BÁO CÁO KỸ THUẬT TRUYỀN SỐ LIỆU

Tìm hiểu về công nghệ Bluetooth

I, Giới thiệu về công nghệ Bluetooth:

1, Bluetooth là gì?

Bluetooth là chuẩn kết nối không dây tầm ngắn thiết kế cho các kết nối cá nhân, bằng sóng vô tuyến qua băng tần chung ISM (Industrial, Scientific, Medical) trong dãy tầng 2.40 – 2.48Ghz.

Công nghệ Bluetooth là một công nghệ dựa trên tần số vô tuyến và bất cứ một thiết bị nào có tích hợp bên trong công nghệ này đều có thể truyền thông với các thiết bị khác với một khoảng cách nhất định về cự li để đảm bảo công suất cho việc phát và nhận sóng.

Mục đích: thay thế dây cable giữa máy tính và các thiết bị điện tử lại với nhau một cách thuận lợi, giá thành rẻ.

2, Đặc điểm của công nghệ Bluetooth:

* Không cần dùng dây cáp
* Không làm ảnh hưởng sức khỏe con người
* Chi phí thấp
* Tốn ít năng lượng (0.3mAh cho chế độ chờ và tối đa 30mAh trong chế độ truyền dữ liệu).
* Không gây nhiễu cho các thiết bị không dây khác.
* Có tính tương thích cao nên được nhiều nhà sản xuất phần cứng và phần mềm hỗ trợ
* Tốc độ truyền dữ liệu có thể đạt tối đa 1Mbps
* Khoảng cách giao tiếp ngắn
* An toàn và bảo mật cao

3, Các chuẩn blutooth hiện nay:

* Chuẩn 1.0: tốc độ xấp xỉ 1Mbps nhưng gặp nhiều vấn đề về tương thích
* Bluetooth 1.1: phiên bản nâng cấp và sửa lỗi của 1.0, không có cải thiện về tốc độ đường truyền
* Bluetooth 1.2 + ERD: Tốc độ của chuẩn Bluetooth lên đến 2.1 Mbps với chế độ cải thiện kết nối truyền tải – ERD (enhanced data rate).
* Bluetooth 2.0 + ERD: Được công bố vào tháng 7/2007 với nhiều cải tiến như: tốc độ ổn định và truyền tải dữ liệu nhanh hơn.
* Bluetooth 2.1 + ERD: là thế hệ nâng cấp của Bluetooth 2.0. có hiệu năng cao hơn và tiết kiệm năng lượng hơn.
* Bluetooth 3.0 + HS: có tốc độ truyền dữ liệu đạt mức 24Mbps – bằng sóng BT – High Speed, tương đương chuẩn Wi-Fi thế hệ đầu tiên, phạm vi hiệu quả nhất chỉ trong vòng 10m.
* Bluetooth 4.0: Là sự kết hợp của Bluetooth 2.1 và 3.0 với ưu điểm là truyền tải dữ liệu nhanh và tiết kiệm năng lượng hơn.
* Bluetooth 5.0: được giới thiệu chính thức vào tháng 12/2016, với tốc độ nhanh gấp 2 và khoảng cách xa gấp 4 lần so với chuẩn 4.0. Tuy nhiên rất ít thiết bị tích hợp được phiên bản này, và nó vẫn chưa được phổ biến.

4, Ứng dụng của Buetooth:

* Truyền tải dữ liệu giữa các thiết bị
* Chia sẻ kết nối mạng qua Bluetooth
* Kết nối với các thiết bị ngoại vi
* Ứng dụng doanh nghiệp như: định vị, quét mã vạch, thiết bị y tế…
* Thay cho các điều khiển bằng tia hồng ngoại

II, Kỹ thuật truyền dữ liệu trong Bluetooth:

1, Một số thuật ngữ trong công nghệ Bluetooth:

1.1, Master Unit:

Là thiết bị duy nhất trong 1 Piconet, Master thiết lập đồng hồ đếm xung và kiểu bước nhảy (hopping) để đồng bộ tất cả các thiết bị trong cùng piconet mà nó đang quản lý, thường là thiết bị đầu tiên chuyển đổi dữ liệu, quyết định số kênh truyền thông. Mỗi Piconet có 1 kiểu hopping duy nhất.

