

فصل

بلوتوث



❖ اهداف آموزشی

- ❖ آشنایی کلی با فناوری بلوتوث
- ❖ آشنایی با روش ایجاد شبکه به کمک بلوتوث
- ❖ آشنایی با مزایای بلوتوث
- ❖ آشنایی با سطح امنیتی فناوری بلوتوث
- ❖ آشنایی با حالت‌های مختلف دستگاه بلوتوث

▣ بلوتوث

بلوتوث در لغت به معنای دندان آبی است. این لغت برگرفته از نام هارالد بلاتاند یکی از پادشاهان دانمارکی است که در سال‌های ۹۴۰ تا ۹۸۵ پس از میلاد، در دانمارک زندگی می‌کرده است. این پادشاه دو کار بزرگ در سلطنتش انجام داد: به طور صلح‌آمیز دانمارک، سوئد و نروژ را متحد کرد و دین مسیحیت را در اسکاندیناوی رواج داد. بلاتاند به دندان آبی شهرت داشت که علت آن دقیقاً مشخص نیست. برخی منابع تاریخی علت این نام‌گذاری را علاقه زیاد این پادشاه به خوردن تمشک آبی و رنگی شدن دندان‌های او می‌دانند.

▣ مقدمه‌ای بر بلوتوث

بلوتوث یک فناوری بی‌سیم با برد کوتاه است که دستگاه‌های الکتریکی از قبیل موبایل، پرینتر، دوربین‌های دیجیتال و لپ‌تاپ‌ها را بدون سیم به هم متصل می‌کند. بلوتوث طرحی تحقیقاتی بود که شرکت اریکسون موبایل سوئد کار بر روی آن را در سال ۱۹۹۴ شروع کرد. سرپرستان این تیم اریکسون و پاپ هارتسن بودند هدف آنها ایجاد ارتباطی رادیویی و ارزان قیمت بین موبایل‌های شناخته شده توسط اریکسون و امکانات جانبی آنها نظیر هندزفری و ... بود. کار مهندسی در سال ۱۹۹۵ شروع شد و فکر اولیه فراتر از تلفن‌های همراه و گوشی‌های آنها توسعه یافت تا شامل همه انواع وسایل همراه شود. اسم بلوتوث برای این فناوری داده شده، زیرا امیدوار بودند بتواند به طور صلح‌آمیز وسایل مختلف را متحد کند.

در سال ۱۹۹۸ اریکسون یک موافقت‌نامه با IBM، اینتل، نوکیا، توشیبا و ماکروسافت امضا کرد که بر پایه این موافقت‌نامه، گروه Bluetooth special Interest Group را به وجود آورد. هدف این گروه نظارت بر پیشرفت بلوتوث و عمومی ساختن آن بود. این سیستم به صورت نقطه به نقطه و



نقطه به چند نقطه می‌تواند فعالیت کند. در مورد عملکرد نقطه به نقطه می‌توان رابطه هندزفری بی‌سیم یک موبایل به عنوان دستگاه دیوایس متحرک و خود موبایل به عنوان بیس مثال زد. در مورد نقطه به چند نقطه هم می‌توان اداره‌ای را مثال زد که در آن چند پرینتر و فقط یک دستگاه کامپیوتر رومیزی وجود دارد. در اینجا می‌توان این کامپیوتر را با استفاده از سیستم بلوتوث به چند پرینتر موجود ارتباط داد و از طریق کامپیوتر به عنوان بیس از تمام پرینترها به صورت همزمان یا جداگانه استفاده کرد. سیستم بلوتوث به وسیله امواج رادیویی به روی فرکانس ۲/۴۵ گیگاهرتز کار می‌کند و سرعت انتقال داده توسط آن ۷۲۰ کیلوبایت بر ثانیه است.

❑ مصرف باتری دستگاه بلوتوث

دستگاه بلوتوث از نظر مصرف باتری، به سه کلاس تقسیم می‌شود:

کلاس ۱) شامل دستگاههایی که طولانی‌ترین برد را دارند. بیشترین برد آنها تقریباً ۱۰۰ متر است.

کلاس ۲) برد این نوع دستگاهها متوسط است. بیشترین برد آنها ۱۰ متر است.

