به نام خدا

ساختار شبکه‌ی GPRS

سید محمد جواد اسماعیلی

بهار ۹۰

فهرست مطالب

مقدمه

از اوایل دهه ۶۰ میلادی که شبکه های تلفن همراه سلولی معرفی شدند نزدیک به ۵۰ سال می‌گذرد. در آن زمان تنها سرویسی که این شبکه ها ارائه می‌دادند مکامله بود؛ آن هم بصورت آنالوگ و با کیفیت بسیار پایین. با گذشت زمان و پیشرفت تکنولوژی و همگام با آن، سطح انتظار کاربران، خدمات این شبکه ها نیز توسعه یافت بطوری که در حال حاضر نسل چهارم این شبکه ها امکان دسترسی به اینترنت با سرعت ۱۷۰mbps برای تمام کاربران فراهم کرده است. از طرف دیگر طی این ۵۰ سال، پیشرفت این شبکه‌ها به سمتی بوده که مرز بین شبکه های تلفن همراه و شبکه‌های کامپیوتری در حال محو شدن است؛ و این شبکه‌ها در حال ادغام با یکدیگر هستند. در این رابطه می‌توان به شبکه های Wimax یا همون IEEE802.16M اشاره کرد که اتحادیه بین‌المللی مخابرات (ITU) از آن به عنوان شبکه های نسل چهارم تلفن همراه یاد می‌کند.

۱- نسل‌های شبکه‌های تلفن همراه

۱-۱- شبکه‌های نسل اول (1G): صدای آنالوگ

این شبکه‌ها اولین سیستم‌های تلفن همراه سلولی به شکل امروزی بودند. این سیستم، اولین بار در آمریکا و توسط شرکت مخابراتی AT&T اختراع، نصب و راه اندازه شد. در ادامه به بررسی چند تکنولوژی (سیستم) پیاده شده از این نسل اشاره می کنیم.

(Improved Mobile Telephone System) IMTS -۱-۱-۱

این سیستم در دهه ۱۹۶۰ میلادی نصب و راه اندازه شد. طریقه کار این سیستم به این صورت بود که یک فرستنده-گیرنده ۲۰۰ واتی در نقاط مرتفع نصب می‌شد و برای ارسال و دریافت از دو فرکانس مختلف بهره می‌برد به خاطر همین امکان ارسال و دریافت همزمان مقدور بود.

این سیستم دارای ۲۳ کانال در طیف فرکانسی MHz ۴۵۰-۱۵۰ بود. به دلیل کم بودن تعداد کانال ها کاربران کمی می توانستند به طور همزمان از شبکه استفاده کنند.

یکی از مهمترین مشکلات این شبکه اختلال در سیستم های رادیویی تا شعاع چند صد کیلومتری به خاطر قدرت بالای آنتن فرستنده-گیرنده مرکزی بود. (سیستم های رادیویی و تلویزیونی در طیف فرکانسی MHz-۱GHz ۱ فعالیت می‌کنند)

(Advanced Mobile Phone System) AMPS -۲-۱-۱

در سال ۱۹۸۲ شرکت Bell Labs سیستم تلفن همراه پیشرفته را معرفی کرد. این سیستم بسیاری از مشکلات IMTS را حل کرد؛ از جمله این که با کاهش قدرت آنتن مرکزی شعاع سلول ها کوچکتر شد (در حدود ۱۰Km تا ۲۰) و در نتیجه تعداد آنتن بیشتری در واحد سطح قابل نصب بود که نتیجه آن استفاده چند باره از یک فرکانس مقدور می شد و این یعنی افزایش تعداد کاربران در واحد سطح. سیتم. AMPS دارای ۸۲۳ کانال دوطرفه همزمان است که البته برای جلوگیری از تداخل فرکانسی به هر آنتن ۴۵ کانال اختصاص داده می‌شد. پهنای باند هر کانال ۳۰KHz است و برای باند فرکانسی ۸۵۰ مگاهرتز منتشر می‌شود. همینطور که مشخص است AMPS از FDM برای تقسیم پهنای باند استفاده می کند.

خصوصیت دیگر این سیستم پشتیبانی از پاس کاری یا hand off است. یعنی یک کاربر در حین مکالمه می‌تواند از منطقه تحت پوشش یک آنتن خارج شده و منطقه تحت پوشش آنتن دیگر قرار گیرد، بدون قطع شدن ارتباط.

۱-۲- شبکه های نسل دوم (2G) صدای دیجیتال

شبکه‌های نسل اول دارای مشکلات متعددی بودند از جمله کیفیت پایین صدا به خاطر مدولاسیون آنالوگ، امنیت پایین: چرا که داده هایی از مدولاسیون مستقیمی بر روی کانال ارسال می شدند و از آنجایی که همه این فرکانس ها را می‌دانند می‌توانند مکالمات کاربران را شنود کنند بدون اینکه کاربر متوجه شود. همچنین به خاطر بزرگ بودن سلول ها تعداد کاربران قابل پشتیبانی کم بود. اینجا بود که شبکه های نسل دوم ارائه شدند. امروزه ۳ سیستم عمده نسل سوم در حال فعالیت هستند که ما به معرفی آنها می پردازیم. البته شبکه های دیگری هم وجود دارد که در واقع همین شبکه‌ها هستند که شرکت های مختلف با توجه به شرایط خود تغییرات اندکی در آن ایجاد کرده اند.

(Digital Advanced Mobile Phone System) D-AMPS -۱-۲-۱

این سیستم همان AMPS است که به صورت دیجیتال در آمده است. این سیستم با AMPS کاملا سازگار بوده به طوری که در شبکه‌های این سیستم، تلفن های نسل اول و دوم می توانند به طور مسالمت آمیز در کنار یکدیگر فعالیت کنند. بنابراین در یک سلول ممکن است یک کانال در حال کار بصورت آنالوگ باشد و کانال بعدی بصورت دیجیتال. نسبت کانال های دیجیتال به آنالوگ را MTSD (مرکز سوئیچینگ) به طور دینامیک با توجه به نسبت تلفن های آنالوگ به دیجیتال تعیین می کند. D-AMPS مانند ورژن آنالوگ خودش بر روی باند ۸۵۰ مگا هرتز و از FDM برای تخصیص کانال به کاربران استفاده می‌کند. البته برای پاسخگویی به تقاضای بالای کاربران بعدها باند ۱۹۰۰ مگاهرتز

هم به این شبکه اختصاص داده شد و نیز برای افزایش تعداد کاربران از TDM نیز در کنار FDM استفاده شده. یعنی در این سیستم ۳ کاربر به طور همزمان با استفاده از تقسیم زمانی می‌توانند بر روی یک کانال فعالیت کنند.

۱-۲-۲- GSM (Global System for Mobile Communication)

سیستم D-AMPS بصورت گسترده در ایالات متحده نصب و راه‌اندازی شد ولی در دیگر نقاط جهان از جمله در اروپا و همچنین ایران از سیستمی بنام GSM استفاده می‌شود.

در GSM هم مثل D-AMPS از FDM و TDM (درکنار هم) برای اختصاص کانال به کاربران استفاده می شود. البته با اندکی تفاوت. مثلا در AMPS پهنای باند کانال ها ۳۰KHz بود ولی در GSM پهنای باند کانال به ۲۰۰KHz افزایش یافته است و یا اینکه در D-AMPS همانطور که اشاره شد ۳ کاربر بر روی یک کانال فعال بودند ولی در GSM این تعداد ۸ تا است. این سیستم بر روی دو باند فرکانسی ۱۸۰۰MHz و ۱۹۰۰ کار می‌کند که در باند ۹۰۰MHz دارای ۱۲۴ زوج کانال و در باند ۱۸۰۰ مگاهرتز دارای ۳۷۴ زوج کانال است که هر زوج کانال به ۸ کاربر اختصاص داده می شود.

