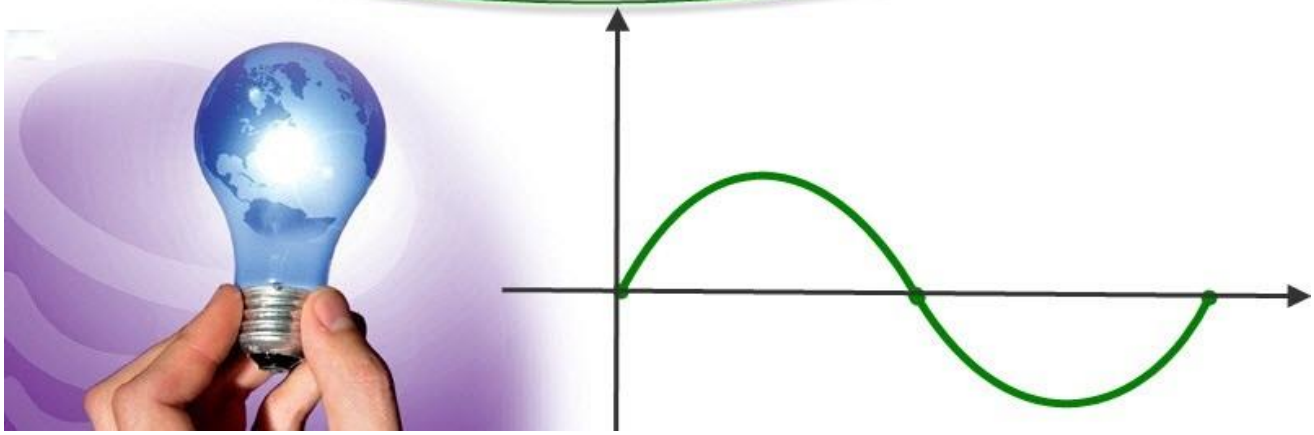
بسم الله الرحمن الرحیم



موضوع پروژه:

کنترل و هدایت از راه دور توسط SMS در سیستم موبایل

فهرست مطالب

فصل چهارم

مفهوم GPRS با رویکرد IT

فصل اول

مفاهیم مربوط به شبکه ها و اجزا آنها

مقدمه:

ا ستفاده از شبکه های کامپیوتری در چندین سال اخیر ر شد فراوانی کرده و سازمانها و مو سسات اقدام به برپایی شبکه نموده اند. هر شبکه کامپیوتری باید با توجه به شرایط و سیا ست های هر سازمان، طراحی و پیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساختهای لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می آورند؛ در صورتی که این زیر ساختها به در ستی طراحی ن شوندع در طمان ا ستفاده از شبکه مشکلات متفاوتی پیش امده و باید هزینه‌های زیادی به منظور نگهداری شبکه و تطبیق ان با خواسته های مورد نظر صرف شود.

در زمان طراحی یک شبکه سوالات متعددی مطرح می شود:

- برای طراحی یک شبکه باید از کجا شروع کرد؟
- چه پارامترهایی را براید در نظر گرفت؟
- هدف از برپاسازی شبکه چیست؟
- انتظار کاربران از شبکه چیست؟
- آیا شبکه موجود ارتقاء می یابد و یا یک شبکه از ابتدا طراحی می شود؟
- چه سرویس ها و خدماتی بر روی شبکه ارائه خواهد شد؟

به طور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری، ابتدا بید خواسته ها شناسایی و تحمل شون، مثلا در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم و این شبکه باید چه سرویس ها و خدماتی را ارائه نمایند؛ برای تامین سرویس ها و خدمات مورد نظر اکثریت کاربران، چه اقداماتی باید انجام داد؛ مسائلی چون پروتکل مورد نظر برای ا ستفاده از شبکه، سرعت شبکه و از همه مهمتر مسائل امنیتی شبکه، هر یک از اینها باید به دقت مورد برر سی قرار گیرد. سعی شده ا ست پس از ارائه تعاریف اولیه، مطالبی پیرامون کاربردهای عملی ان نیز ارائه شود تا در تصمیم گیری بهتر یاری کند.

۱- تاریخچه پیدایش شبکه

در سال ۱۹۵۷ نخستین ماهواره یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. در همین دوران رقابت سختی از نظر تسلیحاتی بین دو ابر قدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد. وزارت دفاع آمریکا در اکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیر نظامی که در امتداد دانشگاه ها بودند، تلاش برای اتصال کامپیوترها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دوتای آنها در MIT ، یکی در دانشکده کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت (ARPA net) نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز بر قرار گردید.

در سال ۱۹۷۰ شرکت معتبر زیراکس، یک مرکز تحقیقاتی در پالوآلتو تاسیس کرد. این مرکز در طول سالها مهمترین فناوری های مرتبط با کامپیوتر را معرفی کرده است و از این نظر به یک مرکز تحقیقاتی افسانه ای بدل گشته است. این مرکز تحقیقاتی که پارک (PARC) نیز نامیده می شود. به تحقیقات در زمینه شبکه های کامپیوتری پیوست، تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل کردید.

در این سال ها حرکتی غیر انتفاعی به نام MERIT که چندین دانشگاه بنیان گذار آن بودند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لاز را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر OECPOP نخستین بستر اصلی یا Backbone شبکه های کامپیوتری را ساختند. تا سال‌ها نمونه های اصلاح شده این کامپیوتر با نام PCP یا Primary Communications Processor نقش میزبان را در شبکه ها ایفا می رکد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michnet نام داشت.

در سال ۱۹۷۳ موضوع رساله دکترای آقای باب مت کالف(Bob Metcalfe) درباره مفهوم اترنت در مرکز پارک مورد آزمایش قرار گرفت. با تثبیت اترنت تعداد شبکه های کامپیوتری رو افزایش گذاشت.

روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص بر روی کامپیوتر مرکزی اجرا می شد و ارتباط کاربران را بر قرار می کرد. اما در سال ۱۹۷۶ نرم افزار جدیدی به نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می داد تا از طریق یک ترمینال به صورت تعاملی مستقیما به سیستم MERIT متصل شوند. این، نخستین باری بود که کاربران می توانستند در هنگام برقراری ارتباط از خود بپرسند: « کدام میزبان؟».

از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته‌ای یا Packet Switching است. قبل از معرفی شدن این روش از سوچینگ مداری یا Circuit Switching برای تعیین مسیر ارتباطی استفاده می شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP از مفهوم Packet switching استفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MIL net در آرپانت، همچنان از پروتکل قبلی پشتیبانی می کرد و به ارائه خدمات نظامی می پرداخت. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت. در این سال‌ها حجم ارتباطات شبکه ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد.

مسیریابی در این شبکه به کمک آدرس های IP به صورت ۳۲ بیتی انجام می گرفته است. هشت بیت اول آدرس‌ها IP به صورت تخصیص‌داده‌شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه‌ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه های LAN و شبکه های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند.

در آدرس دهی ۳۲ بیتی اولیه، بقیه۲۴ بیت آدرس به میزبان در شبکه اشاره می کرد. در سال ۱۹۸۳ سیستم نامگذاری دامنه ها (Domain Name System) به وجود آمد و اولین سرویس دهنده نامگذاری (Name server) راه اندازی شد و استفاده از نام به جای آدرس های عددی معرفی شد. در این سال تعداد میزبان های اینترنت از مرز ده هزار عدد فراتر رفته بود.

۱-۱ مدل های شبکه

در شبکه، یک کامپیوتر می تواند هم سرویس دهنده و هم سرویس گیرنده باشد. یک سرویس دهنده (Server) کامپیوتری است که فایل‌های اشتراکی و همچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بعهده دارد را نگهداری می کند.

برای آنکه سرویس گیرنده"Client" بتواند به سرویس دهنده دسترسی پیدا کند، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات در خواست شده را به سرویس گیرنده ارسال خواهد کرد.

سه مدل از شبکه‌هایی که مورد استفاده قرار می‌گیرند، عبارتند از:

۱- شبکه نظیر به نظیر"Peer-to-peer"

۲- شبکه مبتنی بر سرویس دهنده "Server-Based"

۳- شبکه سرویس دهنده/ سرویس گیرنده "Client Server"

مدل شبکه نظیر به نظیر:

در این شبکه ایستگاه ویژه‌ای جهت نگهداری فایل‌های اشتراکی و سیستم عامل شبکه وجود ندارد. هر ایستگاه می‌تواند به منابع سایر ایستگاه‌ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می‌تواند هم بعنوان Server وهم بعنوان Client عمل کند. در این مدل هر کاربرخود مسئولیت مدیریت‌و ارتقاءدادن نرم‌افزارهای ایستگاه خود را بعهده دارد. از آنجایی که یک ایستگاه مرکزی عملیات شبکه وجود ندارد، این مدل برای شبکه‌ای با کمتر از ۱۰ ایستگاه بکار می رود.

۱-۱-۱ مدل شبکه مبتنی بر سرویس دهنده:

در این مدل شبکه، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل‌ها و نرم افزارهای اشتراکی نظیر واژه پردازها، کامپایلرها، بانک‌های اطلاعاتی و سیستم عامل شبکه را در خود نگهداری می‌کند. یک کاربر می‌تواند به سرویس دهنده دسترسی پیدا کرده و فاسل‌های اشتراکی را از روی آن به ایستگاه خود منتقل کند.

۱-۱-۲ مدل سرویس دهنده/ سرویس گیرنده:

در این مدل یک ایستگاه در خواست انجام کارش را به سرویس دهنده ارائه می‌دهد و سرویس دهنده پس از اجرای وظیفه محوله، نتایج حاصل را به ایستگاه درخواست کننده عودت می‌دهد. در این مدل حجم اطلاعات مبادله شده شبکه، در مقایسه با مدل مبتنی بر سرویس دهنده کمتر است و این مدل دارای کارایی بالاتری می‌باشد.

هر شبکه اساسا از سه بخش ذیل تشکیل می‌شود:

ابزارهایی که به پیکربندی ا صلی شبکه مت صل می شوند بعنوان مثال: کامپیوترها، چاپگرها، هاب‌ها "Hubs" سیم‌ها، کابل‌ها و سایر رسانه‌هایی که برای اتصال ابزارهای شبکه استفاده می‌شوند.

۱-۲ ریخت شناسی شبکه "Net work Topology"

توپولوژی شبکه ت شریح کننده نحوه ات صال کامپیوترها در یک شبکه به یکدیگر ا ست. پارامترهای اصلی در طراحی یک شبکه، قابل اعتماد بودن و مقرون به صرفه بودن است. انواع توپولوژی‌ها در شبکه کامپیوتری عبارتند از :

۱- توپولوژی ستاره‌ای "Star" :

در این توپولوژی، کلیه کامپیوترها به یک کنترل کننده مرکزی با هاب متصل هستند. هر گاه کامپیوتری بخواهد با کامپیوتر دیگری تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ار سال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مق صد منتقل شود. اگر کامپیوتر شماره یک بخواهد اطلاعاتی را به کامپیوتر شمار ۳ بفرستد، باید اطلاعات را ابتدا به هاب ارسال کند، آنگاه هاب آن اطلاعات را به کامپیوتر شماره سه خواهد فر ستاد. نقاط ضعف این توپولوژی آن ا ست که عملیات کل شبکه به هاب واب سته ا ست. این بدان معنا ست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد.

نقاط قوت توپولوژی ستاره عبارتند از:

- ☒ نصب شبکه با این توپولوژی ساده است.
- ☒ توسعه شبکه با این توپولوژی به راحتی انجام می شود.
- ☒ اگر یکی از خطوط متصل به هاب قطع شود، فقط یک کامپیوتر از شبکه خارج می‌شود.

۱-۲-۱ توپولوژی حلوقی "Ring" :

این توپولوژی تو سط شرکت IBM اختراع شد و به همین دلیل ا ست که این توپولوژی بنام "IBM Tokenring" مشهور است.

در این توپولوژی کلیه کامپیوترها به گونه‌ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه می سازد. کامپیوتر مبدا اطلاعات را به کامپیوتری بعدی در حلقه ارسال نموده و آن کامپیوتر آدرس اطلاعات را برای خود کپی می‌کند، آنگاه اطلاعات را به کامپیوتر بعدی در حلقه منتقل خواهد کرد و به

همین ترتیب این روند ادامه پیدا می‌کند تا اطلاعات به کامپیوتر مبدا می‌رسد. سپس کامپیوتر مبدا این اطلاعات را از روی حلقه حذف می‌کند. نقاط ضعف توپولوژی فوق عبارتند از:

- ☒ اگر یک کامپیوتر از کار بیفتد، کل شبکه متوقف می شود.
- ☒ به سخت افزار پیچیده نیاز دارد"کارت شبکه آن گران قیمت است".
- ☒ برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توپولوژی فوق عبارتند از:

- ☒ نصب شبکه با این توپولوژی ساده است.
- ☒ توسعه شبکه با این توپولوژی به راحتی انجام می‌شود.
- ☒ در این توپولوژی از کابل فیبر نوری می‌توان استفاده کرد.

۱-۲-۲ توپولوژی اتوبوسی "BUS" :

در یک شبکه خطی چندین کامپیوتر به یک کابل بنام اتوبو سی متصل می شوند. در این توپولوژی، رسانه انتقال بین کلیه کامپیوترها مشترک است. یکی از مشهورترین قوانین نظارت بر خطوط ارتباطی در شبکه‌های محلی اترنت استو توپولوژی اتوبوس از متداولترین توپولوژی‌هایی است که در شبکه محلی مورد استفاده قرار می گیرد. سادگی، کم هزینه بودن و توسعه آسان این شبکه، از نقاط قوت توپولوژی اتوبوسی می‌باشد. نقطه ضعف عمده این شبکه آن است که اگر کابل اصلی که بعنوان پل ارتباطی بین کامپیوترهای شبکه می‌باشد قطع شود، کل شبکه از کار خواهد افتاد.

۱-۲-۳ توپولوژی "Mesh" :

در این توپولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می‌شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوترها ارتباطی مجزا دارد. بنابراین، این توپولوژی دارای بالاترین درجه امنیت و اطمینان می‌باشد. اگر یک کابل ارتباطی در این توپولوژی قطع شود، شبکه همچنان فعال باقی می‌ماند. ار نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصا زمانی که تعداد ایستگاه‌ها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مقرون به صرفه نیست. برای مثال، در یک شبکه با صد ایستگاه کاری، ایستگاه شماره یک نیازمند به نود و نه می‌باشد. تعداد کابل‌های مورد نیاز در این توپولوژی با رابطه N(N-1)/2 محاسبه می شود که در آن N تعداد ایستگاه‌های شبکه می‌باشد.

۱-۲-۴ توپولوژی درختی "Tree"

این توپولوژی از یک یا چند هاب فعال یا تکرار کننده برای اتصال ایستگاه‌ها استفاده می‌کند. هاب مهمترین عنصر شبکه مبتنی بر توپولوژی درختی است: زیرا کلیه ایستگاه‌ها را به یکدیگر متصل می‌کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار و تقویت آن اطلاعات و سپس ارسال آنها به ایستگاه دیگر می‌باشد.

۱-۲-۵ توپولوژی ترکیبی "Hybrid" :

این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام استخوان بندی "bone Back" به یکدیگر مرتبط شده‌اند. هر شبکه تو سط یک پل ارتباطی "Bridg" به کابل استخوان بندی متصل می‌شود.

پروتکل برای برقراری ارتباط بین رایانه‌های سرویس گیرنده و سرویس دهنده قوانین کامپیوتری برای انتقال و دریافت داده مشخص شده‌اند که به قرار داد یا پروتکل مو سومند. این قرار دادها و قوانین به صورت نرم افزاری در سیستم برای ایجاد ارتباط ایفای نقش می‌کنند. پروتکل با قرارداد، در واقع زبان مشترک کامپیوتری است که برای درک و فهم رایانه بهنگام درخواست و جواب متقابل استفاده می شود. پروتکل تعیین کننده مشخصه‌های شبکه، روش دستر سی و انواع فیزیکی توپولوژی‌ها، سرعت انتقال داده‌ها و انواع کابل کشی است.

۱-۳ پروتکل‌های شبکه:

ما در این دستنامه تنها دو تا از مهمترین پروتکل‌های شبکه را معرفی می‌کنیم:

پروتکل کنترل انتقال/ پروتکل اینترنت

"Protocol/InternetProtocol TCP/IP=Transmission control"

پروتکل فوق شامل چهار سطح است که عبارتند از :

الف- سطح لایه کاربرد "Application"

ب- سطح انتقال "Transporter"

ج- سطح اینترنت "Internet"

د- سطح شبکه "Net work"

از مهمترین و مشهورترین پروتکل‌های مورد استفاده در شبکه اینترنت است این بسته نرم افزاری به اشـــکال مختلف برای کامپیوترها و برنامه‌های مختلف ارائه می‌گردد. Tcp /ip از مهمترین پروتکل‌های ارتباطی شـبکه در جهان تلقی می‌شـود و نه تنها بر روی اینترنت و شـبکه‌های گسـترده گوناگون کاربرد دارد، بلکه در شبکه‌های محلی مختلف نیز مورد استفاده قرار می‌گیرد و در واقع این پروتکل زبان مشترک بین کامپیوترها به هنگام ارسال و دریافت اطلاعات یا داده می باشد. این پروتکل به دلیل سادگی مفاهیمی که در خود دارد اصطلاحا به سیستم باز مشهور است، بر روی هر کامپیوتر و ابررایانه قابل طراحی و پیاده سـازی اسـت. از فاکتورهای مهم که این پروتکل بعنوان یک پروتکل ارتباطی جهانی مطرح می گردد، به موارد زیر می توان اشاره کرد:

۱- این پروتکل در چارچوب UNIX Operating System ساخته شده و توسط اینترنت بکار گرفته می‌شود.

۲- بر روی هر کامپیوتر قابل پیاده سازی می‌باشد.

۳- بصورت حرفه ای در شبکه‌های محلی و گسترده مورد استفاده قرار می‌گیرد.

۴- پیشتیبانی از مجموعه برنامه‌ها و پروتکل های استاندارد دیگر چون پروتکل انتقال فایل "FTP" و پروتکل دو سویه "Point to point Protocol=PPP".

بنیاد و اسـاس پروتکل Tcp/ip آن اسـت که برای دریافت و ارسـال داده‌ها یا پیام پروتکل مذکور؛ پیام‌ها و داده ها را به بسته های کوچکتر و قابل حمل‌تر تبدیل می کند، سپس این بسته ها به مقصد انتقال داده می شود و در نهایت پیوند این بسته ها به یکدیگر که شکل اولیه پیام ها و داده ها را بخود می‌گیرد، صـورت می‌گیرد. یکی دیگر از ویژگی های مهم این پروتکل قابلیت اطمینان آن در انتقال پیام هاسـت، یعنی این قابلیت که به برر سی و بازبینی بسته ها و محا سبه بسته های دریافت شده دارد. در ضمن این پروتکل فقط برای ا ستفاده در شبکه اینترنت نمی با شد. بسیاری از سازمان و شرکت ها برای ساخت و زیر بنای شبکه خصوصی خود که از اینترنت جدا می باشد نیز در این پروتکل استفاده می کنند.

پروتکل سیستم ورودی و خروجی پایه شبکه "System=Net work basic input/ output Bios" وا سطه یا رابطی ا ست که تو سط IBM بعنوان ا ستانداردی برای د ستر سی به شبکه تو سعه یافت. این پروتکل داده‌ها را از لایه بالاترین دریافت کرده و آنها را به شبکه منتقل می کند. سیستم عاملی که با این پروتکل ارتباط برقرار می‌کند سیستم عامل "NOS" نامیده می شود کامپیوترها از طریق کارت شبکه خود

به شبه متصل می شوند. کارت شبکه به سیستم عامل ویژه‌ای برای ارسال اطلاعات نیاز دارد. این سیستم عامل ویژه را Net BIOS می‌نامند که در حافظه ROM کارت شبکه ذخیره شده است.

BIOS Net همچنین رو شی را برای د ستر سی به شبکه ها با پروتکل‌های مختلف مهیا می‌کند. این پروتکل از سخت افزار شبکه مستقل است. این پروتکل مجموعه‌ای از فرامین لازم برای درخواست خدمات شبکه‌ای سطح پایین را برای برنامه‌های کاربردی فراهم می‌کند تا جلسات لازم برای انتقال اطلاعات در بین گره‌های یک شبکه را هدایت کنند.

در حال حاضر وجود "Net BIOS Net BEUI =Net BIOS Enhansed User Interface" امتیازی جدید می‌دهد که این امتیاز در واقع ایجاد انتقال ا ستاندراد ا ست و Net BEUI در شبکه‌های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده‌ها را نیز را دارد. اما چون یک پروتکل غیر قابل هدایت است به شبکه های محلی محدود شده است.

۱-۴ مدل OSI Open System Interconnection :

این مدل‌مبتنی بر قراردادی است که‌ساز مان اسـتا ندارد های جهانی ایزو بعنوان مرحله‌ای ازاستانداردسازی قرار دادهای لایه های مختلف توسعه دارد. نام این مدل مرجع به این دلیل ا.اس.آی است چونکه با اتصال سیستم‌های باز سرو کار دارد و سیستم‌هایی هستند که برای ارتباط با سیستم‌های دیگر باز هستند. این مدل هفت لایه دارد که اصولی که منر به ایجاد این لایه ها شده اند عبارتند از :

۱- وقتی نیاز به سطوح مختلف از انتزاع است، لایه‌ای باید ایجاد شود.

۲- هر لایه باید وظیفه مشخصی داشته باشد.

۳- وظیفه هر لایه باید با در نظر گرفت قراردادهای استاندارد جهانی انتخاب گردد.

۴- مرزهای لایه باید برای کمینه کردن جریان اطلاعات از طریق رابط‌ها انتخاب شوند.

اکنون هفت لایه را به نوبت از لایه پایین مورد بحث قرار می‌دهیم:

۱- لایه فیزیکی :

به انتقال بیتهای خام بر روی کانال ارتباطی مربوط می‌شود. در اینجا مدل طراحی با رابط های مکانیکی، الکتریکی، و رسانه انتقال فیزیکی که زیر لایه فیزیکی قرار دارند سروکار دارد.

۲- لایه پیوندها:

مبین نوع فرمت‌هاســـت مثلا شـــروع فریم، پایان فریم، اندازه فریم و روش انتقال فریم. وظایف این لایه شامل موارد زیر است:

مدیریت فریم‌ها، خطایابی و ارســـال مجدد فریم‌ها، ایجاد تمایز بین فریم‌ها داده و کنترل و ایجاد هماهنگی بین کامپیوتر ارســـال کننده و دریافت کننده داده‌ها، پروتکل های معروف برای این لایه عبارتند از:

الف- پروتکل SDLC که برای مبادله اطلاعات بین کامپیوترها بکار می رود و اطلاعات را به شـــکل فریم سازماندهی می کند.

ب- پروتکل HDLC که کنترل ارتباط داده‌ای سطح بالا زیر نظر آن ا ست و هدف از طراحی آن این است که با هر نوع ایستگاهی کارکند از جمله ایستگاههای اولیه، ثانویه و ترکیبی.

۳- لایه شبکه:

وظیفه این لایه، مسـیریابی‌می‌باشـد، این مسـیریابی عبارتسـت از: تعیین مسـیر متناسـب برای انتقال اطلاعات. لایه شبکه آدرس منطقی هر فریم را بررسی می‌کند و آن فریم را بر اساس جدول مسیریابی به مسـیریاب بعدی می‌فرسـتد. لایه شـبکه مسـئولیت ترجمه هر آدرس منطقی به یک آدرس فیزیکی را بر عهده دارد. پس می توان گفت برقراری رتباط یا قطع آن، مولتی پلکس کردن از مهمترین وظایف این لایه است. از نمونه بارز خدمات این لایه، پست الکترونیکی است.

۴- لایه انتقال:

وظیفه ارســـال مطمئن یک فریم به مقصـــد را بر عهده دارد. لایه انتقال پس از ارســـال یک فریم به مقصد، منتظر می‌ماند تا سیگنالی از مقصد مبنی بر دریافت آن فریم دریافت کند. در صورتی که لایه محل در منبع سیگنال مذکور را از مقصد دریافت نکند. مجددا اقدام به ارسال همان فریم به مقصد خواهد کرد.

۵- لایه اجلاس:

وظیفه برقراری یک ارتباط منطقی بین نرم افزارهای دو کامپیوتری که به یکدیگر متصـــل هســـتند به عهده این لایه ا ست. وقتی که یک ایستگاه بخواهد به یک سرویس دهنده متصل شد، سرویس دهنده فرایند برقراری ارتباط را بررسی می کند، سپس از ایستگاه، درخوا ست نام کاربر، و رمز عبور را خواهد کرد. این فرایند نمونه ای از یک اجلاس می باشد.

۶- لایه نمایش:

این لایه اطلاعات را از لایه کاربرد دریافت نموده، آنها را به شکل قابل فهم برای کامپیوتر مقصد تبدیل می کند. این لایه برای انجام این فرایند اطلاعات را به کدهای ASCII و یا Unicode تبدیل می کند.

۷- لایه کاربرد:

این لایه امکان دسترسی کاربران شبکه را با استفاده از نرم افزارهایی چون E-mail و .... فراهم می سازد.

۱-۵ مفاهیم مربوط به ارسال سیگنال و پهنای باند

پهنای باند(Bandwidth) به تفاوت بین بالاترین و پایین ترین فرکانس سهایی که یک سیستم ارتباطی می‌تواند ارسال کند، گفته می شود. به عبارت دیگر منظور از پهنای باند مقدار اطلاعاتی است که می توان در یک مدت زمان معین ارسال شود. برای وسایل دیجیتال، پهنای باند بر حسب بیت در ثانیه و یا بایت در ثانیه بیان می شود. برای وسایل آنالوگ، پهنای باند، بر حسب سیکل در ثانیه بیان می شود.

دو روش برای ارسال اطلاعات از طریق رسانه های انتقالی وجود دارد که عبارتند از: روش ارسال باند پایه (Baseband) و روش ارسال باند پهن (Broadband).

در یک شبکه LAN ، کابلی که کامپیوترها را به هم وصل می کند، فقط می تواند در یک زمان یک سیگنال را از خود عبور دهد، به این شبکه یک شبکه Baseband می گوئیم. به منظور عملی ساختن این روش و امکان استفاده از آن برای همه کامپیوترها، داده‌ای که توسط هر سیستم انتقال می‌یابد، به واحدهای جداگانه ای به نام packet شکسته می شود. در واقع در کابل یک شبکه LAN، توالی packet های تولید شده توسط سیستم های مختلف را شاهد هستیم که به سوی مقاصد گوناگونی در حرکت‌اند .

۱-۶ عملکرد یک شبکه packet-switching

برای مثال وقتی کامپیوتر شما یک پیام پست الکترونیکی را انتقال می دهدع این پیام به packet های متعددی شکسته می شود و کامپیوتر هر packet را جداگانه انتقال می دهد. کامپیوتر دیگری در شبکه که بخواهد به انتقال داده بپردازد نیز در یک زمان یک packet را ارسال می کند. وقتی تمام packet هایی که بر روی هم یک انتقال خاص را تشکیل می دهند، به مقصد خد می رسند، کامپیوتر دریافت کننده انها را به شکل پیام الکترونیکی اولیه بر روی هم می چیند. این روش پایه و اساس شبکه‌های packet-Switching می باشد.

