông qua UART (quản lý theo cơ chế interrupt). Khi dữ liệu đã được truyền hết thì UART sẽ gây ra một event trong OSAL.



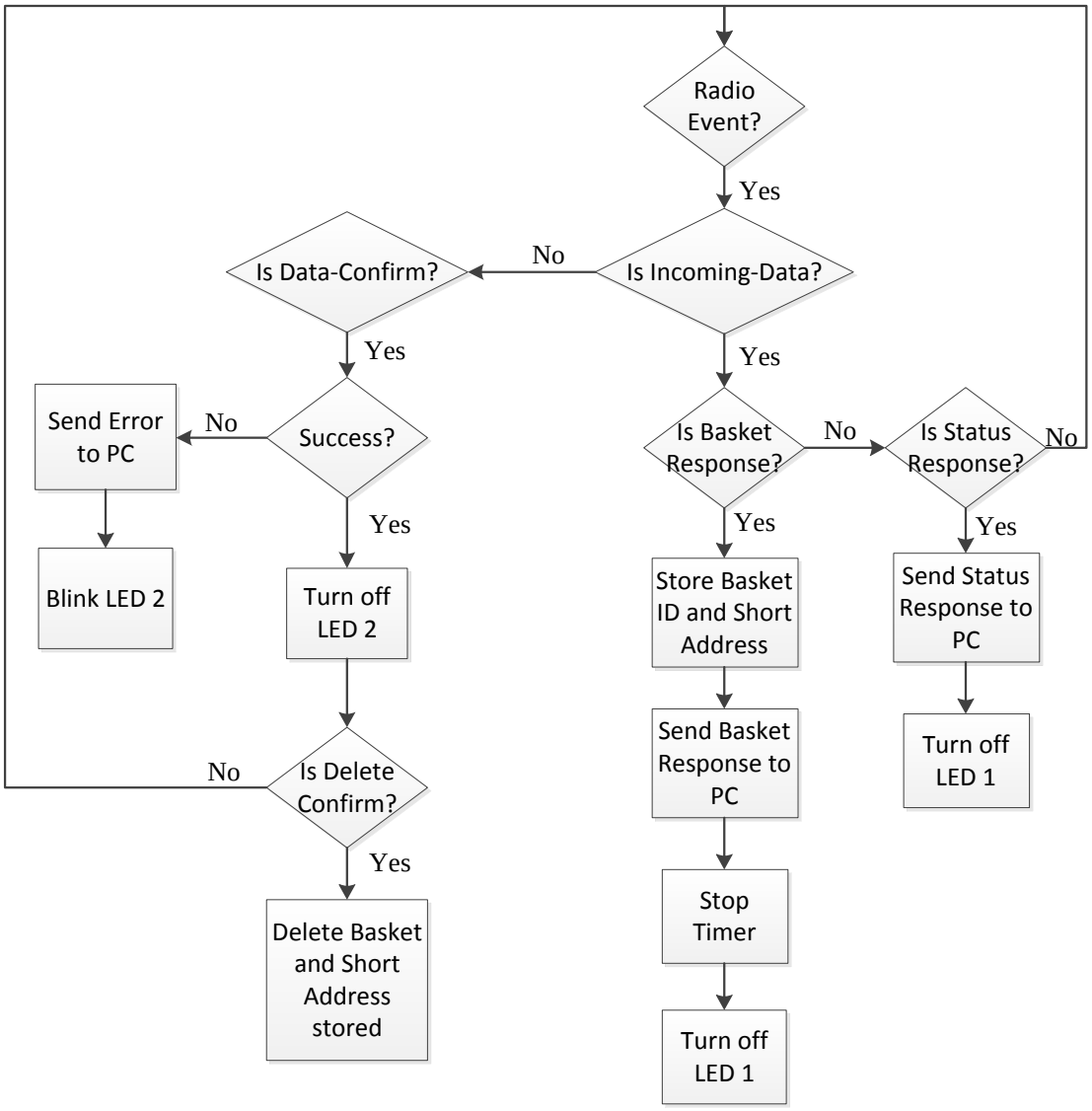
Hình 3-12: Sự kiện của scanner trong cashier

- PC Event : khi PC truyền dữ liệu xuống thông qua UART (điều khiển bằng DMA) sẽ gây ra một event trong OSAL.



Hình 3-13: Sự kiện của pc trong cashier

- Radio Frequency Event : gây ra khi có bất cứ sự thay đổi của mạng, có rất nhiều sư kiện dạng này tuy nhiên, chúng tôi chỉ tập trung vào 2 sự kiện chính là có frame dữ liệu và frame ack.



Hình 3-14: Sự kiện của radio trong cashier

3.3 Thiết bị handheld

3.3.1 Nguyên tắc hoạt động

Để hiện thực ứng dụng trên thiết bị cần ba quá trình xử lý dữ liệu:

Quá trình kết nối mạng:

- Khi ứng dụng khởi động sẽ tự động kết nối với mạng ZigBee với cấu hình sẵn và LED2 trạng thái sẽ nhấp nháy khi kết nối.
- Kết nối thành công LED2 trạng thái sẽ tắt.