نرخ انتقال هر کانال در سیستم GSM برابر ۲۷۰۸۸۳ بیت بر ثانیه است که بین ۸ کاربر تقسیم می شود یعنی هر کاربر ۳۳۸۵۴ بیت بر ثانیه. البته حجم بسیار بالای این اطلاعات جهت تشخیص و اصلاح خطا و همچنین سرآیند فریم های داده استفاده می‌شود که در نهایت ۱۳kbps برای داده واقعی کاربر باقی می‌ماند.

۱-۲-۳- CDMA (Code Division Multiple Access)

سیستمهای D-APMS و GSM از FDM و TDM برای تخصیص کانال استفاده می‌کند ولی CDMA از روش کاملا متفاوتی بهره می برد. در CDMA به جای تقسیم کل پهنای باند به کانال های باریک، اجازه می‌دهد تمام کاربران از تمام ظرفیت کانال برای ارسال و دریافت استفاده کنند. برای تفکیک آنها از تئوری رمز گذاری استفاده می کند. مبانی نظری CDMA در کتاب شبکه های کامپیوتری تنن بام ویراست ۴ فصل دوم به طور کامل تشریح شده است.

۱-۳- شبکه های نسل ۲/۵ صدای دیجیتال و داده

این نسل از شبکه ها همانطورکه از نام آن نیز مشخص است نسلی مستقل نیست و از تغییراتی بر روی شبکه های نسل دوم ایجاد شده است. سنگ‌بنای این سیتم استفاده از سرویس های مبتنی بر سوئیچینگ بسته‌ای در سیستم‌های مبتنی بر سوئیچینگ مداری است. یعنی برای راه اندازی یک شبکه نسل ۲/۵ بر روی شبکه‌های نسل دوم باید تجهیزات مبتنی بر سوئیچینگ بسته‌ای بر روی سیستم نصب شود. ۲ تا از اصلی ترین این سیستم ها GPRS و EDGE می‌باشند که در ادامه به تشریح آنها می‌پردازیم.

(General Packet Radio Service) GPRS -۱-۳-۱

همانطور که اشاره شد این سیستم بر روی شبکه‌های نسل دوم قابل نصب و اجرا است و چنانکه گفته شد این سیستم از سوئیچینگ بسته‌ای کاملا پشتیبانی می کند.

تفاوت سوئیچینگ مداری و بسته ای چیست؟ در شبکه های تلفنی عمومی و تلفنی همراه وقتی قرار می‌شود بین دو کاربر اتصال برقرار شود، یک مدار واقعی بین دو کاربر ایجاد می‌شود. این یعنی اینکه طرفین چه داده‌ای ارسال کنند، یا نه، کانال اشغال باقی خواهد ماند. ولی در سوئیچینگ بسته‌ای داده به پکت‌هایی تقسیم می‌شود و هر پکت می‌تواند به طور مستقل از سایر پکت‌ها و از مسیرهای مختلف به مقصد ارسال شود. این دو تکنولوژی را می توانید در شکل زیر مشاهده کنید.

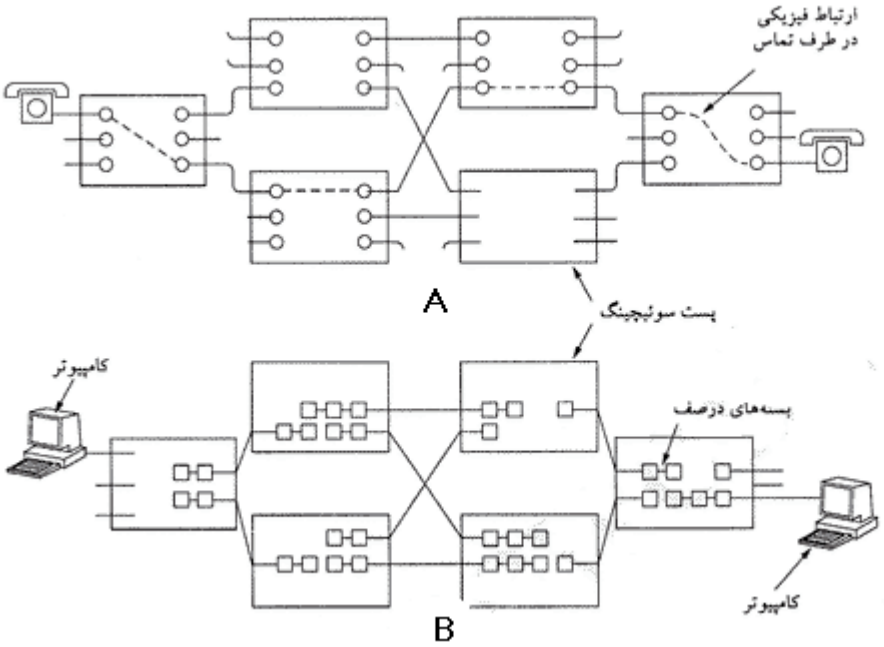

Figure 1- A-Circuit Switching , B-packet Switching

از آنجایی که در سوئیچینگ مداری، کانال بطور دربست در اختیار کاربر است و ارتباطی به حجم داده‌های ارسالی کاربر ندارد هزینه آن با توجه به زمان مکالمه محاسبه می‌شود و قاعدتا هزینه بالایی دارد. ولی در سوئیچینگ بسته‌ای محاسبه هزینه بر اساس حجم داده های ارسالی کاربر خواهد بود و ارتباطی به طول دوره اتصال به شبکه ندارد، به همین دلیل معمولا تمام کاربران GPRS همواره آنلاین هستند و هزینه زیادی هم برایشان ندارد. البته این دو مدل سوئیچینگ تفاوت های دیگری هم با هم دارند از جمله آنها می توان به ارائه QOS متفاوت به کاربران اشاره کرد. شبکه تلفن همراه اول در ایران در حال حاضر از این سیستم استفاده می‌کند.

(Enhancer Data rate for GSM Evolution) EDGE -۲-۳-۱

این سیستم هم مانند GPRS بر روی شبکه های نسل دوم از جمله GSM قابل نصب و راه اندازی است. نرخ انتقال بصورت تئوری برابر با ۱۷۱/۲kbps است و دلیل این سرعت بالا با وجودی که از سیستم GSM استفاده کند، (سرعت انتقال در GSM برابر با ۲۱/۴kbps-۸ است) اختصاص هر ۸ برش زمانی به یک کاربر است. همانطور که گفته شد هر کانال ۲۰۰KHz در شبکه های GSM به کمک TDM به ۸ برش زمانی تقسیم و این ۸ برش به ۸ کاربر داده می شود. ولی در GPRS هنگامی که شبکه خلوت است (که اغلب اوقات نیز چنین است) BTS (آنتن) به طور اتوماتیک این ۸ برش زمانی را به یک کاربر اختصاص می‌دهد. ولی در EDGE علاوه بر این روش از افزایش نرخ بیت بر باد (Bit/Baud) نیز برای افزایش سرعت استفاده می‌کنند. البته این موضوع (افزایش bit/baud) باعث افزایش خطا در محیط های پر نویز می‌شود. و این یعنی کاهش دوباره سرعت؛ ولی در محیط های بدون نویز این روش کارایی بالایی دارد به طوری که نرخ انتقال در EDGE در حالت تئوری برابر با ۴۷۳/۶kbpsاست که در عمل این مقدار به ۲۳۶/۸ می‌رسد که باز هم رقم بسیار بالایی است (در مقایسه با GPRS) به خاطر همین سرعت بالا از EDGE با عنوان نسل ۲/۷۵ یاد می‌شود. در ایران نیز شبکه ایرانسل از این سیستم استفاده می‌کند.

۱-۴- شبکه های نسل سوم (3G) صدای دیجیتال و داده

شبکه های نسل ۲/۵ همانطور که گفته شد نسل مستقل نبودند چرا که برای راه اندازه نیازمند زیر ساخت‌های شبکه های نسل دوم بودند. و به همین دلیل پاگیر محدودیت‌های این شبکه ها نیز بودند، که از این محدودیت ها می‌توان به سرعت نسبتا پایین، سازگاری کم با شبکه های کامپیوتری و شبکه های IP از جمله اینترنت، اشاره کرد.