1.2, Slaver Unit:

Là tất cả các thiết bị còn lại trong Piconet, một thiết bị không là Master thì phải là Slave. Tối đa là 7 Slaver dạng Active và 255 Slave dạng Inactive trong 1 Piconet.

Có 3 dạng Slave:

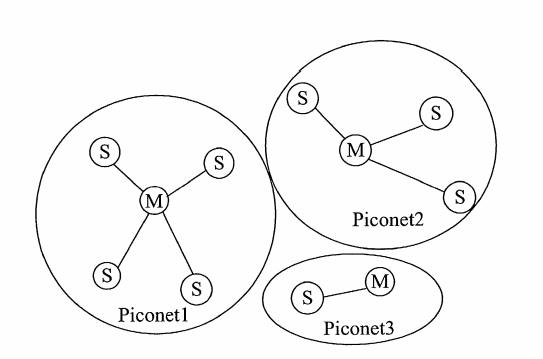
* Active: Slave hoạt động, có khả năng trao đổi thông tin với Master và các Slave Active khác.
* Standby: là một dạng inactive, Slave này không trao đổi dữ liệu, sóng radio không tác động lên, có thể coi như là những thiết bị trong nằm ngoài vùng kiểm soát của Master.
* Parked: là một dạng inactive, Slave ở trạng thái “ngủ” và sẽ được Master gọi dậy bằng tín hiệu báo hiệu.

1.3, Piconet:

Là tập hợp các thiết bị được kết nối thông qua kỹ thuật Bluetooth theo mô hình Ad-Hoc ( kiểu mạng được thiết lập cho nhu cầu truyền dữ liệu hiện hành và tức thời, tốc độ nhanh và kết nối sẽ tự động hủy sau khi truyền xong).

Trong Piconet chỉ có 1 thiết bị là Master, các thiết bị còn lại là Slave.

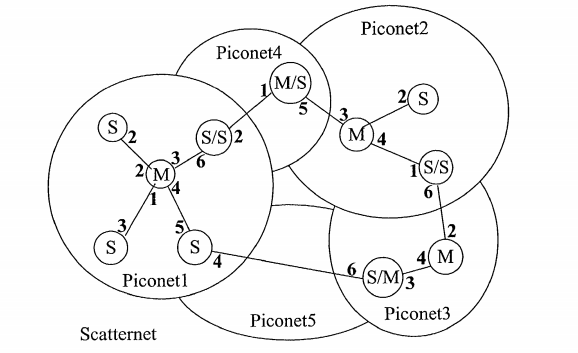
2 Slave muốn thực hiện liên lạc phải thông qua Master bởi chúng không bao giờ kết nối trực tiếp với nhau. Master sẽ đồng bộ các Slave về thời gian và tần số. Trong 1 Piconet sẽ có tối đa 7 Slave đang hoạt động tại 1 thời điểm.



Hình 1, mô hình truyền dữ liệu trong một piconet bluetooth thông thường

1.4, Scatternet:

Là 2 hay nhiều Piconet độc lập và không đồng bộ, các Piconet này kết hợp lại truyền thông với nhau.

Một thiết bị có thể vừa là Master của Piconet này vừa là Slave của Piconet khác. Vai trò của thiết bị trong Piconet không cố định, nghĩa là nó có thể thay đổi từ Master thành Slave và ngược lại.

Hình 2, mạng phân tán trong bluetooth thông thường

1.5, Kết nối theo kiểu Ad-Hoc:

Không có sự phân biệt giữa các radio units, nghĩa là không có sự phân biệt vào vị trí hay khoảng cách.

Kết nối Ad-Hoc dựa vào sự liên lạc giữa các điểm, không cần thiết bị hỗ trợ kết nỗi giữa các thiết bị di động, không cần mạch điều khiển trung tâm cho các unit dự vào để thiết lập kết nỗi. Trong Bluetooth, nó giống như một số lượng lớn các kết nối Ad-Hoc cùng tồn tại trong một vùng mà không cần bất kỳ một sự sắp xếp nào, các network độc lập cùng tồn tại chồng chéo lên nhau.

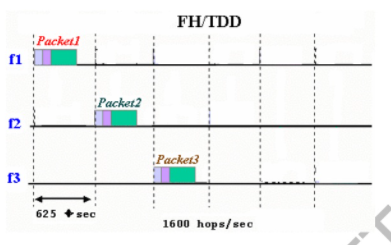
1.6, Các liên kết vật lý trong Bluetooth:

* + Asynchronous connectionless (ACL): là một kết nối point-to-multipoint giữa Master và tất cả các Slave trong Piconet
  + Synchronous connection-oriented (SCO): là kết nối point-to-point giữa 1 Master và 1 Slave trong 1 Piconet.