در مقابل روش Base band ، روش Broadband قرار دارد. در روش اخیر، در یک زمان و در یک کابل، چندین سیگنال حمل می شوند. از مثالهای شبکه Broadband که ما هر روز از آن استفاده می کنیم، شبکه تلویزیون است. در این حالت فقط یک کابل به منزل کاربران کشیده می شود، اما همان یک کابل، سیگنالهای مربوط به کانالهای متعدد تلویزیون را بطور همزمان حمل می نماید. از روش Broadband به طور روز افزونی در شبکه های WAN استفاده می شود.

از آنجائی که در شبکه های LAN در یک زمان از یک سیگنال پشتیبانی می شود، در یک لحظه داده ها تنها در یک جهت حرکت می کنند. به این ارتباط half-duplex گفته می شود. در مقابل به سیستم هایی که می توانند به طور همزمان در دو جهت با هم ارتباط بر قرار کنند half-duplex گفته می شود. مثالی از این نوع ارتباط شبکه تلفن می باشد. شبکه های LAN با داشتن تجهیزاتی خاص بصورت half-duplex عمل کنند.

فصل دوم

شبکه های بی سیم با نگاهی به Wi –Fi -Bluetooths

مقدمه:

از آنجا که شبکه های بی سیم، در دنیای کنونی هر چه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال‌های رادیویی اند، مهمترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است.

نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آنها که به مدد پیکربندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت، تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط امواج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان می دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی سیم بازه ی وسیعی از کاربردها، از ساختارهای پیچیده‌ایی چون شبکه های بی سیم سلولی –که اغلب برای تلفن های همراه استفاده می شود– و شبکه های محلی بی‌سیم (WLAN-Wireless LAN) گرفته تا انواع ساده‌ای چون هدفون های بی سیم، را شامل می شوند.

از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می کنند مانند صفحه کلیدها، ماوس ها و برخی از گوشی های همراه، در این دسته بندی جای می‌گیرند. طبیعی ترین مزیت استفاده از این شبکه های عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و همچنین امکان ایجاد تغییر در ساختار مجازی آنها ست. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردند: WWAN ، WLAN و WPAN .

مقصود از WWAN ، که مخفف Wireless WAN است، شبکه هایی با پوشش بی سیم بالا ست. نمونه ایی از این شبکه ها، ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می کند. کاربرد شبکه های WPAN یا Wireless Personal Area Network برای موارد خانگی است. ارتباطی چون Bluetooth و مادون قرمز در این دسته قرار می گیرند.

شبکه های WPAN از سوی دیگر در دسته ی شبکه های Ad Hoc نیز قرار می گیرند. در شبکه های Ad hoc ، یک سخت افزار، به محض ورود به فضای تحت پو شش آن، به صورت پویا به شبکه ا ضافه می‌شـــود. مثالی از این نوع شـــبکه ها، Bluetooth اســـت. در این نوع، تجهیزات مختلفی از جمله کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گو شی تلفن همرا، در صورت قرار گرفتن در محیط تحت پوشش، وارد شبکه شده‌و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند.

تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی سیم(WLAN) در ساختار مجازی آنهاست. به عبارت دیگر، ساختار مجازی شبکه های محلی بی سیم بر پایه‌ی طرحی ایستا ست در حالی که شبکه های Ad hoc از هر نظر پویا هستند. طبیعی است که در کنار مزایایی که این پویایی برای استفاده کنندگان فراهم می کند، حفظ امنیت چنین شبکه هایی نیز با م شکلات ب سیاری همراه ا ست. با این وجود، عملا یکی از راه حل های موجود برای افزایش امنیت در این شـــبکه ها، خصـــوصـــا در انواعی همچون Bluetooth ، کا ستن از شعاع پو شش سیگنال های شبکه ا ست. در واقع مستقل از این حقیقت که عمل کرد Bluetooth بر ا ساس فر ستنده و گیرنده های کم توان ا ستوار ا ست و از این مزیت در حقیقت که عمل کرد.

Bluetooth بر ا ساس فر ستنده و گیرنده های کم توان ا ستوار ا ست و این مزیت در کامپیوترهای جیبی برتری قابل توجه ای محســـوب می گردد، همین کمی توان ســـخت افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پو شش ا ست که در برر سی امنیتی نیز مزیت محسوب می گردد. به عبارت دیگر این مزیت به همراه استفاده از کدهای رمز نه چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه ها به حساب می‌آیند.

۲-۱ مشخصات و خصوصیات WLAN

تکنولوژی و صـــنعت WLAN به اوایل دهه ی ۸۰ میلادی باز می گردد. مانند هر تکنولوژی دیگری، پیشـــرفت شـــبکه های محلی بی ســـیم به کندی صـــورت می پذیرفت. با ارائه‌ی اســـتاندارد IEEE b□□□□□□ ، که پهنای باند نسبتا بالایی را برای شبکه های محلی امکان پذیر می ساخت، استفاده از این تکنولوژی وســـعت بیشـــتری یافت. درحال حاضـــر، مقصـــود از WLAN تمامی پروتکل‌هاو استانداردهای‌خانواده‌ی□□□□□□ IEEE است.

۲-۲ همبندی های ۱۱ ، ۸۰۲

در یک تقسیم بندی کلی می توان دو همبندی (توپولوژی) را برای شبکه های محلی بی سیم در نظر گرفت. ساده‌ترین همبندی، فی البداهه (Ad hoc) و برا ساس فرهنگ واژگان ا ستاندارد ۱۱ ، ۸۰۲ ، IBSS ا ست. در این همبندی ایستگاه ها از طریق ر سانه بی سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده(تبادل پیام) از تجهیزات یا ایستگاه واسطی ا ستفاده نمی کنند. واضح ا ست که در این همبندی به سبب محدودیت های فا صله هر ایستگاهی ضرورتا نمی تواند با تمام ایستگاه های دیگر در تماس با شد. به این ترتیب شرط اتصال م ستقیم در همبندی IBSS آن ا ست که ایستگاه ها در محدوده عملیاتی بی سیم یا همان برد شبکه بی سیم قرار داشته باشند.

۲-۲-۱ همبندی IBSS

همبندی دیگر زیر ساختار است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسی ایستگاه های موجود در یک مجموعه سرویس را به سیستم توزیع متصل می‌کند. در این همبندی تمام ایستگاه ها با نقطه دسترسی تماس می گیرند و اتصال مستقیم بین ایستگاه ها وجود ندارد در واقع نقطه دسترسی وظیفه دارد فریم ها(قاب های داده) را بین ایستگاه ها توزیع و پخش کند.

۲-۲-۲ همبندی زیر ساختار در دو گونه BSS و ESS

در این همبندی سیستم رسانه ای است که از طریق آن نقطه دسترسی(AP) با سایر نقاط دسترسی در تماس ا ست و از طریق ان می توان فریم ها را به سایر ایستگاه ها ار سال نماید. از سوی دیگر می تواند بسته ها را دراختیار ایستگاه های متصل به شبکه سیمی نیز قرار دهد. در ا ستاندارد ۱۱ ، ۸۰۲ تو صیف ویژه ای بای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین می کند که سیستم توزیع می بایست ارائه نماید. بنابراین سیستم توزیع می‌تواند یک شبکه ۳ ، ۸۰۲ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می‌کند.

ا ستاندارد ۱۱ ، ۸۰۲ با ا ستفاده از همبندی خا صی محدوده عملیاتی شبکه را گسترش می دهد. این همبندی به شکل مجموعه سرویس گسترش یافته (ESS) برپا می شود. در این روش یک مجموعه گسترده و متشکل از چندین BSS یا مجموعه سرویس پایه از طریق دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه های سرویس پایه مبادله شده و انتقال پیام ها شکل می گیرد.

در این همبندی ایســـتگاه ها می توانند در محدوده عملیاتی بزرگتری گردش نایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می شود.

در واقع سیستم توزیع ستون فقرات شبکه های محلی بی سیم است و می تواند با استفاده از فناوری بی سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه د سترسی به عنوان یک لایه عملیاتی ساده ا ست که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مق صدش می با شد. نکته قابل توجه در این همبندی آن ا ست که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه های سیار داخل ESS را صرفنظر از پویایی و تحرکشـــان به صـــورت یک شـــبکه منفرد در ســـطح لایه MAC تلقی می کنند. به این ترتیب پروتکل های رایج شبکه های کامپیوتری کوچکترین تاثیری از سیار بودن ای ستگاه ها و ر سانه بی سیم نمی پذیرند. جدول ۲-۱ همبندی های رایج در شبکه های بی سیم مبتنی بر ۱۱ ، ۸۰۲ را به اختصار جمع بندی می کند.

802.11 Topologies		
Independent Basic Service Set (IBSS) ("Ad Hoc 'or' Pee; to Peer"	Infrastructure	
	Basic Service Set (BSS)	Extended Service Set (ESS)

جدول ۲-۱- همبندیهای رایج در استاندارد ۱۱ و ۸۰۲

معماری معمول در شبکه های محلی بی سیم بر مبنای ا ستفاده از AP ا ست. با نصب یکAP ، عملا مرزهای یک سلول مشخص می شود و با روش هایی می توان یک سخت افزار مجهز به امکان ارتباط بر ا ساس ا ستاندار ۱۱ ، ۸۰۲ b را میان سلول های مختلف حرکت داد. گ ستره ای که یک AP پو شش می دهد را BSS-Basic Service set می نامند. مجموعه‌ی تمامی ســـلول های یک ســـاختار کلی شـــبکه، که ترکیبی از BSS هایی شبکه را ست، را ESS-Extended Service Set می نامند. با ا ستفاده از ESS می توان گستره‌ی وسیع تری را تحت پوشش شبکه‌ی محلی بی سیم درآورد.

در سمت هر یک از سخت افزارها که معمولا مخدوم ه ستند، کارت شبکه یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می کند. AP علاوه بر ارتباط با چند کارت شبکه ی بی سیم، به ب ستر پر سرعت‌تر شبکه‌ی سیمی مجموعه نیز مت صل ا ست و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی سیم و شبکه اصلی برقرار می شود.

همان گونه که گفته شد، اغلب شبکه های محلی بی سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز مو سوم ا ست، پیاده سازی می شوند. با این وجود نوع دیگری از شبکه های محلی بی سیم نیز وجود دارند که از همان منطق نقطه به نقطه ا ستفاده می کنند. در این شبکه ها که عموما Ad Hoc نامیده می شوند یک نقطه ی مرکزی برای دسترسی وجود ندارد و سخت افزارهای همراه مانند کامپیوترهای کیفی و جیبی یا گوش های موبایل با ورود به محدوده ی تحت پو شش این شبکه، به دیگر تجهیزات م شابه مت صل می‌گردند. این شبکه‌ها به ب ستر شبکه‌ی سیمی مت صل نی ستند و به همین منظور IBSS(Independent Basic Service Set) نیز خوانده می شوند.

شبکه های Ad hoc از سویی م شابه شبکه های محلی درون دفتر کار ه ستند که در انها نیازی به تعریف و پیکربندی یک سیستم رایانه ای به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می توانند پرونده های مورد نظر خود را با دیگر گره ها به اشتراک بگذارند.

به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر ا ستانداردها، لایه د ستر سی به ر سانه (MAC) در استاندارد ۱۱ ، ۸۰۲ می بایست از دید لایه های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیار بودن ایستگاه های کاری را به گونه ای شفاف پوشش دهد که از دید لایه های بالاتر استاندارد این سیار بودن احساس نشود. این نکته سبب می شود که لایه MAC در این ا ستاندارد وظایفی را بر عهد ه بگیرد که معمولا تو سط لایه های بالاتر شبکه انجام می شوند. در واقع این ا ستاندارد لایه های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می کند و به طور مشخص لایه فیزیکی جدید از فرکانس های رادیویی به عنوان ر سانه انتقال بهره می برد.

۲-۳ لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می دهد. اول انکه رابطی برای تبادل فریم های لایه MAC جهت ارسال و دریافت داده ها فراهم می کند. دوم اینکه با استفاده از روش های ت سهیم فریم های داده را ارا سال می کند و در نهایت و ضعیت ر سانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار می دهد. سه تکنیک رادیویی مورد ا ستفاده در لایه فیزیکی این ا ستاندارد به شرح زیر می‌باشند :

- استفاده از تکنیک رادیویی DSSS
- استفاده از تکنیک رادیویی FHSS
- استفاده از امواج رادیویی مادون قرمز

در این استاندارد لایه فیزیکی می تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون PPM ۱۶- و PPM-۴ مبادله می شوند.

علاوه بر استاندارد IEEE ۸۰۲،۱۱-۱۹۹۹ دو الحاقیه IEEE ۸۰۲،۱۱a و IEEE ۸۰۲،۱۱b تغییرات و بهبودهای قابل توجهی را به استاندارد اولیه اضافه کرده است.

۲-۳-۱ دسترسی به رسانه

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تا حدودی به روش دسترسی CSMA/CD شباهت دارد. در این ایستگاه های کاری قبل از ارسال داده کانال رادیویی را کنترل می کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه یک زمان تصادفی صبر کرده و مجددا اقدام به کنترل کانال رادیویی می کنند. در روش CSMA/CA ایستگاه فرستنده ابتدا کانال فرکانسی را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد اقدام به ارسال می کند. گیرنده فلید کنترلی فریم یا همان CRC را چک می کند و سپس یک فریم تصدیق می فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجددا فریم را ارسال می کند. این عمل تا زمانی ادامه می یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم ها به تعداد آستان های مشخصی برسد که پس از آن فرستنده فریم را دور می اندازد.

در شبکه های بی سیم بر خلاف اترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

الف- پیاده سازی مکانیزم آشکارسازی تصادم به روش ارسال رادیویی دو طرفه نیاز دارد که با استفاده از آن ایستگاه سیار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می شود.

ب- در یک شبکه بی سیم، بر خلاف شبکه های سیمی، نمی توان فرض کرد که تمام ایستگاه های سیار امواج یکدیگر را دریافت می کنند. در واقع در محیط بی سیم حالاتی قابل تصور است که به انها نقاط پنهان می گوییم.

۲-۳-۱-۱ روزنه های پنهان

برای غلبه بر این مشکل، استاندارد ۸۰۲،۱۱ از تکنیکی موسوم به اجتناب از تصادم و مکانیزم تصدیق استفاده می کند. همچنین با توجه به احتمال بروز روزنه های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به شنود مجازی رسانه یا VCS استفاده می شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می فرستد. هنگامی که گیرنده این فریم را دریافت می کند، رسانه را کنترل می کند و در صورتی که رسانه آزاد باشد فریم کنترلیCTS را به نشانی فرستنده ارسال می کند.

تمام ایستگاه هایی که فریم های کنترلی RTS/CTS را دریافت می کنند وضعیت کنترل رسانه خود موسوم به شاخص NAV را تنظیم می کنند. در صورتی که سایر ایستگاه ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می کنند که مرتبا به صورت پویا تغییر می کند. به این ترتیب مشکل روزنه های پنهان حل شده و تصادم ها نیز به حداقل مقدار می‌رسند.

شعاع پوشش شبکه ی بی سیم بر اساس استاندارد ۸۰۲،۱۱ به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند:

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه بی سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹ متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵ متر (برای فضاهای باز) در استاندارد ۸۰۲،۱۱b متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال

حاضـر با توجه به گیرنده ها و فرسـتنده های نسـبتا قدرتمندی که مورد اسـتفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجو دارد که نمونه های عملی آن فراوان اند.

با این وجود شعاع کلی یی که برای استفاده از این پروتکل (۸۰۲،۱۱b) ذکر می شود چیزی میان ۵۰ تا ۱۰۰ متر است. این شعاع عملکرد مقداریست که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و می تواند مورد استناد قرار گیرد.

۲-۳-۲ پل ارتباطی

یکی از عملکردهای نقاط د ستر سی به عنوان سوییچ های بی سیمع عمل ات صال میان حوزه های بی سیم است. به عبارت دیگر با استفاده از چند سوئیچ بی سیم می‌توان عملکردهای مشابه Bridge برای شبکه‌های بی‌سیم را به دست آورد.

اتصال میان نقاط د سترسی می تواند به صورت نقطه به نقطه، برای ایجاد اتصال میان دو زیر شبکه به یکدیگر، یا به صورت نقطه ای به چند نقطه یا بالعکس برای ایجاد اتصال میان زیر شبکه های مختلف به یکدیگر به صورت همزمان صورت گیرد.

نقاط دسترسی که به عنوان پل ارتباطی میان شبکه های محلی با یکدیگر استفاده می شوند از قدرت بالاتری برای ار سال داده استفاده می کنند و این به معنای شعاع پو شش بالاتر است. این سخت افزارها معمولا برای ایجاد اتصال میان نقاط و ساختمان هایی به کار می روند که فا صله‌ی آنها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فا صله، فا صله ای متو سط بر اساس پروتکل ۸۰۲،۱۱b برای پروتکل های دیگری چون ۸۰۲،۱۱a می توان فواصل بیشتری را نیز به دست آورد.

از دیگر استفاده ی نقاط د سترسی با برد بالا می توان به امکان تو سعه شعاع پو شش شبکه های بی سیم ا شاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوش یک شبکه‌ی بی سیم، می توان از چند نقطه‌ی دسترسی بی‌سیم به صورت همزمان و پشت‌به‌پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هر یک از ساختمان‌ها، سطح پو شش شبکه را تا ساختمان‌های دیگر گسترش داد.

۲-۴ خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی های مبتنی بر سیستم توزیع را مهیا می سازد. معمولا خدمات توزیع توسط نقطه دسترسی فراهم می شوند. خدمات توزیع در این استاندارد عبارتند از:

- پیوستن به شبکه
- خروج از شبکه بی سیم
- پیوستن مجدد
- توزیع
- مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیار و نقطه دسترسی فراهم می کند. هر ایستگاه کاری قبل از ارسال داده می بایست با یک نقطه دسترسی بر روی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می دهد که فریم های ارسال شده به سمت ایستگاه سیار را به درستی در اختیارش قرار دهد. خروج از شبکه بی سیم هنگامی بکار می رود که بخواهیم اجباراً ارتباط ایستگاه سیار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس مجدد هنگامی مورد نیاز است که ایستگاه سیار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه"پیوستن به شبکه بی سیم" است با این تفاوت که در این سرویس ایستگاه سیار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است.

این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می کند که با نقطه دسترسی قبلی تماس گرفته و فریم های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیار فرستاده شده‌اند. با استفاده از سرویس‌توزیع فریم‌های لایه MAC به مقصد مورد نظر شان می‌رسند.مجتمع سازی سایر شبکه‌های محلی و یا یک یا چند شبکه محلی بی‌سیم دیگر متصل می کند. سرویس مجتمع سازی فریم های ۸۰۲،۱۱ را به فریم های ترجمه می کند که بتوانند در سایر شبکه ها(به عنوان مثال ۸۰۲،۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم های سایر شبکه ها نیز به فریم‌های سایر شبکه ها نیز به فریم‌های ۸۰۲،۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه های کاری سیار قرار می گیرند.

۲-۵ ویژگی های سیگنال های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می شود که با استفاده از آن پهنای باند سیگنال از سالی بسیار بزرگتر از پهنای باند سیگنال اطلاعات بشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می‌شـــود آن اســـت که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی های جالب توجه سیگنال های طیف گسترده نهفته است. این ویژگی های عبارتند از:

- پایین بودن توان چگالی طیف به طوری که ســـیگنال اطلاعات برای شـــنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می رسد.
- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیک پذیری و دقت بالا
- امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال ۱۹۸۵ مجوز استفاده از این سیگنال ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

۲-۵-۱ سیگنال های طیف گسترده با جهش فرکانسی

در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می کند.

۲-۵-۱-۱ تکنیک FHSS(PN-Code=Pseudo Noise Code)

در این حالت سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگتری در مقایسه با سیگنال اطلاعات انتخاب می شود. با توجه به اینکه فرکانس های pn-code با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملا تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می گوییم.

۲-۵-۱-۲ تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

بر اساس مقررات FCC و سازمان های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ۴۰۰ میلی ثانیه است که برابر با حداقل ۲/۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲،۱۱ حداقل فرکانس جهش در امریکای شمالی و اروپا ۶ مگا هرتز و در ژاپن ۵ مگا هرتز می باشد.

۲-۵-۲ سیگنال های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال بر روی باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کد به گونه ای ا ست که نویز و تداخل بر ساند. برای پخش کردن سیگنال هر بیت واحد با یک کد تسهیم می شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می گردد. در استاندارد ۸۰۲،۱۱ روش مدلاسیون مورد استفاده در سیستم های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفا ضلی تهسیم می شود. در نتیجه نیازی به فاز مرجع برای باز سازی سیگنال وجود ندارد.

از آنجا که در استاندارد ۸۰۲،۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می شوند و در گیرنده نیز یک آشکارساز تفاضلی سیگنالهای داده را دریافت می کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال های داده تغییر می کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت های داده تغییر می کند.جدول زیر ایده مدولاسیون فاز را نشان می دهد.

بیتهای فرد	بیتهای زوج	اختلاف فاز
۱	۱	$Pi/4^3$
۰	۱	$Pi/4^3$
۰	۰	Pi/4
۱	۰	Pi/4

جدول ۲-۲- مدولاسیون تفاضلی

۲-۵-۲-۱ مدولاسیون فاز

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می گیرند و چهار نماد را پدید می‌آورند. واضح است که در این روش تسهیم، دامنه سیگنال ثابت است. در روش تسهیم تفاضلی سیگنال اطلاعات با توجه به میزان اختلاف فاز و نه مقدار فاز تسهیم و مخابره می شوند. به عنوان مثال در روش pi/4-DQPSK ، چهار مقدار تغییر فاز ۳-pi/4 ، 3pi/4 ، pi/4 ، و pi/4 است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می تواند دو بیت را کد گذاری نماید.

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیما توسط یک دنبالع از کدهای شبه تصادفی تسهیم می شود. در این تکنیک نرخ بیتی شبه کد تصادفی، نرخ تراشه نامیده می شود. در استاندارد ۸۰۲،۱۱ از کدی موسوم به کد بارکر برای تولید کدها تراشه سیستم DSSS استفاده می شود. مهمترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه ان یک فیلتر تطبیقی دیجیتالی قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

کدهای باکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد ۸۰۲،۱۱ مورد استفاده قرار می گیرد، از کد بارکر با طول ۱۱ (N=11) استفاده می شود. این کد به ازاء یک نماد، شش مرتبه تغییر فاز می دهد و این بدان معنی است که سیگنال حامل نیز به ازائ هر نماد ۶ مرتبه تغییر فاز خواهد داد.

۲-۵-۲-۲ کدهای بارکر

لازم به یاداوری است که کاهش پیچیدگی سیستم ناشی از تسهیم تفاضلی DPSK به قیمت افزایش نرخ خطای بیتی به ازائ یک نرخ سیگنال به نویز ثابت و مشخص است.

۲-۵-۳ استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه های بی سیم، طراحی شبکه سلولی به گونه ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد.

۲-۵-۳-۱ سه کانال فرکانسی F1 , F2 , F3

با استفاده از یک طراحی شبکه سلولی خاص، تنها با استفاده از سه فرکانس متمایز F3,F2,F1 امکان استفاده مجدد از فرکانس فراهم شده است.

۲-۵-۳-۲ شبکه سلولی

در این طراحی به هر یک از سلول های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می رود. نکته جالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است.

۲-۵-۴ پدیده چند مسیری

در این پدیده مسیر و زمان‌بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می‌کند. پیاده سازی‌های اولیه از استاندارد ۸۰۲،۱۱b از تکنیک FHSS در لایه فیزیکی استفاده می کردند. از ویژگی های قابل توجه این‌تکنیک مقاومت قابل توجه آن در برابر پدیده مسیری است. در این تکنیک از کانالهای متعددی(۷۹ کانال) با پهنای باند نسبتا کوچک استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می دهند. این تغییر می‌دهند. این تغییر کانال هر ۴۰۰ میلی ثانیه بروز می کند لذا مشکل چند مسیری به شکل قابل ملاحظه ای منتفی می شود. زیرا گیرنده، سیگنال اصلی(که سریع تر از سایرین رسیده و عاری از تداخل است)را دریافت‌کرده و کانال فرکانسی خود را عوض می کند و سیگنال های انعکاسی زمانی به گیرنده می‌رسد که گیرنده کانال فرکانسی قبلی خود را عوض کرده و در نتیجه توسط گیرنده احساس و دریافت نمی شوند.

۲-۶-۱ مقایسه مدلهای ۸۰۲،۱۱

۲-۶-۱-۱ استاندارد ۸۰۲،۱۱b

همزمان با برپایی استاندارد IEEE۸۰۲،۱۱b یا به اختصار، ۱۱b در سال ۱۹۹۹ ، انجمن مهندسین برق الکترونیک تحول قابل توجهی در شبکه سازی های رایج و مبتنی بر اترنت ارائه کرد. این استاندارد در زیر لایه دسترسی به رسانه از پروتکل CSMA/CA سود می برد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است:

- استفاده از تفکیک رادیویی DSSS در باند فرکانسی۲/۴ GHz به همراه تکنیک کدگذاری CCK.
- استفاده از تکنیک رادیویی FHSS رد باند فرکانسی ۲/۴ GHz به همراه تکنیک کدگذاری CCK.
- استفاده از امواج رادیویی مادون قرمز

در اســـتاندارد ۸۰۲،۱۱ اولیه نرخ های ارســـال داده ۱ و۲ مگا بیت در ثانیه اســـت. در حالی که در ا ستاندارد ۸۰۲،۱۱b با ا ستفاده از تکنیک CCK و روش تسهیم QPSK نرخ ار سال داده به ۵/۵ مگابیت در ثانیه افزایش می یابد همچنین با به کارگیری تکنیک DSSS نرخ ارســـال داده به ۱۱ مگابیت در ثانیه می رسد.

به طور ســنتی این اســتاندارد از دو فناوری DSSS یا FHSS اســتفاده می کند. هر دو روش فوق برای ارسال داده با نرخ های ۱ و۲ مگابیت در ثاینه مفید هستند. جدول زیر سرعت مختلف قابل دسترسی در این استاندارد را نشان می دهد.

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC ، مخابره و ار سال فرکانس های رادیویی را کنترل می کند. این کمیســـیون باند فرکانس خاصـــی موســـوم به ISM را به محدوده۲/۴ GHz تا GHz ۲/۴۸۳۵ برای فناوری های رادیویی استاندارد IEEE ۸۰۲،۱۱ b اختصاص داده است.

Bits/Symbol	Symbol Rate	Modulation	Code Length	Data Rate
1	1SMPs	BPSK	11(Barker Sequence)	1Mbps
2	1SMPs	QPSK	11(Barker Seq)	2 Mbps
4	1.375SMPs	QPSK	8CCK	5.5Mbps
8	1.375SMPs	QPSK	8CCK	11Mbps

جدول ۲-۳- نرخهای ارسال داده در استاندارد ۸۰۲،۱۱b

۲-۶-۱-۱-۱ اثرات فاصله

فا صله از فر ستنده بر روی کارایی و گذردهی شبکه های بی سیم تاثیر قابل توجهی دارد. فوا صل رایج در اســتاندارد ۸۰۲،۱۱ با توجه به نرخ ارســال داده تغییر می کند و به طور مشــخص در پهنای باند ۱۱ Mbps این فاصــله ۳۰ تا ۴۵ متر و در پهنای باند ۵/۵ Mbps ، ۴۰ تا ۴۵ متر و در پهنای ۲Mbps، ۷۵ تا ۱۰۷ متر است. لازم به یادآری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل اســتقرار فرســتنده و گیرنده و شــرایط فیزیکی و محیطی تغییر می کنند. در اســتاندارد ۸۰۲،۱۱b پروتکلی وجود دارد که گیرنده بسته به ملزم به ارسال بسته تصدیق می نماید. توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزهای تصدیق رایج در سطح لایه انتقال (نظیر انچه در پروتکل TCP اتفاق می افتد) عمل می کند.