در سال ۱۹۹۲ اتحادیه جهانی مخابرات (ITU) طراحی به نام IMT2000 را به عنوان اولین شبکه نسل سوم معرفی کرد و قرار شد تا همه کشورهای عضو با برنامه ریزی و رعایت قوانین مربوط به اتحادیه از جله اختصاص فرکانس ۲GHz بمنطور این شبکه، بستر های مناسب برای نصب و راه اندازی این سیستم را محیا کنند.

طبق پیشنهادهای سازمان، قرار شد این سیستم که بین المللی بود تا سال ۲۰۰۰ راه اندازی شود و سرعت انتقال ۲Mpbs به همه کاربران ارائه دهد، ولی تا سال ۲۰۰۰ هیچ سیستمی نصب و راه اندازی نشد. چرا که بعدها مشخص شد این سیستم به طور کامل عملی نیست.

سرویس هایی که قرار بود IMT2000 در اختیار کاربران قرار دهد عبارت بودند از:

۱- انتقال صدا با کیفیت عالی

۲- پیام رسانی (سرویس جایگزین ایمیل ، چت ، SMS و ...)

۳- مالتی مدیا (پخش موسیقی، تماشای فیلم و ...)

۴- دسترسی به اینترنت با سرعت بسیار بالا

پس از آن شرکت های مختلف طرح های بسیار زیادی ارائه کردند که از بین آنها دو طرح W-CDMA و CDMA2000 پذیرفته شدند و در بسیاری از کشورها به طور عملی اجرایی شدند.

۱-۴-۱- W-CDMA (UMTS) Wide-CPMA

این طرح توسط شرکت سوئدی اریکسون ارائه شد و اتحادیه اروپا نیز از آن حمایت کرده و نام UMTS (Universal Mobile Telecommunication System) را بر آن نهاد.

از آنجائیکه این سیستم در اروپا پیاده شد و در اروپا نیز سیستم های نسل دوم GSM بود این سیستم (UMTS) سازگاری کامل با تلفن های GSM داشت به طوری که موبایل های GSM می‌توانند از یک سلول GSM خارج شده و وارد یک سلول UMTS شوند (بدون قطعی ارتباط).

از لحاظ فنی ساختار این شبکه ها همان CDMA است البته با کمی تغییرات بهینه سازی. در CDMA پهنای باند کانال ها ۱/۲۵MHz بود ولی W-CDMA این مقدار به ۵MHz افزایش پیدا کرده است. سرعت انتقال داده نیز در این سیستم بصورت عملی در حدود ۲Mbps است.

۱-۴-۲- CDMA2000

این سیسم نیز بسیار شبیه W-CDMA است و توسط شرکت آمریکایی Qualcomm ارائه شد. بر خلاف W-CDMA، با GSM سازگار نیست. از لحاظ فنی بر مبنای CDMA طراحی شده و دارای نرخ انتقال عملی ۱۱۰۰k برای دانلود و ۴۰۰kb برای آپلود می‌باشد همانند W-CDMA دارای کانالهای ۵MHz برای انتقال است.

۱-۵- شبکه های نسل چهارم (4G) انتقال داده با سرعت بسیار بالا

امروزه حجم داده های تولیدی کاربران نسبت به گذشته بسیار بالا رفته و قاعدتا برای انتقال این حجم بالای اطلاعات استفاده از شبکه های با سرعت بالا امری غیر قابل اجتناب است. از طرف دیگر تحولات جامعه اطلاعاتی به سمتی است که شبکه های کامپیوتری و تلفن همراه در حال ادغام هستند. بنابراین نیاز به شبکه هایی حس می‌شد تا بتواند هم محدودیت سرعت را برطرف کند و هم سازگاری کاملی با شبکه های کامپیوتری و از جمله آن، اینترنت داشته باشد و از طرف دیگر سرویس‌های مکالمه بلادرنگ را برای تلفن های همراه فراهم کند، شبکه های 4G تمام این خصصیات را یکجا در خود دارند.

سرعت انتقال اطلاعات در شبکه های 4G تا ۱۰ برابر 3G قابل افزایش است (به طور تئوری ۱۷۰Mbps) یکی از تفاوت‌های شبکه های نسل سوم و چهارم در این است که مدل تجاری شبکه های 3G با تمرکز بر انتقال صدا (تماس

تلفنی) بناشده است ولی در شبکه های 4G تمرکز به انتقال داده است (مانند شبکه های کامپیوتر)؛ و انتقال صوت (تماس تلفنی) به عنوان جزئی از خدمات این نسل شناخته شوند.

دو تا از مهمترین سیستم های مبتنی بر 4G , LTE-Advanced و IEEE802.16M یاهمان شبکه های Wimax می‌باشند. البته قبل از 4G شبکه های نسل ۳/۵، ۳/۷۵ و ۳/۹ نیز ارائه شدند که مانند GPRS و EDGE مبتنی بر شبکه های نسل قبل خود بودند که از میان آنها می توان به LTE، HSPA، HSPA+ و ... اشاره کرد که تمرکز این شبکه ها نیز بر افزایش سرعت انتقال بود.

۲- ساختار شبکه های GSM

از آنجایی که موضوع بحث ما شبکه های GPRS است و GPRS نیز بر روی شبکه‌های نسل دوم از جمله GSM قابل نصب و راه اندازی است، ابتدا مختصری در مورد ساختار این شبکه بحث می کنیم تا جلوتر هنگام بررسی GPRS با ابهام روبرو نشویم.

در بحثی که گذشت در مورد توانایی ها و امکانات یک شبکه GSM بحث کردیم.

در این قسمت ساختار داخلی این شبکه و اجزای آن را مورد بررسی قرار می‌دهیم.

شبکه GSM از سه بخش اساسی تشکیل شده است.

۱- MS یا Mobile station

۲- BSS یا Base station Subsystem

۳- NSS یا Network Switching Subsystem

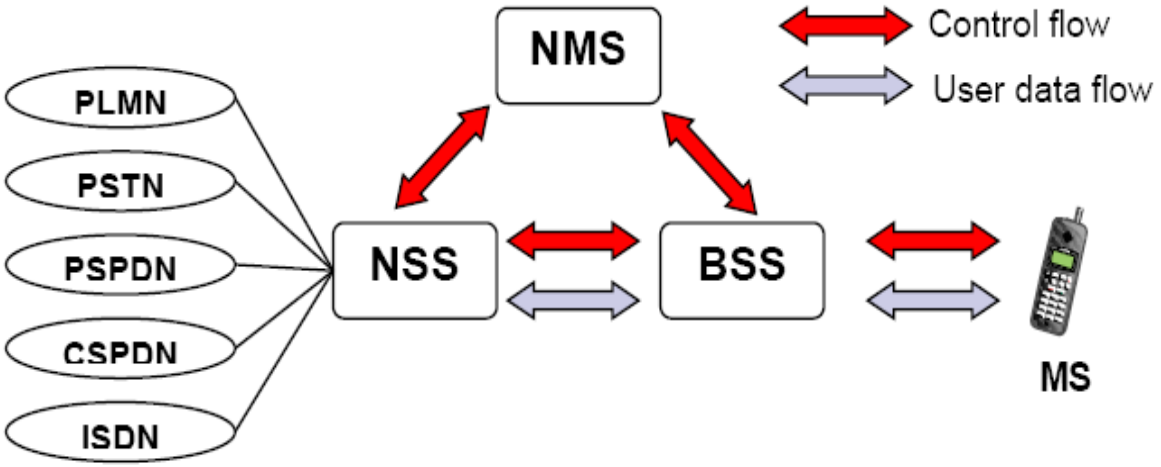

Figure 2- GSM Components

در زیر به شرح وظایف هر یک از این قسمتها می پردازیم.