کلاس ۳) این دستگاهها بیش از یک متر نمی‌تواند با دستگاه ارتباط برقرار کند.

این اطلاعات در جدول زیر نشان داده شده است:

Device Power Class	Maximum Permitted Power mW(dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~ 100 meters
Class 2	2.5mW (4 dBm)	~ 10 meters
Class 3	1 mW (0 dBm)	~ 1 meter

جدول ۱ - کلاس‌های مصرف باتری بلوتوث

❑ روش ارتباطی بلوتوث

در یک شبکه دستگاهها یا در یک زمان تنها در یک جهت کار می‌کند که به آن Half Duplex Communication گفته می‌شود و یا اینکه همزمان دو جهت را تحت پوشش دارد و به Full Duplex Communication معروف است. چون Bluetooth طوری طراحی شده که بتواند در شرایط مختلف کار کند، می‌تواند هم half-Duplex و full-Duplex باشد.



□ روش اجتناب از تداخل در بلوتوث

با استفاده از بلوتوث در منازل و ادارات و اماکن عمومی احتمال تداخل امواج بالا می‌رود. اما بلوتوث به راحتی این مشکل را حل می‌کند. همان طور که گفته شد فرکانس بلوتوث ۲/۴۵ گیگاهرتز است. این فرکانس میانه است، فرکانس دقیق بلوتوث ۲/۴۰ گیگاهرتز تا ۲/۴۸ گیگاهرتز است. در این رنج فرکانس ۷۹ کانال رادیو فرکانس متفاوت وجود دارد. برای اینکه در امواج به کار رفته در دستگاه‌های بلوتوثی که در برد یکدیگر قرار دارند اختلال رادیویی ایجاد نشود، هر دستگاه در هر ثانیه ۱۶۰۰ بار این ۷۹ را به صورت شانسی انتخاب می‌کند. در این صورت اگر دو دستگاه در برد یکدیگر قرار داشته باشند و بر حسب شانس هر دو یک کانال رادیویی مشترک را انتخاب کنند، زمان اشتراک آنها به قدری کوتاه است که هیچ تداخلی باعث نمی‌شود. بنابراین بلوتوث از فناوری جهش فرکانس در طیف گسترده^۱ بهره می‌جوید که احتمال استفاده از یک فرکانس برابر در دو دستگاه را صفر می‌کند. بلوتوث می‌تواند همزمان با ۸ دستگاه ارتباط داشته باشد. به شرطی که این دستگاهها در شعاع ۱۰ متر باشند.

□ نسخه‌های بلوتوث

□ نسخه 1.0 و 1.0B

دستگاههایی که از این نسخه‌ها استفاده می‌کردند، مجبور بودند آدرس سخت‌افزاری دستگاه را در فرآیند Hand shaking دو دستگاه فاش کنند که در این صورت اصل پنهان نگه داشتن هویت دستگاه نقض می‌شد. نسخه‌های 1.0 و 1.0B بلوتوث مشکلات و نارسایی‌های متعددی داشتند و اغلب شرکت‌های تولیدکننده در برقراری ارتباط محصولاتشان با یکدیگر با مشکل مواجه می‌شدند.

□ نسخه 1.1

دستگاههایی که از نسخه 1.1 بلوتوث استفاده می‌کردند قابلیت عملکرد بیشتری داشتند.

- ❖ امکان پشتیبانی از کانال‌های بدون رمزگذاری اضافه شد؛
- ❖ نشانگر قدرت سیگنال دریافتی اضافه^۲ شد؛
- ❖ بسیاری از خطاهای موجود در 1.0b در این نسخه اصلاح شد.

1. Frequency hopping spread spectrum

2. RSSI

□ نسخه 1.2

بسیاری از دستگاههای جدید بلوتوث دار مانند جدیدترین تلفنهای همراه با نسخه جدید بلوتوث یعنی 1.2 به فروش می‌رفتند. این نسخه با نسخه 1.1 سازگاری دارد و تغییرات عمده آن به شرح زیر می‌باشند:

- سیستم تطبیقی AFH که با اجتناب از به کارگیری فرکانسهای پر استفاده باعث کاهش تداخل فرکانسهای رادیویی می‌شود؛
- افزایش سرعت انتقال؛
- اتصالات گسترده همزمان^۱؛ که با امکان ارسال مجدد بسته‌های آسیب دیده، کیفیت صدای ارتباطات صوتی را بهبود می‌بخشد؛
- پشتیبانی رابط کنترل میزبان (HCL) برای WIRE UART.3؛
- دسترسی HCI به اطلاعات زمانی ارتباطات بلوتوث.