Quá trình nhận dữ liệu từ người dùng:

- Người dùng quét một Basket ID từ Scanner, LED1 sáng. Handheld sẵn sàng cho người dùng quét Product IDs.
- Khi quét Product IDs, LED2 sẽ nhấp nháy báo đã nhận dữ liệu.
- Khi quét xong các Product IDs, người dùng quét lại Basket ID để lưu vào bộ nhớ flash và LED1 tắt.

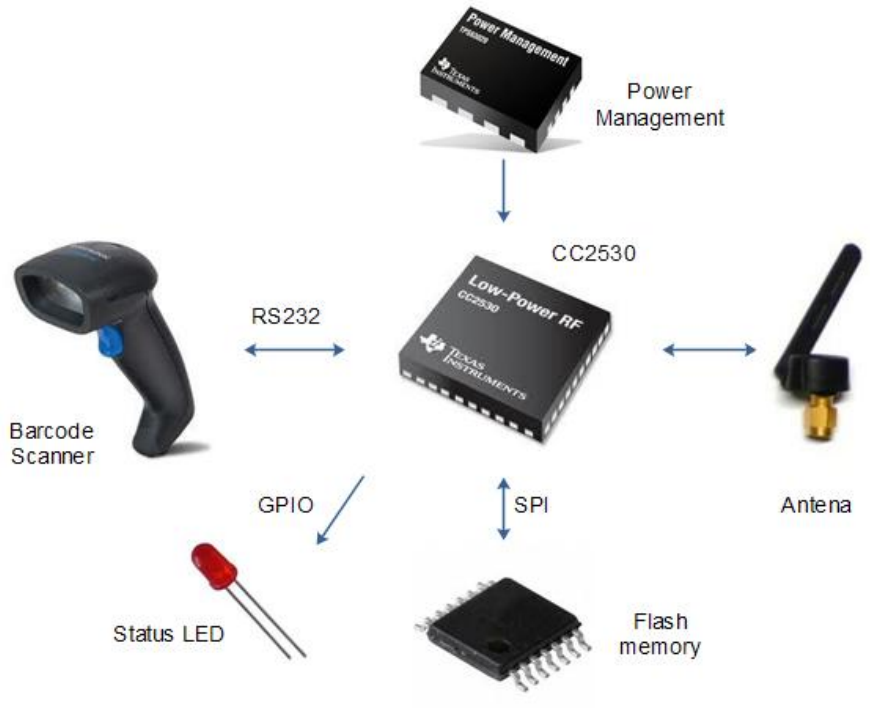
Quá trình nhận dữ liệu và trả lời cho hệ thống:

- Yêu cầu dữ liệu: Đọc bộ nhớ flash và tìm dữ liệu, nếu có thì gửi dữ liệu theo địa chỉ của thiết bị yêu cầu.
- Xóa dữ liệu: Yêu cầu xóa một Basket hoặc toàn bộ trong flash.

3.3.2 Hardware

Phần cứng yêu cầu cần:

- 1 module scanner: giao tiếp với CC2530F256 thông qua UART
- 1 module radio: được tích hợp sẵn trên CC2530F256, 8k Bytes RAM, 256k Bytes Flash
- 1 module quản lý nguồn: sử dụng 2 Pin AA ~ 3.3V cho MCU và một mạch boost từ 3.3V lên 5V cho Scanner.
- 1 Flash 256kBytes: cho việc lưu trữ dữ liệu người dùng
- 2 LED trạng thái: LED1 (báo đang nhập sản phẩm vào basket), LED2(báo trạng thái không được kết nối bằng cách chớp nháy chu kì 1s, và nhấp nháy khi nhập sản phẩm)



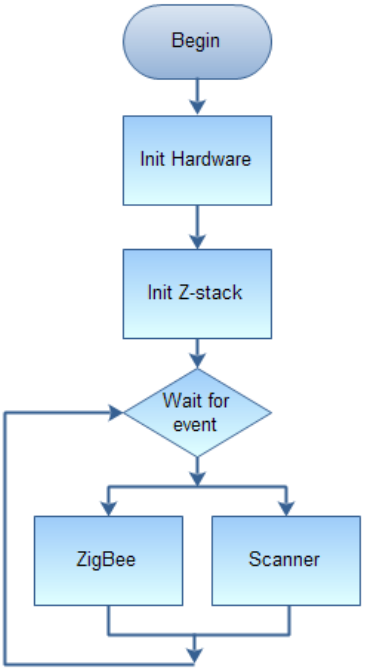
Hình 3-15: Các phần cứng cho hiện thực

Các thành phần phần cứng sẽ giao tiếp với vi điều khiển CC2530 theo như Hình 3-15. Barcode scanner sau khi giải mã vạch sẽ truyền dữ liệu về CC2530 thông qua RS232. Các dữ liệu cần thiết được lưu trữ trong Serial Flash Memmory thông qua SPI.