MS -۱-۲

این قسمت که همان گوشی موبایل می باشد خود از دو قسمت سیم کارت و گوشی تشکیل شده است

(Subscriber Identity Module Card) SIMCard

این قسمت در اصل نقشی یک کلید ورود و یا یک شناسنامه برای شناسایی و ورود به شبکه را دارد. سیم کارت در واقع حافظه کوچکی است که حاوی ۵ عدد ثابت و مقداری حافظه برای ذخیره برخی داده‌ها در داخل خود می‌باشد. این ارقام عبارتند از IMSI که شماره ی سریال منحصر بفرد است؛ PIN که یک شماره رمز است. Puk که برای بازیابی PIN در صورت مسدود شدن PIN مورد استفاده قرار می گیرد؛ KI یک شماره رمز سری است که برای تشخیص هویت از آن استفاده می شود و KC نیز یک کلمه رمز می باشد.

گوشی

این قسمت نیز شامل یک دستگاه الکترونیکی بیسیم برای اتصال به شبکه است و نقشی شبیه یک کارت شبکه بیسیم در یک شبکه، وایرلس را دارد. همچنین این قطعه شامل یک شماره سریال منحصر بفرد است (IMEI)

BSS -۲-۲

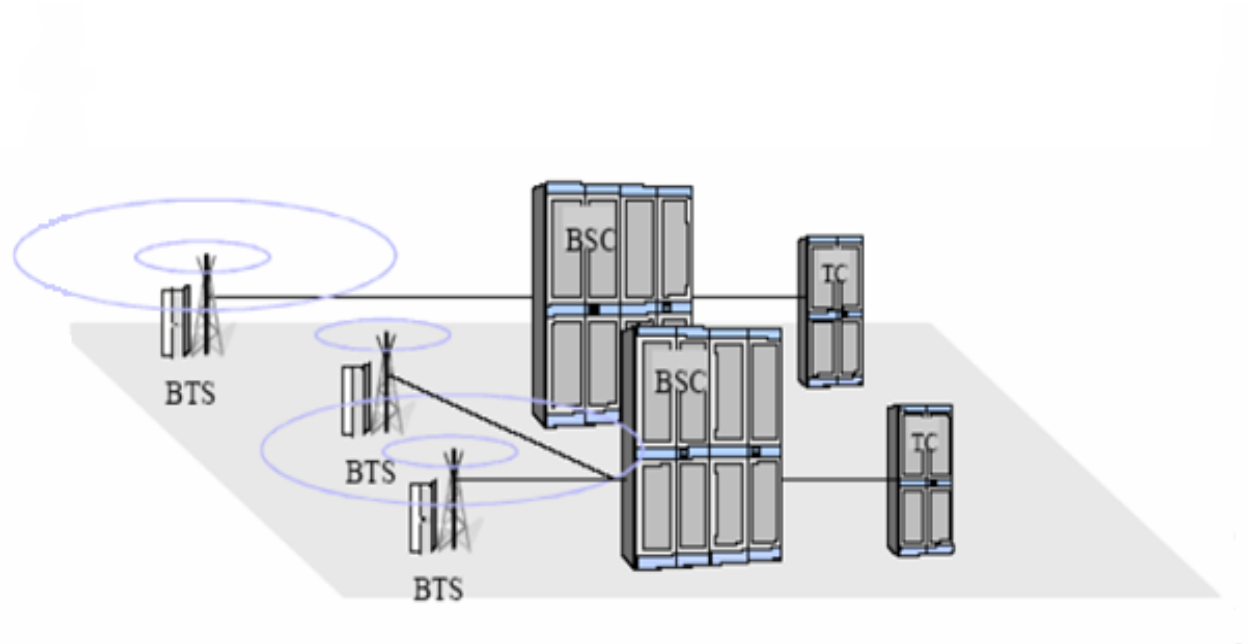

Figure 3- BSS

این قسمت وظیفه ارتباط با MS را بر عهده دارد که خود نیز به بخش های BSC،BTS و TC تقسیم می‌شود

(Base Transceiver station) BTS

در واقع همان آنتن های مخابراتی هستند که در گوشه و کنار دیده می شوند که وظایف زیر را بر عهده دارد.

- کد کردن، رمز کردن، مالتی پلکس کردن و مدوله کردن
- سنکرون کردن زمانی و فرکانسی
- ارسال و دریافت رادیویی سیگنال ها (صوت و دیتا) با MS
- دیکد کردن، رمز گشایی و دمالتی پلکس کردن

BSC (Base Station Controller)

معمولا چندین آنتن (BTS) تحت مدیریت یک BSC ارائه سرویس می‌کند. این قسمت وظایف زیر را بر عهده دارد.

-مدیریت منابع رادیویی سلول‌های تحت کنترل خود

-مدیریت پاس کاری (hand over) در داخل سلول

-کنار هم چیدن کانالهای ترافیکی با نرخ کم (به منظور کاهش تعداد خطوط از BSC به MSC، BTS)

-مدیریت توان BTS ها

-کنترل پرش فرکانسی

TC (Trans Coder)

این قسمت نیز عهده دار وظایف زیر است:

-ایجاد ریت ۱۳kbps برای اطلاعات صحبت بعد از فرایند Speech Coding

-اضافه نمودن اطلاعات in band signaling

-هدایت کانال های سیگنالینگی

NSS (Network Switching Subsystem) -۳-۲

NSS ارتباط بین موبایل با دیگر اجزای شبکه را مدیریت می‌نماید.

دیتا بیس های اطلاعاتی مشترکین از قبیل شماره‌ها سرویس‌ها اطلاعات امنیتی و انتقال موبایل و محل UPDATE شدن آن را مدیریت می کند.

MSC یا GMSC عمل سوئیچ مکالمه بین BSC ها را با دیگر اجزای شبکه ثابت یا موبایل فراهم می‌کند.

اجزای NSS:

MSC(Mobile Services Switching Centre):

- MSC یک سوئیچ ISDN پیشرفته است.
- تعدادی BSC را مدیریت نموده و محدوده جغرافیایی آنها را تحت کنترل دارد.
- عمل سوئیچ مکالمات را بین BSC ها و دیگر اجزای شبکه انجام می دهد.
- با شبکه تلفن ثابت (PSTN) در ارتباط است.

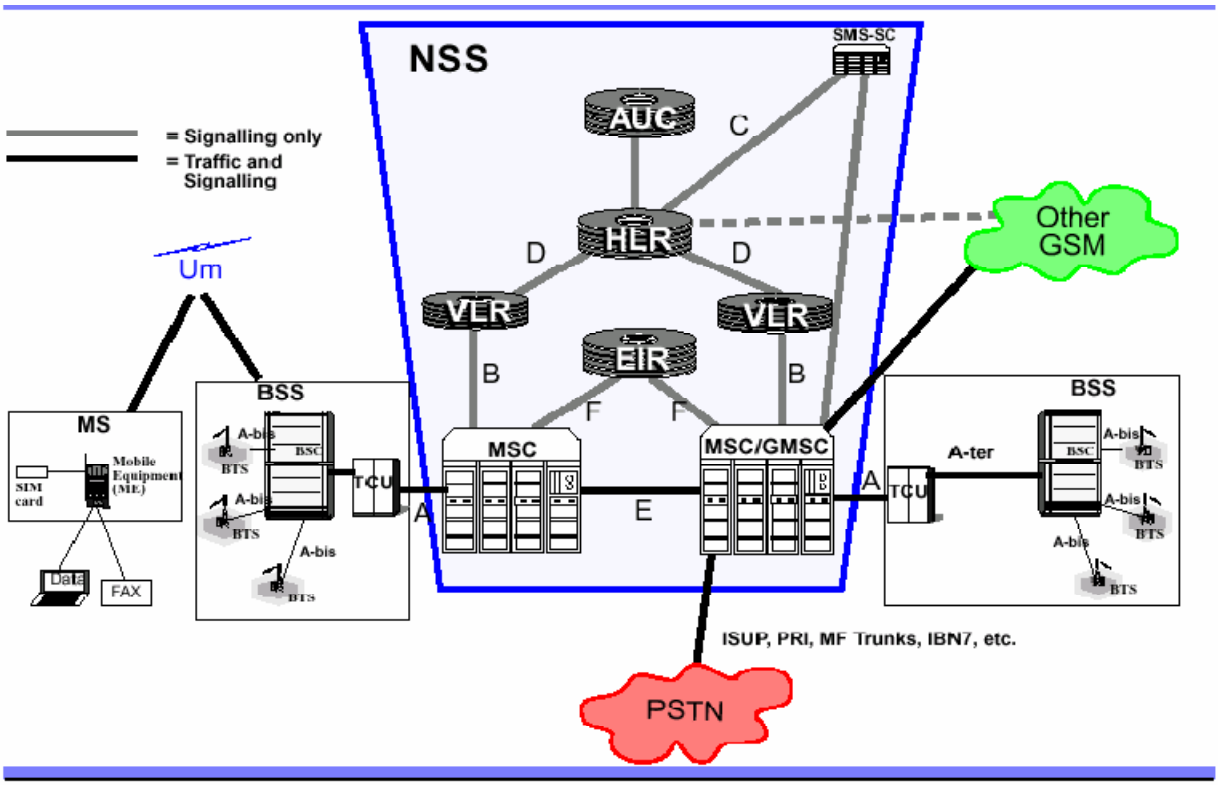

Figure 4- NSS

- تحت SIGNALING NO.7 و (ISUP,SCCP) با دیگر اجزای شبکه در ارتباط است.