□ نسخه 2.0

امکان دارد چندین تکنولوژی ارتباط وجود داشته باشد؛ ولی تمام آنها در حالت معمول یک هدف دارند و آن سرعت بیشتر است. این نسخه نرخ انتقال داده را تا ۳ برابر نسبت به مشخصه عمومی بلوتوث سرعت بخشید. هم چنین این نسخه اتصال چندین دستگاه به یکدیگر را ارتقاء داد. به همراه بلوتوث 2.0 به اضافه نرخ داده ارتقاء یافته، کاربران به طور کارا تر توانستند که چندین دستگاه بلوتوث را در یک زمان استفاده نمایند. در نتیجه شبکه‌های شخصی بلوتوث^۲ و پیکونت‌ها رایج‌تر شدند. در اینجا لیستی از ویژگی‌های اصلی و ارتقا یافته نسخه 2.0 آمده است.

- ☆ قابلیت سازگار بودن با نسخه‌های قبلی؛
- ☆ افزایش سرعت انتقال ۳ برابر؛
- ☆ ارتقای نرخ داده تا 3Mbps؛
- ☆ برخورداری از پروتکل‌های توزیع شده که وظیفه‌شان کنترل دستیابی به رسانه است؛
- ☆ کاهش نرخ خطای بیتی؛
- ☆ مصرف کم انرژی ناشی از کاهش یافتن چرخه‌های کاری؛
- ☆ کارایی بالاتر در حالت‌های چند ارتباطی، به دلیل پهنای باند بیشتر.

1. ESCO

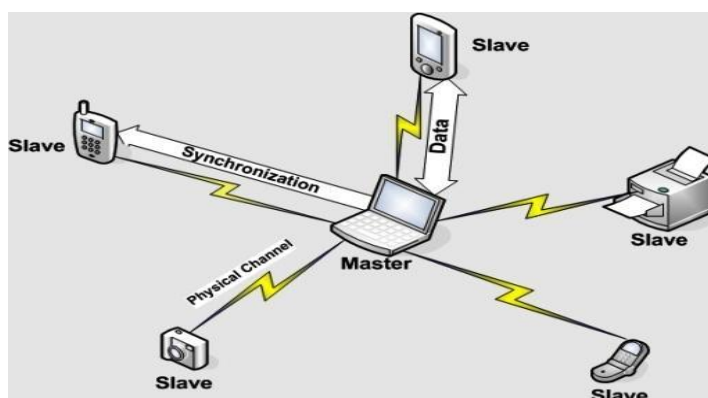
2. PAN



شکل ۳- نسخه های بلوتوث

□ ایجاد شبکه با کمک تکنولوژی بلوتوث

تکنولوژی بلوتوث به گونه ای طراحی شده است که در محیط های چند کاربره به راحتی می تواند کار کند. پس یکی از بزرگ ترین مزایای این تکنولوژی، آن است که به کمک آن می توان تجهیزات دارای بلوتوث را در یک شبکه قرار داد. ارتباطی که بلوتوث برقرار می کند یا از نوع نقطه به نقطه^۱ است و یا از نوع ارتباط نقطه به چند نقطه^۲ می باشد.



شکل ۴- ایجاد شبکه با فناوری بلوتوث

1. Point to Point
2. Point to Multi point



شبکه‌هایی که به این صورت ایجاد می‌شوند، در دو گروه قرار می‌گیرند:

❑ **Piconet**: این شبکه حداکثر حاوی هشت دستگاه می‌باشد که حداقل باید یکی از آنها Master و حداکثر هفت تای دیگر Slave باشند.

❑ **Scatternet**: حداکثر شامل ده شبکه از نوع Piconet می‌باشد.

دستگاههای یک شبکه Piconet باید تحت پوشش یک فرکانس رادیویی و با یک کانال ارتباطی مشترک، ارتباط برقرار نمایند. آدرس هر دستگاه به صورت یک آدرس ۴۸ بیتی منحصر به فرد می‌باشد که بر مبنای پروتکل IEEE 802.11 یا WLAN ایجاد شده است.

