# تکنولوژی بلوتوث
# کاربردها، پیچیدگی‌ها و تهدیدهای ایمنی...

تهیه و تنظیم: غلامحسن کشاورز افشار

## بلوتوث

**هر روزه مردم با تکنولوژی جدیدی روبه‌رو می‌شوند و دنیای پیچیده و پیشرفته امروزی آنها را وادار به حرکت می‌کند. اما سرعت این حرکت به قدری زیاد است که حتی متخصصان را هم به تعجب واداشته است. با ظهور هر تکنولوژی، مردم مشتاق هستند تا با آن آشنا شوند ولی بلافاصله تکنولوژی پیشرفته دیگری خلق می‌شود. یکی از این تکنولوژی‌ها، Bluetooth است که به ارتباط بی‌سیم با برد کوتاه مربوط می‌شود. این تکنولوژی در تمام قطعات، وسایل الکترونیکی و ارتباطی کاربرد دارد و استفاده از آن تنها به شبکه‌ها و اینترنت مربوط نمی‌شود، به طوری که امروزه حتی موس و کیبورد Bluetooth هم به بازار آمده است.**

■■■

فرض کنید در منزلتان از تکنولوژی Bluetooth استفاده می‌کنید و در حال چک کردن E-mail های خود از طریق تلفن همراه هستید، در همان حال نامه‌ای از دوست خود دریافت می‌کنید. شما نامه او را از طریق Bluetooth به پرینتر که به این سیستم مجهز است ارسال و یک پرینت از آن تهیه می‌کنید. در همان حال تلویزیون هم مشغول پخش برنامه‌ای است که بلافاصله تصویر را به مانیتور انتقال داده و توسط CD-Writer که به تکنولوژی Bluetooth مجهز است تصاویر را روی CD ذخیره می‌کند. اینها تنها برخی از موارد استفاده تکنولوژی Bluetooth در زندگی امروز است. تجهیزات مجهز به این تکنولوژی در کنار هم شبکه‌ای خانگی به نام PAN (Personal Area Network) را ایجاد می‌کنند.

## پیشینه نام بلوتوث

انتخاب نام بلوتوث برای این فناوری بسیار جالب است. این نام از نام یک پادشاه دانمارکی به نام «هرالد بلاتند» (Harald Blaatand) گرفته شده است. کلمه Blaatand پس از انتقال به زبان انگلیسی به شکل Bluetooth تلفظ شد که به معنی دندان آبی است. این پادشاه که بین سال‌های ۹۴۰ تا ۹۸۶ زندگی می‌کرد، توانست دانمارک و نروژ را که در جنگ‌های مذهبی با هم مشکل داشتند، متحد کند و از آن پس شهرت زیادی کسب کرد. در واقع تکنولوژی Bluetooth هم بر پایه اتحاد یکپارچه سامانه‌های کامپیوتر در قالبی بدون سامانه تأکید دارد که نماد کار و تلاش پادشاه دانمارکی است.

لوگوی بلوتوث مخفف نام هرالد بلوتوث و با ترکیبی از خطوط باستانی ژرمن‌ها است که نشان h آن به صورت نشان b تصویر شده است.

بلوتوث مجموعه‌ای از قوانین ارتباطی برای تبادل داده در فواصل کوتاه است. بلوتوث را می‌توان هم در دستگاه‌های قابل حمل (مانند تلفن همراه) و هم در دستگاه‌های ثابت به کار برد. هدف از استفاده از بلوتوث، فراهم آوردن بستری برای ارتباط چند دستگاه، صرف‌نظر از تفاوت‌های سخت‌افزاری آنان است.

