الباب السادس

تصميم شبكة المحمول

الفصل الأول

تقنية شبكات المحمول

المقدمة

Global System for Mobile Communications
G.S.M.

كيف تعمل شبكة الهاتف المحمول؟

الاتصال الاسلكي تطور بشكل ملحوظ في السنوات الماضية . تقدير عدد المستخدمين للشبكة في السنوات القادمة كبير جدا , وخدمات الشبكة الحالية بتزايد كبير لتوفير نقل المعلومات بكميات كبيرة , وذلك يدعو الى اتساع الشبكة و زيادة عدد الاجهزة المستخدمة لتوسيع الشبكة.

لذلك فان الحل الأمثل لاستخدام الشبكة بشكل فعال هو الاستخدام الديناميكي للأجهزة , فهذا يعني أن تخطيط الشبكة الطبيعي يجب تغيره الى تخطيط ديناميكي , بحيث لا تستخدم الأجهزة فقط لمنطقة معينة بل تكون بشكل ديناميكي متغير على حسب الطلب واستخدام الشبكة .

ولتوضيح المعنى بطريقة أخرى , ففي حال استخدام الكثير من المستخدمين للشبكة بمنطقة واحدة فان الضغط يكون كبير عليها , أما الشبكة المجاورة لها فيكون الضغط ضعيف عليها لذلك فان على الشبكة المشاركة مع الأخرى لتخفيف الضغط عليها

تستخدم شبكة GSM الترددات حول 900 MHz أو 1800 MHz و تقسم الى قنوات لكي تسمح بنقل الصوت و المعلومات على شكل معلومات ديجيتال (Digital) , حيث تتكون الشبكة من عدة أجهزة لكل منها وظيفتها و تكون هذه الأجهزة متصلة مع بعضها البعض , بحيث يتم التوصيل بينها اما عن طريق كابل أو لاسلكي . كل من الموبايل و محطة الارسال والاستقبال في الشبكة يستخدمان كل منهما قناتين بفارق 54 أو 95 MHz, الموبايل يرسل بالموجة المنخفضة Uplink ويستقبل بالموجة المرتفعة Downlink . تجد بكل منطقة عدد كبير من محطات الارسال والاستقبال في الشبكة وذلك يتعلق بعدد المستخدمين للشبكة ويتم حساب درجة استخدام الشبكة بحسابات الاحصاء و التوقعات

تتألف شبكة الهاتف المحمول من شبكة إلكترونية من المحطات الرئيسية، وتغطي كل منها منطقة محددة)الخلية(وتوجه الاتصالات في شكل موجات الراديو من وإلى محطات المستخدمين.

تتبع الاتصالات المتنقلة المبدأ العام للاتصالات الهاتفية؛ حيث يتم ربط اثنان من المستخدمين البعيدين من خلال أجهزة الشبكة الخاصة بمشغل مسؤول عن إدارة الخدمة، وعلى عكس الهواتف الثابتة، ليست الأسلاك النحاسية أو الألياف البصرية في شبكة الهاتف المحمول هي التي توفر الحلقة الأخيرة ولكن إرسال الراديو هو ما يقوم بذلك، إذ يتصل الهاتف المحمول للمستخدم عبر الهواء بهوائي محطة أساسية متصل بدوره بالسنترال المركزي للمشغل، جهاز كمبيوتر، ثم يقوم السنترال بتوجيه الاتصال إلى الطرف المقابل على الشبكة الثابتة أو عبر محطات أخرى. وللتمكن من الاتصال يجب أن يكون مستخدم الهاتف المحمول داخل نطاق المحطات الرئيسية، حيث إن المحطات الرئيسية لها نطاق محدود ولا تغطي سوى مساحة صغيرة حولها تسمى "الخلية")ومن هنا يستخدم الاسم البديل "الشبكات الخلوية" غالبا مع شبكات المحمول(، ولتغطية أقصى قدر من المساحة وضمان قدرة المستخدمين دائما على الاتصال، يقوم المشغلون بنشر الآلاف من الخلايا المزودة بهوائيات، مع ضمان ترابط الخلايا وبالتالي عدم فقدان الموقع الحالي للمستخدمين.