❑ مزایای بلوتوث

❑ ارتباط بی‌سیم

دستگاههایی که با سیم کار می‌کنند، از طریق رابط‌های سریال یا موازی و یا USB به کامپیوتر متصل می‌شوند. اگر از ارتباط سریال استفاده شود در هر سیکل زمانی یک بیت ارسال می‌شود و ارتباط موازی در هر سیکل ۸ تا ۱۶ بیت را ارسال می‌نماید. این مقادیر در دنیای ارتباطات پرسرعت امروزی بسیار کم است که این مشکل با امواج بلوتوث حل شده است.

❑ قیمت ارزان فناوری بلوتوث

یکی دیگر از دلایل استفاده از تراشه‌های بلوتوث قیمت بسیار مناسب آن است. این تکنولوژی از محدوده فرکانس ۲/۴۰ تا ۲/۴۸ گیگاهرتز که محدوده‌ای رایگان است استفاده می‌کند که ۷۹ کانال ارتباطی را شامل می‌شود.

❑ سرعت انتقال اطلاعات در بلوتوث

از ارتباط همزمان استفاده شود نرخ انتقال اطلاعات ۴۲۳ کیلوبایت در ثانیه خواهد بود. در این نوع ارتباط دستگاه فرستنده و گیرنده به طور همزمان قادر به دریافت و ارسال اطلاعات هستند. در نوع دیگر ارتباط که ارتباط غیر همزمان نام دارد نرخ انتقال اطلاعات ۷۲۰ کیلوبایت در ثانیه خواهد بود. البته با وجود سرعت بیشتر این ارتباط نسبت به ارتباط همزمان، قابلیت ارسال و دریافت در یک زمان را ندارد.



□ برتری بلوتوث در مقابل تکنولوژی مادون قرمز

فرستنده مادون قرمز و گیرنده آن می‌بایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، در غیر این صورت و وجود داشتن مانعی در بین راه، انتقال اطلاعات به درستی صورت نمی‌گیرد. یکی دیگر از مشکلات مادون قرمز اصطلاح «یک به یک» است. به این معنی که فقط می‌توان اطلاعات را از یک دستگاه تنها به یک دستگاه دیگر ارسال نمود و در یک لحظه قادر به ارسال اطلاعات از یک دستگاه به چند دستگاه نخواهیم بود؛ اما هر دو مشکل IR از طریق بلوتوث قابل رفع است.

□ عدم تداخل امواج بلوتوث با دیگر امواج

برای جلوگیری از تداخل اطلاعات بلوتوث از تکنیکی به نام FHSS استفاده می‌کند و این تکنیک به دستگاهها اجازه می‌دهد که در یک محدوده فرکانسی مشخص شده به صورت خودکار تغییر فرکانس داشته باشند. در واقع در این تکنولوژی یابنده کانال آزاد بیش از ۱۶۰۰ بار در ثانیه کانال‌های ارتباطی را چک می‌کند تا از کانال‌های اشغال شده با خبر باشد و در صورت ایجاد یک ارتباط جدید یک کانال آزاد را به آن ارتباط اختصاص دهد.

□ اتوماتیک بودن

دستگاههای مجهز به تراشه‌های بلوتوث به طور خودکار یکدیگر را تشخیص داده و ارتباط برقرار کرده و داده‌ها بدون دستور ما یا با دستور ما انتقال پیدا می‌کنند.

□ کم مصرف بودن

احتیاج به انرژی بسیار کم برای برقراری ارتباط با وسایل دیگر موجب صرفه‌جویی زیاد در مصرف باتری می‌شود. هر سیگنال بلوتوثی که که گوشی تلفن همراه ارسال یا دریافت می‌کند فقط ۱ میلی‌وات از باتری آن را مصرف می‌کند؛ یعنی در واقع می‌توانیم بگوییم که این فعالیت تأثیری روی باتری ندارد.

□ حالت‌های دستگاه بلوتوث

یک دستگاه بلوتوث می‌تواند در یکی از حالات زیر باشد:



□ Standby (آماده به خدمت)

هنگامی است که دستگاه روشن است ولی به پیکونت وصل نیست.