3.3.3 Software

Sofware cho ứng dụng bao gồm các thành phần cơ bản sau dựa theo việc xử lý dữ liệu từ các thiết bị ngoại vi:

- Giao tiếp với Scanner thông qua UART: 9600 baud rate, none parity bit, stop bit là 1
- Giao tiếp với bộ nhớ Flash M25PE20: xây dựng bộ thư viện thao tác như cấu hình, đọc, ghi, xóa …
- Giao tiếp với mạng ZigBee: sử dụng Z-stack của TI

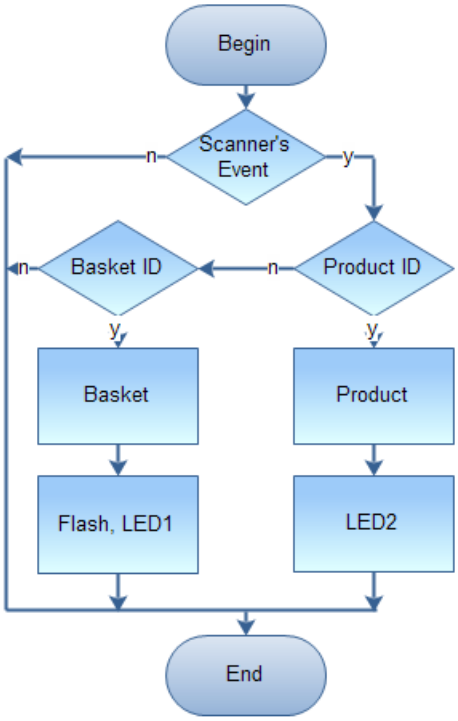


Hình 3-16: Sơ đồ mô tả tổng quát task ứng dụng trong Handheld

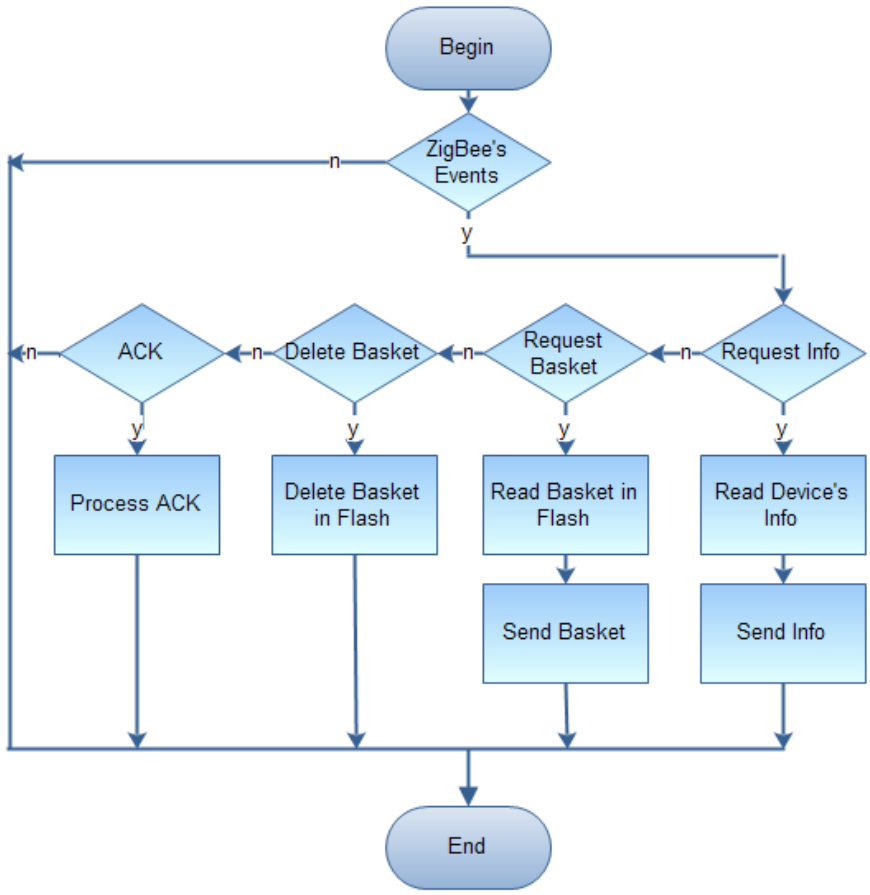
Như lưu đồ (xem Hình 3-16), khi cấp nguồn hay khởi động thiết bị, việc đầu tiên là khởi tạo phần cứng gồm các cấu hình cho CC2530 và các thiết bị ngoại vi được sử dụng trong quá trình hoạt động của hệ thống. Tiếp theo là khởi tạo các thông số, thành phần của Z-stack và tiến hành thiết lập kết nối với mạng ZigBee. Và tùy theo sự kiện từ hệ thống như dữ liệu từ scanner hoặc từ Z-stack, ứng dụng sẽ thực hiện hành vi tùy theo sự kiện nào xảy ra. Sau đó, ứng dụng rơi vào trạng thái chờ sự kiện. Chú ý, ứng dụng ở đây hay một endpoint trong trong lớp ứng dụng của ZigBee chỉ là một task trong OSAL, ngoài ra còn các task của các lớp trong Z-stack sẽ chạy đồng thời, chúng ta sẽ không nói rõ trong phần hiện thực này (tham khảo thêm [2]).