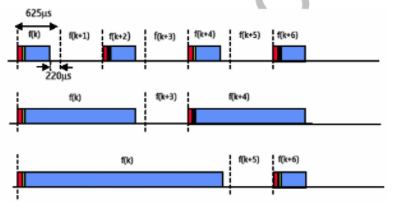
**2, Kỹ thuật truyền dữ liệu trong Bluetooth:**

2.1, Kỹ thuật nhảy tần số trong công nghệ Bluetooth:

Việc truyền dữ liệu trong Bluetooth được thực hiện bằng sử dụng kỹ thuật nhảy tần số, nghĩa là các packet được truyền trên những tần số khác nhau. Giải bằng tần ISM 2.4Ghz được chia thành 79 kênh, với tốc độ nhảy là 1600 lần trong 1 giây, điều đó có thể tránh được nhiễu tốt và chiều dài của các packet ngắn lại, tăng tốc độ truyền thông.



Hình 3 Các packet truyền trên các tần số khác nhau

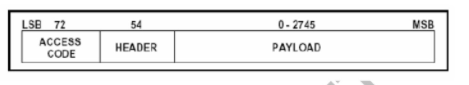


Hình 4 Các packet truyền trên khe thời gian

Việc truyền nhận sử dụng các khe thời gian. Chiều dài 1 khe thời gian thông thường là 625 micro seconds. Một packet thường nằm trong 1 khe đơn, nhưng cũng có thể mở rộng ra 3 hay 5 khe. Với các packet đa khe, yêu cầu tần số phải không đổi cho đến khi toàn bộ packet gửi xong.

Sử dụng packet đa khe, tốc độ truyền dữ liệu cao hơn hờ phần headter của một packet chỉ đòi hỏi 1 lần 220 micro second (là thời gian chuyển đổi sau mỗi packet) Có thể hiểu ngắn gọn là thời gian truyền 3 packets đơn khe sẽ lớn hơn thời gian truyền 1 packet 3-khe. Bù lại trong môi trường có nhiễu tín hiệu truyền, các packet dài chiếm nhiều timeslot dễ bị nhiễu hơn do đó dễ bị mất hơn.

Mỗi packet chứa 3 phần: Access Code (Mã Truy cập), Header, Payload.



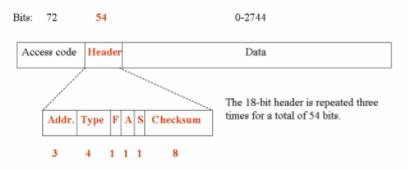
Hình 5 Cấu trúc gói tin Bluetooth

Kích thước Access Code và Header là cố định.

* Access Code: gồm 72 bits, dùng trong việc đồng bộ dữ liệu, định danh, báo hiệu
* Header: gồm 54 bits, trong đó
  + 3 bits dùng để định địa chỉ => có tối đa 7 Slave
  + 4 bits tiếp theo cho biết loại packet
  + 1 bit điều kiển luồng
  + 1 bit ARQ: cho biết packet là Broadcast không có ACK
  + 1 bit Sequencing: lọc bỏ những packet trùng do truyền lại
  + 8 bits HEC: kiểm tra tính toàn vẹn của header

Tổng cộng có 18 bits, các bit đó được mã hóa với 1/3 FEC (Forward Error Correction) để có được 54 bit.

* Payload: phần chứa dữ liệu truyền đi, có thể thay đổi từ 0 tới 2744 bit/packet. Payload có thể là dữ liệu Voice hoặc data.



Hình 6 Số lượng các bit trong 1 gói tin

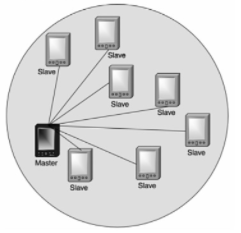
2.2, Cách thức hoạt động của Bluetooth:

2.2.1, Cơ chế truyền và sửa lỗi:

Có 3 phương pháp được sử dụng trong việc kiểm tra tính đúng đắn của dữ liệu truyền đi:

* Forward Error Correction: thêm 1 số bit kiểm tra vào phần Header hay Payload của Packet
* Automatic Repeat Request: dữ liệu sẽ được truyền lại cho tới khi bên nhận gửi thông báo là đã nhận đúng
* Cyclic Redundancy Check: mã CRC thêm vào các packet để kiểm tra chúng liệu Payload có đúng không.
* Bluetooth sử dụng FEC để sửa sai do nhiễu tự nhiên khi truyền khoảng cách xa, FEC cho phép phát hiện lỗi, biết sửa sai và truyền đi tiếp.