الخلايا الحضرية والخلايا الريفية

يعتمد حجم الخلية على العديد من العوامل، مثل نوع المحطات الرئيسية المستخدمة، والتضاريس)السهول والجبال والوديان وغيرها(، وموقع التركيب)المناطق الريفية أو الحضرية(، والكثافة السكانية، كما يُحدَّد حجم الخلية بنطاق الهاتف المحمول، الذي يجب أن يكون قادرا على توفير حلقة الإرجاء . والأهم من ذلك هو أن المحطات الرئيسية لديها قدرة إرسال محدودة، ولا يمكنها التعامل سوى مع عدد معين من المكالمات في وقت واحد، ولذلك نجد في المناطق الحضرية، ذات الكثافة السكانية المرتفعة وعدد الاتصالات الكبير، أن الخلايا تكون كثيرة وصغيرة ولا تبعد عن بعضها البعض سوى بمئات أو حتى عشرات الأمتار، أما في المناطق الريفية، ذات الكثافة السكانية الأقل بكثير، فنجد أن حجم الخلية يكون أكبر بكثير، وأحيانا تبعد الخلية عن الخلية الأخرى بعدة كيلومترات ولكن نادرا ما تتجاوز أكثر من عشرة كيلومترات. ومن المهم التأكيد على أن الحد من قوة الإشارة المنبعثة من المحطات الرئيسية يقلل بدوره من تغطية الخلايا، وتحسين قدرة الشبكة على نقل المكالمات الصوتية أو نقل البيانات الذي يقتضي بالضرورة زيادة عدد المحطات الرئيسية.

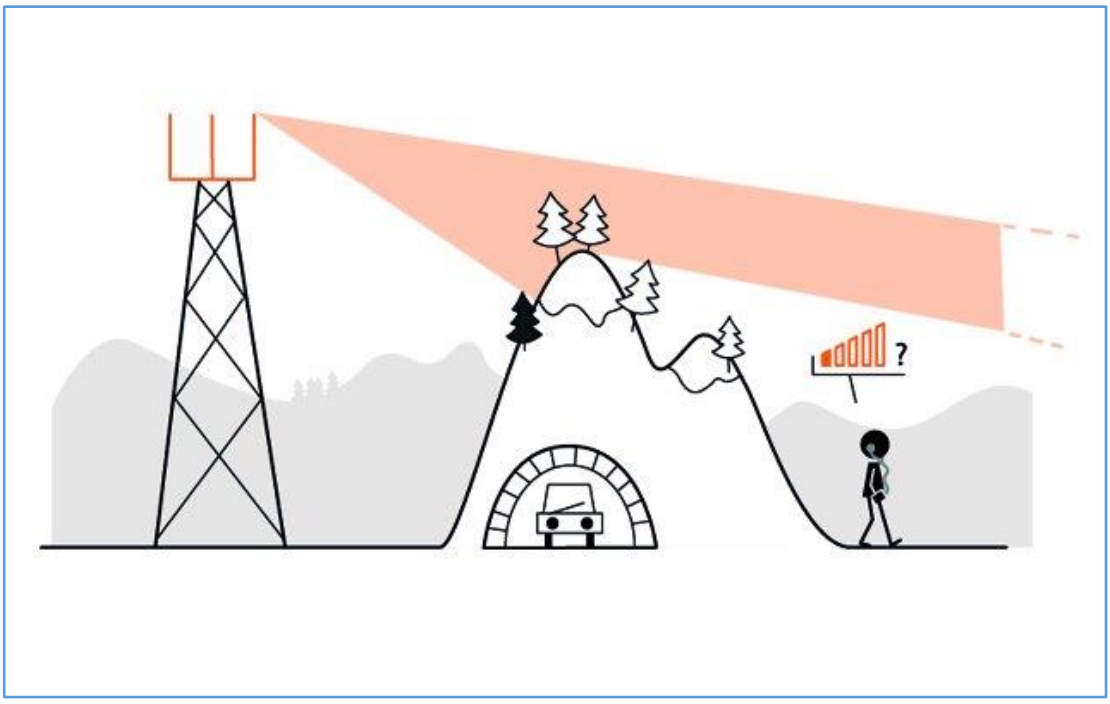
التغطية و الجودة

مع انتشار الاتصالات المتنقلة أصبحت شبكات المحمول بنية تحتية إستراتيجية للاقتصاد في كثير من البلدان، ولهذا فإن انتشار تلك الشبكات يخضع للسياسات واللوائح العامة لضمان وصول الجميع إلى خدمات الهاتف المحمول.