Quá trình xử lý dữ liệu từ Scanner (xem Hình 3-17), khi Scanner truyền dữ liệu qua UART của CC2530 sẽ tạo một ngắt của DMA và tạo một sự kiện tới task ứng dụng để yêu cầu xử lý dữ liệu từ thiết bị. Tùy thuộc vào dữ liệu, task ứng dụng sẽ phân loại hai kiểu dữ liệu (theo một quy

ước trước): Basket ID và Product ID hoặc không phải dữ liệu cần thiết (dữ liệu rác). Hành vi sau đó của task ứng dụng sẽ tùy vào trạng thái dữ liệu trước đó, ở đây chúng tôi không đề cập chi tiết ở đây. Quá trình này xử lý việc người dùng quét các sản phẩm và đóng gói theo từng các basket, sau đó lưu vào bộ nhớ Flash như đã định nghĩa ở mục 1.3.2.



Hình 3-17: Sơ đồ xử lý dữ liệu từ Scanner trong Handheld



Hình 3-18: Sơ đồ xử lý dữ liệu từ mạng ZigBee trong Handheld

Quá trình nhận và trả lời message từ mạng ZigBee (xem Hình 3-18), khi có một gói dữ liệu cho task ứng dụng, Z-stack sẽ tạo ra một sự kiện cho task biết để xử lý. Chú ý cách tạo sự kiện này sẽ được cấu hình ngay từ lúc khởi tạo cho Z-stack (tham khảo thêm [2]). Tùy theo dữ kiện từ message từ các thiết bị khác trong mạng yêu cầu (với hệ thống này thì đó thường là các thiết bị Cashier), ta sẽ có các xử lý sau (xem thêm thông tin ở Bảng 3-1):

- Yêu cầu thông tin của thiết bị (được xem như là trạng thái thiết bị trong mạng): ứng dụng sẽ đọc các thông tin cần thiết và gửi lại cho thiết bị yêu cầu.
- Yêu cầu một basket: ứng dụng sẽ tìm trong bộ nhớ Flash xem có basket yêu cầu hay không. Nếu có thì gửi basket cho thiết bị yêu cầu, còn không thì không làm gì.
- Yêu cầu xóa một basket: ứng dụng tìm basket yêu cầu xóa trong bộ nhớ Flash và xóa nó.
- Nhận ACK: ứng dụng sẽ báo cho người dùng việc gửi dữ liệu không thành công bằng cách bật LED1 trên thiết bị.

Để cho dễ cho việc lưu trữ và đọc dữ liệu thì bộ nhớ Flash được bố trí như sau:

- Header
    - Số lượng Basket: 1byte, có tối đa 255 Basket trong Flash
    - Số thứ tự Basket cuối cùng: 1byte
    - Chiều dài tối đa của một Basket: 2byte

- Data
  - Một cờ: 1 byte, cho biết vùng nhớ có basket hay không
  - Data của Basket: có chiều dài được định nghĩa header của Flash

Mỗi Basket sẽ được lưu trong với một kích thước cố định được quy định bởi chiều dài tối đa và có cấu trúc dữ liệu như sau:

```
typedef struct {
  char id[BASKET_ID_LEN];
  uint8 len;
  Product prods[MAX_PRODS];
}Basket;
```

Trong mỗi Basket chứa một số sản phẩm nhất định (do giới hạn bộ nhớ của thiết bị) và cấu trúc dữ liệu của sản phẩm như sau:

```
typedef struct Product{
  uint8 id[PRODS_ID_LEN];
  uint8  num;
}Product;
```

Toàn bộ ứng dụng trên Handheld được hiện thực trong một task của OSAL. Sử dụng cơ chế tạo event trong OSAL của Z-stack để gửi sự kiện đến task này cho việc xử lý. Có 2 nhánh sự kiện chính cho 2 luồng dữ liệu:

- Sự kiện có dữ liệu từ Scanner
- Sự kiện từ mạng ZigBee, Z-stack

3.4 Ứng dụng trên PC (personal computer)

3.4.1 Nguyên tắc hoạt động

Yêu cầu chung :

- Ngôn ngữ lập trình : Java. Thiết kế giao diện sử dụng thư viện SWING , AWT của Java.

- Chương trình có chức năng nhận các gói dữ liệu từ Cashier thông qua giao tiếp COM , tiến hành xử lý và xuất kết quả về thông tin sản phẩm, giá tiền, … cho khách hàng.

- Chương trình sử dụng file excel chứa thông tin của hàng hóa , và thông tin gói sản phẩm thành tiền.

Mụcđíchchínhcủa PC application :

- Chương trình được hiện thực để giả lập một chương trình tính tiền trong siêu thị.

- Chương trình có mục đích demo cho hệ thống hardware bên dưới, nên các vấn đề về cơ sở dữ liệu đượ chiện thực ở mức giả lập, khi đưa vào thự ctế, phải xây dựng lại cơ sở dữ liệu.

Cácgóidữ liệu :

Định nghĩa dữ liệu ra và vào theo như Bảng 3-1

- Dữ liệuvào:

- Góidữ liệuthôngthường (Packet A): là góidữ liệuchứacácthôngsố củagiỏ hàng:

  + Ký tự nhậndạng.

  + Địa chỉ MAC của handle gửiđến.

  + Địnhdạngchiềudàicủa mã góidữ liệuvà mã sảnphẩm .

  + Mã góidữ liệu, số lượngloạisảnphẩm.

  + [Mã sảnphẩm] , [số lượngsảnphẩm].

- Góidữ liệuthêmvàohoặcbớtracácsảnphẩmtronggiỏ hàng (Packet B) :

  + Ký tự nhậndạng.

  + Mã sảnphẩm.