□ Inquiry (در حال جستجو)

هنگامی است که دستگاه درخواست‌هایش را برای پیدا کردن دستگاههایی که می‌تواند به آنها وصل شود می‌فرستد.

□ Page (فراخوانی)

مربوط به گره اصلی در پیکونت است و به معنی پیغام‌هایی است که دستگاه برای دعوت گروه‌های پیرو جهت اتصال به پیکونت ارسال می‌کند.

□ Connect (اتصال)

وقتی که ارتباط موفقیت‌آمیز بین گره اصلی و دستگاه جدید برقرار شود. دستگاه جدید که نقش پیرو را بازی می‌کند به حالت Connected در آمده و یک آدرس فعال دریافت می‌کند.

□ Transmit (ارسال)

حالتی است که دستگاه در حال ارسال داده خود می‌باشد. وقتی که ارسال داده تمام شد به حالت Connected در می‌آید.

□ Sniff (حالت کم مصرف دستگاه)

مربوط به گره پیرو می‌باشد و به اندازه بازه زمانی از قبل تعیین شده استراحت می‌کند. دستگاه در زمان مشخص شده برای انتقال اطلاعات بیدار می‌شود (فعال می‌شود)، سپس دوباره به حالت غیر فعال بر می‌گردد تا Sniff مشخص شده بعدی فرا برسد.

□ Hold (حالت انتظار)

حالت کم مصرف دیگری است که گره پیرو به مدت از پیش تعیین شده‌ای غیر فعال است، اگرچه در این حالت انتقال داده‌ای صورت نمی‌گیرد.



وقتی که دستگاه پیرو داده‌ای برای ارسال یا دریافت نداشته باشد ممکن است دستگاه اصلی، آن را به سمت حالت استراحت هدایت کند. وقتی که دستگاه وارد حالت استراحت می‌شود، آدرس فعال خود را در پیکونت رها می‌کند. این آدرس پس از آن به گره پیرو که گره اصلی آن را از حالت غیر فعال دوباره فعال می‌کند، اختصاص داده می‌شود.

□ امنیت بلوتوث

در این قسمت، تهدیدات امنیتی بلوتوث و روش‌های حفاظت در برابر این تهدیدات را بررسی می‌کنیم.

□ تهدیدات امنیتی مرتبط با فناوری بلوتوث

با رعایت نکات ایمنی و به کارگیری پتانسل‌های خاصی نظیر «تأیید» و یا «رمزنگاری» می‌توان یک محیط ایمن ارتباطی را ایجاد نمود که دارای شرایط ایمنی مساعدی باشد. تعداد زیادی از دستگاههایی که از بلوتوث استفاده می‌نمایند، از کدهای عددی کوچک (موسوم به Pin code) در مقابل رمزهای عبوری استفاده می‌نمایند و همین موضوع می‌تواند مشکلات امنیتی خاص خود را به دنبال داشته باشد. در صورتی که افراد غیر مجاز قادر به تشخیص و ردیابی یک دستگاه بلوتوث گردند، می‌توانند اقدام به ارسال پیام‌های ناخواسته نموده و یا حتی‌الامکان استفاده از دستگاه بلوتوث را غیر ممکن نمایند. یک مهاجم می‌تواند با استفاده از مکانیزم‌های موجود به اطلاعات موجود بر روی دستگاه مورد نظر دستیابی و حتی به آنان آسیب رساند. برخی دیگر از تهدیدات امنیتی مربوط به بلوتوث در زیر آمده است:

- ❖ استراق سمع شبکه از طریق یک دستگاه هک شده درون شبکه. شبکه‌های بلوتوث در برابر حملات منع سرویس آسیب‌پذیرند. هکرها می‌توانند به وسیله دستگاههایی که قادرند امواجی در فرکانس ۲/۴ گیگاهرتز بفرستند، ترافیک کاذب در شبکه به وجود آورند.
- ❖ حمله SNARF که مهاجمان می‌توانند اطلاعات موجود بر روی دستگاه دارای بلوتوث را سرقت کنند.
- ❖ آسیب‌پذیری کاربر مجاز شبکه توسط هکرها که می‌توانند اطلاعات را استراق نمایند و یا بلوتوث مورد نظر را از کار ببندازند.
- ❖ حمله Blue Jacking که حمله سرریز در شبکه‌های معمولی است.