این تکنولوژی از فناوری‌های رادیویی استفاده می‌کند. داده را به

**بلوتوث مجموعه‌ای از قوانین ارتباطی برای تبادل داده‌ها در فواصل کوتاه است که می‌توان در دستگاه‌های قابل حمل و دستگاه‌های ثابت به کاربرد**

قسمت‌های کوچک‌تر تقسیم می‌کند و تکه تکه به مقصد می‌فرستد. در حالت عادی سیستم ماژول کردن (تقسیم‌بندی داده به قطعات کوچک‌تر) آن براساس سیستم گاوسی است و می‌تواند تا یک مگابیت بر ثانیه اطلاعات را انتقال دهد. یکی از ویژگی‌های بلوتوث این است که صرفنظر از نوع دستگاه می‌تواند انتقال را انجام دهد و از این رو امروزه به طور عام مورد استفاده قرار می‌گیرد.

Bluetooth®

## استاندارد بلوتوث

امروزه، بسیاری از وسایل ارتباطی مانند PDA،PC،موبایل، پرینتر و... از پروتکل‌های متفاوت و ناسازگار با یکدیگر استفاده می‌کنند که همین امر باعث عدم ارتباط مناسب بین آنها خواهد شد. بنابراین شرکت‌های مربوطه تصمیم به ایجاد یک استاندارد مشترک برای انواع وسایل ارتباطی گرفتند تا ارتباط میان آنها تحت یک پروتکل ثابت و مشخص برقرار شود. در حال حاضر شرکت‌های Ericsson، Intel، IBM، Nokia و Toshiba از پدیدآورندگان و توسعه‌دهندگان این تکنولوژی هستند. این شرکت‌ها در ۲۰ می ۱۹۹۹ با تشکیل گروهی به نام Bluetooth SIG (Special Interest Group) موفق شدند استانداردهای مربوط به بلوتوث را ایجاد کنند. پیش از این استاندارد بلوتوث، نخستین‌بار توسط «ال ام اریکسون» توسعه و گسترش یافت.

بلوتوث در حال حاضر در سه کلاس عرضه می‌شود که بسته به میزان برق مصرفی گیرنده آن تا ۱ متر، ۱۰ متر و ۱۰۰ متر را پشتیبانی می‌کند. به این خاطر که بلوتوث از فناوری رادیویی استفاده می‌کند، نیازی نیست که دو دستگاه همدیگر را ببینند. از همین رو می‌توانند بسته به نوع دستگاه فرستنده، گیرنده‌شان حتی فاصله زیادی از هم داشته باشند. بلوتوث و wifi هر دو جزو فناوری‌هایی به حساب می‌آیند که توسط شرکت‌های تجاری تولید شده و استاندارد جهانی ندارند. wifi نسبت به بلوتوث می‌تواند تا برد بیشتری دستگاه‌ها را ببیند و با سرعت بیشتری انتقال داده را انجام دهد، اما سخت‌افزار پیش نیاز آن و همچنین برق مصرفی زیادی دارد. wifi و بلوتوث از یک بازه فرکانسی استفاده می‌کنند، اما روش ماژول کردنشان متفاوت است. بلوتوث به عنوان جایگزین کابل‌ها در محیط کوچک مطرح است و wifi به عنوان جایگزین برای ارتباطات بزرگ‌تر و شبکه‌های محلی. سرعت فناوری فعلی تا ۳ مگابیت بر ثانیه رسیده است. در ماژول کردن‌های استاندارد و پایه، بلوتوث از همان فناوری فرکانسی گاوسی (gfsk) استفاده می‌کند، اما در فناوری جدید خود از ترکیبی از gfsk و انتقال فازی (psk) استفاده می‌کند.

عوامل بسیاری موجب شده تا شرکت‌ها و مؤسسات ارتباطی به دنبال استفاده از Bluetooth باشند. یکی از این عوامل محدودیت در انتقال Data از طریق سیم است. دستگاه‌هایی که با سیم کار می‌کنند از طریق رابط‌های سریال یا پارالل و یا USB به کامپیوتر متصل می‌شوند. اگر از ارتباط سریال استفاده شود در هر سیکل زمانی یک بیت ارسال می‌شود و ارتباط پارالل در هر سیکل ۸ تا ۱۶ بیت را ارسال می‌کند. این مقادیر در دنیای ارتباطات پرسرعت امروزی بسیار کم است. تا چندی پیش در مقام کشورهای پیشرفته برای ارتباط اینترنت، به‌طور کامل از ارتباطات سیمی و تکنولوژی‌هایی چون ISON و DSL استفاده می‌شد. البته این سیستم‌ها هنوز هم جزو پرطرفدارترین و کاربردی‌ترین وسایل ارتباطی در جهان هستند.