- Góidữ liệuchứathông tin cậpnhậttrạngtháimạnghiệntại (Packet C):

  + Ký tự nhậndạng.

  + Địa chỉ MAC của handle

  + Địa chỉ SHORT của handle.

  + Địa chỉ PARENT của handle.

- Góidữ liệubáolỗitừ hệ thống (Packet D):

  + Ký tự nhậndạng.

  + Mã lỗi.

- Dữ liệu ra:

- Góidữ liệuyêucầucậpnhậttrạngtháimạnghiệntại (Packet E):

  + Ký tự nhậndạng.

- Góidữ liệuyêucầuxóagóidữ liệuđã xử lý xong ở handle (Packet F):

  + Ký tự nhậndạng.

+ Mã gói dữ liệu đã xử lý xong.

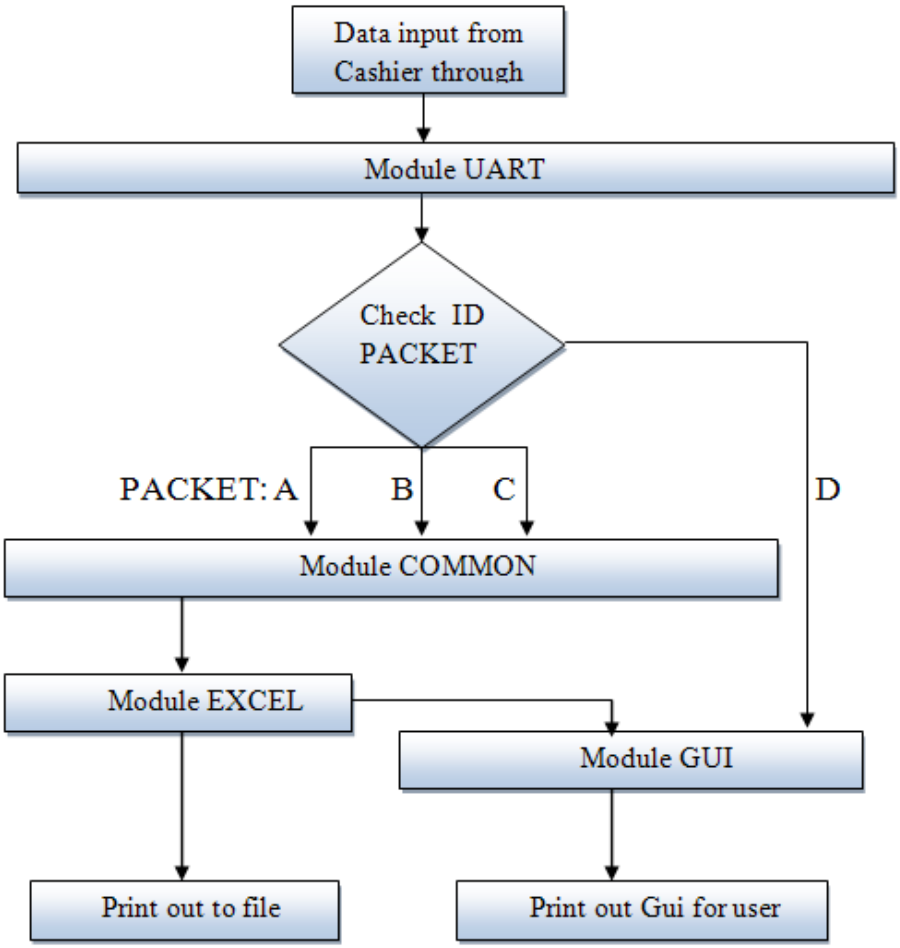
3.4.2 Hiện thực

Cấu trúc chương trình gồm các khối sau:

- UART: các hàm thực hiện việc kết nối, đọc, ghi dữ liệu từ COM.
- EXCEL: các hàm thực hiện việc đọc, ghi, tạo file excel.
- COMMON: các hàm xử lý dữ liệu vào và trả về dữ liệu cho người dùng.
- GUI: Xử lý giao diện để xuất ra cho người dùng xem.

Quá trình thực hiện chương trình:

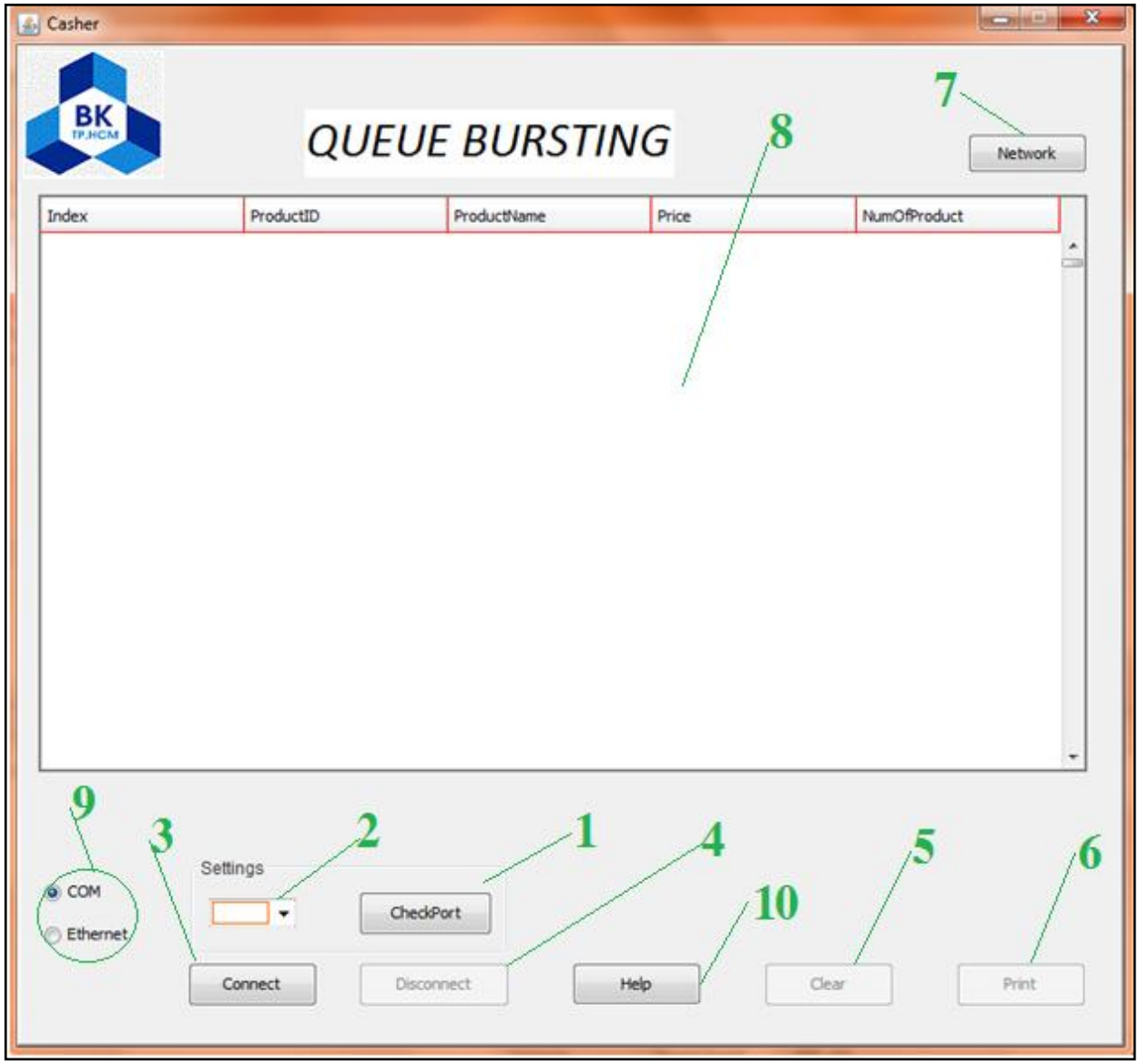
- Khi người user quét 1 mã vạch, sẽ tùy vào từng trường hợp mà gói dữ liệu được gửi lên PC như thế nào. Phân biệt các gói bằng các ID đã được định nghĩa ở trên.
- Nếu gói nhận được là gói hàng thông thường (A, B, C) thì dữ liệu sẽ được đưa qua module COMMON để xử lý và xuất ra màn hình, phần sau sẽ trình bày rõ hơn.
- Nếu gói nhận được là gói thông báo lỗi hệ thống (D) thì sẽ xuất hiện thông báo người dùng và lỗi đó sẽ được lưu xuống log.txt.
- Sau mỗi lần nhận xong, chương trình sẽ gửi 1 mã lệnh xuống hardware yêu cầu xóa gói dữ liệu mà hardware đã lưu trước đó.



Hình 3-19: Sơ đồ hiện thực ứng dụng trên PC

3.4.3 Giới thiệu ứng dụng PC

Giao diện chính của chương trình demo như hình :