در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستند نرسد، فرستنده فرض می‌کند که بسته از دست رفته است و مجددا آن بسته را ارسال می کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می یابد(Fall Back) تا در نهایت به مقدار ۱ Mbps برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته ای را برای آن گیرنده ارسال نمی کند. به این ترتیب فاصله نقش مهمی در کارایی(میزان بهره وری از شبکه) و گذردهی (تعداد بسته های غیر تکراری ارسال شده در واحد زمان) ایفا می کند.

۲-۶-۱-۱-۲ پل بین شبکه ای

بر خلاف انتظار بسیاری از کارشناسان کامپیوتری، پل بین شبکه ای یا Bridging در استاندارد ۸۰۲،۱۱b پوشش داده نشده است. در پل بین شبکه ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط یک شبکه محلی با یک یا چند شبکه محلی دیگر فراهم می شود. این کاربرد به خصوص در مواردی که بخواهیم بدون صرف هزینه کابل کشی(فیبر نوری یا سیم مسی) شبکه محلی دو ساختمان را به یکدیگر متصل کنیم بسیار جذاب و مورد نیاز ی باشد. با وجود اینکه استاندارد ۸۰۲،۱۱b این کاربرد را پوشش نمی دهد ولی بسیاری از شرکت ها پیاده سازی های انحصاری از پل بی سیم را به صورت گسترش‌وتوسعه استاندارد ۸۰۲،۱۱b ارائه کرده اند. پل‌های بی‌سیم نیز توسط مقررات FCC کنترل می‌شوند و گذردهی موثر یا به عبارت دیگر توان موثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ۴ وات بیشتر باشد. بر اساس مقررات FCC توانت سیگنال های ساطع شده ر شبکه های محلی نیز نباید از ۱ وات تجاوز نماید.

۲-۶-۲ Standard ۸۰۲،۱۱ a

استاندارد ۸۰۲،۱۱a ، از باند رادیویی جدیدی برای شبکه های محلی بی سیم استفاده می کند و پهنای باند شبکه های بی سیم را تا ۵۴ Mbps افزایش می دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیون موسوم به OPDM است. نرخ های ارسال داده در استاندارد IEEE ۸۰۲،۱۱a عبارتند از: ۶،۹،۱۲،۱۸،۲۴،۳۶،۴۸،۵۴ Mbps که بر اساس استاندارد، پشتیبانی از سرعت های ۶،۱۲،۲۴ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه های محلی بی سیم، استاندارد IEEE ۸۰۲،۱۱a را نسل آینده IEEE۸۰۲،۱۱ تلقی می کنند و حتی برخی از محصولات مانند تراشه های Atheros و کارت

های شبکه PCMCIA/Card bus محصول Card Access Inc. استاندارد IEEE ۸۰۲،۱۱a را پیاده‌سازی کرده‌اند.

بدون شک این پهنای باند و سیع و نرخ داده سریع محدودیت هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد IEEE۸۰۲،۱۱a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE۸۰۲،۱۱b کاهش یابد. علاوه بر آن به سبب افزایش سربارهای پردازشی در پروتکل، تداخل، و تصحیح خطاهاع پهنای باند واقعی به مراتب کمتر از پهنای باند اسمی این استاندارد است. همچنین در بسیاری از کاربردها امکان سنجی و حتی نصب تجهیزات اضافی نیز مورد نیاز است که به تبع ان موجب افزایش قیمت زیرساختار شبکه بی سیم می شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد IEEE ۸۰۲،۱۱b بوده و به همین خاطر به نقاط دسترسی یا ایستگاه پایه بیشتری نیاز خواهیم داشت که افزایش هزینه زیرساختار را به دنبال دارد. این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می شود:

UNII-1@5.2GHz
UNII-2@5.7GHz
UNII-3@5.8GHz

یکی از تصورات غلط در زمینه استانداردهای ۸۰۲،۱۱ این باور است که ۸۰۲،۱۱a قبل از ۸۰۲،۱۱b مورد بهره برداری واقع شده است. در حقیقت ۸۰۲،۱۱b نسل دوم استانداردهای بی سیم (پس از ۸۰۲،۱۱) است و ۸۰۲،۱۱a نسل سوم از این مجموعه استاندارد به شمار می رود. استاندارد ۸۰۲،۱۱a بر خلاف ادعای بسیاری از فروشندگان تجهیزات بی سیم نمی تواند جایگزین ۸۰۲،۱۱b شود زیرا لایه فیزیکی مورد استفاده در هر یک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هر یک متفاوت است.

افزایش در پهنای باند در مقایسه با استاندارد ۸۰۲،۱۱b (در استاندارد ۸۰۲،۱۱a حداکثر پهنای باند Mbps) می باشد.استفاده از طیف فرکانسی خلوت(باند فرکانسی ۵GHz) استفاده از ۱۲ کانال فرکانسی غیرپوشا(سه محدوده فرکانسی که در هر یک ۴ کانال غیر پوشا وجود دارد)

۲-۶-۲-۱ افزایش پهنای باند

ا ستاندارد۸۰۲،۱۱a در مقایسه با ۸۰۲،۱۱b و پهنای باند ۱۱ Mbps حداکثر پهنای باند ۵۴ Mbps را فراهم می کند. مهمترین عامل افزایش قابل توجه پهنای باند در این ا ستاندارد ا ستفاده از تکنیک پیشرفته مدولاسیون، موسوم به OFDM است. تکنیک OPDM یک تکنولوژی (فناوری) تکامل یافته و بالغ در کاربردهای بی سیم به شمار می رود. این تکنولوژی مقاومت قابل توجهی در برابر تداخل رادیویی داشته و تاثیرکمتری از پدیده چند مسیری می پذیرد.

OFDM تحت‌عناوین مدولاسیون چند حاملی و یا مدولاسیون‌چندآهنگی‌گسسته نیز شناخته می‌شود. این تکنیک مدولا سیون علاوه بر شبکه‌های بی سیم در تلویزیون های دیجیتال(در اروپا، ژاپن و ا سترالیا) و نیز به عنوان تکنولوژس پایه در خطوط مخابراتی ADSL مورد استفاده قرار می گیرد.

تکنیک OFDM از روش QAM و پردازش سیگنال های دیجیتال ا ستفاده کرده و سیگنال داده را با فرکانس های دقیق و مشخصی تسهیم می کند. این فرکانس ها به گونه ای انتخاب می شوند که خاصیت تعهامد را فراهم کنند و به این ترتیب علی‌رغم همپوشانی فرکانسی هر یک از فرکانس های حامل به تنهایی آشکار می شوند و نیازی به باند محافظت برای فاصله گذاری بین فرکانس ها نیست.

در کنار افزایش پهنای باند در این ا ستاندارد فوا صل مورد ا ستفاده نیز کاهش می یابند. در واقع باند فرکانسی ۵GHz تقریبا دو برابر باند فرکانسی «ISM 2.4GHz» است که در استاندارد ۸۰۲،۱۱b مورد استفاده قرار می گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه های بی سیم متفاوت و متغیر ا ست ولی به عنوان یک قاعده سررا ست می توان فوا صل در این ا ستاندارد را یک سوم محدوده فرکانسی ۲/۴GHz (۸۰۲،۱۱b) در نظر گرفت. در حال حا ضر محدوده عملیاتی (فا صله از فر ستنده) در محصولات مبتنی بر ۸۰۲،۱۱a و پهنای باند ۵۴ Mbps در حدود ۱۰ تا ۱۵ متر است. این محدوده در پهنای باند ۶Mbps در حدود ۶۱ تا ۸۴ متر افزایش می یابد.

۲-۶-۲-۲ طیف فرکانسی تمیزتر

طیف فرکانسی UNII در مقایسه با طیف ISM خلوت تر ا ست و کاربرد دیگری برای طیف UNII به جز شبکه های بی سیم تعریف و تخصیص داده نشده است. در حالی که در طیف فرکانسی ISM تجهیزات بی سیم متعددی نظیر تجهیزات پز شکیع اجاق های مایکروویو، تلفن های بی سیم و نظایر آن وجود درند. این تجهیزات بی سیم در باند ۲/۴GHz یا طیف ISM هیچگونه تداخلی با تجهزات باند UNII (تجهیزات بی سیم ۸۰۲،۱۱a) ندارند.

۲-۶-۲-۳ کانال های غیر پوشا

باند فرکانسی UNII ، دوازده کانال منفرد و غیر پوای فرکانس را برای شبکه سازی فراهم می کند. از این ۱۲ کانال مشخص (UNII-1,2) در شبکه های محلی بی سیم مورد استفاده قرار می گیرند. این ویژگی غیر پو شایی گسترش و پیاده سازی شبکه های بی سیم را ساده تر از باندISM می کند که در آن تنها ۳ کانال غیر پوشا از مجموع ۱۱ کانال وجود دارد.

۲-۶-۲-۴ همکاری Wi-Fi

ائتلاف"همکاری اترنت بی سیم" یا (WCEA)http://www.wi.fi.org کنسر سیومی از شرکت های Cisco, 3Com, Enterasys, Luncent و سایر شرکت های شبکه سازی ا ست. اعضاء WECA از طریق همکاری م شترک تلاش دارند تا قابلیت همکاری تجهیزات بی سیم با یکدیگر را ت ضمین نمایند. برنامه گواهینامه Wi-Fi که توسط این گروه مطرح شده است نقش کلیدی در گسترش و پذیرش استاندارد IEEE ۸۰۲،۱۱ ایفا می کند و درحال حاضر این اتلاف برای بیش از۱۰۰محصول گواهی سازگاری Wi-Fi صادر کرده‌است و تعداد این‌محصولات رو به افزایش‌است. با گسترش فزاینده محصولات IEEE ۸۰۲،۱۱a برنامه دیگری برای صدور گواهینامه برای این نوع محصولات نیز ارائه می کند.

۲-۶-۳ IEEE۸۰۲،۱۱The Next Standard

این استاندارد مشابه IEEE۸۰۲،۱۱b از باند فرکانسی ۲/۴GHz یا طیف ISM استفاده می کند و از تکنیک OPDM به عنوان روش مدولاسیون بهره می برد. البته PBCC نیز یکی از روش های جایگزین و تحت برر سی برای انتخاب مدولا سیون در این ا ستاندارد به شمار می رود. ۸۰۲،۱۱g از نظر فرکان سی، تعداد کانال های غیر پوشا، و توان مشابه۸۰۲،۱۱b است. محدوده های عملیاتی نیز کم و بیش مشابه ه ستند. با این تفاوت که ح سا سیت OFDM به نویز تا حدودی این محدوده عملیاتی را کاهش می دهد. پهنای باند ۵۴Mbps یکی از اهداف احتمالی این ا ستاندارد جدید به شمار می رود. یکی دیگر از مزایای جالب توجه ۸۰۲،۱۱g سازگاری با ۸۰۲،۱۱b ا ست. در نتیجه ارتقاء از تجهیزات ۸۰۲،۱۱b به ا ستاندارد ۸۰۲،۱۱g امری سرراست خواهد بود. جدول ۲-۴ سه استاندارد شبکه های بی سیم را با یکدیگر مقایسه می کند.

	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
کابردهای‌احتمالی	-جایگزین شبکه‌های سیمی - فراهم اوردن تحرک‌وسیار بودن کاربران -شبکه سازی در محل هایی که استفاده از سیم میسر نیست - پل سازی بین‌شبکه‌های‌محلی‌در فواصل‌دور	- جایگزین شبکه های سیمی - فرا هم کننده پهنای‌باند زیاد درکاربردهای (صدا،تصویر،CAD و نظایر آن) - شبکه سازی در محلهایی که ا ستفاده از سیم میسر نیست.	-ارتقاء شبکه های ۸۰۲،۱۱b و رقیبی برای۸۰۲،۱۱a - کارایی مشابه با ۸۰۲،۱۱aدر فواصل طولانی
مزایا	-استاندارد رایج و تکامل‌یافته - قیمت منطقی - گذردهی قابل قبول در فاصله ز یاد(نرخ ارسال داده)	- گذردهی(نرخ‌ارسال‌داده)بالادرفواصل‌کم -افزایش تعداد کا نالهای فر کانسی غیرپوشا(۴برابربیشتر از ۸۰۲،۱۱b) - تداخل فرکانسی کمتر	- سازگاری با ۸۰۲،۱۱b -محدوده عملیاتی زیاد(نظیر ۸۰۲،۱۱b) - گذردهی(نرخ

			ارسال داده)بیشتر
معایب	-داربودن کمترین گذردهی(نرخ ارسال داده) در مقایسه با سایر فناوریهای بی سیم(۱۱Mbps) - استفاده از تنها ۳ کانال فرکانسی غیر پوشا	-فناوری نسبتا گران -ناسازگاری با ۸۰۲،۱۱b - محدوده عملیاتی کوچک -محدودیت های FCCبرروی آنتنها (حداکثرتوان مجاز) در هر باند فرکانسی	- محدودیتها کانال فرکانسی نظیر۳ کانال ۸۰۲،۱۱b غیرپوشا

جدول ۲-۴- استانداردهای شبکه بی سیم

۲-۷ معرفی شبکه بلوتوث

این تکنولوژی که شبکه محلی شخصی نیز نامیده می شودع از یک بازه کوتاه امواج رادیویی برای ارتباطی داخلی بین یک شبکه کوچک بی سیم استفاده می کند. بلوتوث همچنین می توان به عنوان پلی بین شبکه های موجود بکار رود. در واقع اصلی ترین هدفی که بلوتوث دنبال می کند امکان برقراری ارتباط بین ابزارهای کاملا متفاوت است. بعنوان مثال می توان با Bluetooth بین یک گوشی تلفن همراه و یک PDA ارتباط برقرار کرد. بلوتوث از پهنای باند ۲/۴GHz استفاده می کند که نزدیک به پهنای باند دیگر شبکه های بی سیم است. جدول ۲-۵ خلاصه ای از شبکه های بلوتوث آرایه می دهد.

شرح	خصوصیت
انتشار امواج با تکنیک پرش فرکانس(FSHH)	لایهی فیزیکی
۲/۴ GHz	باند مورد استفاده
۱۶۰۰ Hop/sec	سرعت پرش فرکانس
۱Mbps	سرعت انتقال داده
۱۰ تا ۱۱۰ متر	حداکثر برد

جدول ۲-۵- مشخصات شبکه بلوتوث

بلوتوث یک شبکه تک کاره است یعنی از هیچ نقطه دسترسی برای ارتباط بین نودها استفاده نمی شود و تمام نودها مشتوری هستند. با این حال همواره یک رابطه مستر-اسلیو بین نودها وجود دارد. این نوع ارتباط بین نودها یک پیکونت را شکل می دهد. در هر پیکنوت تا ۸ وسیله می توانند شرکت داشته باشد که یکی از آنها مستر و بقیه اسلیو می شوند یک اسلیو در یک پیکونت می تواند نقش مستر را در پیکونت دیگری بازی کند به این ترتیب زنجیره ای از پیکونت ها به وجود می‌آید که به آن یک اسکاترنت می‌گویند.

حداکثر میان فاصله بین دستگاه ها بستگی به کلاس شبکه برپا شده دارد که کلاس نیز به نوبه خود بستگی به میزان توان دستگاهها دارد.

جدول ۲-۶ مشخصات این کلاس ها را نشان می دهد.

برد شبکه	توان دستگاه	کلاس
بیش از ۱۱۰ متر	۱۰۰Wm	کلاس ۱
بیش از ۱۰ متر	۱۰Wm	کلاس ۲
کمتر از ۱۰ متر	۱Wm	کلاس ۳

جدول ۲-۶- مشخصات کلاس ها

مهمترین مزایای شبکه های بلوتوث را می توان به صورت زیر خلاصه کرد:

- جایگزین مزایای شبکه های بلوتوث در ابزارهای کوچک کامپیوتری مانند ماوس.
- آسان بودن اشتراک فایل بین دستگاههای متفاوت مثلا یک PDA یک کامپیوتر کیفی.
- هماهنگی دستگاههای مجهز به تکنولوژی بلوتوث بدون دخالت کاربر.
- اتصال به اینترنت برای بسیاری از دستگاهها، مثلا یک گوشی تلفن همراه می تواند به عنوان یک مودم برای یک کامپیوتر کیفی به کار رود.

۲-۷-۱ مولفه های امنیتی در بلوتوث

بلوتوث از پروتکلهای تشخیص هویت، احراز صلاحیت و رمزنگاری، مدهای امنیت از جمله امنیت در سطح پیوند؛ کنترل دسترسی جداگانه برای دستگاهها و سرویسها، و استفاده از انواع شناسه بستگی به نوع دستگاه، حمایت می کند.

امنیت در سطح پیوند تکنیک هایی را برای ساختن یک لایه پیوند امن فراهم می کند. در این تکنیکها با رمزنگاری و تشخیص هویت در سطح پیوند، پیوند امنی بین دستگاههای بلوتوث فراهم می شود. رمزنگاری و احراز هویت در بلوتوث بر اساس یک کلید پیوندی صورت می گیرد که بین هر دو دستگاه مرتبط با هم وجود دارد. برای تولید این کلید اولین باری که دو دستگاه در صدد ارتباط با یکدیگر بر می آیند، متد Pairing فراخوانده می شود که توسط آن دو دستگاه هویت یکدیگر را احراز کرده و یک کلید مشترک برای برقراری پیوند ایجاد می نمایند.

همچنین دستگاهها برای ارتباط با هم از یک عدد هویت شخصی در زمان مقداردهی اولیه ارتباط استفاده می کنند. این عدد در واقع مانند یک رمز عبور برای ارتباط با یک دستگاه بلوتوث عمل می کند. علاوه براین بلوتوث از تکنیکی به نام برش فرکانس استفاده می کند. در این روش فرکانس ارتباطی بین دو دستگاه بر اساس الگوریتم توافقی بین خود شان در محدوده فرکنس مجاز ۱۶۰۰ بار در ثانیه، عوض می شود تا علاوه برا یانکه ویز کمتری در ارتباطات ایجاد شود دست یافتن به داده واقعی رد و بدل شده بین دو دستگاه برای هکرها هم دشوار شود.

فصل سوم

امنیت در شبکه با نگرشی به شبکه بی سیم

مقدمه

اینترنت یک شـــبکه عظیم اطلاع رســـانی و یک بانک وســـیع اطلاعاتی اســـت که در آینده نزدیک د ستر سی به آن بای تک تک افراد ممکن خواهد شد. کار شنا سان ارتباطات، بهره گیری از این شبکه را یک ضرورت در عصر اطلاعات می دانند.

این شبکه که از هزاران شبکه کوچکتر تشکیل شدهع فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته ا ست. طبق آخرین امار بیش از ششصد میلیون رایانه از تمام نقاط جهان در این شبکه گسترده به یکدیگر متصل شده اند. که اطلاعات بی شماری را در تمامی زمینه ها از هر سنخ و نوعی به ا شتراک گذا شته اند. گفته می شود نزدیک به یک صد میلیارد صفحه اطلاعات با مو ضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است.

این اطلاعات با سرعت تمام در بزرگراههای اطلاعاتی بین کاربران رد و بدل می شود و تقریبا هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده ها اعمال نمی شود. حمایت از جریان آزاد اطلاعات، گ سترش روز افزون اطلاعات و ب ستر سازی برای ات صال به شبکه های اطلاع ر سانی شعار دولتهاست. این در حالی است که گستردگی و تنوع ازلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است.

انتشار تصاویر مستهجن،ایجاد پایگاههایی با مضامین پورنوگرافی و سایتهای شوء استفاده از کودکان و انواع قاچاق در کشـورهای پیشـرفته صـنعتی بخصـوص در خاسـتگاه این شـبکه جهانی یعنی آمریکا، کارشـناسـان اجتماعی را بشـدت نگران کرده، به گونه ای که هیات حاکمه را مجبور به تصـویب قوانینی مبتنی بر کنترل این شـبکه در سـطح آمریکا نموده اسـت. هشـدار، جریمه و بازداشـت برای برپاکنندگان پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده اند.

ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشـی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشـی منطقی اسـت، زیرا هر جامعه ای چهارچوبهای اطلاعاتی خاص خود را دارد و طبیعی اسـت که هر نوع اطلاعاتی که این حد و مرزها را بشـکند می تواد سـلامت و امنیت جامعه را به خطر

اندازد علی‌الرغم وجود جنبه ای مثبت شبکه های جهانیع سوء استفاده از این شبکه های رایانه ای توسط افراد بزهکار، امنیت ملی را در کشـــورهای مختلف با خطر روبرو ســـاخته اســـت. از این رو بکارگیری فیلترها و فایروالهای مختلف برای پیشگیری از نفوذ داده ها مخرب و مضر و گزینش اطلاعات سالم در این شبکه ها رو به افزایش ا ست. خو شبختانه با وجود هیاهوی بسیاری که شبکه اینترنت را غیر قابل کنترل معرفی می‌کند، فناوری لازم برای نترل این شبکه و انتخاب اطلاعات سالم رو به گسترش و تکامل است.

۳- امنیت شبکه های اطلاعاتی و ارتباطی

۳-۱ اهمیت امنیت شبکه

چنانجه به اهمیت شبکه های اطلاعاتی(الکترونیکی) و نقش ا سا سی ان دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه ها مشخص می گردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصـــل نخواهد شـــد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوء استفاده های مادی و معنوی هستند. همچنین دستکاری اطلاعات-به عنوان زیربنای فکری ملت ها تو سط گروههای سازماندهی شده بین المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت ها و تهدیدی ملی محسوب می شود.

برای کشـــور ما که بســـیاری از نرم افزارهای پایه از قبیل ســـیســـتم عامل و نرم افزارهای کاربردی و اینترنتی، از طریق وا سطه ها و شرکتهای خارجی تهیه می شودع بیم نفوذ از طریق راههای مخفی وجود دارد. اکنون که بانکها و بســـیاری از نهادها و دســـتگاههای دیگر از طریق شـــبکه به فعالیت می پردازندع جلوگیزی از نفوذ عوامل مخرب در شبکه به صورت مسئله ای استراتژیک درخواهد آمد که نپرداختن به ان باعث ایراد خ ساراتی خواهد شد که بعضاً جبران ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلا از طرف شرکت مایکرو سافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟

نکته جالب اینکه بزرگترین شرکت تولید نرم افزارهای امنیت شبکه، شرکت چک پوینت ا ست که شعبه ا صلی آن در ا سرائیل می با شد. م سا له امنیت شبکه برای کشورها، م ساله ای ا ستراتژیک ا ست؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها

به صورت محصولات نرم افزاری قابل خریداری نیستند، پس می بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند.

امروزه اینترنت آنقدر قابل دسترس شده که هر کس بدون توجه به محل زندگی، ملیت، شغل و زمان می‌تواند به ان راه یابد و از آن بهره ببرد. همین سهولت دسترسی آن را در معرض خطراتی چون گم شدن، ربوده شدن، مخدوش شدن یا سوء استفادهاز اطلاعات موجود در ان قرار می دهد. اگر اطلاعات روی کاغذ چاپ شده بود و در قفسه ای از اتاقهای محفوظ اداره مربوطه نگهداری می شد، برای دسترسی به آنها غیر مجاز می بایست از حصارهای مختلف عبور می کردند، اما اکنون چند اشاره به کلیدهای رایانه ای برای این منظور کافی است.

۳-۲ سابقه امنیت شبکه

اینترنت در سال ۱۹۶۹ به صورت شبکه های بنام آرپانت که مربوطبه وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخشهایی از سیستم اطلاعاتی به دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیر یاز اثرات مخرب حملات اطلاعاتی بود.

در سال ۱۹۷۱ تعد ادی از رایانه های دانشگاهها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند.

با بروز رخدادهای غیر منتظره در اطلاعات، توجه به مساله امنیت بیش از پیش اوج گرفت. در سال ۱۹۸۸، آرپانت برای اولی بار با یک حادثه امنیتی سرا سری در شبکه، مواجه شد که بعدا، «کرم موریس» نام گرفت. رابرت موریس که یک دان شجو در نیویورک بود، برنامه هایی نو شت که می توان ست به یک رایانه‌ی دیگر راه یابد و در ان تکثیر شود و به همین ترتیب به رایانه های دیگر هم نفوذ کند و به صورت هندسی تکثیر شود. ان زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه های متصل به شبکه در امریکا از کار بیفتد.

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی(IRST) شکل گرفت که در هماهنگی فعالیتهای مقابله با حملات ضد امنیتی، آموزش و تجهیز شبکه ها و روشهای پیشگیرانه نقش موثری داشت. با رایج تر شدن و استفاده عام از اینترنت، مساله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث،

اختلال در امنیت شبکه،WINK/OILS WORM در سال ۱۹۸۹ ، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می شد. از آن زمان حملات امنیتی- اطلاعاتی به شبکه ها و شبکه جهانی روز به روز افزایش یافته است. گرچه اینترنت در ابتدا، با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمنیان آن را بیش از پیش روشن نموده است.

۳-۲ جرائم رایانه ای و انترنتی

ویژگی برجسته فناوری اطلاعات، تاثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را به مقادیر وسیعی از داده ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این بادل و تکامل نه تنها بین انسانها بلکه مابین انسانها و رایانه ها، همچنین بین خود رایانه ها نیز وجود دارد. استفاده وسیع از پست الکترونیک، و دستیابی به اطلاعات از طریق وب سایتهای متعدد در اینترنت نمونه هایی از این پیشرفتها می باشد که جامعه را به طور پیچیده‌ای دگرگون ساخته اند. سهولت در دستر سی و جستجوی اطلاعات موجود ر سیستمهای رایانه ای توام با امکانات عملی نامحدود ر مبادله و توزیع اطلاعات، بدون توجه به فوا صل جغرافیایی، منجر به رشد سرسام آور مقدار اطلاعات موجود در آگاهی که می توان از آن بدست آورد، شده است.

این اطلاعات موجب‌افزایش تغییرات اجتماعی او اقتصادی پیش بینی نشده گردیده است. اما پیشرفتهای مذکور جنبه خطرناکی نیز دارد که پیدایش انواع جرایم و همچنین بهره برداری از فناوری جدید در ارتکاب جرایم بخشی از آن به شمار می رود. بعلاوه عواقب و پیامدهای رفتار مجرمانه می تواند بیشتر از قبل و دور از تصور باشد چون که محدودیتهای جغرافیایی یا مرزهای ملی آن را محدود نمی کنند. فناوری جدید مفاهیم قانونی موجود را دچار چالشهایی ساخته است.

اطلاعات و ارتباطات راه دور به راحت ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به شمار نمی روند. جنایتکاران غالباً در مکانهایی به غیر از جاهایی که آثار و نتایج آنها ظاهر می شود، قرار دارند. سوء استفاده گسترده مجرمین، به ویژه گروه های جنایتکار سازمان نیافته از

فناوری اطلاعات سبب‌گشته‌است که سیاستگذاران جنایی اغلب کشورهای‌جهان با استفاده از ابزارهای سیاست‌جنایی در صدد مقابله با آنها برآیند.