قبل از طرح مسئله استفاده از Bluetooth متخصصان اعتقاد داشتند که در ارتباطات نزدیک از اشعه مادون قرمز استفاده شود. مثلاً در کنترل از راه دور تلویزیون از این سیستم استفاده می‌شود. تکنولوژی مادون قرمز IrDA نام دارد و مخفف Infrared Data Association است. در عمل ثابت شده که استفاده از این استاندارد قابل اطمینان است و هزینه بسیار کمی را دربردارد. ولی با این وجود معایبی نیز دارد. نخستین مشکل، حرکت نور در خط راست است. فرستنده مادون قرمز و گیرنده آن می‌بایست در مقابل هم قرار گیرند تا ارسال اطلاعات صورت گیرد، در غیر این صورت وجود 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 شما فقط می‌توانید اطلاعات را از یک دستگاه تنها به یک دستگاه دیگر ارسال کنید و در یک لحظه قادر به ارسال اطلاعات از یک دستگاه به چند دستگاه نخواهید بود اما هر دو مشکل IrDA از طریق Bluetooth قابل رفع است.

سرعت انتقال اطلاعات در استاندارد Bluetooth بستگی به نوع سیستم ارتباطی دارد. مثلاً اگر از ارتباط همزمان یا Synchronous 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 غیرهمزمان یا Asynchronous نام دارد نرخ انتقال اطلاعات ۷۲۱ 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. البته در تکنولوژی‌هایی مانند WiFi که بر پایه Bluetooth است، برد مؤثر و نرخ انتقال اطلاعات بیشتر می‌شود. Bluetooth از سیستم بسیار حساسی برخوردار است و از این لحاظ با استفاده از آن، احتمال تداخل بین دستگاه‌های مجهز به امواج رادیویی به حداقل می‌رسد و حتی در صورت بروز تداخل در ارتباط بلافاصله اطلاعات از بین رفته مجدداً به طور خودکار برای دستگاه گیرنده ارسال خواهد شد.

## تهدیدات امنیتی مرتبط با فناوری Bluetooth

Bluetooth مانند بسیاری از تکنولوژی‌های دیگر می‌تواند تهدیدات امنیتی خاص خود را برای استفاده کننده به دنبال داشته باشد. با رعایت نکات ایمنی و بکارگیری پتانسیل‌های خاصی نظیر «تائید» و یا «رمزنگاری» می‌توان یک محیط ایمن ارتباطی را ایجاد کرد که دارای شرایط ایمنی مساعدی باشد. متأسفانه تعداد زیادی از دستگاه‌هایی که از Bluetooth استفاده می‌کنند، از کدهای عددی کوچک (Pin code) در مقابل رمزهای عبور استفاده می‌کند و همین موضوع می‌تواند مسائل و مشکلات امنیتی خاص خود را به دنبال داشته باشد.

در صورتی که افراد غیرمجاز قادر به تشخیص و ردیابی یک دستگاه Bluetooth شدند، می‌توانند اقدام به ارسال پیام‌های ناخواسته کرده و یا حتی امکان استفاده از دستگاه Bluetooth را غیرممکن سازند. یک مهاجم می‌تواند با استفاده از مکانیزم‌های موجود به اطلاعات موجود بر روی دستگاه موردنظر دستیابی و حتی به آنان آسیب برساند. Bluesnarfing نمونه‌ای در این زمینه است که مهاجمان با استفاده از یک اتصال Bluetooth می‌توانند اطلاعات موجود بر روی یک دستگاه مجهز به تکنولوژی Bluetooth را سرقت کنند. ویروس‌ها و سایر کدهای مخرب نیز می‌توانند از فناوری Bluetooth برای آلودگی دستگاه موردنظر استفاده کنند.