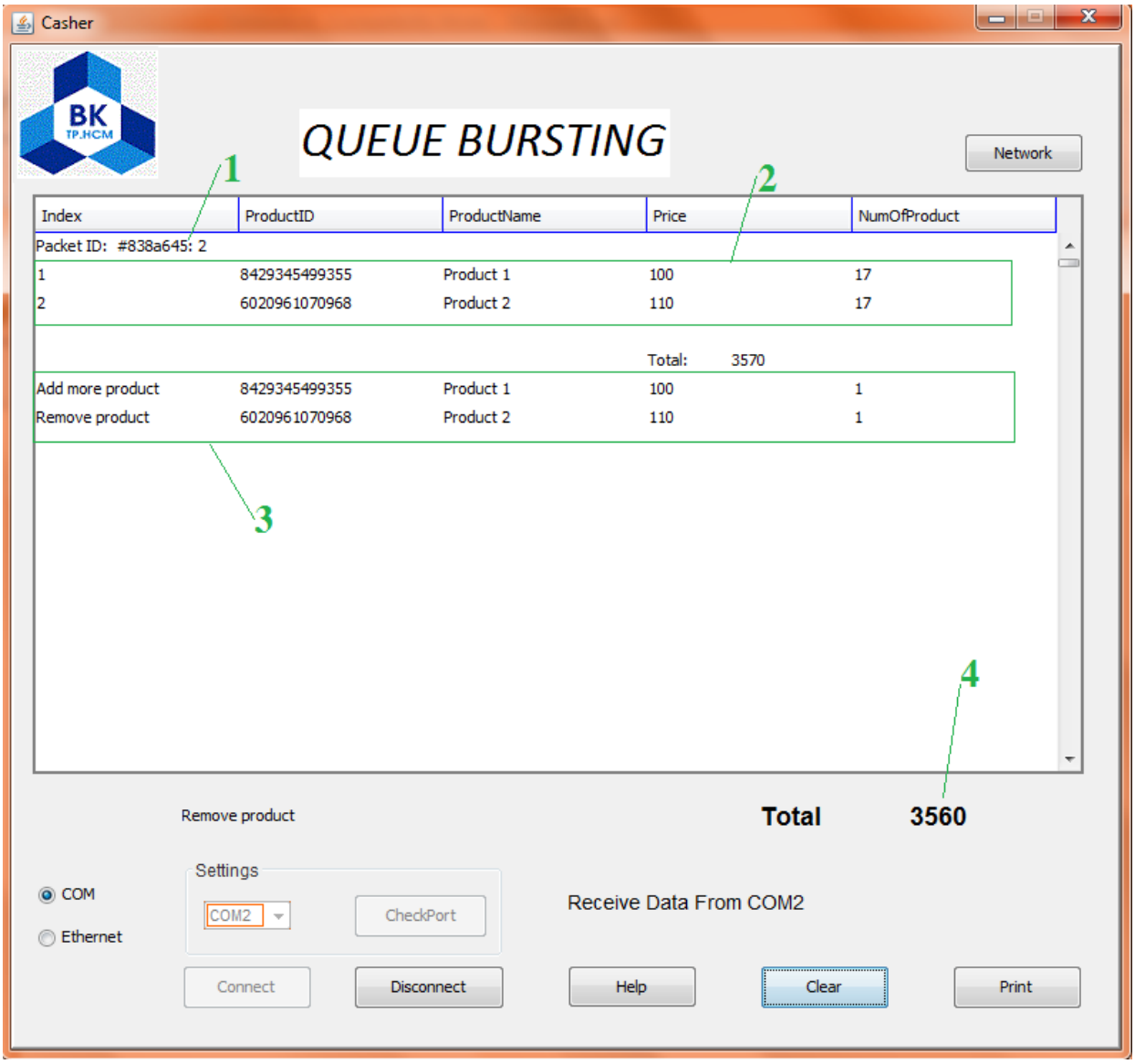
Hình 3-20: Giao diện chính của chương trình demo

Giải thích giao diện chính của chương trình demo:

- (1): buton "CheckPort" : có chức năng quét hết các COM port trên máy xác định xem trên máy PC có các COM port nào để người dùng sử dụng kết nối với cashier.
- (2): "Choice" : những COM port trên máy sẽ được liệt kê ở khung này, người dùng sẽ chọn COM port muốn kết nối ở đây.
- (3): button "Connect" : có chức năng yêu cầu kết nối với COM port đã được chọn.
- (4): button "Disconnect": có chức năng yêu cầu hủy kết nối với COM port.
- (5): button "Clear": có chức năng clear vùng (8) sau khi đã hoàn thành việc thanh toán với 1 khách hàng.

- (6): button "Print": giả lập chức năng in hóa đơn. Thông tin giao dịch sẽ được lưu xuống 1 file excel.
- (7): button "Network": có chức năng xem các handle có trong hệ thống.
- (8): Vùng xuất hiện các thông tin hàng hóa.
- (9): Cho phép chọn loại kết nối với handle, COM hay Ethernet. Nhưng hiện tại demo chỉ hiện thực kết nối thông qua COM. Có thể sử dụng để mở rộng sau này.
- (10): button "Help": hiện thông tin của demo.

Khi kết nối thành công có thể tiến hành quét gói bình thường : và thông tin của các sản phẩm trong gói sẽ được hiển thị trên giao diện chương trình



Hình 3-21: Giao diện khi thanh toán.

Giải thích giao diện khi sử dụng quét gói tính tiền :

- (1): Hiển thị packet id của khách hàng và số lượng loại sản phẩm trong gói hàng.

- (2): Thông tin chi tiết từng loại hàng : gồm ID sản phẩm, tên sản phẩm, giá trên 1 đơn vị sản phẩm, số lượng sản phẩm.
- (3): Thông tin những sản phẩm khách hàng yêu cầu thêm vào hoặc bỏ ra.
- (4): Tổng số tiền mà khách hàng phải trả cho gói hàng của mình.

Đối với mỗi khách hàng, có thể có nhiều gói hàng cùng quét, và sau khi quét hết số hàng của 1 khách hàng, người thu ngân sẽ tính tiền.

Bấm button Print để ghi xuống file và kết thúc 1 khách hàng.Thông tin gói hàng sẽ được lưu xuống 1 file excel định dạng nhưHình 3-22 :

#838a645				
Index	**IDProduct**	**NameProduct**	**PRICE**	**NumOfProduct**
1	8429345499355	Product 1	100	17
2	6020961070968	Product 2	110	17
	Total	2 Product	3570	
Add more product				
Index	**IDProduct**	**NameProduct**	**PRICE**	**NumOfProduct**
1	8429345499355	Product 1	100	1
	Total	1 Product	100	
Remove product				
Index	**IDProduct**	**NameProduct**	**PRICE**	**NumOfProduct**
1	6020961070968	Product 2	110	1
	Total	1 Product	110	
	Total	4 Product	3780	

Hình 3-22: Định dạng file excel thể hiện hóa đơn tính tiền

Những thông tin trên màn hình chính lúc thanh toán sẽ được lưu xuống file excel đầy đủ, và tên file sẽ là thời gian thanh toán và packet ID để dễ đối chiếu, kiểm tra.