تصویب کنوانسیون جرایم رایانه ای در اواخر سال ۲۰۰۱ و امضای آن توسط ۳۰ کشور پیشرفته، تصویب قوانین مبارزه با این جرایک قانون گذاران داخلی و تشکیل واحدهای مبارزه با آن در سازمان پلیس بیشتر کشورهای پیشرفته و تجهیز آنها به جدیدترین سخت افزارها و نرم افزارهای کشف این گونه جرایم و جذب و بارگیری بهترین متخصصین در واحدهای مذکور، بخشی از اقدامات مقابله ای را تشکیل می دهد.

۳-۲-۱ پیدایش جرایم رایانه ای

در مورد زمان دقیق پیدایش جرم را یا نه ای نمی توان اظهار نظر قطعی کرد. این جرم زائیده تکنولوژی اطلاعاتی و انفورماتیکی است، بنابراین به طور منظم بعد از گذشت مدت کوتاهی از شیوع و کاربرد تکنولوژی اطلاعات، باب سوء استفاده نیز قابل طرح است. شیوع استعمال این تکنولوژی و برابری کاربران آن حداقل در چند کشور مطرح جهان به صورت گسترده، امکان بررسی اولین مورد را دشوار می سازد. در نهایت آن چه مبرهن است اینکه در جامعه آمریکا رویس موجب شد برای اولین بار اذهان متوجه سوء استفاده های رایانه ای شود.

۳-۲-۲ قضیه رویس

آلدون رویس حسابدار یک شرکت بود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه ای، قسمتی از پولهای شرکت را اختلاس رد. انگیزه رویس در این کار انتقام گیری بود.

مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می خرید و با استفاده از تجهیزات خود از قبیل کامیونها، انبار و بسته بندی و سرویس دهی به گروه های فروشندگان، آنها را عرضه می کرد. به دلیل وضعیت خاص این شغل، قیمتها در نوسان بود و ارزیابی امور تنها می توانست از عهده رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده دار شود.کلیه امور حسابرسی و ممیزی اسناد و مدرک و صورت حسابها به صورت اطلاعات مضبوط در نوارهای الکترونیکی بود.

رویس در برنامه ها، دستور العمل های اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می داد. با تنظیم درامد اجناس وی مبلغی را کاهش می داد و مبالغ حاصله را به حسابهای مخصوص واریز می کرد. بعد در زمانهای خاص چکی به نام یکی از هفده شرکت جعلی و ساختگی خودش صادر

و مقداری از مبالغ را برداشت می کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار بردا شت کند. اما او بر سر راه خودش م شکلی دا شت و ان این بود که مکانیسمی برای توقف عملکرد سیستم نمی توانتست بیندیشد. بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم اعتراض کرد و به مدت ده سال به زندان محکوم شد. از این جا بود که مبحث جدیدی به نام جرم رایانه ای ایجاد شد.

۳-۲-۳ تعریف جرم رایانه ای

تا کنون تعریفهای گوناگونی از جرم رایانه ای از سوی سازمانها، متخ صصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم است. جرم رایانه ای یا جرم در فضای مجازی(سایر جرایم) دارای دو معنی و مفهوم ا ست. در تعریف مضیق، جرم رایانه ای صرفا عبارت از جرایمی است که در فضای سایبر رخ می دهد.

از این نظر جرایمی مثل هرزه نگاری، افترا، آزار و اذیت سوء ا ستفاده از پ ست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و و سیله ارتکاب جرم بکار گرفته می شود، در زمره جرم رایانه ای قرار نمی گیرند.

در تعریف موسع از جرم رایانه ای هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه به طور مستقیم یا غیر مستقیم رخ می دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه ای نامیده می شود.

بر این اساس این گونه جرایم را می توان به سه دسته تقسیم نمود:

دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می شوند. مانند سرقت، تخریب و غیره... .

د سته دوم: جرایمی ه ستند که در آنها رایانه به عنوان ابزار و سیله تو سط مجرم برای ارتکاب جرم بکار گرفته می شود.

د سته سوم: جرایمی‌هستند که می توان آنها را جرایم رایانه ای محض نامید. این نوع از جرایم کاملا با جرایم‌کلاسیک تفاوت‌دارند و در دنیای مجازی به وقوع می‌پیوندند اما آثار آنها دردنیای واقعی ظاهرمی‌شود، مانند دسترسی غیر مجاز به سیستم های رایانه ای.

۳-۲-۴ طبقه بندی جرایم رایانه ای

طبقه بندی های مختلفی از جرایم رایانه ای تو سط مراجع مختلف انجام گرفته ا ست. برای آ شنایی شما با آنها موارد مهم به شرح زیر اکتفا می شود.

۳-۲-۴-۱ طبقه بندی OECDB

در سال ۱۹۸۳ «او.ای. سی.دی.بی» مطالعه امکان پذیری اعمال بین الملل و هماهنگی قوانین کیفری را به منظور حل مسئله جرم یا سوء استفاده های رایانه ای متعهد شد. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه ای، تحلیل سیستاتهای قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوء استفاده هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند.

بدین گونه اولین تقسیم بندی از جرایم رایانه ای در سال ۱۹۸۶ ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی کرد و پیشنهاد کرد در قوانین ماهوی ذکر شود. این پنج دسته عبارتند از:

الف- ورود، تغییر، پاکر کردن و یا متوقف سازی داده های رایانه ای و برنامه ای که به بطور ارادی با قصد انتقال غیر قانونی وجوه یا هر چیز با ارزش دیگر صورت گرفته باشد.

ب- ورود، تغییر، پاک کردن و یا متوقف سازی داده های رایانه ای و برنامه های رایانه ای که بصورت عمدی و به قصد ارتکاب جعل صورت گرفته با شند. یا هر گونه مداخله دیگر در سیستمهای رایانه ای که به صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه ای و یا ارتبازات صورت گرفته باشد.

ج- ورود، تغییر، پاک کردن و متوقف سازی داده های رایانه ای و یا برنامه های رایانه ای.

د- تجاوز به حقوق انحصاری مالک یک برنامه رایانه ای حفاظت شده با قصد بهره برداری تجاری از برنامه ها و ارائه آن به بازار.

هـ- دستیابی یا شنود در یک سیستم رایانه ای و یا ارتباطی که اگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبوریا تخطی از تدابیر امنیتی و چه با هدف غیرشرافتمندانه وی موضوع صورت گرفته‌باشد.

۳-۲-۴-۲ طبقه بندی شورای اروپا

کمیته منتخب‌جرایم رایانه‌ای شـــورای اروپا، پس از بررســـی نظرات «او.ای.ســـی.دی.بی» و نیز بررســی‌های حقوقی- فنی دو لیســت تحت عناوین لیســت حداقل و لیســت اختیاری را به کمیته وزراء پیشنهاد داد و آنان نیز تصویب کردند. این لیستها بدین شرح هستند:

- لیست اختیاری

الف- کلاهبرداری رایانه ای

ب- جعل رایانه ای

ج- خسارت زدن به داده های رایانه ای یا برنامه های رایانه ای

د- دستیابی غیر مجاز

هـ - ایجاد مجدد و غیر مجاز یک برنامه رایانه ای حمایت شده

و- ایجاد مجدد غیر مجاز یک توپوگرافی.

- لیست اختیاری

الف- تغییر داده های رایانه ای و یا برنامه های رایانه ای

ب- جاسوسی رایانه ای

ج- استفاده غیر مجاز از رایانه

د- استفاده غیر مجاز از برنامه رایانه حمایت شده.

۳- ۲-۴-۳ طبقه بندی اینترپول

سالها ست که اینترپول در مبارزه با جرایم مرتبط با فناوری اطلاعات فعال می با شد. این سازمان با بهره‌گیری از کار شنا سان و متخصصین کشورهای عضو اقدام به تشکیل گروههای کاری در این زمینه کرده ا ست. رو سای واحدهای مبارزه با جرایم رایانه ای کشورهای با تجربه عضو سازمان در این گروه کاری گرد هم آمده اند.

گروههای کاری منطقه ای در اروپا، آسیا، آمریکا و افریقا مشغول به کارند. و زیر نظرکمیته راهبردی جرایم فناوری اطلاعات، مستقر در دبیرخانه کل اینترپول فعالیت می نمایند. گروه کاری اروپایی اینترپول با حضور کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال ۱۹۹۰ تشکیل شد. این گروهها هر سال سه بار تشکیل جلسه می دهند و در ژانویه سال ۲۰۰۱ سی امین گردهمایی آن در دبیرخانه کل تشکیل گردید. تهیه کتابچه راهنمای پیجویی جرایم رایانه ای، کتاب و سی

دی راهنمای جرایم رایانه ای، تشکیل دوره های آموزشی برای نیروهای پلیس در طول سال گذشته، تشکیل سیستم اعلام خطر که مرکب از سیستم های پاسخگوی شبانه روزی، نقاط تماس دائمی شبانه روزی، تبادل پیام بین المللی در قالب فرمهای استاندارد در زمینه جرایم رایانه ای واقعه می باشد و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم رایانه ای از جمله اقدامات گروه کاری مذکور می باشد. گروه کاری مذکور می‌باشد. گروه کاری آمریکایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان و متخصصین کشورهای کانادا، ایالات متحده، آرژانتین، شیلی، کلمبیا، جامائیکا و باهاماست.

گروه کاری آفریقایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان آفریقای جنوبی، زیمبابوه،نامبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، لسوتو و رواندا در ژوئن سال ۱۹۹۸ تشکیل گردید. آنها کارشان را با برگزاری یک دوره آموزشی آغاز نمودند و دومین دوره آموزشی آنها با مساعدت مالی سفارتخانه های انگلیس برگزار شد. گروه کاری جنوب اقیانوس آرام، و آسیا در نوامبر سال ۲۰۰۰ در هند تشکیل شد و کار شناسانی از کشورهای استرالیا، چین، هنگ کنگ، هند، ژاپن، نپال و سریلانکا عضو آن هستند. این گروه کاری با الگو قرار دادن کمیته راهبردی جرایم مربوط به فاوری اطلاعات به منظور ایجاد و هماهنگی میان اقدامات گروههای کاری منطقه ای در محل دبیرخانه کل اینترپول تشکیل گردیده است.

سازمان پلیس جنایی بین المللی جرایم رایانه را به شرح زیر طبقه بندی کرده است:

۱- دستیابی غیر مجاز

۱-۱- نفوذ غیر مجاز

۱-۲- شنود غیرمجاز

۱-۳- سرقت زمان رایانه

۲- تغییر داده های رایانه ای

۲-۱- بمب منطقی

۲-۲- اسب تروا

۲-۳- ویروس رایانه ای

۲-۴- کرم رایانه ای

۳- کلاهبرداری رایانه ای

۳-۱- صندوقهای پرداخت

۳-۲- جعل رایانه ای

۳-۳- ماشینهای بازی

۳-۴- دستکاریها در مرحله ورودی/ خروجی

۳-۵- ابزار پرداخت(نقطه فروش)

۳-۶- سوء استفاده تلفنی

۴- تکثیر غیر مجاز

۴-۱- بازیهای رایانه ای

۴-۲- نرم افزارهای دیگر

۴-۳- توپوگرافی نیمه هادی

۵- سابوتاژ رایانه ای

۵-۱- سخت افزار

۵-۲- نرم افزار

۶- سایر جرائم رایانه ای

۶-۱- سیستمهای تابلویی اعلانات الکترونیک

۶-۲- سرقت اسرار تجاری

۶-۳- سایر موضوعات قابل تعقیب

۳-۲-۴-۴ طبقه بندی در کنوانسیون جرایم سایبرنتیک

این کنوانسیون در اواخر سال ۲۰۰۱ به امضای ۳۰ کشور پیشرفته رسیده است و دارای وظایف زیر می‌باشد:

الف- هماهنگ کردن ارکان تشکیل دهنده جرم در حقوق جزایی ماهوی داخلی کشورها و مسائل مربوطه در بخش جرایم سایبر اسپیس.

ب- فراهم آوردن اختیارات لازم آیین دادرسی کیفری برای پیجویی و تعقیب چنین جرائمی علاوه بر جرایم دیگر که با استفاده از سیستمهای رایانه ای ارتکاب می یابند.

ج- تدوین سیستم سریع موثر همکاری بین المللی کنوانسیون بین المللی جرایم رایانه ای بوداپست (۲۰۰۱) جرم را موارد زیر تعریف نموده است:

۱- نفوذ غیر مجاز به سیستمهای رایانه ای

۲- شنود غیر مجاز اطلاعات و ارتباطات رایانه ای

۳- اخلال در داده های رایانه ای

۴- اخلال در سیستمهای رایانه ای

۵- جعل رایانه ای

۶- کلاهبرداری رایانه ای

۷- سوءاستفاده از ابزارهای رایانه ای

۸- هرزه نگاری کودکان

۹- تکثیر غیر مجاز نرم افزارهای رایانه ای و نقص حقوق ادبی و هنری

۳-۲-۵ شش نشانه از خرابکاران شبکه ای

۱- در صورت مفوذ یک خرابکار به شبکه شما ممکن است حساب بانکی تان تغییر کند.

۲- خرابکاران شبکه ای آن قدر تلاش می کنند تا بالاخره موفق به ورود به اینترنت شما شوند. لازم به ذکر است که در برخی مواردی در صورتی که یک خرابکار بتواند به حساب بانکی شما نفوذ کند فایل آن به طور خودکار بسته نمی شود.

۳- گاهی اوقات خرابکاران برای نفوذ به یک رایانه ناچارند کد جدیدی به آن وارد کنند. برای این کار لازم است رایانه دوباره راه اندازی شود. بنابراین راه اندازیهای مجدد رایانه، که به طور غیر منتظره انجام می‌شود، می تواند نشانه ای از نفوذ خرابکاران شبکه ای به رایانه شما باشد.

۴- بعضی اوقات خرابکاران شبکه ای تنها با حذف بخشهایی از یک فایل می توانند راه نفوذ خود در آن را مخفی نگه دارند. بنابراین قسمتهای حذف شده از یک فایل می توانند نشان دهنده مسیر مفوذ خرابکاران شبکه ای به یک فایل از رایانه باشد.

۵- گاهی با این که انتظار می رود ارتباط بین دو رایانه از طریق شبکه، در زمانهایی مشخص، بسیار کم باشد ترافیک زیادی در آن مسیر ملاحظه می شود. چه بسا خرابکاران شبکه ای در حال تلاش برای نفوذ به ان سیستمها باشند و همین امر موجب ترافیک سنگین بین انها شود.

۶- بخشهایی در سیستم هر شرکت وجود دارد که جدا از بقیه سیستم بوده و تنها افراد معدودی به آن دسترسی دارند، گاهی می توان خرابکاران شبکه ای را در چنین بخشهایی پیدا کرد.

۳-۳ منشا ضعف امنیتی در شبکه های بی سیم و خطرات معمول

خطر معمول در کلیه ی شبکه های بی سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنالهای رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قادرند در صورت شکستن موانع نه چندان قدرتمند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جا زده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس‌دهندگان سازمان و مجموعه، تخریب‌اطلاعات، ایجاد اختلال در ارتباطات گروه‌های شبکه با یکدیگر، تولید داده های غیر واقعی و گمراه کننده، سوء استفاده از پهنای باند موثر شبکه و دیگر فعالیت های مخرب جود دارد. در مجموع در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایقی مشترک صادق است:

- تمامی ضعف های امنیتی موجود در شبکه های سیمی، در مورد شبکه های بی سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه ای چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه های بی سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه ای را نیز موجب است.

- نفوذگران، با گذر از تدابیر امنیتی موجود، می توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم های رایانه ای دست یابند.

- اطلاعات حیاتیی که یا رمز نشده اند و یا با روشی با امنیت پایین رمز شده اند، و میان دو گره در شبکه های بی سیم در حال انتقال می باشند، می توانند توسط نفوذگران سرقت شده یا تغییر یابند.

- حمله های DOS به تجهیزات و سیستم های بی سیم بسیار متداول است.

– نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه های بی سیم، می توانند به شبکه ی مور نظر بدون هیچ مانعی متصل گردند.

– با سرقت عناصر امنیتی، یک نفوذگر می تواند رفار یک کابر را پایش کند. از این طریق می توان به اطلاعات حساس دیگری نیز دست یافت.

– کامپیوترهای قابل حمل و جیبی، که امکان و اجازه ی استفاده از شبکه ی بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.

– یک نفوذگر می تواند از نقاط مشترک میان یک شبکه ی بی سیم در یک سازمان و شبکه ی سیمی آن(که در اغلب موارد شبکه ی اصلی و حساس تری محسوب می گردد) استفاده کرده و با نفوذ به شبکه ی بی سیم عملا راهی برای دست یابی به منابع شبکه ی سیمی نیز بیابد.

– در سطحی دیگر، با نفوذ به عناصر کنترل کننده ی یک شبکه ی بی سیم، امکان ایجاد اختلال در عملکرد شبکه نیز وجود دارد.

۳-۳-۱ امنیت و پروتکل WEP

در این قسمت بررسی روش‌ها و استانداردهای امن سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۱۱، ۸۰۲ سرویس های مجزا و مشخصی را برای تامین یک محیط امن بی‌سیم در اختیار قرار می‌دهد.

این سرویس‌ها اغلب تو سط پروتکل WEP(Wired Equivalent privacy) تامین می‌گردند و وظیفه ی آن ها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است. درک لایه‌ای که این پروتکل به امن سازی آن می‌پردازد اهمیت ویژه‌ای دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه‌ی ارتباطی بی سیم که مبتنی بر استاندارد ۱۱، ۸۰۲ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

۳-۳-۲ قابلیت ها و ابعاد امنیتی استاندارد ۱۱، ۸۰۲

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم بر اساس استاندارد ۱۱، ۸۰۲ فراهم می‌کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت این است که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای ا شتراک هستند. به عبارت دیگر نفوذگران بعضاً با ا ستفاده از راه های ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم، وجود دارد، به شبکه‌ی بی سیم نفوذ می کنند که این مقوله نشان دهنده‌ی ا شتراکی هرچند جزیی میان امنیت در شبکه های سیمی و بی‌سیمی است که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی‌سیم تعریف می گردد:

- ☒ Authentication
- ☒ Confidentiality
- ☒ Integrity

۳-۲-۳-۱ Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل د ستر سی به شبکه‌ی بی سیم ا ست. این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

۳-۲-۳-۲ Confidentiality

محرمانگی هدف دیگر WEP ا ست. این بعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده ا ست. سیا ست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی‌سیم است.

۳-۲-۳-۳ Integrity

هدف سوم از سرویس‌ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

۳-۳-۳ خدمات ایستگاهی:

بر اساس این استاندارد خدمات خاصی در ایستگاه های کاری پیاده سازی می شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر ۱۱،۸۰۲ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیرمجاز بر خلاف شبکه های سیمی، در شبکه های بی سیم قابل اعمال ۱۱، ۸۰۲ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می نماید.

۳-۳-۳-۱ هویت سنجی:

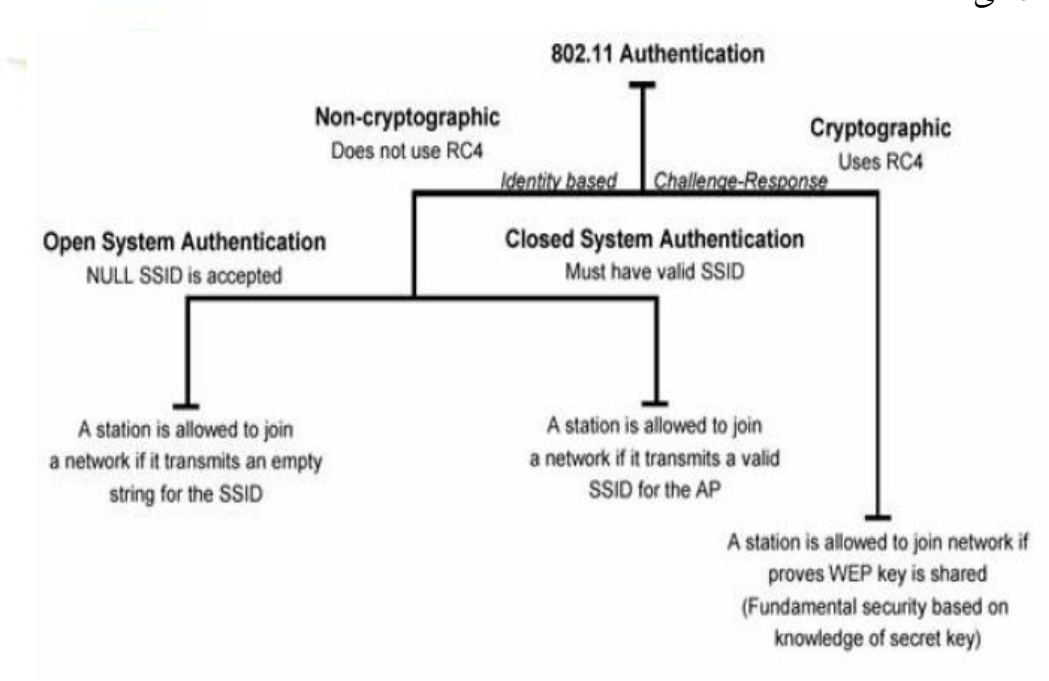
سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که شبکه بی سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۱۱، ۸۰۲ دو گونه خدمت هویت سنجی را تعریف می‌کند:

–Non- Cryptographic System Authentication
–Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله ای است. در ابتدا ایستگاهی که می خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می کند. ایستگاه گیرنده نیز فریمی در پاسخ می فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده تر است و فرض می کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهره گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می گردد.

در یک شبکه بی سیم، تمام ای ستگاه های کاری و سایر تجهیزات قادر ه ستند ترافیک داده ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می شود که توسط تمام ایستگاه های کاری قابل دریافت ا ست. این ویژگی سطح امنیتی یک ارتباط بی سیم را تحت تاثیر قرار می دهد. به همین دلیل در ا ستاندارد ۱۱، ۸۰۲ پروتکلی مو سوم به WEP تعبیه شده ا ست که بر روی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می شود. این ا ستاندارد در پی آن ا ست تا با ا ستفاده از این الگوریتم سطح اختفاء و پوشش را معادل با شبکه‌های سیمی نماید.

همانگونه که مطرح شد استاندارد ۱۱، ۸۰۲ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه ی بی سیم را به نقاط د ستر سی ار سال می کنند، دارد که یک روش بر مبنای رمزنگاری است و دیگری از رمزنگاری استفاده نمی‌کند. شکل زیر شمایی از فرآیند Authentication را در این شبکه ها نشان می‌دهد:



شکل ۳-۱- رمزگذاری RC4

همان گونه که در شکل بالا نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری ای استفاده نمی‌کند.

۳-۳-۱-۱ Authentication بدون رمزنگاری(Non-Cryptographic System Authentication)

در رو شی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد در هر دو روش مخدوم متقا ضی پیو ستن به شبکه، درخوا ست ار سال هویت از سوی نقطه ای د ستر سی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.

در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت رو به رو می‌شوند و تنها آدرس آن ها توسط نقطه‌ی دسترسی نگاهداری می شود. به همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

در روش دوم از این نوع، باز هم یک SSID به نقطه‌ی دسترسی ارسال می گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی د ستر سی صادر می‌گردد که SSID ار سال شده جزو SSID های مجاز برای د ستر سی به شبکه با شند. این روش به Closed System Authentication موسوم است.

نکته ای که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی ا ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارائه نمی دهند و عملاً تنها راهی برای آگاهی ن سبی و نه قطعی از هویت درخوا ست کننده ه ستند. با این و صف از آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه ای در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخ داد حمله به آن بسیار کم ا ست. هرچند که با توجه پو شش نسبتاً گسترده ی یک شبکه ی بی سیم- که مانند شبکه های سیمی امکان محدود سازی دسترسی به صورت فیزیکی بسیار دشوار است- اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

۳-۳-۳-۱-۲ Authentication با رمزنگاری RC4 (Shared key authentication)

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تایید می‌شود.

در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن را به مخدوم می فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می کند. در صورت همسانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است:

الف) در این روش تنها نقطه‌ی دسترسی است که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی که با آن در حال تبادل داده‌های رمزی است نقطه‌ی دسترسی اصلی است.

ب) تمامی روش هایی که مانند این روش بر پایه ی سوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man – in- the- middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می گیرد و به گونه‌ای هر یک از دو طرف را گمراه می‌کند.

۳-۳-۳-۲ اختفا اطلاعات (سرویس privacy یا Confidentiality)

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانگی عموماً از تکنیک های رمزنگاری استفاده می گردد، به گونه ی که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

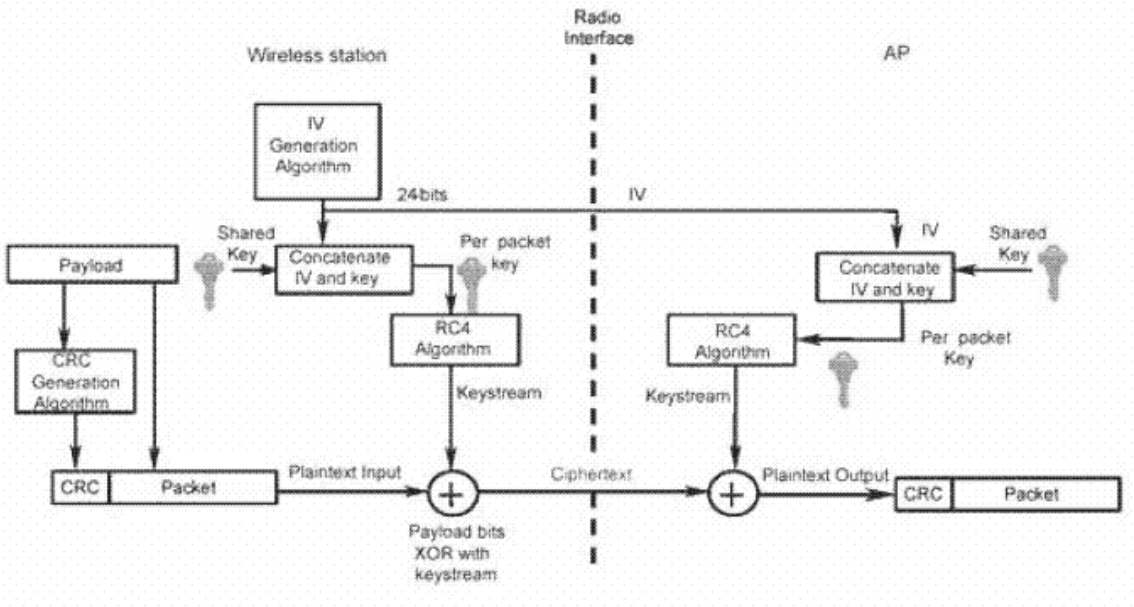
در استاندارد ۱۱، b۸۰۲، از تکنیک های رمزنگاری WEP استفاده می گردد که بر پایه ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته ی نیمه تصادفی تولید می گردد و توسط آن کل داده رمز می شود. این رمزنگاری بر روی تمام بسته ی اطلاعاتی پیاده می شود. به بیان دیگر داده های تمامی لایه های بالایی اتصال بی سیم نیز توسط این روش رمز می گردند، از IP گرفته تا لایه های

بالاتری مانند HTTP از آنجایی که این روش عملاً اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه های محلی بی سیم مبتنی بر استاندارد ۱۱، b۸۰۲ است، معمولاً به کل پروسه ی امن سازی اطلاعات در این استاندارد به اختصار WEP گفته می شود.