هر وسیله مبتنی بر بلوتوث یک آدرس ۴۸ بیتی منحصر بفرد دارد. رویه تأیید، استفاده از کلیدهای متقارن است و رمزنگاری با کلیدی ۱۲۸ بیتی انجام می‌شود (البته در دستگاه‌های مختلف این طول کلید رمزنگاری مختلف است و بستگی به مقداری دارد که در کارخانه تعریف می‌شود). این کلید ۱۲۸ بیتی که بصورت Random انتخاب می‌شود وظیفه انجام مذاکرات امنیتی بین دستگاه‌ها را برعهده دارد.

وقتی دو سیستم مبتنی بر بلوتوث یک کانال ارتباطی بین همدیگر برقرار می‌کنند، هر دو یک کلید آغازین را ایجاد می‌کنند. برای این کار یک کلید عبور (Pass Key) یا شماره شناسایی شخصی وارد ارتباط می‌شود و کلید آغازین ساخته می‌شود و کلید پیوندی (Link Key) بر اساس کلید آغازین محاسبه می‌شود. از این به بعد کلید پیوندی برای شناسایی طرف ارتباط استفاده می‌گردد.

اولین چالش امنیتی، کلید عبور (Pass Key) است که به اختصار PIN نامیده می‌شود. مثل هر کلید دیگری، کلیدهای طولانی از کلیدهای کوتاه امن‌تر هستند. اگر هکری بتواند کلید عبور را کشف کند، می‌تواند کلیدهای آغازین ممکن را محاسبه کند و بعد از آن کلید پیوندی را بدست آورد.

## مزایای Bluetooth

عوامل بسیاری موجب شده تا شرکت‌ها و مؤسسات ارتباطی درپی استفاده از Bluetooth باشند. یکی از این عوامل محدودیت در انتقال Data از طریق سیم است.

وسایل مجهز به تراشه‌های بلوتوث حدود ۱۰ متر برد دارند و می‌توانند داده‌ها را با سرعت ۷۲۰ کیلوبایت در ثانیه از طریق دیوارها، کیف‌ها و پوشاک انتقال دهند.

هیجان انگیزتر آنکه اتصال بین وسایل بلوتوث می‌تواند بدون دخالت مستقیم ما انجام بگیرد. وقتی دو وسیله مجهز به تراشه‌های بلوتوث نزدیک یکدیگر قرار می‌گیرند، نرم‌افزار نهاده شده در تراشه‌های فرستنده / گیرنده (Server / Client) بلوتوث به طور خودکار یک ارتباط را برقرار می‌سازد و داده‌ها را منتقل می‌کند. با این همه، برد کوتاه و سرعت محدود بلوتوث باعث شده است که برای شبکه‌های محلی (LAN) بی‌سیم کمتر مرسوم می‌باشد.

## انتقال داده ها

انتقال داده‌ها در بلوتوث از یک معماری لایه‌ای پیروی می‌کند. این توصیف از سیستم بلوتوث، لایه‌های انتقال هسته‌ای بلوتوث که شامل کانال‌های L2CAP هستند را تعریف می‌کند. تمام قابلیت‌های بلوتوث از نوع معماری انتقال یکسان پیروی می‌کنند.

به منظور راندمان و بهره‌وری بالاتر، معماری انتقال اطلاعات در بلوتوث شامل زیر بخش‌های لایه‌ای منطقی می‌شود که بین پیوند منطقی و انتقال اطلاعات منطقی متمایز می‌شوند. این زیر بخش‌ها شامل درک عمومی و مشترکی از پیوند منطقی است که انتقال مستقلی را بین دو یا چند وسیله فراهم می‌کند.