GMSC به MSC هایی گفته می شود که با شبکه ثابت PSTN یا ISDN ارتباط دارند.

HLR (Home location register):

هر سیم کارت مربوط به یک HLR خاص بوده و UPDATE شدن هر مشترک در هر MSC/VLR و هر LOCATION AREA با کسب اجازه و اطلاع رسانی به HLR انجام می گردد.

دیتا بیس و اطلاعات مربوط به هر مشترک از قبیل شماره سیم کارت (IMSI) شماره تماس (MSISDN) سرویس‌ها و کدهای امنیتی و محل فعلی موبایل را نگهداری می‌نماید.

نوع سرویس هایی که مشترک مجاز به استفاده از آنها است (انتقال مکالمه نمایشگر و ...) و اجازه رومینگ در اپراتورهای مختلف در HLR تعیین می شود.

VLR (Visitor Location Register):

همچنان که از نام آن پیداست حافظه ای برای ثبت اطلاعات مشترکین UPDATE شده است.

معمولا همراه با یک MSC نصب شده و واحد اندازه گیری آن (k) کیلو مشترک است.

اطلاعات لازم برای UPDATE شدن مشترک و سرویسهای مشترک و برقراری مکالمات مشترک را از HLR دریافت می‌کند. به عنوان مثال IMEI, MSISDN, IMSI و آدرس HLR مشترک ملاقات شده در آن ثبت می‌شود.

یک حافظه دینامیکی است که همواره در حال ضبط LOCATION AREA هر مشترک (در صورت تحرک و تغییر) می‌باشد.

همیشه آماده است تا برای مشترکین UPDATE شده‌اش به منظور PAGE شدن و به تقاضای HLR یک MSRN تولید نماید.

:(Equipment Identity Register)EIR

حافظه ای برای ذخیره نمودن اطلاعات شماره سریال گوشی ها (IMEI) است و تعیین کننده گوشی های مجاز و غیر مجاز استفاده از شبکه می باشد.

:(Authentication Centre) AUC

شامل یک دیتا بیس حفاظت شده است که کلید رمز امنیتی (Ki) مربوط به تمامی سیم کارت‌ها را نگهداری می‌نماید.

هنگام UPDATE شدن هر مشترک به کمک VLR و روند تعیین هویت از هر گونه سوء استفاده جلوگیری می‌نماید.

(General Packet Radio Service) GPRS -۳

در بخش ۱-۳ در مورد سرویس ها و امکانات یک شبکه نسل ۲/۵ و ذیل آن شبکه GPRS صحبت شد. دیدیم GPRS شبکه ای است که سرویس های مبتنی بر سوئیچینگ بسته ای را برای شبکه های نسل دوم (از جمله آن GSM) که مبتنی بر سوئیچینگ مداری هستند ارائه می دهد. بنابراین برای راه اندازی GPRS نیاز است تا تغییراتی در بخش سخت افزاری و نرم افزاری GSM ایجاد شود.

در این بخش به ساختار این شبکه و ارتباط آن با شبکه های خارجی IP و همچنین ارتباط آن با ساختمان GSM می‌پردازیم.

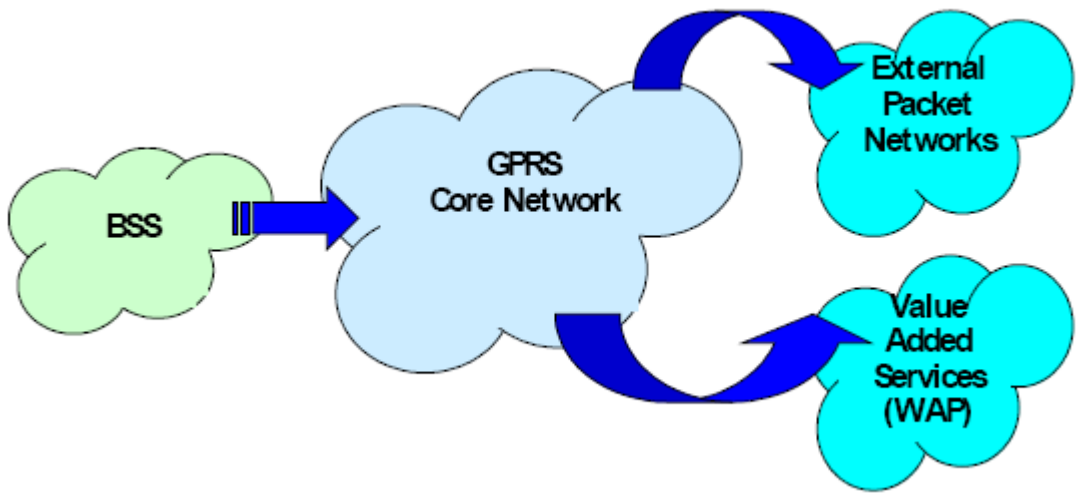

Figure 5- GPRS access to packet switched networks

خصوصیات یک شبکه GPRS را می توان بصورت زیر لیست کرد:

- می تواند با کمترین تغییرات برای سیستمهای GSM راه اندازی شود
- می تواند بیش از یک شبکه مبتنی بر Packet Switching را پشتیبانی کند
- می تواند برای کاربران مختلف Qos متفاوتی را ارائه دهد (بر حسب بودجه)
- با شبکه های نسل سوم و چهارم سازگار است.
- از کانکشن های Point 2 Point، Point 2 Multipoint پشتیبانی می‌کند
- ارتباطی مطمئن با شبکه های دیگر برقرار می‌کند.
- توانایی مانیتورینگ و پیگیری اعمال کاربران برای اقدامات قانونی
- پشتیبانی از رومینگ
- وجود افزونگی در این شبکه‌ها (یعنی در صورت از کار افتادگی یک Node شبکه از کار نیفتد و به کار خود ادامه دهد).
- تبدیل پروتکل بین شبکه های مختلف
- ترجمه آدرس به کمک NAT و NAPT

۳-۱- سخت افزار و نرم افزار مورد نیاز شبکه های GPRS

برای نصب و راه اندازی یک شبکه GPRS لازم است تا ابزار و تجهیزات زیر به آن اضافه شود.

- PCU (Packet Control Unit)
- SGSN (Serving GPRS Support Node)
- GGSN (Gateway GPRS Support Node)
- BG (Border Gateway)
- CG (Charging Gateway)
- DNS (Domain Name Service)
- fire wall
- back bone

PCU

وظیفه PCU تفکیک ترافیک Packet Switching، Circuit Switching از یکدیگر و انتقال آنها به ترتیب به شبکه های GPRS و GSM است.

این واحد همچنین مدیریت بیشتر بخشهای شبکه GPRS از جمله مدیریت منابع رادیویی را بر عهده دارد. این واحد می‌تواند هم در بخش BTS، BSC و یا بقیه قسمتهای بین MS، MSC قرار بگیرد.