کلیدهای WEP اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت می توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی‌ترکیب‌شده ویک‌کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه ی ۸۰ بیت (که تعداد آن ها از مرتبه ی ۲۴ است) به اندازه یی بالاست که قدرت پردازش سیستم های رایانه یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفای نمی کند.

هر چند که در حال حاضر اکثر شبکه های محلی بی سیم از کلیدهای ۴۰ بیتی برای رمز کردن بسته های اطلاعاتی استفاده می کنند ولی نکته یی که اخیراً بر اساس یک سری آزمایشات به دست آمده است، این است که روش تامین محرمانگی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute- force نیز آسیب پذیر است و این آسیب پذیری ارتباطی به اندازه ی کلید استفاده شده ندارد.

نمایی‌از روش ا ستفاده شده تو سط WEP برای تضمین محرمانگی در شکل زیر نمایش داده شده است:



شکل ۳-۲- امنیت شبکه WEP

۳-۳-۳-۳ حفظ صحت اطلاعات (Integrity):

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست های امنیتی ای که Integrity را تضمین می‌کنند روش هایی‌هستند که امکان تغییر اطلاعات در حین تبادل را به کمترین میزان تقلیل می‌دهند.

در استاندارد ۱۱، ۸۰۲b نیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم های بی سیم و نقاط دسترسی کم می شود. روش مورد نظر استفاده از یک کد CRC است. همان طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمز شدن بسته تولید می شود. در سمت گیرنده، پس از رمزگشایی، CRC داده های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می گردد که هرگونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متاسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب پذیر است.

۳-۳-۴ ضعف های اولیه‌ی امنیتی WEP

متاسفانه استاندارد ۱۱، ۸۰۲b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می گیرد باید توسط کسانی که شبکه‌ی بی سیم را نصب می‌کنند به صورت دستی پیاده سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل های اساسی

در مبحث رمزنگاری است، با این ضعف عملاً روش های متعددی برای حمله به شبکه های بی سیم قابل تصور است. سهل انگاری های انجام شده از سوی کاربران و مدیران شبکه مانند تغییر ندادن کلید به صورت مداوم، لو دادن کلید، استفاده از کلیدهای تکراریا کلیدهای پیش فض کارخانه و دیگر بی توجهی ها نتیجه یی جز در صد نسبتاً بالایی از حملات موفق به شبکه های بی سیم ندارد. این مشکل از شبکه های بزرگتر بیش تر خود را نشـــان می دهد. حتی با فرض تلاش برای جلوگیری از رخ داد چنین ســـهل انگاری هایی، زمانی که تعداد مخدوم های شـــبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گهگاه خطاهایی در گوشه و کنار این شبکه ی نسبتاً بزرگ رخ می‌دهد که همان باعث رخنه در کل شبکه می شود.

پایه‌ی امنیت در استاندارد ۱۱، ۸۰۲ بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می شود، هرچند که برخی از تولید کننده گان نگارش‌های خاصـــی از WEP را با کلیدهایی با تعداد بیت های بیش‌تر پیاده ســـازی کرده اند.

نکته ای که در این میان اهمیت دارد قائل شـــدن تمایز میان نســـبت بالا رفتن امنیت و اندازه‌ی کلیده‌است. با وجود آن که با بالا رفتن اندازه‌ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می رود، ولی از آن جا که این کلیدها توسط کاربران و بر اساس یک کلمه ی عبور تعیین می شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان طور که در قسمت های پیشین نیز ذکر شد، دست یابی به این کلیدها فرآیند چندان سختی نیست، که در آن صورت دیگر اندازه ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی های انجام شده فهرستی از ضعف های اولیه یا این پروتکل است:

۱. استفاده از کلیدهای ثابت WEP (Initialization Vector- IV)

۲. استفاده از CRC رمز نشده

۳-۳-۴-۱ استفاده از کلیدهای ثابت WEP :

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه های کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است. از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

:Initialization Vector –IV

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس IV تولید می شود، محدوده ی IV عملاً نشان دهنده ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به‌عبارت‌دیگر در صورتی‌که IV کوتاه باشد در مدت‌زمان کمی می توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ی استفاده شده مطمئن نباشیم. بسیاری از کارت های شبکه از IVهای ثابت استفاده می کنند و بسیاری از کارت‌های شبکه ی یک تولید کننده ی واحد IV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی است نفوذگر در مدت زمانی معین به ثبت داده های رمز شده ی شبکه بپردازد و IV های بسته های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IV های استفاده شده در یک شبکه ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

ضعف در الگوریتم:

از آن جایی که IV در تمامی بسته های تکرار می شود و بر اساس آن کلید تولید می شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IV ها و بسته های رمز شده بر اساس کلید تولید شده بر مبنای آن IV ، به کلید اصلی دست پیدا کند. این فرآیند عملی زمان بر است ولی از آن جا که احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

۳-۳-۴-۲ استفاده از CRC رمز نشده:

در پروتکل WEP، کد CRC رمز نمی شود. لذا بسته های تاییدی که از سوی نقاط دسترسی بی سیم به سوی گیرنده ارسال می شود بر اساس یک CRC رمز نشده ارسال می گردد و تنها در صورتی که نقطه ی دسترسی از صحت بسته اطمینان حاصل کند تایید آن را می‌فرستد. این ضعف این امکان را فراهم می کند که نفوذگر برای رمز گشـــایی یک بســـته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشـده اسـت، به راحتی عوض‌کند و منتظر عکس العمل نقطه‌ی دسـترسـی بماند که آیا بسـته ی تایید را صادر می کند یا خیر.

ضعف‌های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هستند.

نکته‌ای که در مورد ضعف های فوق باید به آن ا شاره کرد این ا ست که در میان این ضعف ها تنها یکی از آن ها به ضـــعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می گردد و بقیه ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

۳-۴ مولفه های امنیتی در بلوتوث

بلوتوث از پروتکلهای تشخیص هویت، احراز صلاحیت و رمزنگاری؛ مدهای امنیت از جمله امنیت در سطح پیوند؛ کنترل دسترسی جداگانه برای دستگاهها و سرویس ها؛ و استفاده از انواع شناسه بستگی به نوع دســتگاه، حمایت می‌کند. امنیت در ســطح پیوند تکنیک‌های را برای ســاختن یک لایه پیوند امن فراهم می کند. در این تکنیکها با رمزنگاری و تشـــخیص هو یت در ســـطح پیو ند، پیو ند امنی بین دستگاههای بلوتوث فراهم می شود.

رمزنگاری و احراز هویت در بلوتوث بر اســاس یک کلید پیوندی صــورت می گیرد که بین هر دو دستگاه مرتبط با هم وجود دارد. برای تولید این کلید اولین باری که دو دستگاه در صدد ارتباط با یکدیگر بر می آیند، متد Pairing فرا خوانده می شـود که توسـط آن دو دسـتگاه هویت یکدیگر را احراز کرده و یک کلید مشترک برای برقراری پیوند ایجاد می نمایند.

همچنین د ستگاهها برای ارتباط با هم از یک عدد هویت شخ صی در زمان مقدار دهی اولیه ارتباط استفاده می کنند. این عدد در واقع مانند یک رمز عبور برای ارتباط با یک دستگاه بلوتوث عمل می کند.

علاوه بر این بلوتوث از تکنیکی به نام برش فرکانس استفاده می کند. در این روش فرکانس ارتباطی بین دو دستگاه بر اساس الگوی توافقی بین خودشان در محدوده فرکانس مجاز ۱۶۰۰ بار در ثانیه، عوض

می شود تا علاوه بر اینکه نویز کمتری در ارتباطات ایجاد شود دست یافتن به داده واقعی رد و بدل شده بین دو دستگاه برای هکرها هم دشوار شود.

۳-۴-۱ خطرات امنیتی:

موارد و آسیب پذیریهای امنیتی در بلوتوث وجود دارند که باعث می شوند کاربران ترجیح دهند علاوه بر تدابیر امنیتی پیش فرض بلوتوث اقدامات امنیتی بیشتری برای امن کردن شبکه خود بکار برند. با اینکه استاندارد شبکه های بلوتوث بستری امن را فراهم می سازد اما بسیاری از دستگاه های این شبکه با رعایت نکردن این استاندارد نواقص خطرناکی در احراز هویت و مکانیزمهای انتقال اطلاعات خود دارند که شبکه را نا امن می سازد. جدول ۳-۱ برخی از نکات امنیتی شبکه های بلوتوث را که باید مورد توجه قرار بگیرد توضیح می دهد.

توضیحات	مورد
بلونوس احراز صلاحیت دستگاهها را فراهم می کند نه	عدم احراز صلاحیت کاربر
در هنگام ساخته شدن یک لینگ کد پیوندی آن پیوند بین دستگاهها رد و بدل می شود که این ممکن است امکان دزدیده شدن آن را فراهم آورد	استراق سمع ناشی از اشتراک گذاری کد پیوندی
فقط پیوندهای بین دو دستگاه مجاور رمزگذاری و احراز هویت می شوند و در هر نقطه میانی مسیر عملیات رمزگشایی صورت می گیرد. امنیت بین مبدا و مقصد اصلی باید به وسیله یک کاربردی جدا از استاندارد بلوتوس تامین گردد.	فراهم نبودن امنیت End to End

جدول ۳-۱- برخی از نکات امنیتی شبکه های بلوتوس

لیستی از مهمترین آسیبها و حملات که در شبکه های بلوتوث وجود دارد به شرح زیر است:

- استراق سمع شبکه از طریق یک دستگاه هک شده درون شبکه شبکه های بلوتوث در برابر حملات منع سرویس آسیب پذیرند. هکرها می توانند به وسیله دستگاههایی که قادرند امواجی در فرکانس ۲/۴GHz بفرستند، ترافیک کاذب در شبکه بوجود آورند.

- حملات SNARF
- حملات در پشتی
- حمله Blue Jacking که بسیار شبیه حمله سرریز در شبکه های معمولی است.
- آسیب پذیری کاربر مجاز شبکه

۳-۴-۲ مقابله با خطرات:

۳-۴-۲-۱ اقدامات مدیریتی:

مدیران شبکه‌ها با سیاستگذاری و وضع قوانینی، نحوه استفاده کاربران از شبکه و مسئولیت‌های آنان را مشخص کنند.

۳-۴-۲-۲ پیکربندی درست شبکه :

مدیران شبکه ها باید اطمینان پیدا کنند که تمام دستگاهها از کد هویت شخصی برای احراز هویت استفاده می کنند. همچنین در لایه کاربرد حفاظت برنامه ها باید با کلمه عبور تامین گردد.

۳-۴-۲-۳ نظارت اضافی بر شبکه :

بعضی برنامه های کاربردی تولید شده اند که امنیت شبکه های بلوتوث را کنترل می کنند و امنیت بیشتری را برای این شبکه ها فراهم می آورند. یکی از این برنامه ها Blue Watch می باشد که برای محیط ویندوز طراحی شده است.

۳-۵- Honeypot تدبیر نو برای مقابله با خرابکاران

Honeypot یکی از ابزارهایی است که متخصصین برخورد با هکرها و مدیران شبکه از آن برای شناسایی و به دام انداختن هکرها و نفوذگران استفاده می کنند. این وسیله از این بعد که می تواند اطلاعات بسیار دقیق و مفیدی از هکر و نحوه ی هک کردن را در اختیار مدیران شبکه قرار دهد بسیار مورد توجه است به گونه ای که تحقیقات گسترده ای در جهت ارتقا کارآمدی این وسیله در حال انجام است.

۳-۵-۱ تعریف Honeypot :

یک منبع سیستم اطلاعاتی می با شد که بر روی خود اطلاعات کاذب و غیرواقعی دارد و با ا ستفاده از ارزش و اطلاعات کاذب خود ســـعی در کشـــف و جمع آوری اطلاعات و فعالیت های غیرمجاز و غیرقانونی بر روی شبکه می کند. به زبان ساده Honeypot یک سیستم یا سیستمهای کامپیوتری متصل به شبکه و یا اینترنت ا ست که دارای اطلاعات کاذب بر روی خود می با شد و از عمد در شبکه قرار می گیرد تا به عنوان یک تله عمل کرده و مورد تهاجم یک هکر یا نفوذگر (Attacker) قرار بگیرد و با ا ستفاده از این اطلاعات آنها را فریب‌داده و اطلاعاتی از نحوی ورود آنها به شبکه‌و اهدافی که در شبکه دنبال می‌کنند جمع‌آوری‌کند.

۳-۵-۲ نحوه تشخیص حمله و شروع عملکرد Honeypot:

در مســـیر منتهی به Honeypot نباید هیچ ترافیکی ایجاد شـــود یعنی هرگونه ارتباطی با Honeypot فعالیت غیرمجاز و غیرقانونی محسوب شده و می‌تواند یک دزدی، حمله و یا سرقت محسوب شود.

۳-۵-۳ مزایای Honeypot :

۱- جمع آوری بسته های اطلاعاتی کم حجم ولی با ارزش:

Honeypot ها حجم کوچکی از اطلاعات را جمع آوری می کنند. مثلاً به جای ثبت روزانه GB[1] داده توســـط ســـایر تکنولوژی های برقراری امنیت اطلاعات، Honeypot مثلاً MB[1] اطلاعات جمع‌آوری می‌کند ولی چون مطمئن هســـتیم که اطلاعاتی که یک Honeypot جمع آوری می‌کند مربوط به فعالیتی غیرمجاز است در نتیجه این اطلاعات بسیار مفید بوده و تجزیه و تحلیل حجم کوچکی از اطلاعات آسان و ارزان است.

۲- ابزارها و تاکتیهای جدید:

Honeypot ها طراحی شـــده‌اند تا هر چیزی که به ســـمتشـــان منتهی می‌شـــود ثبت کنند بنابراین Honeypot می‌تواند ابزارها و تاکتیکهایی جدید را که هکرها به کمک آنها به ســـیســـتم حمله می کنند را ثبت کند.

۳- نیاز به کمترین سخت افزار برای پیاده سازی:

در یک کامپیوتر Pentium که دارای ۱۲۸ MBRAM است قابل پیاده سازی است.

۴- قابل پیاده‌سازی در میحط‌های IPV۶ و رمز شده:

برخلاف اغلب تکنولوژیهای امنیت (مثل سیستمهای IDS) که در محیط های رمز شده بخوبی کار نمی‌کنندHoneypot به راحتی قابل پیاده‌سازی در این محیط‌ها است و در این محیط‌ها به خوبی‌کار می‌کند.

۵- سادگی:

Honeypot ها بسیار ساده‌اند زیرا الگوریتم پیچیده ای ندارند که بخواهند توسعه یابند جداول حالت ندارند که نیاز به پشتیبانی داشته باشند.

۶- شناسایی نقاط ضعف سیستم:

مدیر سیستم می تواند با مشاهده تکنیک ها و روشهای استفاده شده توسط نفوذگر بفهمد که سیستم چگونه شکسته می شود و نقاط آسیب پذیر سیستم را شناسایی و نسبت به ترمیم آنها اقدام کند. هدف اصلی یک Honeypot شبیه سازی یک شبکه است که نفوذگران سعی می کنند به آن وارد شوند اطلاعاتی که بعد از حمله به یک Honeypot به د ست می آید می تواند برای کشف آ سیب پذیری های شبکه فعلی و رفع آنها استفاده شود.

۳-۵-۴ تقسیم بندی Honeypot از نظر کاربرد:

۱) Honeypot Production

۲) Research Honeypot

۳-۵-۴-۱ producation Honeypot:

این نوع سیستم وقتی که سازمان می خواهد شبکه و سیستم هایش را با کشف و مسدود کردن نفوذگران حفاظت‌کند و نفوذگر را از طریق قانون در دادگاه مورد پیگرد قرار دهد مورد استفاده قرار می‌گیرد. Honeypot هایی که کاربرد production دارند به سه طریق می توانند در برابر حملات از شبکه محافظت کنند.

۱) به روش prevention (پیشگیری)

۲) به روش Detection (کشف یا شناسایی)

۳) به روش Response (پاسخ)

۳-۵-۴-۱-۱ Prevention :

در بعضـــی‌از حملات نفوذگران با اســـتفاده از ابزارهایی رنجی از شـــبکه‌ها را پویش می‌کنند تا آسیب‌پذیری سرورهای موجود در شبکه را شناسایی کنند این ابزارها پس از پیدا کردن آسیب پذیریهای موجود در سیستم به این سیستمها حمله می کنند در روش پیشگیری Honeypot سرعت این گونه حملات را کند می‌کند و حتی بعضـــی اوقات آنها را متوقف نیز می کند به این دســـته از Honeypotها، Honeypot های چســـبنده (Sticky) می گویند در این روش Honeypot هنگام پویش توســـط نفوذگر نسبت به آدرسهایی که در شبکه موجود نیست واکنش نشان می دهد Labrea Tarpit جزو این دسته از Honeypot ها است. به طور کلی هدف پیشگیری (Prevention) کند کردن سرعت عملیات نفوذگر و توقف حمله است.

۳-۵-۴-۱-۲ Detection (کشف یا شناسایی):

وظیفه اش عمل کشف و شناسایی ناتوانی های بخش پیشگیری است کشف یک حمله کار بسیار مشکلی است. وقتی یک حمله شناسایی شود می توان خیلی سریع به آن واکنش نشان داد و آن را متوقف و یا حداقل اثرش را کم کرد می توان از تکنولوژیهای امنیتی مثل IDS و فایلهای ثبت وقایع (Log) در مرحله شناسایی استفاده کرد ولی بدلیل اینکه این تکنولوژی ها داده های زیادی را ثبت می کنند تجزیه و تحلیل آنها زمانبر اســت و بســیاری از این داده ها غیر مفید بوده و در شـناســایی نفوذگر و اهدافش ما را کمک نمی کنند و در محیط های رمز شـده نیز بخوبی کار نمی کنند. Honeypot ها در کشـف و ردیابی یک حمله نســـبت به تکنولوژیهای مذکور برتری دارند. Honeypot داده های کم و با درجه اطمینان درستی بالاتری جمع آوری می کنند که تجزیه و تحلیل آنها آسان بوده و ارزش بیشتری دارند. همچنین Honeypotها در محیط های رمز شده نیز می توانند بخوبی کار کنند.

۳-۵-۴-۱-۳ Response (پاسخ):

یکی از چالشهایی که هر سازمانی می تواند با آن روبرو شود این است که بعد از شناسایی و کشف حمله چگونه به آن پاسخ دهد معمولا در پاسخ مناسب به یک حمله دو مشکل وجود دارد. اول اینکه اکثر سیستمهایی که مورد حمله قرار گرفته اند را نمی توان بخاطر تجزیه و تحلیل مناسب از کار انداخت زیرا online بودن آنها امری ضروری و حیاتی است دوم اینکه حتی اگر سیستم را نیز از کار بیاندازیم به دلیل وجود کثرت داده ها در سیستم تشخیص داده های متعلق به نفوذگری آسان نیست. بنابراین این اســـتفاده از Honeypot در چنین ســـازمانی این امکان را فراهم می کند که در مواقع لزوم برای تجزیه و

تحلیل کامی داده ها آنها را از شبکه خارج کنیم بدلیل اینکه Honeypot همیشه فعالیتهای غیرقانونی و بد اندیشـــانه را ذخیره می کند بنابراین مطمئن هســـتیم که اطلاعات موجود در آنها مربوط به یک هکر و یا یک نفوذگر ا ست و به همین دلیل ا ست که تجزیه و تحلیل یک Honeypot هک شده بسیار آ سانتر از یک سیستم واقعی است و در نتیجه می توان در برابر حمله پاسخ سریع و موثری داد.

۳-۵-۴-۲ Research Honeypot :

این نوع سیستم وقتی که سازمان می خواهد فقط امنیت شبکه و سیستمهای خود را با آموختن روشهای نفوذ، منشا نفوذ، ابزارها و Exploit های مورد استفاده نفوذگر مستحکم تر کند، استفاده می شود.

۳-۵-۵ تقسیم بندی Honeypot از نظر میزان تعامل با نفوذگر:

Honeypot ها از لحاظ میزان تعامل و درگیری با نفوذگر به سه دسته تقسیم می شود.

۱- Low Interaction Honeypots (Honeypotهای با تعامل کم)

۲- (Medium Interaction Honeypots Honeypot های با تعامل متوسط)

۳- High Interaction Honeypots (Honeypot های با تعامل بالا)

Interaction نوع ارتباطی که نفوذگر با Honeypot دارد را مشخص می کند.

۳-۵-۵-۱ Low Interaction Honeypots:

ارتباط و فعالیتی محدود با نفوذگر دارند و معمولاً با سرویسها و سیستم عاملهای شبیه سازی شده کار می‌کنندو ســـطح فعالیت‌نفوذگر را محدود به ســـطوح شـــبیه‌ســـازی شـــده می‌کنند به عنوان‌مثال LowInteraction Honeypots می تواند شـــامل یک Windows Server 2000 به همراه سرویسهای مثل Telner و FTP باشد. یک نفوذگر می تواند ابتدا با استفاده از Telner روی Honeypot نوع سیستم عامل آن را تشخیص داده سپس با حدس زدن رمز عبور و یا با هر روش دیگری وارد شبکه شود بدون اینکه اطلاع داشته باشد که در یک گرفتار شده است. بر اساس فعالیتی که نفوذگر در می تواند اطلاعات زیر را جمع آوری کرده و در اختیار متخصص شبکه قرار دهد.

۱) زمان نفوذگر و یا هکر به سیستم

۲) پروتکلی که از آن استفاده کرده

۳) آدرس FTP مبدا و مقصد

در این نوع Honeypot، نفوذگر نمی تواند هیچ گونه ارتباطی با سیستم عامل برقرار کند و این مساله میزان خطر را کاهش می دهد چون پیچیدگیهای سیستم عامل حذف می شود و به دلیل اینکه ما سطح فعالیت نفوذگر را محدود کرده ایم بنابراین اعمالی که نفوذگر انجام می دهد محدود شده و در نتیجه Honeypot اطلاعات‌محدودی را می‌تواند ثبت کند. این نوع Honeypot فقط قادر به شناسایی حمله‌های شناخته شده است و نمی‌تواند حمله های ناشناخته را تشخیص دهد. سادگی نگهداری‌و توسعهHoneypot کم واکنش همچنین پایین بودن ریسک خطر آن از نقاط قوت Honeypot کم واکنش محسوب می شود. از این Honeypotها می توان برای اهداف Production استفاده کرد.

۳-۵-۵-۲ Honey Pot با تعامل متوسط(HoneyPot Medium Intraction):

Honeypot با تعامل متوسط در مقایسه با Honeypot نوع کم واکنش امکان بیشتری برای تعامل با نفوذگر فراهم می کند ولی هنوز هم نفوذگر هیچ ارتباطی با سیستم عامل ندارد Daemon های جعلی فراهم شده پیشرفته ترند و دانش بیشتری راجع به سرویسهای ارائه شده دارند. در این حالت میزان خطر افزایش می یابد. احتمال اینکه نفوذگر یک حفره امنیتی یا یک نقطه آسیب پذیری پیدا کند بیشتر است زیرا پیچیدگی Honeypot افزایش می یابد و نفوذگر امکان بیشتری برای ارتباط با سیستم و بررسی آن دارد و راحت‌تر فریب می‌خورد.

همچنین با توجه به تعامل بیشتر، امکان حمله های پیچیده تری وجود دارد که می توان با ثبت و آنالیز کردن آنها به نتایج دلخواه دست یافت. همانطوری که گفته شد نفوذگر هیچ ارتباطی با سیستم عامل ندارد و در سطح برنامه های کاربردی فعالیت می کند. توسعه یک Honeypot با تعامل متوسط کاری پیچیده و زمانبر است. باید دقت شود که تمام Daemon های جعلی تا جایی که ممکن است ایمن شوند. نسخه های توسعه یافته این سرویسها نباید دارای همان آسیب‌پذیری نسخه های واقعی باشند زیرا این اصلی ترین دلیل جایگزینی‌آنها با نسخه‌های‌جعلی است. کسی‌که می‌خواهد چنین سیستمی‌را طراحی و پیاده سازی کند،باید از دانش‌خوبی‌درمورد پروتکلها، سرویسها و برنامه‌های‌کاربردی ارائه شده برخوردار باشد ازاینHoneypotها می‌توان هم برای اهداف دسته Research و هم برای اهداف‌دسته Production استفاده‌کرد.

۳-۵-۵-۳ High Interaction Honeypot:

یکی از اهداف نفوذگر امکان دسترسی به اطلاعات در ماشینی که به اینترنت وصل است می باشد این نوع Honeypot چنین امکانی را در اختیار نفوذگر قرار می دهد. به محض اینکه نفوذگر این امکان را پیدا کند کار اصلی او شروع می شود در این نوع Honeypot ما یک سیستم واقعی را در اختیار نفوذگر قرار می‌دهیم و هیچ چیز شبیه سازی شده نیست و نفوذگر با سیستم عامل واقعی و شبکه واقعی سر و کار دارد و میزان دسترسی وی به شبکه بیشتر است در نتیجه میزان عملی که می تواند انجام دهد بیشتر شـده و Honeypot می تواند فعالیت بیشـتری از نفوذگر و اهداف مورد نظر وی جمع آوری کند. از این Honeypotها می توان برای اهداف دسته Reseach استفاده کرد.

۳-۵-۵-۳-۱ مزایای استفاده از High Interaction Honeypot :

متخصص شبکه با تجزیه و تحلیل اطلاعات Honeypot می تواند اطلاعات زیر را در مورد نفوذگر بدست آورد.

- نفوذگران بیشتر از چه ابزارها و Exploitهایی استفاده می کنند.
- از چه کشورهایی هستند.
- به دنبال چه نقاط آسیب پذیری هستند
- میزان دانش آنها در مورد نفوذگری
- جمع آوری اطلاعات و اسناد زیاد برای تحلیل
- به دلیل و سیع بودن سطح فعالیت نفوذگر اغلب این نوع Honeypot ها رفتارهایی از فرد نفوذگر را به ما نشان می دهند که ما انتظار نداشته ایم و یا نمی توانسته ایم حدس بزنیم.

۳-۵-۵-۳-۲ معایب استفاده از High Interaction Honeypot:

- طراحی، مدیریت و نگهداری آن فوق العاده زمانبر است.
- سیستم باید دائماً تحت نظر باشد در غیر این صورت نه تنها هیچ کمکی نمی کند بلکه خودش به عنوان یک نقطه خطر یا حفره امنیتی مطرح می شود.
- دارای ریسک بالا زیرا نفوذگر یک سیستم واقعی را در اختیار دارد و ممکن است به سیستم های اصلی شبکه صدمه بزند. بنابراین هیچ سیستمی بر روی شبکه را نمی توان امن در نظر گرفت.

فصل چهارم

مفهوم GPRS با رویکردIT

۴-۱- ویژگیهای GPRS

GPRS یک سرویس ارزش افزوده جدید در نسل سوم تلفن همراه است که امکان ارسال و دریافت اطلاعات با دیتا را روی شبکه تلفن همراه فراهم می رساند.

GPRS مخفف General packet Radio service (سرویس عمومی پکتهای رادیویی) است که در حقیقت تکمیل شده اطلاعات سوئیچینگ مداری (SMS(circute switching می باشد.

در ابتدای امر ذکر این‌نکته ضروری است که GPRS هیچ ارتباطی با GPS(-Global positioning system – سیستم جهانی موقعیت سنجی) ندارد.

GPRS در حقیقت یک لایه Packet-switched به شبکه GSM موجود در موبایل شما اضافه می‌کند که خیلی بهتر از استاندارد ارتباطی Circute switched شبکه GSM است.