2.2.2, Quá trình hình thành 1 Piconet



Hình 7 Mô hình Piconet

Một piconet được tao ra bằng 4 cách:

* Có Master rồi, Master thực hiện Paging để kết nối với 1 Slave
* Một Unit (Master hay Slave) lắng nghe tín hiệu mà thiết bị của nó truy cập được.
* Khi có sự chuyển đổi vai trò giữa Master và Slave.
* Khi có một Unit chuyển sang trạng thái Active.

Để thiết lập kết nối mới, tiến trình INQUIRY hay PAGE sẽ bắt đầu. Tiến trình Inquiry sẽ cho phép 1 Unit phát hiện các Unit khác trong tầm hoạt động cùng với địa chỉ và đồng hồ của chúng.

Tiến trình Paging tạo kết nối. Kết nối chỉ thực hiện giữa những thiết bị mang địa chỉ Bluetooth. Unit nào thiết lập kết nỗi sẽ phải thực hiện tiến trình paging và tự động trở thành Master của kết nối.

Sau thủ tục Paging thì Master sẽ thăm dò Slave bằng cách gửi Packet POLL thăm dò hay packet NULL rỗng theo như Slave yêu cầu

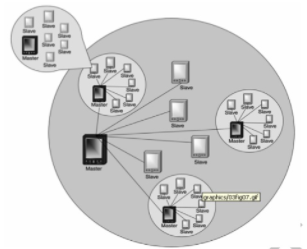
Chỉ có Master gửi tín hiệu POLL cho Slave, ngược lại thì không được.



Hình 8 Quá tình truy vấn tạo kết nối

2.2.3, Quá trình hình thành Scatternet

Một Master hay Slave của Piconet này có thể thành Slave của Piconet khác nếu bị Master của Piconet khác thực hiện tiến trình paging với nó. Có nghĩa là bất kỳ unit nào cũng có thể tạo 1 Piconet mới bằng cách paging một unit đã là thành viên của một Piconet nào đó. Ngược lại, bất kỳ unit nào tham gia trong 1 Piconet đều có thể thực hiện paging lên Master hay Slave của Piconet khác. Điều này có thể dẫn đến việc chuyển đổi vai trò giữa Master và Slave trong kết nối mới này.



Hình 9 Mô hình của 1 Scatternet

Các kết nối bên trong một Piconet được thiết lập thông qua các unit chia sẻ, unit này thuộc về 2 hay nhiều Piconet, nó dùng kỹ thuật phân chia thời gian để chuyển đổi qua lại giữa các Piconet.

**3, Vấn đề an toàn và bảo mật trong Bluetooth:**

3.1, Sơ lược về sự an toàn trong Bluetooth:

Trong công nghệ thì vấn đề an toàn tuyệt đối có lẽ không bao giờ được đảm bảo. Tuy nhiên công nghệ vẫn sẽ càng ngày càng cải tiến, phát triển nâng cao khả năng bảo mật để đảm bảo an toàn thông tin cho người sử dụng.

Bluetooth sử dụng môi trường wireless do đó nảy sinh ra những vấn đề bảo mật của wireless.Lĩnh vực này con người đang khám phá và phát triển nên những rủi ro , gây nhiễu của các tin tặc hay do tự nhiên đang là vấn đề nhức nhối.

Các nguy hiểm đặc biệt, những yếu điểm của mạng không dây và thiết bị tay cầm bao gồm:

* + Những người xấu có thể giành được quyền truy cập bất hợp pháp vào một chi nhánh mạng thông qua kĩ thuật kết nối không dây, một đường vòng đề tránh bất kì các firewall nào.
  + Những thông tin không được mã hóa ( hoặc được mã hóa với kĩ thuật đơn giản ) có thể bị đánh cắp.
  + Tấn công Dos( Denial of Service )
  + Dữ liệu quan trọng có thể bị hỏng do quá trình đồng bộ sai.
  + Kẻ xấu có thể đánh cắp được những đặc điểm nhận dạng của người dùng hợp pháp và giả mạo họ để làm những mục đích xấu.