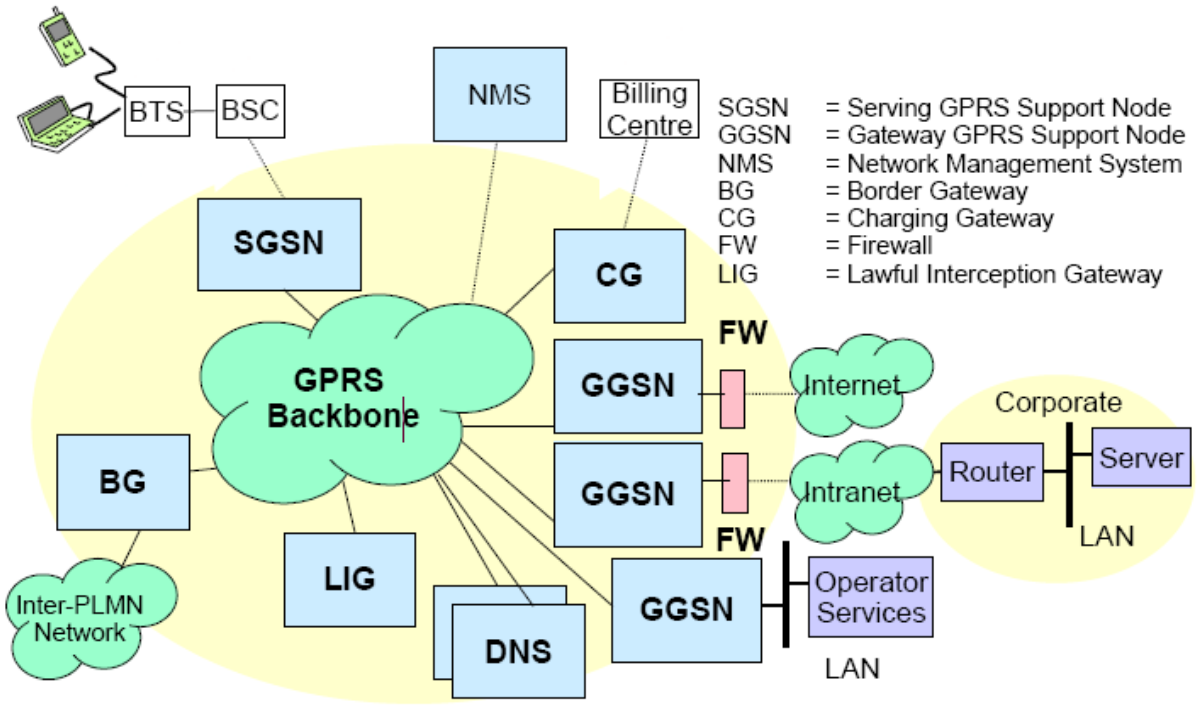

Figure 6- GPRS architecture

PCU

وظیفه PCU تفکیک ترافیک Packet Switching، Circuit Switching از یکدیگر و انتقال آنها به ترتیب به شبکه های GPRS و GSM است.

این واحد همچنین مدیریت بیشتر بخشهای شبکه GPRS از جمله مدیریت منابع رادیویی را بر عهده دارد. این واحد می‌تواند هم در بخش BTS، BSC و یا بقیه قسمتهای بین MS، MSC قرار بگیرد.

SGSN

مهمترین بخش شبکه GPRS است و نقشی همانند MSC در شبکه های GSM دارد.

حداقل یک واحد SGSN در شبکه ی GPRS باید موجود باشد و همچنانکه شبکه گسترده تر می‌شود به تعداد بیشتری واحد SGSN نیاز است. SGSN وظایف زیر را بر عهده دارد.

- تبدیل پروتوکل (مثلا IP به FR)
- فشرده سازی داده ها برای انتقال
- تصدیق کاربران
- انجام مکانیزم رومینگ بین BTS ها و گاها بین SGSN های مختلف
- مسیریابی داده ها به GGSN مناسب در هنگام ارتباط با شبکه‌های خارجی IP
- ارتباط با NSS جهت دستیابی به اطلاعات کاربران از طریق سیگنالینگ شماره ۷ (SS7)

- تولید اطلاعات شارژینگ و ارسال به سیستم صورتحسابگیری
- جمع آوری اطلاعات ترافیکی جهت اهداف مدیریتی شبکه.

GGSN

این بخش را می توان دروازه ای به شبکه های خارجی در نظر گرفت. هر گونه ارتباط با شبکه های خارجی از طریق GGSN برقرار می‌شود.

GGSN مستقل از BTS و حتی SGSN است (از نظر انتقال داده‌ها) و ربطی به مسائلی از قبیل رومینگ و ... ندارد. معمولا دو GGSN در شبکه وجود دارد تا افزونگی نیز تضمین شود. اعمالی که GGSN انجام می‌دهد در زیر لیست شده اند:

- مسیریابی داده هایی که از شبکه های خارجی می آیند به SGSN مناسب (مربوط در SGSN بر عکس این کار صورت می‌گرفت)
- مسیریابی داده‌های ارسالی کاربران به شبکه های خارجی (داده ها توسط SGSN به GGSN می‌رسند)
- تولید اطلاعات شارژینگ و ارسال به سیستم صورتحسابگیری (مثل SGSN)
- این بخش همچنین با مسئله امنیت نیز سروکار دارد
- جمع آوری اطلاعات مربوط به ترافیک [همانند SGSN]
- اختصاص IP استاتیک و یا دینامیک توسط خودش یا با کمک PHCP یا RADIUS سرور

از دید شبکه های بیرونی GGSN مانند یک روتر که وظیفه مسیریابی بسته های IP را بر عهده دارد عمل می‌کند.

وقتی یک بسته اطلاعاتی از شبکه خارجی به منظور یک IP خاص درون شبکه موبایل به GGSN می‌رسد، ابتدا چک می‌کند، اگر آن IP (دستگاه) فعال باشد اطلاعات را برای ارسال به دستگاه (HOST) مورد نظر به SGSN می‌فرستد. اگر IP مورد نظر فعال نبود داده دور ریخته می‌شود. همچنین داده های ارسالی از داخل شبکه به خارج را نیز همانند یک روتر به خارج ارسال می‌کند.

(Border Gateway) BG

BG روتری است که یک تونل GPRS مستقیم بین اپراتورهای GPRS های مختلف ایجاد می‌کند. مزیت این ارتباط امنیت بیشتر آن نسبت به استفاده از شبکه عمومی اینترنت است. (برای ارتباط اپراتورها)

Border Gateway زمانی فعال (قابل استفاده) می‌شود که دو اپراتور با هم تفاهم نامه‌ای امضا کرده باشند.

(Charging Gateway) CG

کاربران شبکه می‌بایست برای استفاده از شبکه هزینه ای پرداخت کنند در شبکه های GSM مقدار این هزینه بر اساس زمان مکالمه فاصله و زمان مکالمه (شب یا روز بودن) تعیین می‌شود.

در شبکه های GPRS این موضوع عملی نسبت که هزینه را بر اساس طول زمان اتصال از کاربر دریافت کرد چرا که کاربر همیشه آنلاین است. در GPRS هزینه بر اساس حجم ترافیک، مقصد، QOS و دیگر پارامترهای مربوط به انتقال

داده محاسبه می‌شود. اطلاعات مربوط به حساب هزینه توسط GGSN، SGSN ها تولید و در قالب رکوردهای به نام CDR ذخیره می‌شود. این اطلاعات توسط CG جمع آوری پردازش شده و به سیستم پرداخت صورتحساب تحویل می‌شود.

انتقال این اطلاعات بین GSN ها و CG تحت پروتکل 'GTP صورت می‌پذیرد.

GPRS Interface ۲-۳

سیستم GPRS چهره جدیدی از شبکه های GSM معرفی می کند. شکل زیر آرایش منطقی سیستم ترکیبی از GSM و GPRS نمایش را می‌دهد. ارتباط دهی سیستم GPRS با سیستم NSS شبکه GSM به کمک SS7 پیاده سازی می شود. نقش رابط GPRS با NSS را SGSNبر عهده دارد.