## ارتباط منطقی و انتقال منطقی

تنوعی از ارتباط‌ها برای پشتیبانی انواع مختلف انتقال داده‌ها لازم است. هر ارتباط منطقی به انتقال منطقی وابسته است که تعدادی از مشخصات را داراست. این مشخصات شامل روند کنترل می‌باشد. مکانیزم تصدیق و تکرار، ترتیب شماره‌گذاری و رفتار زمانبندی. انتقال‌های منطقی می‌توانند از انواع مختلفی از اتصال‌های منطقی باشند. برای جلوگیری از تداخل اطلاعات، Bluetooth از تکنیکی به نام Spread Spectrum Frequency استفاده می‌کند که 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 ۱۵۰۰ بار در ثانیه کانال‌های ارتباطی را چک می‌کند تا از کانال‌های اشغال شده با خبر باشد و درصورت ایجاد یک ارتباط جدید یک کانال آزاد را به آن ارتباط اختصاص دهد. مثلاً اگر یک دستگاه کامپیوتر در حال ارتباط با پرینتر از طریق فرکانس 2/47GHZ باشد و در همین زمان موبایل قصد ارتباط با اسکنر را داشته باشد، با استفاده از تکنیکی که ذکر شد به طور خودکار فرکانس اشغال شده توسط کامپیوتر و پرینتر شناسایی شده و ارتباط موبایل و اسکنر به روی یک فرکانس جدید برقرار می‌شود.

## هسته حامل ترافیک

سیستم هسته بلوتوث تعدادی از حامل‌های ترافیک استاندارد را برای انتقال پروتکل سرویس و اطلاعات مورد نیاز فراهم می‌کند.

نقشه کاربرد موقعیت ترافیک در هسته حامل بلوتوث، مبتنی بر تطبیق مشخصات ترافیک با مشخصات حامل است. یک کاربرد و یا انجام سیستم بلوتوث اصلی، ممکن است استفاده از یک حامل ترافیک متفاوت یا نقشه‌کشی‌های متفاوت را انتخاب کند تا نتیجه مشابهی را

**هدف استفاده از بلوتوث فراهم آوردن بستری برای ارتباط چند دستگاه، صرف‌نظر از تفاوت‌های سخت‌افزاری آنهاست**

دریافت نماید. انواع ترافیک کاربردی برای طبقه‌بندی نوع داده‌ها که ممکن است به هسته اصلی بلوتوث ارائه شده باشد استفاده می‌شود.

## ترافیک داده‌های فرمت‌دار

سرویس‌های لایه L2CAP یک انتقال قاب‌گرا را برای داده کاربر غیرهمزمان و همزمان فراهم می‌کند. داده ارائه شده کاربردی به این سرویس در قاب‌هایی با سایزهای مختلف (بیشتر از اندازه قراردادی برای کانال) قرار داده شده و این قاب‌ها به همان روش مشابه به اجراها (کاربردهای) یکسان، روی وسیله خارجی تحویل داده می‌شوند. برنامه‌های کاربردی هیچ نیازی برای الحاق اطلاعات اضافی به داده‌های در حال انتقال ندارند. کانال‌های اتصال‌گرا (L2CAP) ممکن است برای انتقال نقطه به نقطه داده‌ها، بین دو بلوتوث فعال ایجاد شده باشند. برنامه کاربردی مناسب‌ترین نوع ارتباط منطقی از گزینه‌های موجود در باند پایه را انتخاب کرده و آن را ایجاد و پیکربندی می‌کند تا جریان داده را انتقال دهد و زمانی که پایان پذیرد آن را آزاد می‌کند.