…

**3.2, Sơ lược về bảo mật trong Bluetooth:**

Trong các thiết bị Bluetooth có 4 yếu tố để duy trì sự an toàn ở cấp độ liên kết:

* + BD\_ADDR (Bluetooth device address): một địa chỉ 48bit duy nhất dành cho mỗi thiết bị Bluetooth do IEEE (Institute of Electrical and Electronics Engineers) qui định.
  + Private authentication key: một số ngẫu nhiên dài 128bit dùng cho việc xác nhận người dùng.
  + Private Encryption key: một số dài 8-128bit dùng để mã hóa.
  + RAND: một số ngẫu nhiên hoặc giả ngẫu nhiên 128bit được thay đổi thường xuyên bởi Bluetooth.

Trong Bluetooth Generic Acess Profile, có 3 chế độ bảo mật khi truy cập Bluetooth giữa 2 thiết bị:

* + Security Mode 1: không bảo mật
  + Security Mode 2: bảo mật thi hành ở cấp độ dịch vụ
  + Security Mode 3: bảo mật thi hành ở cấp độ liên kết

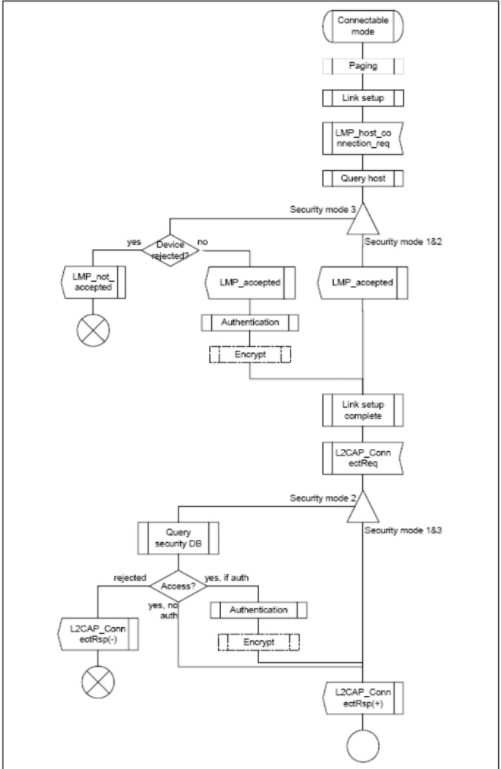
Sư khác biệt giữa mode 2 và mode 3 là ở mode 3 quy trình bảo mật được khởi động trước khi kênh truyền được thiết lập.

Thiết bị có 2 chế độ là “Trusted device” and “Untrusted device”. Một thiết bị khi kết nối với thiết bị trusted sẽ được truy cập vào mọi dịch vụ mà không bị hạn chế.

Dịch vụ có 3 mức độ:

* + Dịch vụ yêu cầu cấp phép và xác nhận
  + Dịch vụ chỉ yêu cầu xác nhận
  + Dịch vụ “mở” đối với tất cả các thiết bị

Mô hình dưới đây miêu tả quá trình thiết lập kênh truyền, khởi đầu của việc xác nhận người dùng.



*Quá trình thiết lập kênh truyền*

Khi xác nhận một thiết bị Bluetooth, nó sẽ thực hiện theo Bluetooth Link Manager Protocol và chế độ pairing hiện thời, tùy thuộc và cấp độ bảo mật được sử dụng.

**3.2.1, Security Mode 1: chế độ không bảo mật**

Ở chế độ này thiết bị sẽ không phải thực hiện bất kì qui trình bảo mật nào, hoạt động bảo mật(xác nhận, mã hóa) hoàn toàn bị bỏ qua (không gửi LMP\_au\_rand, LMP\_in\_rand hoặc LMP\_encryption\_mode\_req).

**3.2.2, Security Mode 2: chế độ bảo mật thi hành ở cấp độ dịch vụ**

Thiết bị sẽ không thực hiện bất kì biện pháp an toàn nào trước khi thiết lập kênh truyền ở cấp độ Logical link control và Adaptation Protocol (nhận được L2CAP\_ConnectReq).