GPRS دارای چند مشخصه و یا قابلیت مهم است که از آن جمله می توان به موارد زیر اشاره کرد.

۱- سرعت:

از مشخصه GPRS می توان به سرعت بالای آن اشاره کرد که به طور تئوری این سرعت متجاوز از ۱۷۱،۲ kb/s است که این سرعت در صورتی قابل دسترس است که برای سیستم GPRS از ۸ تایم اسلات بصورت همزمان استفاده شود و این سرعت تقریباً ۲ تا ۴ برابر بیشتر از سرعت ۵۶ kb/s معمولی برای

انتقال دیتا در شبکه‌های مخابراتی و تقریباً ۱۰ برابر سریعتر از سرویس سوئیچینگ مداری (switching Circute) روی شبکه GSM است.

خطوط معمولی موبایل حداکثر دارای سرعت ۹،۶kb/s می باشند که در صورت استفاده از سرویس High speed Circute Switched Data یا HSCSD حداکثر می توانند از سرعت ۱۴،۴ kb/s بهره ببرند در حالی که با GPRS به صورت عملی به راحتی می توان با سرعت ۴۰kb/s به اینترنت متصل شد.

۲- طریقه اتصال:

GPRS به ما این امکان را می دهد تا همواره ارتباط خودمان را با اینترنت حفظ کنیم و دیگر نیازی نیست برای برقراری ارتباط هر بار به شرکت ارائه دهنده سرویس اینترنت وصل شویم.

۳- هزینه:

برتری دیگر GPRS این است که لازم نیست که ما به میزان زمان ارتباطمان که با GPRS ساپورت می شود پول پرداخت کنیم بلکه هزینه ما معادل حجم اطلاعاتی می با شد که دریافت و یا ار سال کرده ایم، یعنی شما مبلغ ارتباط خود را بر اساس مقدار اطلاعات ورودی و خروجی به شرکت ارائه دهنده سرویس می پردازید و نه بر اساس مدت زمانی که به اینترنت متصل هستید. این به آن معنا است که ممکن است شما تمامی روز بر روی اینترنت باشید اما فقط در هنگام ارسال یک پیغام مبلغی را پرداخت کنید.

پلاس GPRS تمام پروتکل های IP را ساپورت می کند و به صورتی موثر یک لینگ همیشه رو شن می باشد به این معنی که لازم نیست پیغام را از طریق سرور ارسال کنید بلکه می توانید آنها را مستقیماً به وسایل ارتباطی دستی یا موبایل بفرستید. امروزه تمام اپراتورهای شبکه های بزرگ از شبکه GPRS استفاده می کنند ولی امکان اضافه کردن این قابلیت به تمام وسایل موبایل نیست.

PC های کتابی (notebook) و وسایل دستی ارتباطی می توانند با آداپتورها (تنظیم کننده های) GPRS تکمیل شوند. البته اگر موبایل شما GPRS را ساپورت نمی کند باید آن را ارتقا دهید که این قطعات را می توانید از تمام فروشنده های اصلی و بزرگ تهیه کنید.

۴- فوریت:

یکی دیگر از مزایای GPRS که در حقیقت پیامد سرعت بالا و اتصال دائم آن است خصوصیت فوریت است که برای کارهای بحرانی نظیر کنترل کارتهای اعتباری خیلی مهم است.

۵- استفاده از کاربردهای اینترنتی:

نظیر FTP,Chat,Mail ... که توضیح آن در ادامه داده می شود.

۴-۱-۱ موارد لازم برای استفاده از GPRS

۱) گوشی موبایلی که توسط GPRS حمایت شود: یعنی تنها، گوشی های مبتنی بر شبکه GSM نمی‌توانند از سرویس GPRS استفاده کنند بلکه باید خود گوشی سرویس GPRS را حمایت کند.

۲) داشتن یک اشتراک به شبکه موبایلی که GPRS را حمایت می کند.

۳) استفاده از GPRS باید برای کاربر فعال شود: معمولاً دسترسی اتوماتیک به شبکه GPRS توسط بعضی از شبکه های اپراتوری موبایل فعال می شود.

۴) داشتن دانش چگونگی ارسال و دریافت اطلاعات روی سرویس GPRS

۵) مشخص بودن یک مقصد برای ارسال یا دریافت اطلاعات از طریق GPRS (در صورتیکه با SMS این مقصد غالباً یک گوشی موبایل دیگر است.) در صورتیکه در GPRS باید این مقصد مثلاً یک آدرس اینترنتی باشد.

۴-۱-۲ ویژگیهای سیستم سوئیچینگ پکتی

سیستم سوئیچینگ پکتی این امکان را در اختیار شبکه می گذارد که اطلاعات قبل از ارسال به قسمتهای کوچک و جدا از هم ولی مرتبط با هم به نام پکت تجزیه شده و دوباره در انتهایی ترین نقطه دریافت با هم ترکیب شود. در واقع سوئیچینگ پکتی شبیه یک پازل است، مجسم کنید که در یک کارخانه تولید پازل، پازل تهیه می شود، برش می خورد و به تکه های زیادی تقسیم می شود سپس داخل یک کیسه پلاستیکی قرار می گیرد، در طی انتقال از کارخانه به کاربر انتهایی این تکه ها حسابی بهم می ریزد. کاربر انتهایی کیسه را خالی می کند و تمام تکه ها را دوباره جمع می کند و کنار هم می گذارد و دوباره پازل به شکل اصلی در می آید. ذکر این نکته ضروری است که اینترنت بهترین مثال برای شبکه دیتا مبتنی بر Packet می باشد.

در سرویسGPRS، برای ارسال و دریافت اطلاعات سوئیچینگ پکتی از منابع رادیویی استفاده می‌کنند یعنی یک کانال رادیویی برای انتقال اطلاعات اختصاص داده می شود. این کانال ها یا منابع رایویی در یک پریود زمانی ثابت می تواند بصورت توافقی بین چندین کاربر Share بشوند.

تعداد این کاربران بستگی دارد به Applicationها یا کاربردهایی که استفاده می شود و مقدار دیتایی که منتقل می شود.

برای اولین بار توسط سرویس GPRS همکاری بین شبکه اینترنت و شبکه تلفن همراه بوجود آمد و باعث این شد که هر سرویس که استفاده می شود از شبکه اینترنت نظیر Telnet, Email , Web browsing, FTP از طریق شبکه موبایل بوسیله GPRS قابل، دسترس باشد و همچنین باعث بوجود آمدن سرویس های اینترنت Wireless توسط Service provider ها شد.

www (world wide web) اولین اینترفیس ارتباطی مردم برای دسترسی به اینترنت برای تفریح، بدست آوردن اطلاعات، دسترسی به اطلاعات کمپانی ها مختلف، تماس با دوستان و همکاران و ... است.

Web browsing (مرورگر web) یک application خیلی مهم برای GPRS است.

علت استفاده از همان پروتکلهای اینترنت برای شبکه GPRS این است که در حقیقت شبکه GPRS را می توان یک شبکه اصلی Subnetwork در نظر گرفت و هر کدام از گوشیهای موبایل را نیز به عنوان یک host ، یعنی هر ترمینال GPRS می تواند قابلیت داشتن یک IP Address را داشته باشد و همچنین قابلیت آدرس دهی را.

در اینجا ذکر این نکته لازم است که GPRS مانند خود شبکه موبایل محدودیتهایی هم دارد که از آن جمله می توان به محدودیت ظرفیت Cell برای User ها نام برد و یا محدودیت منابع رادیویی، و همچنین اینکه رسیدن به ماکزیمم سرعت تئوری (۱۷۱،۲ kb/s) احتیاج به این دارد که ۸ تایم اسلات بصورت همزمان برای تنها یک کاربر استفاده بشود که این عملاً غیرممکن است.

– در این جا باید به یک مزیت Circute switching نسبت به packet switching اشاره کرد که تاخیر ترانزیت می باشد.

در سیستم packet switching امکان گم شدن یا از بین رفتن packet ها وجود دارد که ارسال مجدد آن باعث بوجود آمدن Delay یا تاخیر ترانزیت می شود در صورتیکه در سیستم Circute switching به دلیل اختصاص یک مدار در کل مدت ارسال بین فرستنده و گیرنده این مشکل بسیار به ندرت اتفاق می افتد.

– GPRS در حال حاضر دارای دو فاز می باشد که فاز اول آن در سال ۲۰۰۰ تا ۲۰۰۱ فعال شد و امکان ارسال اطلاعات از یک کاربر به تنها یک کاربر دیگر را در یک زمان فراهم می کرد (Point to point) و فاز دوم آن که هنوز به طول کامل تعریف نشده انتظار می‌رود از نرخ بالای ارسال دیتا از طریق

تکنولوژیهای نظیر EDGE و همچنین از سال Point to Multipoint و یا از سال اطلاعات از یک کاربر به چند کاربر GPRS در یک زمان حمایت کند.

۴-۱-۳ کاربردهای GPRS

رنج وسیعی از کاربردهای اینترنتی توسط سرویسهای nonvoice شبکه موبایل مانند SMS و GPRS فعال هستند که خصوصاً این کاربردها برای سرویس GPRS بسیار مناسبند از جمله این کاربردها می توان به موارد زیر اشاره کرد.

Chat بطور خلاصه می توان گفت که با سرویس Chat می توان دسترسی به منابع مختلف اطلاعات پیدا کرد. بوسیله این سرویس هر فرد می تواند عضو گروههای (community) مختلف محبوب خود شده و در این زمینه با دیگر افراد تبادل اطلاعات انجام دهد. همانطور که در فازهای مختلف GPRS گفته شده در فاز اول امکان حمایت GPRS از Chat وجود ندارد که به علت عدم سرویس Point to Multipoint می باشد ولی این امکان در فاز دوم عملی می شود.

۴-۱-۴ اطلاعات متنی و قابل مشاهده

رنج وسیعی از اطلاعات متنی می تواند به گوشی موبایل کاربران توزیع شود که از آن جمله می توان به امتیازبندی مسابقات ورزشی، وضعیت آب و هوا، اطلاعات پرواز، تیترهای مهم اخبار، اوقات شرعی، نتایج لاتاری، جوک، طالع بینی، و ضعیت ترافیک- موقعیت مکانی و... ا شاره کرد. این اطلاعات لازم نیست که حتماً بصورت متن باشند بلکه می توانند. بصورت تصویر یا گرافیک و یا دیگر انواع اطلاعات قابل مشاهده نیز باشد.

طول پیام کوتاه با SMS ، ۱۶۰ کاراکتر، برای توزیع اطلاعات هنگامیکه دارای حجم کمی هستند مانند امتیازات ورزشی، درجه حرارت هوا یا نرخ ارز مناسب است ولی هنگامیکه حجم اطلاعات زیاد باشد مانند اخبار یا طالع بینی، با ۱۶۰ کاراکتر فقط می شود عنوان یا تیتر موضوع را اطلاع داد و این باعث تحریک کاربر همیشه به همین علت برای توزیع اطلاعات کوتاه از SMS و برای ارسال و توزیع پیامهایی با کیفیت بالا و محتوای زیاد از GPRS استفاده می شود.

۴-۱-۱ Images : تصاویر ثابت

Image ها مانند عکس، کارت پستال، کارت تبریک و صفحات ثابت Web می تواند از طریق شبکه موبایل فرستاده و یا دریافت بشود همان طوری‌که آنها از شبکه های تلفن ثابت عبو می کند (مانند Fax).

۴-۱-۴-۲ تصاویر متحرک

ارتباطات موبایل به مرحله ای رسیده که دیگر کمتر Text منتقل می شود و بیشتر تصویر است که منتقل می‌شود صنعت Wireless در حال حرکت از پیغامهای متنی به سمت پیغامهای تصویری، تصویری، عکس‌ها، تصاویر ویدیویی و فیلمهای Download شده می باشد از امکان ارسال تصاویر متحرک می توان برای کاربردهای مانند Monitoring parking lost (نمایش تعداد جای پارک موجود) و یا فرستادن تصاویر از بیمار داخل آمبولانس به بیمارستان و یا ویدیوکنفرانس و ... استفاده کرد.

۴-۱-۵ مرورگر web یا web browser

استفاده از سوئیچینگ مداری دیتا برای مرورگر وب یک کاربرد پر دوام برای استفاده کننده های موبایل نبوده که این به علت سرعت پائین سوئیچینگ مداری است که باعث می شود مدت زمان زیادی طول بکشد تا دیتا از سرور اینترنت به مرورگر وب برسد و به همین علت ممکن است کاربر از تصاویر صرف نظر کند و فقط از متن استفاده کند و آن هم ممکن است در انتها به مشکل برخورد کند.

به همین علت مرورگر وب موبایل بهتر است که روی سرویس GPRS برقرار بشود.

با مرورگر وب به راحتی می توان با سرعتی معدل خطوط تلفن معمولی یعنی ۵۶ kb/s صفحات مورد علاقه خود را مرور کرد.

۴-۱-۵-۱ Document های اشتراکی یا کارهای گروهی

از دیگر امکانات GPRS می توان به اشتراک Document ها اشاره کرد. این امکان اجازه می دهد مردم از جاهای مختلف روی یک Document بصورت مشترک در یک زمان کار کنند و در این زمینه اطلاعات کسب شده خودشان را برای تبادل نظر به اشتراک بگذارند. در حقیقتGPRS به ما این امکان را می دهد تا همواره به تقویم کاری و یا اطلاعات اشتراکی همکاران خود دسترسی داشته باشیم.

۴-۱-۵-۲ ایمیل یا پست الکترونیکی

با توجه به ارتباط دائمی با اینترنت و پرداخت هزینه به ازای اطلاعات ورودی- خروجی، شما می‌توانید به نامه‌های الکترونیکی دو ستان یا همکاران خود در هر زمان با حداقل هزینه و حداکثر سرعت پاسخ دهید و یا برای کارهای فوری به دیگران نامه بفرستید.

Plat form ایمیل wireless پیغامها را از پروتکل SMTP (پروتکل ایمیل اینترنت) به SMS براحتی ترجمه می کند و به SMS center می فر ستد. در این نوع سرویس ایمیلها ذخیره می شوند و کاربر یک هشدار (Alert) روی گوشی موبایلش می گیرد و سپس می تواند تمام ایمیلهایش را چک کند.

۴-۱-۶ MMS

تنها بستری که شما می توانید از امکانات صدا، تصویر و ویدئو در سیستم MMS یا (Multi media Messaging serving) که نسخه پیشرفته SMS می باشد، بطور کامل بهره مند شوید، GPRS می باشد.

۴-۱-۷ رتبه کاربرد محیط

۱. پست الکترونیکی داخلی شرکت GPRS

۲. پست الکترونیکی بر روی اینترنت GPRS/SMS

۳. سرویس های اطلاعاتی GPRS

۴. انجام کارهای روزمره GPRS

۵. دسترسی به LAN از راه دور GPRS

۶. انتقال اطلاعات GPRS

۷. مرورگر وب GPRS

۸. دیدن تصاویر غیرمتحرک GPRS

۹. دیدن تصاویر متحرک GPRS/HSCSD

۱۰.گپ دوستانه GPRS/SMS

۱۱. انجام کارهای خانه

۱۲. انجام کارهای گروهی

۱۳. صدا GPRS

۴-۱-۸ کارآیی GPRS :

GPRS در تئوری باید بتواند سرعت انتقال اطلاعات را به ۱۷۱kb/s برساند در حالی که در عمل این سرعت به ۴۰kb/s می رسد. حال آنکه سرعت ارتباط در دستگاههای متفاوت GPRS به مراتب با یکدیگر فرق می کنند.

برای محاسبه سرعت ارتباطات در دستگاههای GPRS بهتر است طرح کدها و ساختمان کلاسهای مربوط به آن را متوجه شویم.

GPRS در کل دارای چهار نوع کد CS۱/CS۲ /CS ۳/CS ۴ می باشد. هر کدام از این کدها قابلیت انتقال اطلاعات، حداکثر با سرعت ۲۱،۴ کیلو بیت در ثانیه را دارند و در هر یک از آنها قسمتی برای تصحیح خطا، در انتقال اطلاعات در نظر است.

CS1 دارای بیشترین سهم برای تصحیح اطلاعات می باشد و فقط در حدود۹ کیلو بیت در ثانیه از ۲۱۰۴ کیلو بیت در ثانیه جهت انتقال اطلاعات باقی می ماند.

CS۲/CS ۳ دارای سرعت بیشتری می باشند و سرعت انتقال اطلاعات در آنها به حدود ۱۳/۴kb/s در CS2 و ۱۵،۶kb/s در CS3 می رسد.

و درcs۴ سرعت انتقال به حداکثر مقدار خود می رسد و هیچ نوع تصحیح اطلاعاتی در این قسمت انجام نمی گیرد. (۲۱/۴ kb/s)

دستگاههای موجود GPRS، تنها CS۲ ، CS۱ را با سرعتی پائین تر ارائه می دهند و در مواقع لازم این دو به جای یکدیگر مورد استفاده قرار می گیرند.

شبکه های GSM و GPRS هر دو امکان استفاده از Timeslot/8 را در هر لحظه از زمان دارند. لذا سرعت انتقال اطلاعات را می توان با کنار هم قرار دادن تایم اسلات ها بیشتر و بیشتر کرد. در عمل سرعت انتقال به علت محدودیت ایجاد شده توسط شرکت ارائه دهنده خدمات و همین طور محدودیت موجود در دستگاهها کاهش می یابد.

همان طور که گفتیم دستگاههای GPRS قادر هستند تعداد محدودی تایم اسلات را با یکدیگر ادغام کنند و بر این اساس به کلاسهای مختلفی تقسیم می شوند کلاس ۲ تنها یک slot برای ارسال اطلاعات و دو solt برای دریافت اطلاعات دارد.

در حالیکه کلاس ۱۲ دارای پنج solt برای هر تنظیمی می باشد.

کلاس ۶ معمول ترین کلاس بکار رفته در دستگاههای GPRS می باشد که یک slot برای ارسال اطلاعات و سه slot برای دریافت داده ها دارا می باشد.

۴-۲ مفهوم شبکه های GSM

شروع شکل گیری GSM در اروپا اوایل دهه ۱۹۸۰ است.در آن زمان اروپا با رشد چشمگیر سیستم سلورلار آنالوگ مواجه بود.۴۵۰۰- C آلمان، پرتقال،TACS اسپانیا، ایتالیا، ایرلند،NMT اسکاندیناوی، RADICOM فرانسه،RTMS ایتالیا،که هیچ کدام با هم سازگار نبود. به همین علت اتحادیه اروپا در سال ۱۹۹۲ یک گروه مطالعاتی تشکیل داد با عنوان Groupe Special Mobile که بعداً به Global System For Mobile Communication تغییر نام یافت.

این گروه موظف بود سیستم موبایلی را برای استفاده در سطح اروپا پیشنهاد نماید که جوابگوی موارد ذیل باشد.

بهبود کیفیت، سیستم و پایانه کم هزینه ، حمایت از جابجایی بین المللی ، حمایت از پایانهای دستی،حمایت از سرویس ها ،استفاده بهینه از طیف فرکانسی، سازگاری با ISDN امروزه GSM رایج ترین تکنولوژی نسل دوم اس که در ۱۱۰ کشور دنیا راه اندازی شده است.

۴-۲-۱ توانایی GSM

این شبکه (GSM) توانایی انتقال Data با سرعت ۹۶۰bps را دارد، بدین معنی که کاربر GSM با این سرعت ها می تواند به کاربران دیگر در GSM و نیز کاربران شبکه های سوئیچ مداری و سوئیچ پاکتی و صل و به مبادله دیتا پردازد.مهمترین سرویس GSM همان سرویس تلفنی می با شد به طوریکه ارتباط تلفنی بین کاربران GSM و هر مشترک تلفنی در سراسر دنیا وجود داشته باشد.

بخ شی از مجموعه ا ستاندارد GSM برای شبکه تلفن همراه می با شد، به عنوان مثال شیوه عر صه سرویس پیام کوتاه در شبکه های موبایل از استاندارد ۰۳۰۴۰ تعریف شده است.

۴-۲-۲ شبکه GSM

GSM یک توصیه کننده می باشد و نوع تجهیزات را مشخص نمی کند. خصوصیات GSM اعمال و رابطه ها را مشخص می کند ولی سخت افزار را معرفی نمی کند.

نتیجه:کاهش محدودیت طراحان تاحدامکان افزایش انتخاب درخرید از تهیه کنندگان مختلف می باشد.

۴-۲-۳ شبکه GSM

شبکه GSM به سه سیستم اصلی تقسیم می شود.

سیستم سوئیچینگ (SS) ، سیستم ایستگاه پایه (BSS)،سیستم پشتیبانی و عملیاتی (OSS)

۴-۲-۳-۱ سیستم سوئیچینگ (The Switching Syst em)

Ss مسئول انجام پردازش های تماس و عملیات مربوطه با مشترک است سیستم سوئیچینگ از واحدهای عملیاتی زیر تشکیل می شود:

ثبت کننده موقعیت گذرا (VLR) ، مرکز تایید (AUC)، ثبت کننده موقعیت دائم (HLR)، ثبت مشخصه تجهیزات (EIR)

۴-۲-۳-۲ سیستم ایستگاه پایه (The Base Station System)

تمام اعمال رادیویی در BSS انجام می پذیرد که BSS شامل کنترل کننده های ای ستگاه پایه (BSC) و ایستگاه های انتقال پایه (BTS) می با شد. BSC(Base station controllers) کلیه اعمال کنترلی و لینکهای فیزیکی بین BTS, MSC را انجام می دهد.

BTS(Base transceiver station)

BTS رابطه رادیویی به دستگاه موبایل را تنظیم می کند.

۴-۲-۴ سیستم پشتیبانی و عملیاتی (The operation support system)

یک نهاد اجرایی ا ست که عملیات شبکه و سیستمهای کنترلی را نمایش می دهد. هدف OSS ارائه پشتیبانی موثر جهت عملیات مرکزی، منطقه‌ای و ناحیه‌ای و فعالیتهای مورد نیاز جهت شبکه GSM می‌باشد.

فصل پنجم

بررسی ومطالعه نسل‌های مختلف موبایل و تهیه SMS در شبکه های موبایل

مقدمه

موارد استفاده از شبکه های بی سیم :

- ☒ توسعه شبکه در نواحی که کابل کشی سخت و غیرممکن است. نظیر دریا، رودخانه و ...
- ☒ توسعه شبکه برای استفادههای موقت
- ☒ عدم امکان کابل کشی در ساختمانهای تاریخی

اولین ارتباط رادیویی در سال ۱۸۹۵ (چند سال بعد از اختراع تلفن)، توسط Guglielmo Marconi، بین نقطه ای در ساحل Isle of wight و یک کشتی یدک کش (در فاصله ۱۸ مایلی یکدیگر) صورت گرفت.

۶ سال بعد او توانست یک سیگنال رادیویی را با موفقیت از عرض اقیانوس اطلس منتقل نماید (از cornwall به New found land) در سال ۱۹۰۲ نیز اولین ارتباط دو طرفه بر فراز اقیانوس اطلس برقرار شد اولین تلفن رادیویی نیز در تاریخ ۱۹۱۵ زمانی که اولین ارتباط رادیویی بین کشتی ها برقرار شد.

اولین تلفن موبایل

اولین سیستم عمومی تلفن موبایل با عنوان Mobile Telephone = MTS System در ۲۵ شهر آمریکا راه اندازی گردید.

۵-۱-۱ مزایا و معایب MTS :

- ☒ Transciver های این سیستم آنقدر بزرگ بودند که فقط با ماشین قابل حمل بودند.
- ☒ استفاده نا کارآمد از طیف فرکانسی
- ☒ سوییچینگ دستی
- ☒ MTS یک سیستم آنالوگ بود.
- ☒ Half- duplex کار می کرد. یعنی کاربر می توانست در یک زمان یا صحبت کند یا گوش بدهد. و برای انتخاب هر کدام از حالتها باید دکمه ای را فشار بدهد.
- ☒ استفاده از یک BS با یک آنتن پر توان که بتواند کل ناحیه تحت پوشش را جوابگو باشد.

IMTS سیستمی بود که بعد از آن آمد و قادر بود که:

کانال های بیشتری فراهم کند. سوییچینگ را به طور خودکار انجام دهد اگر چه که امروزه مبدا تاریخی تلفن سلولی را معرفی نسل اول سیستم سلولی ۱G می دانند، ولی تفاوت عمده سیستم های ۱G و MTS/IMTS در استفاده از مفهوم سلولار است.

با وجودی که سیستم‌های ۱G به خاطر استفاده از سیگنالینگ آنالوگ، امروزه ابتدایی تلقی می‌گردند، ولی هنوز هم عده کثیری در آمریکای شمالی از این سیستم‌ها استفاده می‌کنند.

۵-۱-۲ سیستم های سلولی آنالوگ

آمریکا، اولین سیستم آنالوگ تجاری در آمریکا با عنوان Mobile phone System (Advanced)AMPS در سال ۱۹۸۲ با توانایی انتقال صوت ارائه گردید.

AMPS بسیار موفق بود به طوریکه در حال حاضر میلیونها نفر در آمریکا و استرالیا مشترک این سیستم هستند. AMPS در کانادا، آمریکای مرکزی و جنوبی و استرالیا نیز راه اندازی گردید.

AMPS باند فرکانسی را به چند کانال ۳۰ khz کرد. کانال ها یا برای صوت بودند یا کانالهای کنترلی، کانال های مکالمه از مدولاسیون فرکانسی (FM) استفاده می‌کردند، در حالیکه کانال های کنترلی از BFSK (Binary Frequency Shift Keying) با سرعت ۱۰kb/s استفاده می کردند.

AMPS در سیگنالهای کنترلی‌خود هم‌از Frequency tones وهم از Data messages استفاده‌می‌کند.

برای مقابله با تداخل کانال ها با یکدیگر نیز

ا لف) طرح‌استفاده مجدد از فرکانس با۱۲ گروه فرکانسی‌که‌با آ نتهای omni directionalدسته‌بندی‌می‌شوند.

ب) دسته های ۷ گروهه با سه بخش در هر سلول

باند فرکانس ۸۲۴–۸۴۹ MHz و ۸۶۹–۸۹۴MHz است. در هر ناحیه جغرافیایی دو سرویس پرووایدر می توانند حضور داشته باشند و یکی از باندهای فرکانسی ۲۵MHz را در اختیار بگیرند. (A یا B)

اروپا

در اروپا چندین سیستم نسل اول، مشابه AMPS راه اندازی گردید: Total Access در انگلیس، ایتالیا،اسپانیا،اتریش،ایرلند Nordic mobile telephone(NMT) communication system (TACS)

در چند کشور c–۴۵۰ در آلمانو پرتقال،Radicom2000 در فرانسه، Radio Telephone Mobile System(RTMS) در ایتالیا محبوبترین این شبکه ها TACS و NMT بودند که مجموعاً با همدیگر در سال ۱۹۹۵ میلادی ۵۰٪ مشترکین سیستم سلولار آنالوگ را در اختیار داشتندا ستفاده از سیستمFM برای‌کانال صوتی‌واستفاده ازFSK (Frequency Shift Keying) برای کانال های کنترلی فاصله کانالها:

TACS, NMT, RTMS, NMT- 450 25 KHz
C- 450 10KHz
NMT- 900,Radiocom 2000 12.5 KHz

همه سیستم های فوق الذکر برای تشخیص Handover از سطح‌توان دریافتی در BS استفاده می‌کنند.

به غیر از C-450 که برای تشخیص از تاخیر Round – trip استفاده می‌کند.