□ حفاظت در مقابل تهدیدات

- ❖ اقدامات مدیریتی: مدیران شبکه‌ها با سیاست‌گذاری و وضع قوانینی، نحوه استفاده کاربران از شبکه و مسؤولیت‌های آنان را مشخص کنند.
- ❖ غیر فعال کردن بلوتوث در زمانی که از آن استفاده نمی‌گردد: صرفاً در مواردی که قصد ارسال اطلاعات از یک دستگاه به دستگاه دیگر وجود دارد، می‌بایست پتانسیل بلوتوث فعال گردد و از فعال نمودن آن در سایر موارد اجتناب گردد.
- ❖ استفاده از بلوتوث در حالت نهان: با پیکربندی دستگاه مورد نظر در حالت نهان، سایر دستگاه‌ها قادر به شناسایی دستگاه مورد نظر نخواهند بود. این موضوع باعث نمی‌گردد که دستگاه‌های بلوتوث قادر به برقراری ارتباط با یکدیگر نباشند. در چنین مواردی می‌توان دستگاه‌ها را جفت نمود. بدین ترتیب آنان می‌توانند حتی در حالت نهان نیز با یکدیگر ارتباط برقرار نمایند.
- ❖ پیکربندی درست شبکه: مدیران شبکه‌ها باید اطمینان پیدا کنند که تمام دستگاه‌ها از کد هویت شخصی برای احراز هویت استفاده می‌کنند. همچنین در لایه کاربرد حفاظت برنامه‌ها باید با کلمه عبور تأمین گردد.
- ❖ نظارت اضافی بر شبکه: بعضی برنامه‌های کاربردی تولید شده‌اند که امنیت شبکه‌های بلوتوث را کنترل می‌کنند و امنیت بیشتری را برای این شبکه‌ها فراهم می‌آورند. یکی از این برنامه‌ها Blue Watch می‌باشد که برای محیط ویندوز طراحی شده است.

□ آینده بلوتوث

- ویرایش بعدی بلوتوث LISBON نامیده شده که شامل تعدادی مشخصه است از جمله افزایش امنیت و قابلیت استفاده بیشتر از بلوتوث؛ که ویژگی‌های اصلی آن به ترتیب زیر است:
- **تغییر رمز به صورت اتوماتیک:** به طور تناوبی کدهای رمزی تغییر داده می‌شود تا امنیت افزایش یابد.
- **گسترش پاسخ به درخواست‌ها:** در طول پروسه بازبینی و درخواست، اطلاعات بیشتری جمع‌آوری شده و به دستگاه‌ها امکان فیلترینگ بهتری را جهت ارتباط می‌دهد.



○ **کاهش توان مصرفی:** سبب کاهش توان مصرفی، وقتی که وسایل در وضعیت sniff هستند، می‌شود.

○ **افزایش کیفیت سرویس:** سبب خواهد شد که وقتی ترافیک مخابراتی در یک خوشه پیکونت بالاست، داده‌های صوتی و تصویری با کیفیت بالا ارسال شوند.

○ **جفت شدن وسایل به طور ساده:** به شکل اساسی وظیفه بهبود در جفت شدن وسایل بلوتوث را به عهده دارد. به طوری که در یک زمان هم کارایی و هم امنیت افزایش می‌یابد. انتظار می‌رود که این موارد به طور قابل توجهی در استفاده از بلوتوث افزایش یابد. ویرایش بعد از SEATTLE, LISBON نامیده می‌شود و مشخصه و ویژگی‌های بیشتری را دارد که عمده آنها روی UWB متمرکز شده است. این خصیصه امکان استفاده از بلوتوث را در عرض باند بسیار بالای رادیویی موجب شده که به دنبال آن ارسال و انتقال اطلاعات داده‌ها را با سرعت بسیار بالا فراهم می‌کند.

۸ خودآزمایی فصل سوم

- ۱- تاریخچه‌ای مختصر برای فناوری بلوتوث ارائه دهید.
- ۲- حالت‌های مختلف دستگاهی که بلوتوث دارد، کدامند؟
- ۳- روش اجتناب از تداخل در فناوری بلوتوث چگونه است؟
- ۴- چند نمونه از مزایای بلوتوث را برشمارید.