مهمترین رابط ها به NSS:

SGSN-HLR(Gr) , SGSN-EIR(Gf) , SGSN-MSC(Gs)

بقیه رابط ها به قرار زیر هستند:

Intera-PLMN backbone Network (Gn)
Inter-PLMN backbone Network (Gp)
Internal Network (Gi)

خطوط انتقال (رابط ها) GPRS در زیر توضیح داده شده اند.

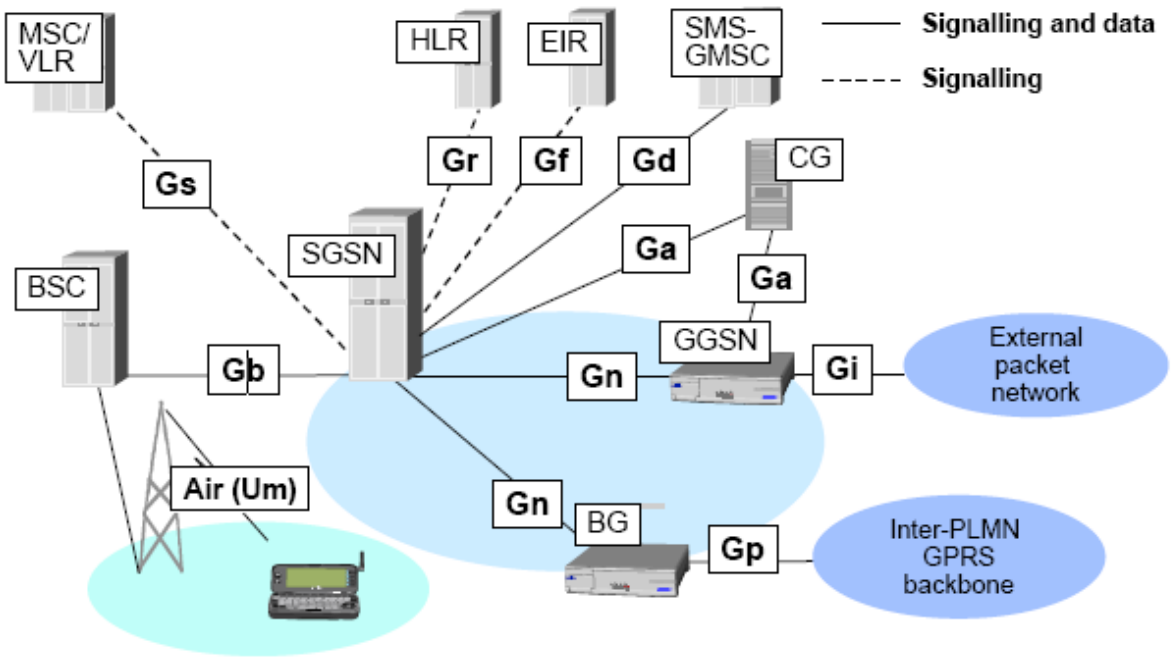

Figure 7- GPRS interfaces

Um: خطوط اتصال رادیویی بین MS و BTS . این اینترفیس با اینترفیس شبکه های GSM تقریبا مشابه است.

Gb: مابین SGSN و BSS قرار دارد. Gb اطلاعات (Data) و سیگنالهای شبکه GPRS را بین شبکه رادیویی GSM (BSS) و شبکه GPRS حمل می‌کند. این خط اتصال (interface) از سرویس های شبکه مبتنی بر FR (Frame Relay) بهره می‌برد.

Gn: بین دو GSM مربوط به یک PLMN قرار می‌گیرد این خط نیز امکان رد و بدل شدن Data و سیگنال را فراهم می کند. در خط اتصال Gn از پروتکل GTP استفاده می‌شود؛ از طریق شبکه ای با ستون فقرات مبتنی بر IP.

Gp: این رابط بین دو GSN مربوط به دو PLMN مختلف قرار می‌گیرد و فانکشن های مثل فانکشن های Gn فراهم می‌کند و علاوه به آن نام فانکشن‌هایی که برای Inter-PLMN Networking نیاز است از قبیل مسیریابی، امنیت و ... را فراهم می‌کند (چون بین دو PLMN مختلف قرار دارد.)

Gr: رابطی بین SGSN و HLR است. Gr امکان دسترسی SGSN به اطلاعات مشترکین در HLR را فراهم می کند. HLR می تواند در PLMN دیگری جز SGSN (مربوط به خودش) قرار گیرد.

Ga: بین GSM ها و CG در داخل یک PLMN قرار می گیرد. Ga اینترفیس با Data و Signaling فراهم می‌کند. این اینترفیس رکوردهای اطلاعاتی مربوط به شارژینگ را که توسط GSN ها ایجاد شده است را به CG انتقال می‌دهد. پروتکل مورد استفاده در Ga، 'GTP است که ورژن ارتقا یافته GTP است.

۳-۳- انتقال اطلاعات در شبکه GPRS

اطلاعات (Packet) کاربران در قالب کانتینرهایی از طریق ستون فقرات، GPRS ارسال می‌شوند. وقتی یک بسته اطلاعاتی از یک شبکه خارجی به GGSN وارد می‌شود، این اطلاعات در یک کانتینر قرار گرفته به SGSN ارسال می‌شود که این کانتینرها از دید کاربر کاملا مخفی است یعنی کاربر این طور حس می‌کند که مستقیما از طریق یک روتر از GGSN به شبکه خارجی متصل است.

در شبکه های ارتباطی داده این رشته مجازی از کانتینرها، تونل نامیده می شود.

GSN ها تونلی از Packet های کاربران ایجاد می‌کنند. (شکل ۸) پروتکلی که برای Tunneling (بین SGSN و GGSN) استفاده می شود GTP نام دارد (GPRS Tunneling Protocol).

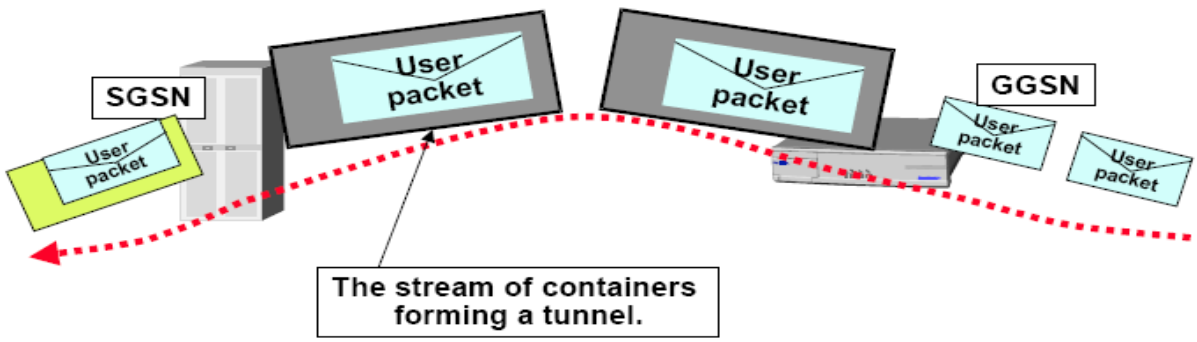

Figure 8- User packets over the GPRS backbone in 'containers'

از طریق ستون فقرات GPRS بسته های IP استفاده می‌شود تا بسته‌های GTP را حمل کنند. بسته های GTP نیز در حقیقت حامل پکت های کاربران هستند. (شکل ۹)

بسته های کاربران، برای مثال بسته های TCP/IP که قسمتهایی از یک ایمیل را حمل می کند در داخل یک بسته GTP حمل می شوند. بسته های GTP نیز از طریق ستون فقرات GPRS و توسط IP و TCP یا UDP حمل میشوند.