Bảng 3-4: Thông tin về các thiết bị handheld trong mạng ZigBee

Index	MacAdd	ShortAdd	ParentAdd	ID
1	01-0A-0B-01-0B-05	0F-0F	0E-0E	A2ER

Để kiểm tra các handheld hiện tại trong hệ thống, nhấn button Network trong màn hình chính. Các thiết bị handheld khi nhận được yêu cầu xác thực thông tin, nó sẽ gửi thông tin của chính bản thân nó cho PC bao gồm: MAC address , short address, parent address. PC application sẽ nhận những thông tin này, đối chiếu cơ sở dữ liệu và xuất ra màn hình như **Error! Reference source not found.**.

Chức năng này giúp kiểm tra, phòng trường hợp handle hết pin, không trả về thông tin gói dữ liệu, và các vấn đề khác khi vận hành hệ thống.

Chương 4.KẾT QUẢ VÀ ĐÁNH GIÁ

4.1 Kết quả đạt được

Sau khi thực hiện đề tài, tiến hành đánh giá và thu được kết quả như sau:

- Xây dựng được một hệ thống hoàn chỉnh và vận hành đúng chức năng như yêu cầu đặt ra, không làm mất thông tin của khách hàng.
- Giảm đáng kể thời gian thanh toán.
- Dễ dàng sử dụng và bảo trì.
- Có khả năng ứng dụng cao trong thực tế.
- Có khả năng mở rộng theo nhu cầu.
- Khắc phục được một số lỗi trong quá trình hoạt động có thể gặp phải như không lấy được dữ liệu, dữ liệu trùng.
- Thể hiện được mô phỏng cách tính tiền trong siêu thị để tiến hành đánh giá ưu điểm của hệ thống.

Tóm lại, kết quả đề tài thực hiện đáp ứng được những yếu cầu cơ bản của hệ thống như đã phân tích ban đầu.

4.2 Hạn chế

Hệ thống được hiện thực có một số hạn chế như sau:

- Hệ thống kiểm tra trong điều kiện nhỏ bé (7 thiết bị) không thể đánh giá hết khả năng của hệ thống và nhược điểm khi triển khai thực tế.
- Việc kiểm tra hệ thống chưa đầy đủ, mới chỉ kiểm tra trong điều kiện bình thường, quy mô, số lượng nhỏ, chưa kiểm định với số lượng khách hàng lớn.
- Hệ thống sử dụng phần cứng có sẵn, cụ thể bộ Kit DK CC2530, chưa thiết kế và hiện thực phần cứng riêng.
- Bảo mật của hệ thống còn hạn chế.

Do đó, hệ thống cần được phát triển và kiểm tra trong các điện kiện khác nhau để thể hiện được ưu điểm và khả năng ứng dụng trong tương lai.

4.3 Hướng phát triển

Trong quá trình phát triển, thiếu sót trong quá trình đánh giá giải pháp nên mô hình có thể hoạt động tốt trong hệ thống vừa. Nhưng nếu hệ thống lớn thì phải có một số cải tiến và nhóm đã có giải pháp cho vấn đề băng thông và tốc độ xử lý. Đó là xây dựng một số data center để backup dữ liệu để cải thiện hiệu suất và băng thông hệ thống, giảm thiểu lỗi ngoài ý muốn xảy ra (hết Pin, môi trường truyền bị nhiễu cao).

Tương lai có thể tinh giản một số chức năng không cần thiết ZigBee stack, giảm thiểu thời gian xử lý để cải thiện tốc độ truyền. Bởi, ZigBee sinh ra để dùng trong các hệ thống điều khiển

không giây mà thời gian thiết bị rảnh rỗi lớn nhằm đáp ứng được thời gian sử dụng Pin lâu dài (hàng năm) của thiết bị ZigBee.

Xây dựng gateway kết nối thiết bị ZigBee với mạng Ethernet để nhiều thiết bị có thể truy xuất vào mạng ZigBee chỉ thông qua gateway này. Như vậy, có thể mở rộng số lượng ứng dụng tính tiền mà không đầu tư thêm thiết bị Cashier, và dễ dàng quản lý hệ thống.

Xây dựng thêm các phương án bảo mật thông tin cho hệ thống.

TÀI LIỆU THAM KHẢO

[1]. ZigBee specifictions ; ZigBee Alliance, http://www.zigbee.org
[2]. Z – stack CC2530-2.5.0; Texas Instrument, http://www.ti.com/tool/z-stack
[3]. Zigbee Wireless Networking ; Drew Gislason, 2008
[4]. ZigBee Wireless Networks and Transceivers; Shahin Farahani PhD, 2008
[5]. IEEE 802.15.4; http://www.ieee.org
[6]. Datasheet CC2530; Texas Instrument, http://www.ti.com/product/cc2530