Ở cấp độ này, một người quản lý bảo mật điều khiển truy cập vào dịch vụ của thiết bị.Trong cấp độ này khía niệm “authorization” cho phép thiết bị A được truy cập vào dịch vụ X hay không.

Thiết bị Bluetooth ở cấp độ này sẽ phân loại yêu cầu an toàn của dịch vụ nó sử dụng theo những đặc điểm sau:

* + Yêu cầu phân quyền (Authorization required)
  + Yêu cầu xác nhận (Authentication required)
  + Yêu cầu mã hóa (Encrytion required)

**3.2.3, Security Mode 3: bảo mật thi hành ở cấp độ liên kết**

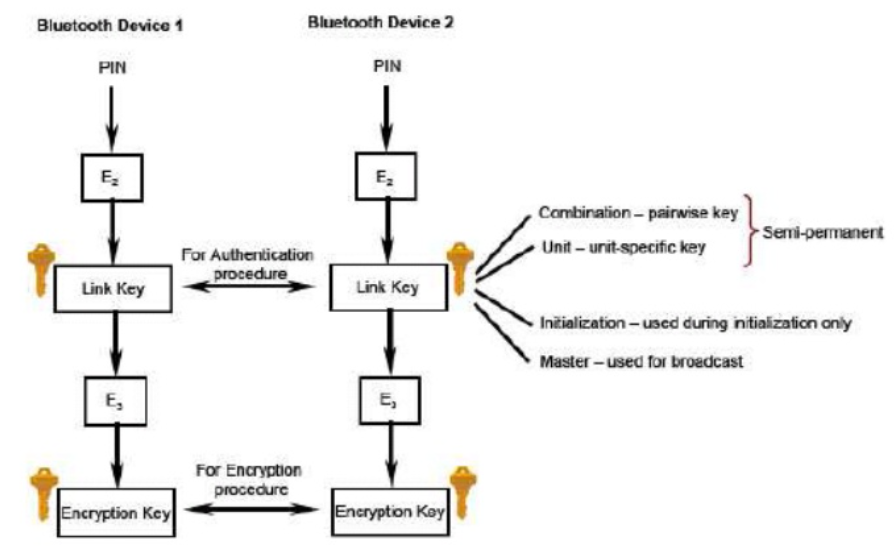
Thiết bị Bluetooth sẽ thực hiện quy trình bảo mật trước khi kênh truyền được thiết lập (nó gửi LMP\_link\_setup\_complete). Chế độ này hỗ trợ việc xác nhận đúng (authentication), một chiều hay hai chiều, và mã hóa.

Những điều này phụ thuộc vào một link key bí mật dùng giữa một cặp thiết bị. Để tạo ra key này, một quy trình pairing được thực hiện khi hai thiết bị thực hiện giao tiếp lần đầu tiên.

Ở cấp độ này, thiết bị có thể bác bỏ yêu cầu kết nối máy chủ (LMP\_host\_connection\_req, đáp lại bằng LMP\_not\_accepted ) tùy thuộc vào cài đặt của máy chủ.

**3.2.4, Tạo Bluetooth key từ số PIN**

Link key được tạo ra trong suốt quá trình khởi tạo, khi hai thiết bị Bluetooth đang liên lạc với nhau.Bằng đặc điểm kỹ thuật Bluetooth, hai thiết bị giao tiếp với nhau ngay lập tức sẽ tạo ra link key trong quá trình khởi tạo, ngay khi người dùng nhập mã PIN vào cả 2 thiết bị.Sau khi hoàn thành, các thiết bị xác nhận một cách tự động và “trong suốt”,đồng thời thực hiện mã hóa. Nó có thể tạo ra link key dùng cho phương thức trao đổi key ở tầng cao hơn và sau đó nhập link key vào Bluetooth module.