هدر بسته های GTP شامل یک تونل ID (TID) است که مشخص می کند مالک این اطلاعات کیست. TID هم شامل IMSI کاربر است (و دیگر شماره های خاص کاربر)

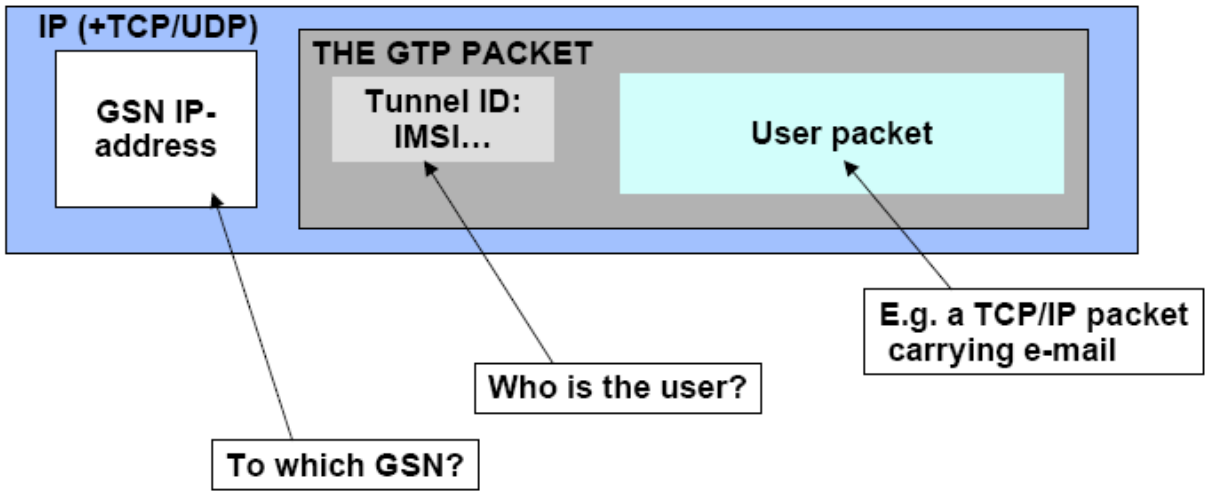

Figure 9- GTP container

TID به SGSN و GGSN اعلام می کند صاحب اطلاعات داخل کانتینر کیست. از نظر کاربران و شبکه های خارجی بسته های GTP که شامل بسته های کاربران هستند می توانند بین GSM به کمک تکنولوژی های مختلفی منتقل شوند از جمله ATM، x.25 و یا FR. تکنولوژی انتخاب شده در GPRS همان IP است.

تمامی المنت های یک شبکه (SGSN، از جمله CG و ...) باید دارای IP آدرس باشند. IP آدرس هایی که در backbone استفاده می‌شوند توسط MS ها و شبکه های خارجی غیر قابل رویت است این همان چیزیست که به آن Private IP Address می‌گویند. این یعنی، بسته های کاربران در هسته GPRS توسط آدرس‌های Private IP بین SGSN و GGSN حمل می‌شوند. این مفاهیم (Private IP Address و Tunneling) در شکل‌های بعدی به تصویر کشیده شده است.

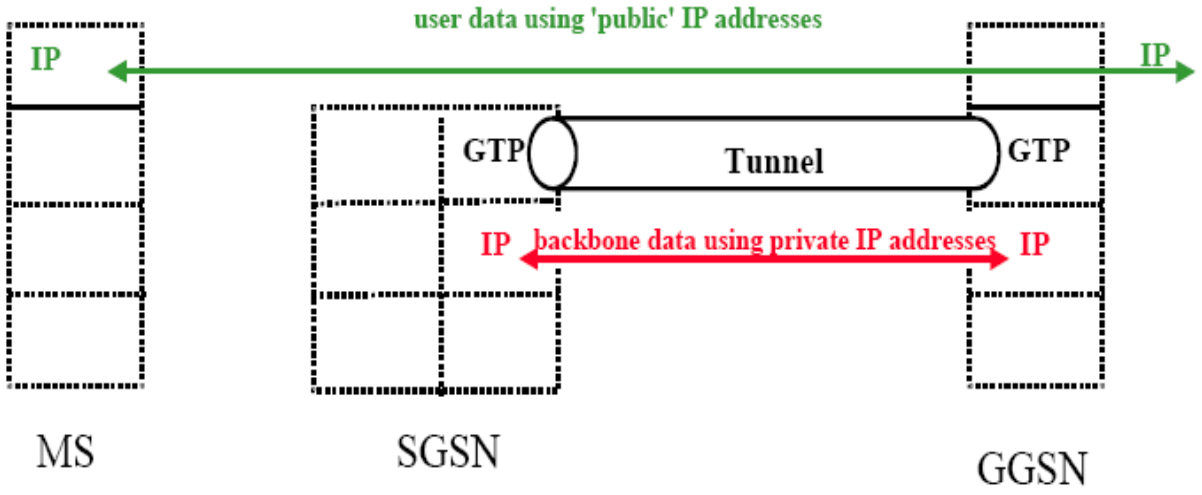

Figure 10. Transfer of packets between the GGSN and the MS

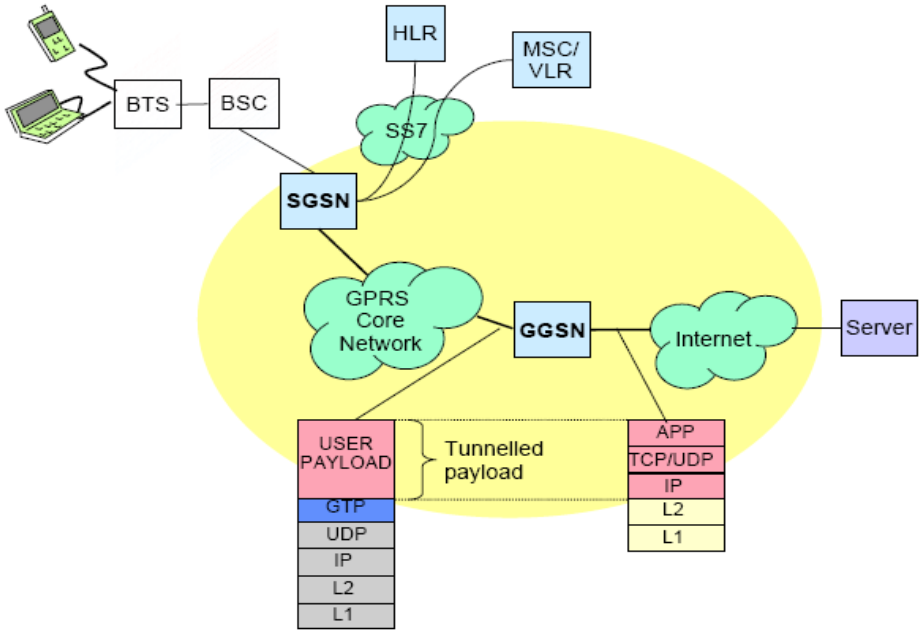

Figure 11- GTP tunneling and user payload

ضمیمه:

SS7 (سیستم سیگنالینگ شماره ۷): سیگنالینگ مبادله اطلاعات بین بخش های مختلف یک شبکه مخابراتی است و طبق تعریف زبانی است که تجهیزات و نودهای مخابراتی را قادر به ارتباط با یکدیگر می‌کند و مثل هر زبانی از لغاتی تشکیل یافته است. یکی از این سیگنالینگ‌ها سیستم ها، SS7 است که بر اساس ارتباطات داده بنا شده است.

x.25 اولین شبکه اتصال گرا که اوایل دهه ۱۹۷۰ وارد سرویس عمومی شد و برای ارتباط اجزای داخلی (Nod ها)شبکه های موبایل و تلفن و ... از آن استفاده می‌شود. سوییچینگ در این شبکه مداری است.

FR(Frame Relay) شبکه‌ای مشابه x.25 است با این تفاوت که پکت‌های ارسالی در این شبکه بر خلاف x.25 دارای پیغام Ack نیستند.

منابع

- شبکه‌های کامپیوتری تنن بام
- اصول طراحی شبکه‌های کامپیوتری ملکی
- آشنای با شبکه‌های GSM قنبریان
- GPRS_Architecture شرکت نوکیا
- Xiong Guangyu GPRS Architecture