ژاپن ، اولین سیستم سلولار آنالوگ ژاپن در سال ۱۹۷۹ در شهر توکیو تحت عنوان (Nippon Telephone and Telegraph) NTT راه اندازی گردید.

۵-۱-۳ مشکلات سیستم های 1G:

عدم استفاده از رمز نگاری: سیستم های نسل اول امکان رمز نگاری موثری را فراهم نمی کنند و به همین دلیل ترافیک صوتیاین شبکه ها به راحتی قابل استراق سمع می باشد.

مشکل دیگر این است که با گوش دادن به کانال های کنترل، شماره شناسایی کاربر به راحتی قابل سرقت است و می توان با استفاده از این شماره به حساب دیگری صحبت نمود.

کیفیت نامطلوب تماس: کیفیت ترافیک آنالوگ در اثر تداخل به سادگی تنزل پیدا می کند. برخلاف ترافیک دیجیتال هیچ گونه مکانیزم کدگذاری یا اصلاح خطا وجود ندارد که بتواند از تداخل جلوگیری کند.

استفاده ناکارآمد از طیف فرکانسی: در سیستم های آنالوگ هر کاربر RF به یک مشرک اختصاص دارد. (چه فعال باشد چه غیرفعال)

۵-۱-۴ سیستم های نسل دوم 2G:

شروع شکل گیری GSM در اروپا اوایل دهه ۱۹۸۰ است. در آنزمان اروپا با رشد چشمگیری سیستم‌های سلولار آنالوگ مواجه بود.NMT در اسکاندیناوی،TACS در انگلیس، ایتالیا، اسپانیا و ایرلند C-۴۵۰U در آلمان و پرتقال Radicom 2000 در فرانسه و RTMS در ایتالیا هیچ یک با دیگری سازگاری نداشتند. این شرایط باعث محدود شدن فعالیت این سیستمها به مرزهای هر کشور و محدودیت بازار می گردید و با نظریه اروپای متحد تعارض داشت.

به همین خاطر اتحادیه اروپا در ۱۹۹۲ یک گروه مطالعاتی تشکیل داد با عنوان Groupe Special Mobile که بعداً به Global System for Mobile communications تغییر نام یافت.

این گروه موظف بود سیستم مبایلی را برای استفاده در سطح اروپا پیشنهاد نماید که جوابگوی موارد ذیل باشد:

بهبود کیفیت صدا ، سیستم و پایانه کم هزینه ، حمایت از جابجایی بین المللی ، حمایت از پایانه های دستی، حمایت از سرویس ها و تسهیلات نوین ، استفاده بهینه از طیف فرکانسی ، سازگاری با ISDN

در سال ۱۹۸۹ وظایف و مسئولیت های گروه GSM به موسسه استاندارد سازی ارتباطات اروپایی ETSI منتقل شد.

مشخصات فاز یک GSM در سال ۱۹۹۰ منتشر گردید و پیاده سازی آن در سال ۱۹۹۱ آغاز شد و تا سال ۱۹۹۳ کشور اروپایی ۳۶ شبکه GSM راه اندازی شد.

۵-۱-۵ سیستم های نسل 2.5G

2.5G مرحله ای بین 3/G,2G در تکنولوژی بافت بی سیم می با شد. به عبارت 2.5G ا ستفاده شد برای توضیح دادن سیستم های 2/G که یک Paket Switched را اجرا می کنند. بر طبق مدارهای سوئیچینگ این لزوماً سرویس سریعی نیست زیرا مجموعه time slots ها برای سرویس مدارهای سوئیچینگ data استفاده می شوند. زمانی‌که عبارت 3/G , 2/G رسماً تعریف شد 2.5G نبود این عبارت برای اهداف بازاریابی بوجود آمده. 2.5G منفعت های زیادی برای 3G فراهم کرد و می توان ا ستفاده کرد از زیربناهای موجود 2/G در شبکه (GSM) و (CDMA).

۵-۲ معرفی شبکه SMS چگونگی کنترل ابزار توسط SMS

سرویس پیام کوتاه (SMS) یک سرویس بی سیم قابل قبولی هست که به طور سراسری پیام دیجیتالی را بین (اعضای عمومی) موبایل و سیستم های خارج آن شبیه Email- voicemail,... ارسال می کند.

۵-۲-۱ تاریخچه و ساختار سرویس پیغام کوتاه

چشم انداز sms به طور بی سیم در سال ۱۹۹۱ در اروپا وارد صحنه شد. جایی که تکنولوژی دیجیتال بی سیم اولین بار در آنها اتفاق افتاد. ا ستانداردهای اروپایی برای digitalwineless هم اکنون به صورت ا ستانداردهای عمومی برای موبایل شناخته شده و سرویس پیغام کوتاه را نیز زیر پو شش خود قرار داد.

در آمریکای شمالی sms نخ ستین روش د ستر سی به شبکه بی سیم دیجیتال بود که با پی شگامی افرادی چون Bell south Mobility و Nexel شناخته شده بود.

SMS ازنقطه‌ای به نقطه‌ای یک مکانیزمی برای ارسال پیغام از یک دستگاه بی‌سیم به یک دستگاه بی سیم دیگر (wineless handset) را موجب می شود. این سرویس از یک مرکز سرویس پیغام کوتاه (SMSC) استفاده می کند که این سیستم برای ذخیره و ارسال SMS استفاده می شود. شبکه بی سیم برای ار سال پیغام کوتاه بین سرویس مرکزی SMS و د ستگاه بی سیم ا ستفاده می شود و در مقابل سرویسی

برای ار سال Text message وجود دارد. (alphanu meric paging) که برای ضخامت ر سیدن پیغام به مقصد می باشد.

م شخ صه بارز این سرویس این ا ست که یک تلفن موبایل در حال حرکت قادر به دریافت و مطلع شدن از پیغام را در هر زمان دارد. به طور مستقل به هر حال data و voice نیز این خصوصیت را دارند.

سرویس پیغام کوتاه همچنین ضخامت دریافت پیغام کوتاه را به وسیله شبکه فراهم می کند که علت عدم موفقیت در شنا سایی آن د ستگاه می با شد، بنابراین پیغام در شبکه ذخیره شده تا هنگامی که مقصد آن قابل دسترس شود .

۵-۲-۲ فواید سرویس پیغام کوتاه

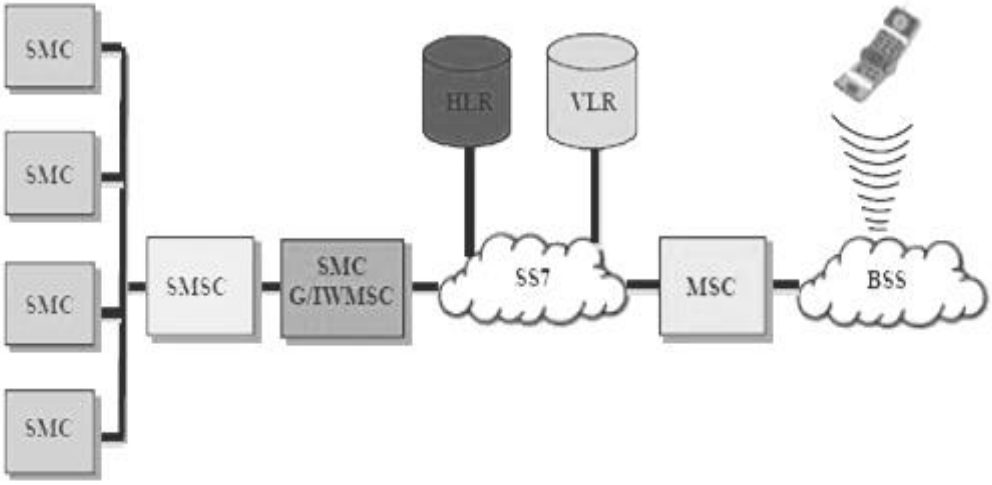
امروزه در جهان رقابتی خصو صیت مهم در موفقیت سرویس های تدارک دهنده، متفاوت بودن آنها می‌باشد. سرویس های پایه ای سابق به طور مثال تکنولوژی صوت (voice) تکامل یافته و SMS نیز یک نیروی قدرتمندی برای سرویس های متفاوت تهیه می کند.

فواید سرویس های ارائه دهنده SMS:

- ☒ تکمیل تلفن‌های بی سیم و شبکه‌های تلفنی از طریق نفوذ و قابلیت اطلاع ر سانی سرویس پیغام کوتاه
- ☒ داشتن یک سرویس alphanumeric paging
- ☒ قابلیت دسترسی به اطلاعات بی سیم به عنوان حقوقی برای کاربران
- ☒ پیش بینی افزایش میزان ســـرویس دهی از قبیل fax mail integnation- Voice mail- e-mail reminder service
- ☒ تمام این فواید به طور سریعی و با ارزش نسبتاً کم قابل دسترسی می باشند و سرمایه گذاری آن در یک دوره کمتر از ۶ ماه قابل به گشت می باشد.

آ سودگی، قابلیت انعطاف و یکپارچگی سرویس Message و د ستیابی data فواید SMS را تصدیق می‌کند. از دیدگاه دیگر، فایده آن قابلیت اســـتفاده دســـتگاه فرســـتنده گیرنده به طورالحاقی به کامپیوتر می‌باشـــد. SMS همچنین احتیاج به یک دســـتگاه جداگانه را برای Message برطرف می کند. به طوریکه می تواند به صورت یکپارچه در یک دستگاه بی سیم (ترمینال موبایل) قرار گیرد.

ساختار پایه در شکل زیر نمایش داه شده است



شکل ۵-۱- توصیف شبکه SMS

۵-۲-۲-۱ Short Message ntities (SMS)

موجودیت ارسال پیغام کوتاه موجودیتی است که توانایی دریافت و ارسال پیغام کوتاه را دارد SMS قابلیت قرار گرفتن در یک موقعیت خاصی از یک شبکه ثابت شده در مکانی که سرویس موبایل قادر به استفاده است مادامی که در حرکت است یا ثابت شده در هر نقطه نامعلوم را دارد.

۵-۲-۲-۲ سرویس مرکزی پیغام کوتاه (SMSC)

مسئولیت (SMSC) برای تقویت و ذخیره فرستادن پیغام کوتاه بین یک SME و Mobile Station را دارد.

۵-۲-۲-۳ رابط بین HLR,SMSC

GMSC هســـت که مرکز ســـوئیچینگ موبایل که قادر به دریافت پیام کوتاه از یک SMSC (مرکز سرویس پیغام کوتاه) و ارائه آن به HLR که برای مسیر یابی اطلاعات و ارسال پیغام کوتاه به نزدیکترین MSC را می باشد (SMS-IWMSC) یک مرکز سوئیچینگی است که قابلیت دریافت یک پیغام کوتاه را از شبکه موبایل و ارائه آن به SMSC مناسب خود را دارد.

۵-۲-۲-۴ ثبات موقعیت دائم (HLR)

HLR یک بانک اطلاعاتی است که برای ذخیره دائمی و مدیریت بر اشتراک ها و دادن خدمات مورد استفاده قرار می گیرد. در هنگام بازر سی بو سیله SMSC، یک بانک اطلاعات (HLR)، اطلاعات روزمره و لازم را برای ارائه کردن به مشـــترکین فراهم می کند. همچنین HLR به SMSC اطلاع می دهد که قبلاً در یک منطقه مشخص تلاش برای دریافت پیام کوتاه بی نتیجه مانده است و آن منطقه اکنون بو سیله شبکه موبایل تحت پوشش قرار گرفته و در دسترس است.

۵-۲-۲-۵ مرکز سوئیچ موبایل

مرکز سوئیچ موبایل(MSC)، کارهای سوئیچی و تماس‌های گرفته شده از طریق موبایل و تماس‌های دریافت شده از دیگر تلفن ها و سیستم های اطلاعاتی را فراهم می کند.

۵-۲-۲-۶ بازدید کننده (VLR)

ثبت محل‌مهمان (VLR) یک بانک اطلاعات‌اســـت که اطلاعات موقت درباره مشـــترکین را شـــامل می‌شود این اطلاعات برای ارائه خدمات به مشترکین توسط MSC مورد نیاز است.

۵-۲-۲-۷ محل اصلی سیستم

تمام کارهای مرتبط با رادیو در یک محل ا صلی سی ستم (BSS) اجرا شده اند. BSS شامل کنترل کننده ا صلی مناطق(BSS)، محل ا صلی transceiver (BSS) است و مسئولیت ا صلی آن جابجایی ترافیک صدا و اطلاعات بین محل های مختلف موبایل است.

۵-۲-۲-۸ محل موبایل

محل موبایل(MS)، قابلیت نهایی‌دریافت و پخش بدون ســیم پیام‌ها مانند تماس‌های تلفنی اســت. شـبکه توزیع‌بی‌سـیم‌مادون سـاختار(INFRASTRACTIUVE) براسـاس‌سـیسـتم توزیع شـماره۷ (SS.7) پایه‌ریزی شده ا ست. SMS از کاربرد ق سمتی از موبایل(MAP) ا ستفاده می کند که روش‌ها و مکانیزم های مکالمه در شبکه های بی سیم را شامل می شود، و از خدمات ایجاد ظرفیت به کارگیری جزئی SS7 (TCAP) استفاده می کند. یک لایه سرویس SMS توانایی‌های توزیع MAR را مورد استفاده قرار می دهد و ارسال پیام کوتاه بین نقاط مختلف را مقدور می سازد .

۵-۲-۳ اجزای توزیع (مخابره)

لایه کاربرد جزئی موبایل (MAP) ، کارهای ضـروری برای پشـتیبانی خدمات ارسـال پیام کوتاه را تعریف می کند . استانداردهای آمریکایی و استانداردهای جهانی ، هردو ، یک لایه MAP را برای استفاده

خدمات ا ستفاده جزئی از سی ستم توزیع شماره 7 م شخص کرده اند . ا ستانداردهای آمریکایی تو سط شرکت Telecommunication Industry Assc Ciation منتشر شده است و بر اساس IS – 41 می باشد . استانداردهای جهانی بوسیله موسسه European Telecommunication Standards تعریف شده و بر اساس GSMMAP می باشد .

عملکردهای اصلی MAP که در زیر آمده اند، برای فراهم کردن خدمات پیام کوتاه end – to – end ضروری می باشند .

- درخواست اطلاعات مسیر : پیش از تلاش برای دریافت پیام ، SMSC باید اطلاعات مسیر را به دست آورد تا MSC مورد نیاز برای محل موبایل را در زمان دریافت پیام مشخص نماید . این عمل بوسیله پرسش از HLR و به ترتیب با استفاده از مکانیزم درخواست SMS ، اطلاعات مسیر ارسال برای SM کوتاه در IS 41 و GSM انجام می شود .

- دریافت پیام کوتاه به صورت نقطه به نقطه (Point-to-Point) : این روند باعث می شود SMSC ، پیام کوتاه را به MSC که در محل موبایل مقصد فعال است، ارسال نماید و پیام را به هنگامی که MS در دسترس باشد به آن برساند حتی اگر MS به صورت تماس صدا یا اطلاعاتی مشغول باشد. عملیات تحویل پیام کوتاه یک خدمات تحویل مطمئن است. این عملیات دقیقا بعد از سیستم های اصلی، هنگامی که پیام از MSC به MS ارسال شده است، انجام می شود. بنابراین، نتیجه شامل موفقیت(یعنی تحویل به موبایل مقصد) یا عدم موفقیت در نتیجه یکی از دلایل ممکنه می باشد. ارسال نقطه به نقطه پیام کوتاه به ترتیب از طریق مکانیزم های دریافت نقطه به نقطه پیام کوتاه(SMD-PP) و ارسال پیام کوتاه در IS-41 و GSM صورت می پذیرد .

- نمایش تأخیر پیام کوتاه : این عمل هنگامی فعال می شود که تحویل یک پیام کوتاه توسط SMSC به دلیل یک مشکل موقت ، انجام پذیر نیست و باعث می شود که SMSC از HLR بخواهد که یک آدرس SMSC را به لیست SMSC های خود بیفزاید که هنگامی که به محلی در دسترس رسیدند، SMSC را مطلع نماید. این نمایش تأخیر ارسال پیام کوتاه از طریق مکانیزم های نشان دهنده اخطار SMS و تنظیم اطلاعات تأخیر پیام در IS41 و GSM انجام می شود .

- اخطار مرکز خدمات : این عمل باعث می شود HLR ، به SMSC اطلاع دهد که یک تلاش برای ارسال پیام کوتاه به یک منطقه خاص از موبایل ها، بی نتیجه و ناموفق انجام شده است که آن منطقه اکنون در دسترس شبکه موبایل است. این اخطار مرکز خدمات به ترتیب با استفاده از مکانیزم های احطار SMS و اخطار خدمات در IS41 و GSM صورت می پذیرد .

۵-۲-۳-۱ اجزای خدمات

SMS شامل اجزای خدماتی متعددی متناسب با دریافت و ارسال پیام کوتاه می باشد.

☒ مدت اعتبار : مدت اعتبار نشـــان می دهد که SMSC باید تا چه مدتی قبل از تحویل پیام کوتاه به گیرنده مورد نظر آن را حفظ و ذخیره کند .

☒ تقدم: تقدم جزئی از اطلاعات است که بوسیله SME برای نشان دادن تقدم پیامها فراهم می شود. علاوه بر اینها، SMS امکاناتی را فراهم می کند که زمان ارســال پیام را گزارش می دهد و نشــان می دهد که آیاپیام دیگری ارسال شده یا خیر(GSM)ویا تعداد دیگر پیام ها ی ارسال شده را نشان می دهد (IS41).

۵-۲-۳-۲ خدمات مشترکین :

SMS شامل دو سرویس نقطه به نقطه است .

☒ موبایلی که پیام از آن آغاز شده است (Masm)

☒ موبایلی که پیام به آن خاتمه یافته است (MT-SM)

موبایل‌هایی که پیام کوتاه از آن ها ارسال می شود ، از گوشی به SMSC انتقال می‌یابند و می‌توانند به دیگر م شترکین موبایل یا برای م شترکین در شبکه‌های ثابت مانند شبکه‌های پ ست الکترونیک ار سال می شوند. موبایل‌هایی‌که پیام کوتاه به آنها خاتمه می‌یابد، پیام کوتاه از SMSC به گو شی آنها انتقال می‌یابد و می‌تواند بو سیله مشترکین‌موبایل‌از طریق MO-SM یا دیگرمنابع‌ار سال‌مانند سیستم پست صدا(Voice mail) شبکه های پیج (page) یا کاربرها به دیگر موبایل ها ارسال گردد .

برای MT-SM ، همی شه یک گزارش به SMSC ار سال می شود که تحویل پیام به گو شی مق صد را اطلاع دهد یا عدم موفقیت در تحویل پیام و علت آن را گزارش دهد. به طور مشابه برای MO-SM ، یک گزارش به گوشــی ارســال می شــود و تحویل پیام یا عدم موفقیت در تحویل پیام و علت آن را گزارش نماید .

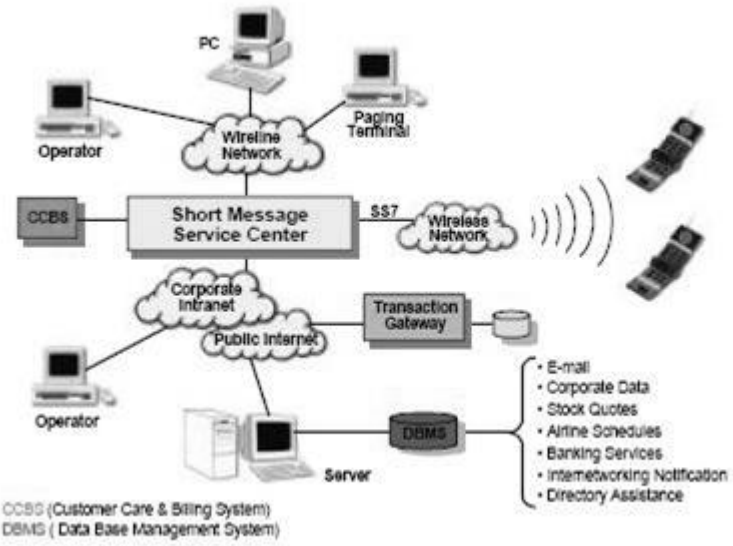
با توجه به روش مورد اســتفاده و کد اطلاعات مورد نظر ، ســرویس پیام کوتاه نقطه به نقطه ، تا ۱۹۰ کاراکتر را به مقصــد مورد نظر ارســال می‌کند. برای پیام هایی که تحویل فوری نیاز دارند، فقط یک بار تلاش جهت تحویل آن صــورت می‌گیرد. برای پیامهایی که تحویل فوری احتیاج ندارند، تا زمانی که درخواست انجام شود، یک یا چند تلاش جهت تحویل پیام انجام می شود .

در شبکه‌های GSM، نوع سرویس پیام به وسیله پروتکل معرف اطلاعات مشخص می شود که نشان می‌دهد که پروتکل با سطح بالا در حال استفاده است یا کارهای داخلی در حال انجام است. مثال‌هایی از انواع سرویس پیام عبارتند از تلکس، تلفاکس گروه ۳ ، ارسال پیام X.400 ، ERMES و تلفن‌های معمولی. در شبکه های IS41 ، نوع خدمات با استفاده از معرف teleservise تشخیص داده می شود.teleservis اصلی شامل مواردزیر است :

- ☒ سرویس ارسال پیام خانه ای (CMT)
- ☒ سرویس پیج (page) خانه ای (CPT)
- ☒ سرویس اخطار پیام صوتی (VMN)

تفاوت CMT و CPT در مکانیزم ارسال پاسخ است که در آن شبکه یا کاربر می تواند آن را برای هر پیام فعال نماید. شناسایی کاربر شامل یک کد پاسخ است که راه عکس العمل خدمات قوی بین SMC ها را راحت تر می کند.

بسیاری از خدمات ، می توانند با مخلوط کردن این اجزاء خدمات ، اجرا و تکمیل گردند . علاوه بر خدمات قبلی، SMS می تواند به صورت خدمات یک طرفه یا دو طرفه مورد استفاده قرار گیرد که د ستر سی بی سیم را در هر جا به هر گونه اطلاعاتی فراهم می کند. با به کار بردن فناوری های جدید و استفاده از سرشاخه ها، سرورها و زمان های جدید طراحی شده برای موبایلها، SMS می تواند وسایل بی سیم را قادر به د ستر سی مطمئن و ار سال اطلاعات از طریق اینترنت یا اینترانت با سرعت بالا و هزینه کمتر نماید یک ساختار کلی شبکه برای درک خدمات جدید SMS در شکل زیر نمایش داده شده است



شکل ۵-۲- ساختار کلی شبکه برای درک خدمات جدید SMS

بعضی از کاربردهای تکنولوژی SMS ، با استفاده مناسب از MT-SM یا MO-SM عبارتند از :

سرویس هشدار: سرویس هشدار معمولا بیشترین سرویس مورد استفاده SMS است مثالهایی از سرویس هشدار با استفاده از SMS عبارت است از:هشدار صوتی یا فاکس که نشان می دهد که پیام صوتی در جعبه پستی گوشی وجود دارد. هشدار پست الکترونیک که نشان می دهد که Email در inbox وجود دارد و سرویس تقویم / یادآوری که یادآوری کننده جلسات و قرارهای برنامه ریزی شده است .

کارهای درونی پست الکترونیک:

خدمات موجود پست الکترونیک(مانند SMTP و X.400)، می توانند به راحتی با SMS انجام شوند تا پست‌های الکترونیک را به صورت دو جزئی در پیام کوتاه و پست الکترونیک درآورند .

کارهای درونی پیج (page) :

خدمات پیج(مانندTAP، TNPP، TDP) همراه با SMS به مشترکین بی‌سیم دیجیتال اجازه می دهند از طریق شبکه های پیجی در دسترس قرار گیرند .

سرویس های اطلاعات :

خدمات اطلاعاتی‌بسیاری از طریق SMS قابل استفاده است که شامل: گزارش‌های آب و هوا، اطلاعات ترافیکی، اطلاعات‌تفریحی(مانند سینما، تئاتر و کنسرتها). اطلاعات اقتصادی (مانند انتقال موجودی، میزان تغییر، بانکداری، خدمات واسطه‌ای‌دلالی)وراهنمای تلفن‌می‌باشند.

۵-۲-۳-۳ خدمات اطلاعاتی موبایل :

SMSC همچنین برای فراهم کردن اطلاعات بی‌سیم کوتاه، قابل استفاده است. در هنگامی که تماسهای گویا وجود دارد، اطلاعات بی سیم نیز ممکن است فعال باشند. بعضی مثالهای اینگونه خدمات عبارتند از : اعزام ناوگان، مدیریت بر موجودی، خرید بلیط سفر، دستور خرید و مدیریت بر تماس مشتریان .

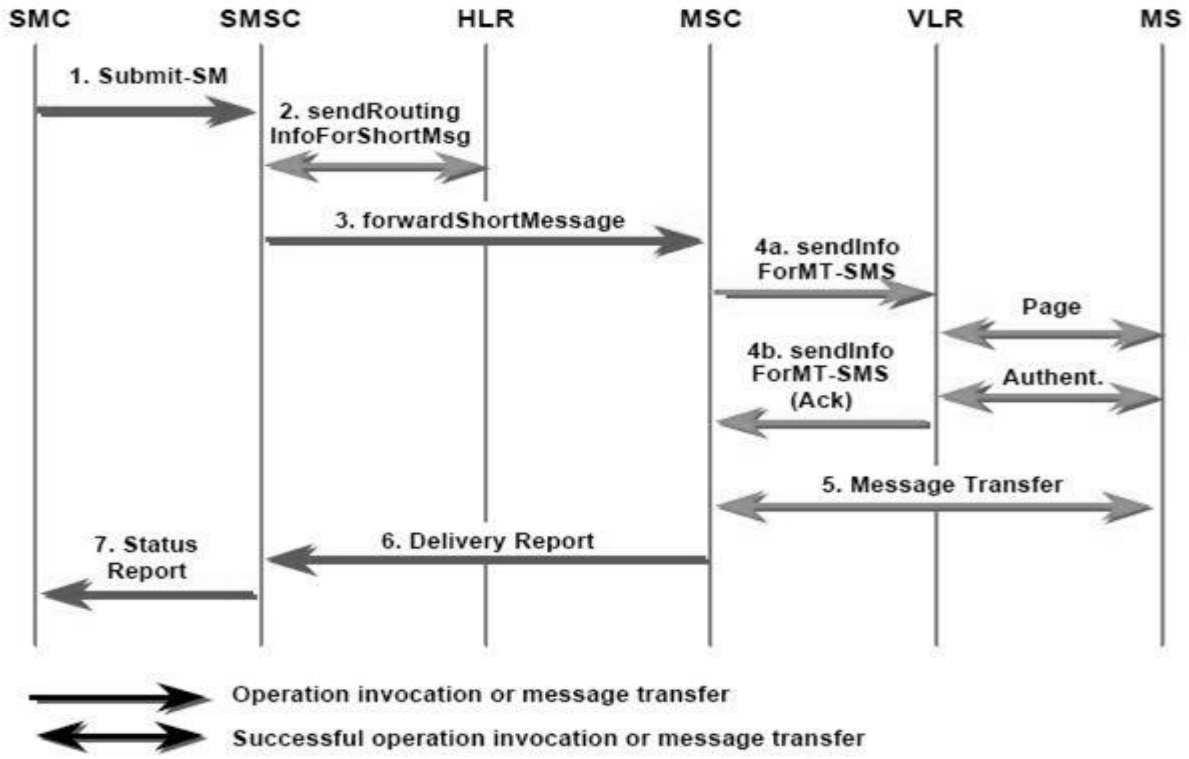
۵-۲-۳-۴ مدیریت و توجه به مشتری :

SMS همچنین برای مخابره اطلاعات binary قابل استفاده است که بدون درخواست و حضور مشتری بوسیله محل و مکان موبایل قابل گزارش است. این قابلیت به کاربرها امکان می دهد با فراهم کردن توانایی برنامه‌ریزی مکان موبایل، به مشتریان خود کمک نمایند. مثالهایی از اینگونه خدمات عبارتند

از : برنامه‌ریزی محل موبایل، که امکان می‌دهد مشخصات مشتری و خصوصیات اشتراک به ایستگاه موبایل‌انتقال یابد(مشتریان، بر اساس اطلاعات ذخیره شده می‌توانند فعال یا غیر فعال باشند)، اعلام میزان شارژ، که بدین ترتیب SMS قادر خواهد بود شارژ مصرف شده در تماس‌تلفنی را گزارش نماید(مانند هزینه تلفن تاکسی) .