تختلف شروط نشر شبكات المحمول بشكل كبير من بلد إلى آخر اعتمادا على الرخص التي تمنحها السلطات أو حجم وكثافة السكان أو المساحة المقرر تغطيتها أو نوع خدمات الهاتف المحمول المقدمة.

تحديات نشر الشبكات

يُترك الأمر للمشغلين لتحسين نشر الشبكات الخاصة بهم من خلال عدة اعتبارات، إذ يجب أن تكون شبكة الهوائيات كبيرة بما يكفي لتبقى في متناول أكبر عدد من المستخدمين المحتملين، كما يجب أن تكون مصممة للتغلب على العقبات الملقاة في طريق انتشار موجات الراديو مثل اختلافات المناظر الطبيعية، والمواد التي تمنع الإشارة أو تضعفها، والأنفاق، وما إلى ذلك أخيرا يجب أن يكون تركيب المحطات القاعدة كثيفا بما فيه الكفاية لتلبية احتياجات حركة المرور واستيعاب أعلى فترات الاتصالات بجودة إشارة مثلى، ولهذا تكون الخلايا الموجودة حول المحطات الرئيسية كبيرة جدا في المناطق الريفية وأقل من ذلك بكثير في المناطق الحضرية السكنية التي بها تكون حركة الاتصالات المحمولة فيها أكثر تركيزا



... لماذا إبعاد المحطات الرئيسية؟ إنها ليست فكرة جيدة

إن تركيب المحطات الرئيسية في أماكن قريبة يمكن المستخدمين من الحصول على اتصالات جيدة أثناء استخدام الطاقة المنخفضة، وبتركيب تلك المحطات في أماكن بعيدة، فإن الأمر يستلزم زيادة

- ارتفاع الأبراج لتغطية مناطق أوسع، مما يجعل تكامل مشهد الهوائيات أكثر صعوبة
- طاقة الهوائيات للتواصل مع أبعد المستخدمين عن وسط الخلية
- طاقة الهاتف المحمول بحيث يمكن أن يوفر حلقة الإرجاع مع هوائي أكثر بعدا

ما معنى GSM ؟

كلمة GSM أختصار لـــ Global System for Mobile Communication و إذا اردنا ان نترجمها حرفيا الى العربية فهي تعني **النظام العالمي للأتصـــال المتحرك** (المحمول), و هي الشبكة الحاليه المتوافقة المواصفات في جميع بلدان العالم .

كيف تعمل شبكة ال GSM

أجزاء الشبكة :

لكى تفهم كيفية عمل شبكة ال GSM من الضروري عليك ان تعرف مكونات الشبكة , و التي تتكون من عدة أجزاء تعمل مع بعضها , هيا بنا لنتعرف على هذه الأجزاء:

1- المحطة المتحركة Mobile station , هي عباره عن جزئين الهاتف المتحرك (الجوال) و يسمى ME Mobile Equipment
البطاقة الذكيه (الشريحه) و تسمى SIM Subscriber Identity Module
2- النظام الفرعي للمحطة أساسيه Base Station SubSystem
و هي عبارة عن مجموعه من :
المحطات الفرعيه BTS Base Terminal Station
وتسمى ايضا Base Transceiver Station
او ما يعرف بالهوائيات و القنوات المتواجده في الميدان , ال BTS يحتوي على جهاز الارسال/الاستقبال الذي يعرف لنا الخليه التي سوف تعطي جهازالموبايل (الجوال) اشارة الراديو التي سوف يرسل و يستقبل عليها , ال BTSمربوط معال BSC الذي سوف نشرحه لاحقا . يجب علينا ان نرتب ال BTS's بشكل يمكنا من تكوين خلايا .