## فرکانس BLUETOOTH

ارتباطات بلوتوث در فرکانس ۲۴۵ مگاهرتز برقرار می‌شوند که از آن در کاربردهای بین‌المللی، صنعتی، علمی و وسایل پزشکی تحت عنوان (ISM) استفاده می‌شود. شمار زیادی از سیستم‌ها، از این فرکانس رادیویی بهره می‌برند. مانند مانیتورهای کنترل‌کننده کوچک و کنترل‌هایی که مخصوص بازکردن درب پارکینگ می‌باشند. همچنین نسل جدید تلفن‌های بی‌سیمی از فرکانس‌های باند (ISM) استفاده می‌کنند. یکی از راه‌هایی که بلوتوث از ایجاد اختلال سیستم‌های دیگر پیشگیری می‌کند، فرستادن سیگنال‌های خیلی ضعیف با قدرت ۱ میلی وات است.

## حفاظت در مقابل تهدیدات

برای حفاظت در مقابل تهدیدات مرتبط با فناوری Bluetooth موارد زیر را در نظر بگیرید:

**غیرفعال کردن Bluetooth در زمانی که از آن استفاده نمی‌شود.** صرفاً در مواردی که قصد ارسال اطلاعات از یک دستگاه به دستگاه دیگر وجود دارد، می‌بایست پتانسیل Bluetooth فعال گردد و از فعال‌نمودن آن در سایر موارد اجتناب شود. با غیرفعال شدن پتانسیل فوق، امکان دستیابی افراد غیرمجاز به دستگاه موردنظر عملی نیست.

**استفاده از Bluetooth در hidden mode**: در صورتی که Bluetooth فعال شده است، اطمینان یابید که در hidden mode و نه discoverable mode پیکربندی شده است. با پیکربندی دستگاه موردنظر در hidden mode، سایر دستگاه‌ها قادر به شناسایی دستگاه موردنظر نخواهند بود. این موضوع باعث نمی‌شود که دستگاه‌های Bluetooth قادر به برقراری ارتباط با یکدیگر نباشند. در چنین مواردی می‌توان دستگاه‌ها را "pair" نمود. بدین ترتیب آنان می‌توانند حتی در hidden mode نیز با یکدیگر ارتباط برقرار نمایند. با این که دستگاه‌ها نظیر تلفن‌های موبایل و یا headset لازم است در ابتدا در discoverable mode به منظور شناسایی یکدیگر پیکربندی گردند ولی در ادامه (پس از این که "paired" شدند) می‌توانند بدون نیاز به شناسایی مجدد اتصال، با یکدیگر ارتباط برقرار نمایند.

درزمان استفاده از تکنولوژی فوق در یک محیط عمومی و در مواردی که دستگاه‌ها pair و در discoverable mode پیکربندی شده‌اند، می‌بایست نکات امنیتی را رعایت نمود. در صورت استفاده از دستگاه موردنظر در یک محیط عمومی، همواره احتمال شناسایی ارتباط، توسط افراد غیرمجاز وجود خواهد داشت.

اکثر دستگاه‌ها ویژگی‌های متعددی را به منظور تأمین طیف وسیع خواسته استفاده‌کنندگان ارائه می‌دهند. فعال نمودن برخی از ویژگی‌های ارائه شده ممکن است شما را در معرض تهدیدات بیشتری قرار دهد. در این رابطه لازم است ویژگی‌های غیرضروری و یا اتصالات Bluetooth، غیرفعال شود. همچنین پیشنهاد می‌شود تنظیمات دستگاه موردنظر بخصوص مقادیر درنظر گرفته شده در ارتباط با سیستم امنیتی دستگاه موردنظر به دقت بررسی شود. سعی کنید صرفاً گزینه‌هائی را فعال نمائید که ضمن تامین خواسته‌های موردنظر، مشکلات و تهدیدات امنیتی خاصی را به دنبال نداشته باشند.

قبل از استفاده از دستگاه پتانسیل‌های امنیتی پیش‌بینی شده را بررسی و با آگاهی کامل از آنان استفاده کنید. ویژگی‌هایی نظیر تائید و رمزنگاری، نمونه‌هائی در این زمینه می‌باشد.

منابع:

http://www.bluetooth.com
http://www.howstuffworks.com
http://www.tebyan.net
http://www.hamshahrionline.ir