۵-۲-۴ مثال موبایل هایی که پیام کوتاه به آنها رسیده :

شکل صفحه بعد،مثال موفق ازMT-SM را شرح می دهد.برای راحتی،روش GSM توضیح داده شده است. اما ، روش IS41 نیز مشابه است.



شکل ۵-۳- توصیف MT-MS

۱. پیام کوتاه از SME به SMSC ارسال شده است.

۲. پس از تکمیل فرآیندهای داخلی ،SMSC از HLR اطلاعات مسیر را برای موبایل مشترک درخواست و دریافت می نماید .

۳. SMSC پیام کوتاه را با استفاده از عمل ارسال پیام کوتاه ، به MSC ارسال می نماید .

۴. MSC اطلاعات مربوط به مشترک را از VLR بدست می آورد. این عمل ممکن است شامل یک روش رسمی (مطمئن) باشد.

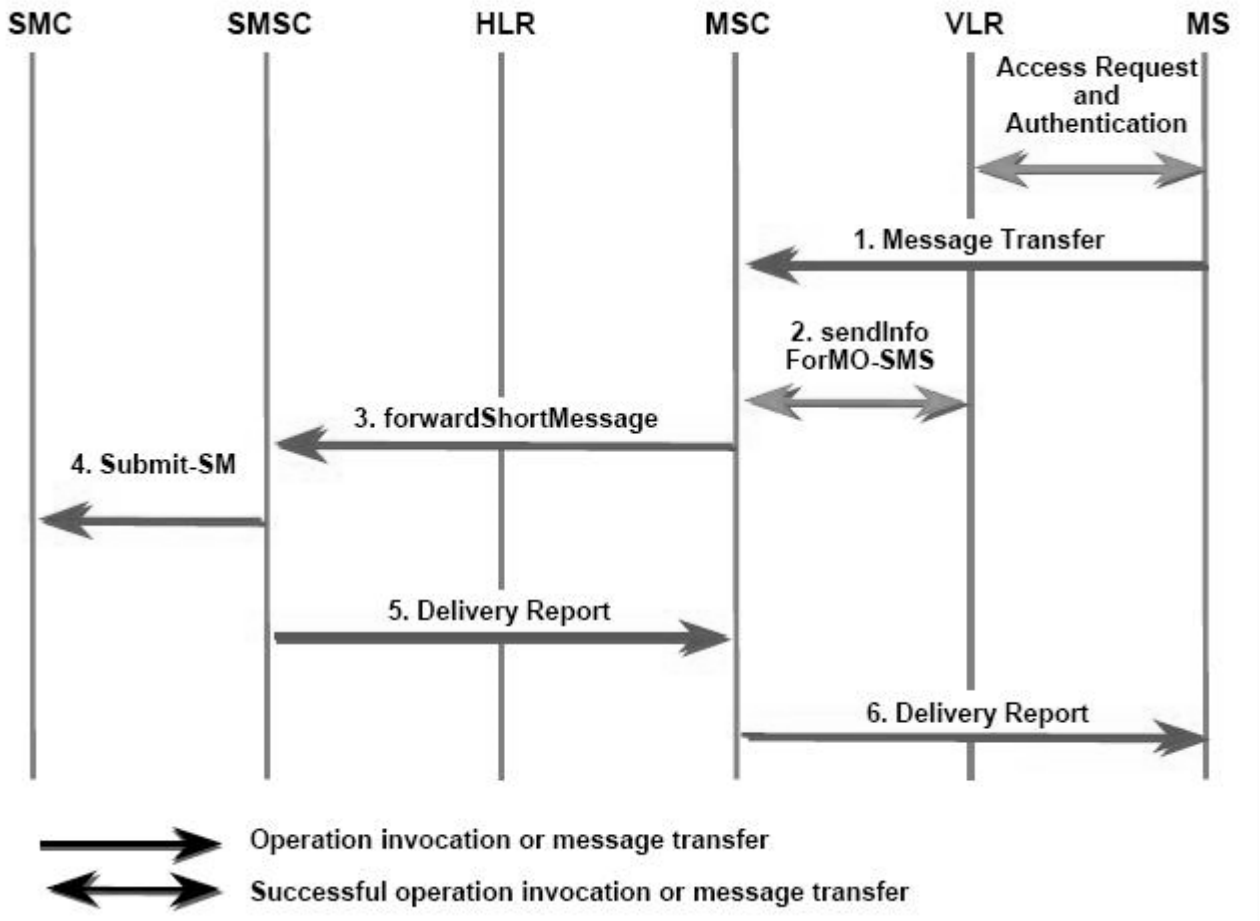
۵. MSC پیام کوتاه را به MS مخابره می‌نماید.

۶. MSC نتیجه عملیات ارسال پیام کوتاه را به SMSC ارسال می نماید.

۷. اگر توسط SME درخواست شده باشد، SMSC یک گزارش وضعیت درباره تحویل پیام کدتا به آن ارسال می نماید .

۵-۲-۵ مثال موبایلی که پیام کوتاه ارسال نموده است

شکل صفحه بعد،یک مثال موفق از MO-SM را شرح می دهد.برای راحتی روش GSM نشان داده شده است. اما روش IS41 نیز مشابه است .



شکل ۵-۴- توصیف MO_SM

۱. MS ، SM را به MSC مخابره می نماید .

۲. MSC از VLR استعلام می‌نماید تا تأ یید شود که ارسال پیام بر خلاف خدمات اضافی درخواست شده یا محدودیت های اعمال شده نباشد.

۳. MSC با استفاده از عمل ارسال پیام کوتاه ، پیام کوتاه را به SMSC ارسال می نماید.

۴. SMSC پیام کوتاه را به SME تحویل می دهد.

۵. SMSC ، نتیجه موفق عمل ارسال پیام کوتاه را به MSC گزارش می نماید.

۶. MSC نتیجه عمل MO-SM را به MSگزارش می نماید.

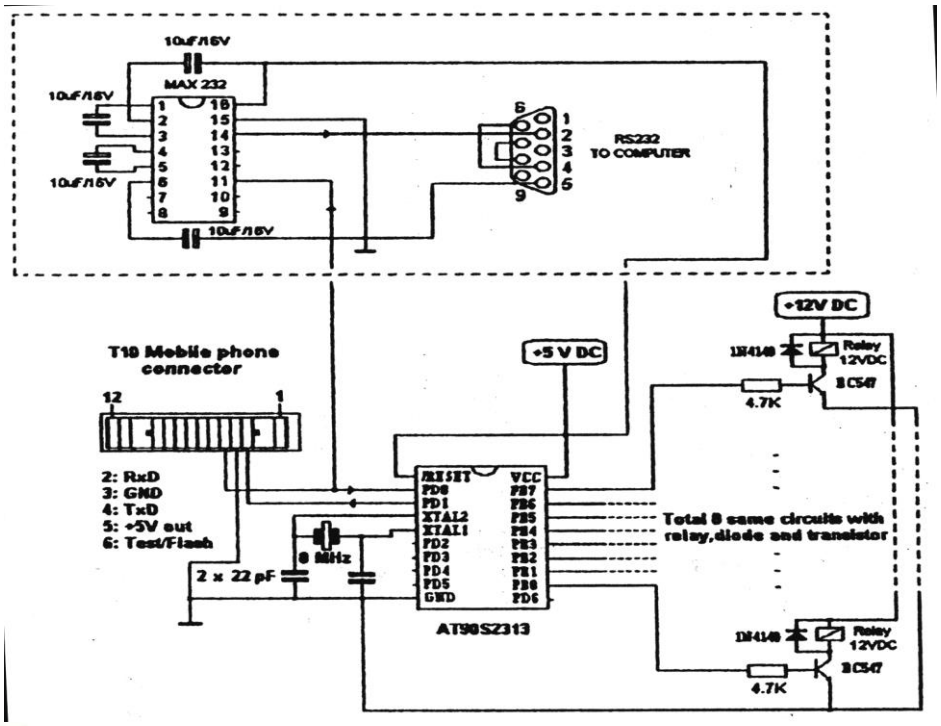
۵-۲-۶ ارائه مداری برای کنترل ابزار به کمک SMS در تلفن همراه

به کمک این مدار می توان تا ۸ و سیله را با فر ستادن پیغام SMS هر نوع گو شی تلفن خاموش و یا روشن کرد. این پروژه در جاهایی که خط تلفن سیمی وجود ندارد، بسیار مفید است. چنانچه یک گوشی همراه اریکسون قدیمی دارید و از آن ا ستفاده نمی کنید، در این پروژه قابل ا ستفاده خواهد بود. به کمک این مدار تنها می توان خاموش یا روشن کرد وسایل الکتریکی را کنترل نمود.

بررسی مدار

سـخت افزار مدار بسـیار سـاده اسـت، زیرا درگاه ارتباطی گوشـی اریکسـون در ولتاژ ۵ ولت و با فرمانهای AT کار می کند (همانند فرمان های مودم اما برای گوشـی همراه). نرم افزار AT۹۰۲۳۱۳ بسـیار م شکل ا ست زیرا باید بایت هفت بیتی (septets) از گو شی را به بایت ۸ بیتی (octets) از AVR تبدیل کند. (septet یک بایت با طول ۷ بیت و octet یک بایت با طول ۸ بیت اسـت). همه این پردازش برای رمز برداری از پیغام sms مورد نیاز است.

پس از ساخت مدار، آن را به گو شی همراه مت صل کرده و سپس تغذیه آن را و صل کنید. به هیچ وجه پیش از اتصال به گوشی، منبع تغذیه را روشن نکنید. اکنون AVR تلاش می کند که پیغام را از اولین خانه حافظه گو شی بخواند. پی شنهاد می شود پیش از ات صال مدار به گو شی همه پیغام های SMS پاک شود. اگر در خانه اول حافظه چیزی وجود نداشته باشد، AVR تا فرستادن پیغام این کار را تکرار می کند. قالب پیغام باید تنها به صورت «۱» یا «۰» باشد. یک برای روشن‌کردن و صفر برای خاموش کردن وسیله به کار می رود. پیغام باید ۸ رقمی باشد. هشت عدد صفر یا یک و یا ترکیبی از آنها.



شکل ۵-۵- شماتیک مدار کنترل از راه دور SMS برای گوشی های اریکسون GSM

برای مثال اگر پیغام ۱۱۰۰۰۱۰۰ را بفرستید، با شروع از طرف راست، وسیله های شماره ۳،۷ و ۸ که رمز آنها یک ا ست رو شن می شود و و سیله های شماره ۱ و ۲ و ۴ و ۵ و ۶ که رمز آنها صفر ا ست، خاموش می گردند. اگر بخواهید، پیغام جدیدی را بفر ستید و حالت بع ضی د ستگاه ها را عوض نکنید، باید همان عدد پیغام قبلی را ار سال کنید. برای مثال اگر بخواهید در حالت قبلی، تنها و سیله شماره ۵ را روشن کنید و وضعیت دستگاه های دیگر را تغییر ندهید، پیغام جدید به صورت ۱۱۰۱۰۱۰۰ خواهد بود. یعنی تنها بیت شماره ۵ از سمت راست، از صفر به یک تغییر می کند و بقیه بیت ها بدون تغییر باقی می مانند. پیغام SMS باید تنها شـامل «۱» یا «۰» باشـد و هیچگونه حرف یا نمادی مثل $,B,A @, و... در آن وجود ندا شته با شد. AVR و سیله ای را که بیت مربوط به آن، حرف یا غیر یک با شد، خاموش می کند. برای مثال اگر پیغام ۱۰۱۱۱$۰۰ارسال شود. AVR علاوه بر دستگاه های شماره ۱،۲ و ۷ دستگاه شماره ۳ را نیز خاموش خواهد کرد. اگر بخواهید دسـتگاه های برقی تحت کنترل را از پیغام افراد دیگر محافظت کنید، رمز منبع (source code) را به گونه ای ا صلاح کنید که AVR پیش از اجرای هر نوع پیغام، شماره تلفن شما را بخواند. در رمز منبع قسمت کوچکی برای خواندن شماره تلفن، شماره مرکز سرویس دهی، تاریخ و زمان پیغام دریافت شـده در نظر گرفته شـده اسـت. این پروژه برای شـبکه تلفن همراه یونان (Telestet) طراحی شده ا ست و اطلاعی ندارم که پیغام SMS کشورهای دیگر همین ترکیب را دارا ست

یا خیر (من از قالب بایت هفت بیتی که گیرنده GSM از شبکه GSM میگیرد ا ستفاده کرده ام). پس از آن که GSM پیغام را دریافت کرد، AVR آن را اجرا می کند و آن را از حافظه گوشی همراه پاک میکند تا اولین مکان حافظه را برای پیغام بعدی خالی نماید. سپس جستجو را برای پیغام جدید آغاز می نماید. اگر پایه ۱ (پایه PD_0) از AVR را به تراشه MAX ۲۳۲ و این تراشه را به رایانه وصل کنید، شما در صفحه window، همه اطلاعاتی را که GSM به AVR می فرستد، می توانید ببینید (مثل شماره تلفن فرستنده، شماره مرکز سرویس دهی، تاریخ و زمان فرمان AT). درگاه COM را در ۹۶۰۰ bps 8n1 تنظیم نمایید.

عیب یابی

شما می توانید مدار تشخیص دهنده (diagnostic) که در شما تیک مدار داخل کادر نقطه چین نشان داده شده است را از طریق درگاه RS ۲۳۲ به PC وصل کنید. پس از روشن کردن گوشی و وصل تغذیه به مدار، AVR فرمان های زیر را به گوشی همرا می فرستد.

1) AT+CPMS="ME" ("ME" انتخاب حافظه خود تلفن)

2) AT+CMGR=1 (خواندن پیام دریافتی از خانه ۱ حافظه)

اگر گوشی همراه به صورت زیر پاسخ دهد:

(این پیغام زمانی فرستاده می شود که پیامی در حافظه تلفن نباشد)

AT+CMGR=1[CR][CR][LF]
+CMS ERROR: 500[CR][LF]

در این‌حالت، AVR دوباره دستورهای۱ و۲ را می‌فرستد.چنانچه‌گوشی همراه به صورت زیر پاسخ‌دهد:

(این پیغامی زمانی که پیام جدیدی در حافظه تلفن رسیده باشد فرستاده می شود)

AT+CMGR=1[CR][CR][LF]
+CMGR: 0.26[CR][LF]
07910396249100002 40C91XXXXXXXXXXXX0000300120515130210 8B1180C068BC162
[CR][LR]
OK[CR][LF]

(XXXXXXXXXXXX شمارنده تلفن فرستنده می باشد).

در این صورت AVR پیغام بایت هفت بیتی را به صورت بایت هشت بیتی رمز برداری می‌کند و انجام می‌دهد (رله ها را فعال یا غیرفعال می کند) و دستور زیر را می فرستد:

(پاک کردن پیام دریافتی از مکان ۱ حافظه) AT+CMGD=1

تا پیغام را از حافظه گوشی پاک کند. شما می توانید با هرگونه ولت متری ولتاژ ۵+ یا صفر ولت درگاه B را برای بررسی پیغام ارسالی آزمایش کنید.

نتیجه گیری

یک نویسنده چینی رمان جدیدش را به صورت SMS منتشر کرده است. ارسال پیام کوتاه در انگلیس چنان محبوب شده ا ست که میلیون ها م شترک تلفن همراه در این ک شور از شدت علاقه به این کار، به جراحت های انگشتان دست مبتلا شده اند. حدود ۳۷ درصد از جوانان و نوجوانان ایتالیایی اعتیاد به استفاده بیش از حد تلفن همراه و ارسال SMS دارند. علاوه بر مشکل انگشتان دست، این گروه با عوار ضی چون بد خلقی و بی‌حو صلگی‌د ست به گریبانند. محققان ا سترالیایی ه شدار دادند که زوج‌های جوان هر روز بیشتر از گذشته از SMS برای گذارندن امور خود و یا حتی پایان دادن به روابطشان استفاده می‌کنند. دانش‌آموزان آمریکایی برای دریافت SMS هنگام حضور در کلاس، در تلفن های همراه خود از زنگی استفاده می‌کند که معلمان نمی توانند صدای آن را بشنوند.

خوب برای اثبات اینکه ارسال پیام کو تاه در میان کاربران جهانی از محبوبیت فوق العاده ای برخوردار است و پرطرفدارترین فعالیت جانبی گوشی داران محسوب می شود باز هم دلیل لازم است؟

شب از نیمه گذ شته ا ست. با صدای زنگ تلفن همراهت از خواب بیدار می شوی. یک پیام کوتاه داری. چشم های خواب آلودت را می مالی و به سختی می خوانی:«می بخشید که این وقت شب مزاحمت شدم می خواستم بهت زنگ بزنم گفتم شاید خواب باشی. راحت بخواب!»

مسلماً اتفاقی مشابه این برای بسیاری از اصحاب گوشی روی داده است و اگرنه نیمه شب بالاخره در طول شبانه روز حتما شما هم پیام های مشابهی دریافت کرده اید. پیام هایی که اصولاً با فلسفه ایجاد سرویس پیام کوتاه متفاوت است ولی این روزها بیشتر حجم SMSهای دریافتی ما را تشکیل می دهد. اما به جرات می توان گفت که بی شترین حجم این پیام ها را پیام هایی غیر ضروری ت شکیل می دهند. قبول ندارید؟ در اطراف خود چند نفر را می شناسید که حاضر باشند مثلاً در مقابل یک دوربین تلویزیونی آخرین SMS ارسالی یا دریافتی شان را بخوانند؟

دکتر یزدان پناه ا ستادیار ارتباطات و جامعه شنا سی در این زمینه می گوید. همان طور که پیدا ست، ا سا ساً SMS برای ار سال پیام های کوتاه و فوری باید ا ستفاده شود. اما شهروندان به میزان زیاد و برای کاربردهای دیگر از آن استفاده می کنند و متاسفانه یک گروه بزرگ از جامعه ما که بیشتر جوان نیز هستند از SMS به خوبی استفاده نمی کنند و با این که اصولاً هزینه استفاده از این سرویس پایین است. اما آنقدر حجم استفاده بالا می رود که هزینه زیادی را برای شهروندان ایجاد می کند.

این استاد دانشگاه معتقد است : از وسایل ارتباطی می توان استفاده مثبت و هم استفاده منفی داشت و برخی متاسفانه تنها به استفاده نادرست از یک وسیله ارتباطی روی می آورند. یزدان پناه با تاکید بر اینکه برای استفاده از هر وسیله باید ابتدا بستر فرهنگی فراهم شده باشد و هنجارهای آن به وجود آمده باشد می‌گوید: به نظر می‌رسد در مورد این وسیله ارتباطی نیز هنوز باید بسترهای فرهنگی لازم ایجاد شود. به نظر این استاد دانشگاه حتی باید پیام های ارسالی توسط سرویس پیام کوتاه تحلیل محتوا شوند. چرا که این SMSها نشانگر بخشی از روحیات مردم ایران است: ضمن این که باید در مورد نحوه استفاده از این وسیله ارتباطی در کشورهای دیگر نیز تحقیق شود، تا بتوان بین بهره گیری از این سرویس در سایر کشورها و ایران مقایسه بهتری انجام داد.

در این میان نکته ای که معمولاً از نظر استفاده کنندگان سرویس پیام کوتاه دور می ماند این است که SMS برای چت و گپ و گفتگو وسیله مناسبی حتی از نظر صرفه اقتصادی نیست. با وجود اینکه هزینه هر پالس SMS حدود یک سوم هزینه یک دقیقه مکالمه با همراه است. اما وقتی از این سرویس برای چت کردن و رد و بدل کردن چندین مکالمه هرچند کوتاه استفاده می شود عملاً هزینه ای بیش از مکالمه به مشترکین تحمیل می شود و این علاوه بر بار اضافی است که طرفین بر شبکه اعمال می کنند.

ارزش افزوده، اصل فراموش شده سازمان بهداشت و سلامت اندونزی با استفاده از سیستم SMS تلفن همراه، خط مستقیمی را راه اندازی کرده که به واسطه آن مردم میتوانند بیماری های همدیگر و شکایات خود را نسبت به مراکز بهداشتی، گزارش دهند. در بلژیک، طرح جالبی برای خبر کردن شهروندان در شرایط اضطراری پیشنهاد شده که بر اساس آن در زمان خطر سراسر به تمامی تلفن های موبایلی که در بلژیک فعال هستند یک پیام کوتاه (SMS) فرستاده می شود و به آنها هشدار می دهد که خطری در راه است. در بسیاری از کشورهای جهان مردم با استفاده از سرویس SMS از آخرین اخبار و ضعیت آب و هوا و جاده ها، و ضعیت بورس قیمت ارز و طلا و ... آگاه می شوند و با استفاده از این سرویس صورت حساب های مالی شان را پرداخت می کنند، بلیت کنسرت و سینما رزرو می کنند و ده ها فعالیت دیگر انجام می دهند که از همه این سرویس ها به عنوان سرویس های ارزش افزوده یاد می شود.

در ایران هم چندی پیش سه شرکت با در اختیار گرفتن لینگ SMS مخابرات برای ارائه این قبیل سرویس های ارزش افزوده تلاش هایی انجام داده اند اما از آنجائی که شبکه همراه ما به طور کامل به

شرکت ها هم به ارائه امکاناتی برای شرکت در مسابقات SMS برنامه های رادیو و تلویزیون و یا ارسال پیام های انبوه تبلیغاتی منحصر شده است. البته در این میان می توان به فعالیت های محدودی از قبیل امکان پرداخت قبض تلفن و برق و ... به وسیله SMS از سوی برخی بانک ها ارایه اطلاعات کتاب ها و نشریات حاضر در نوزدهمین نمایشگاه بین‌المللی کتاب تهران از طریق سرویس پیام کوتاه و یا امکان وبلاگ نویسی از طریق SMS اشاره کرد.

لذا اینجانب سعی کرده ام با نقطه نظر و توجه به شبکه های بی سیم شبکه SMS طریقه ارسال و دریافت SMS را بیان کنم و در آخر مداری پیشنهاد کردم که تا حدی راه گشای سیر تکاملی استفاده از گوشی موبایل و پیغام کوتاه در عامه مردم باشد.

پیوستها:

A

- AMPS: Advance mobile phone sys
- AC: Authentication center
- AIN: Advanced intelligent net works
- AMTS: Advanced mobile telephone system

B

- BTS: Base transceiver subsystem
- BSC: Base station control
- BCF: Base station control function
- Bluetooth
- Broad Band
- BC: Base station
- BSS: Basic service set
- BSSI: Basic service infrastructure

C

- CDMA: code division multiple access
- CMT: cellular messaging teleservice
- CPT: cellular paging telesrvice
- CCK: complementary code keying
- Client
- CSMA/CA: carrier sense multiple access with collision
- CSD: Circuit switched Data
- CRC: cyclic redundancy checking
- CCITT: consultative committee for international teleynophy and telephouy

D

- DCF: distribution coordination function

- DSL: digital subscriber line
- DSSS: direct sequence spread spectrum
- DLS: data link control
- DHCP: dynamic host configuration protocol
- DDP: data delivery protocol

E

- ESS: extended servise set
- EAP: extensible authentication protocol
- EAP: equivalent isotropic ally radiate power
- Ethernet
- Encryption
- ETSI: eunopean telecommunication standard instate
- EDGE: enhanced data rates for GSM evolution

F

- FCS: frame check sequence
- FHSS: spectrum frequency – hopping spreed
- FSK: frequency shift keying
- Frequncy Happing

G

- GMSC: gateway mobile switching ceter
- GSM: global standard for mobiles
- GPRS: genral packet radio servise

H

- HLR: home location register
- HCMTS: high capaclty mobile telephone system
- HSCSD: high speed cincute switched data

I

- IEEE: institute of electric and electvonice engineers
- IAPP: inter access point protocol

- ISM: industrial scientific and medical
- IBSS: independent basic service set
- Identifier
- IMEI: international mobile equipment identity
- ISC: international switching centar
- IMTS: improved mobile telephone service
- IMT: international mobile telecommunications
- ITV: international telecommunication vnion
- ISDN: international services digital network
- IDEN: intergrated digital enhanced network
- Infrastructure
- IR: in fru red
- ISP: internet service provider
- ICT: information and communication technology

L

- LAN: local area networks
- LLC: logical link control
- LEAP: light extensible authentication protocol

M

- MAC: media access control address
- MAN: metropolitan area network
- MAP: mobile application part
- MIN: mobile identification number
- MO-SM: mobile- originated short message
- MS: mobile station
- MSC: mobile switching
- MT-SM: mobile- terminated short message
- MTS: mobile telephone service

N

- NGN: next generation network operating system

- NFS: network files system
- NMS: network management system
- NMT: Nordic mobile telephone

O

- OFDM: orthogonal frequency division multiplexing
- OFDMA: orthogonal frequency division multiplexing access
- OSL: open systems interconnection
- OSS: operation support system
- OS: operating system
- OMA: open mobile alliance

P

- PCF: point coordination function
- PBCC: packet binary convolutional code
- PC: personal computer
- PCI: peripheral component interconnect
- PCMCIA: personal computer memory card interconnect
- PCS: personal communications service
- PKI: public key infrastructure
- PDC: personal digital cellular
- PHS: personal handy systems

Q

- QAM: quadrate amplitude modulation

R

- Radio telephone mobile
- RCC: radio common carriers

S

- SNMP: service of network management protocol
- SSID: service set identifier
- SM: short message
- SMD-PP: short message delivery point-to-point

- SME: short message entity
- SMS: short message service
- SMSC: short message service control
- SMS-GSC: gateway mobile switching center
- SMS-IWMSC: SMS inter working mobile switching center
- SMTP: simple mail transfer protocol
- SS7: signaling system7
- SAP: service access point
- SSCCP: signaling connection control part (ss7)
- SME: short message entites
- SMT: surface mounted technology
- SMC: surface mounted components

T

- TCPIP: transmission control protocol internet protocol
- TACS: total access communications system
- TDMA: time division multiple access
- TGPP: third generation partnership project
- TAP: telocator alphanumeric protocol
- TCAP: transaction capabilities application part
- TDMA: time division multiple access
- TDP: telocator data protocol
- TNPP: telocutor network paging protocol

U

- UNII: unlicensed national information infrastructure
- UMTS: universal mobile telecommunications sys

V

- VOIP: voice over internet protocol
- VLR: visitor location register
- VMN: voice mail notification

W

- WEP: wireless equivalence privacy
- WPA: wring password attempts
- WCDMA: wide band code division multiple access
- WIN: wireless identity module
- WCDMA: wide band code division multiple access
- Wi-Fi: wireless-fidelity