*Quá trình tạo Bluetooth key từ PIN*

Các bước trong tiến trình xác nhận trong Bluetooth (Bluetooth Authentication) diễn ra như sau:

1.Thiết bị claimant truyền địa chỉ 48bit của nó (BD\_ADDR) đến verifier

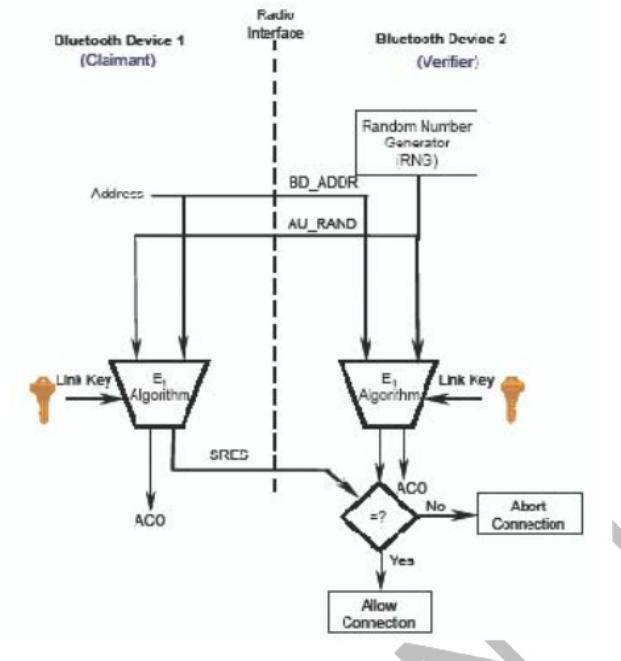
2.Thiết bị verifier truyền một cách challenge ngẫu nhiên 128 bit (AU\_RAND) đến claimant

3.Verifier dùng thuật toán E1 và sử dụng địa chỉ, link key, và challenge làm đầu vào để tính toán một câu trả lời xác nhận (authentication response). Thiết bị Claimant cũng thực hiện cùng thao tác này.

4.Thiết bị Claimant trả kết quả tính được (SRES) về cho Verifier.

5.Verifier sẽ so sánh SRES của claimant với SRES mà nó tính được.

6.Nếu hai giá trị 32 bit này bằng nhau thì Verifier sẽ tiếp tục thực hiện kết nối.



*Quá trình xác thực trong Bluetooth*

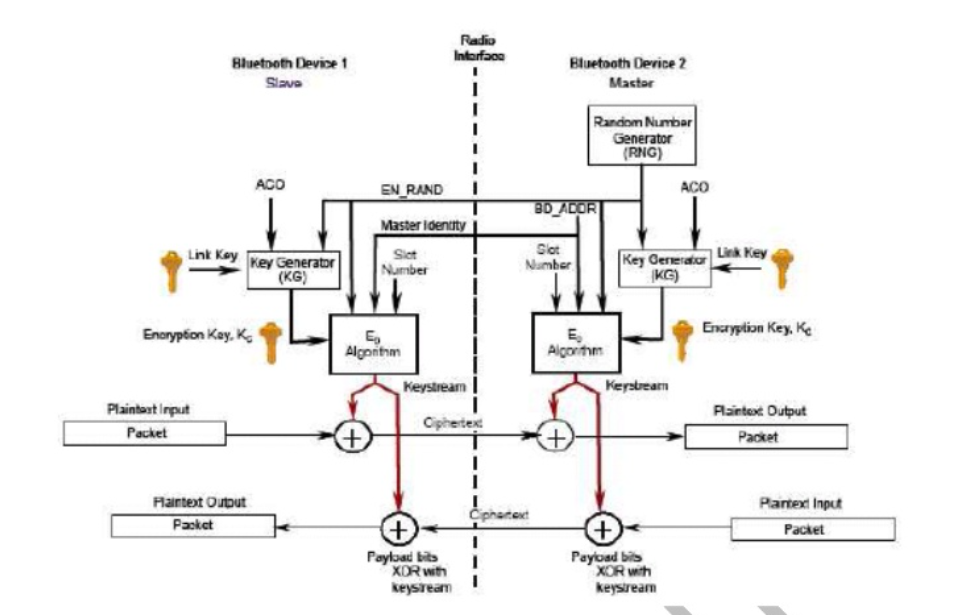
**3.2.5, Tiến trình mã hóa trong Bluetooth**

Có 3 chế độ mã hóa khác nhau để hỗ trợ cho sự an toàn của dịch vụ.

Chế độ mã hóa 1: không thực hiện mã hóa khi truyền thông

Chế độ mã hóa 2: truyền thông đại chúng (broadcast) thì không mã hóa, nhưng truyền cho cá nhân thì phải mã hóa theo link key riêng biệt.

Chế độ mã hóa 3: tất cả mọi sự truyền thông đều phải được mã hóa theo link key của master.



*Quá trình mã hóa trong Bluetooth*