كل BTS يخدم خلية ,اى مكان على سطح الارض يمكن ان يغطى بخليه او عدة خلايا .
ان ابعد نقطة يستطيع ان تغطيها وحدة ال BTS تقريبا 8 كم وتكون عادة في الاماكن الخارجيه الغير مزحومه مثل القرى او ضواحي المدن .
ال BTS النموذجي يغطي زاويه قدرها 120 درجه , اذا نحتاج الى 3 BTS's لتغطية 360 درجة .

مراقب المحطات الفرعيه BSC Base Station controllers :-

و هي التي تدير موارد اتصال الراديو ل BTS واحد او عدة BTS's, تتعامل مع اعداد قناة الراديو , و نظام قفز (وثب) الترددات frequency Hopping و التسليم من خليه لاخرى بمعنى اعطاء الموبايل (الجوال) تردد جديد عندما يغير خليته او موقعه Handovers , في اكثر الاحيان سوف تجد BSC و عدة BTS's في نفس الموقع , لنقل على سطح احدى البنايات .

3- محطة النظام الفرعي للشبكة NSS Network Station SubSystem
و هو يعتبر العقل للشبكة , و تكمن فيه انظمة الفواتير و خدمة توجيه الاتصال الى الشبكات المراد تحقيق الاتصال معها ... الخ

و يتكون ايضامن اجزاء اخرى و هي مركز تبديل (تحويل) مكالمات الموبايل (الجوال)MSC Mobile Switching Center

ويعمل كبدالة اعتيادية مثل المتواجدة في نظام الهواتف السلكية بالاضافه الى ان المركز يوفر جميع الوظائف التي يحتاجها الموبايل (الجوال) مثل:
هل الموبايل مسجل مع الشبكه او ما يعرف بالـ Registration
وايضا التخويل و هل الموبايل مصرح له باستخدام الشبكة او ما يسمى بال Authentication ,
ايضا يقدم وظيفة تحديث موقع الموبايل (الجوال) في الشبكة او ما يعرف بال Location Updating و التسليم بين ال BTS's و ما يعرف بال HandOvers
و يقدم لنا وظيفة توجيه او تحويل الاتصال للمشتركين المتجولين romaing subscriber
الـ MSC يقدم لنا الاتصال و الربط مع الشبكات المحليه الثابته مثل شبكة مقسم الهواتف السلكي PTSN او الشبكة الرقمية للخدمات المتكاملة ISDN .
لغةالتخاطب بين هذه الخدمات في الشبكه هي النظام الاشاري رقم سبعه او مايعرف بال Signalling System number 7 SS7 و هي ايضا في الشبكات السلكيه كمقسم الهاتف .
هذا المركز هو النظام الذي تتحدث اليه جميع ال BSC's.
سجل المقرالرئيسي (الموطن) HLR Home Location Register
و هو عبارة عن سجل دائم تحفظ فيه الاعدادات الخاصه لكل مشترك للتمكين الشبكه من التحكم في الاتصال الخاصل لمشترك مثلا هل المشترك محول مكالماته او هل عنده خدمة الانتظار او الخ و أيضا يوفر سجل مخزن فيه مكان الموبايل (الجوال) الحالي , الشبكه تحتوي على HLR واحد , ولكن يمكن ان نوزع عدة HLR's بمعنى انهن متماثلات .

سجل مقر الزوار VLR Visitor Location Register

وهو عباره عن سجل مؤقت تحفظ فيه الاعدادت الضروريه لتشغيل الموبايل (الجوال) , الموبايل (الجوال) دائما يتحدث الى ال VLR , كل MSC يحتوي على VLR

مركز التخويل AuC Authentication Center

هذا هو مركز الامن للشبكة الذي يعطي الاوامر بالتخويل للموبايل (الجوال) بإستخدام الشبكة

سجل تعريف الاجهزةEIR Equipment Identity Register

و هو عباره عن قاعدة معلومات لكل ارقام التعريف لجهاز الوبايل (الجوال) , و هو عبارة عن رقم يوضع داخل الجهاز من قبل الشركة المصنعه له و كلجهاز في العالم له رقم خاص به و هو ما يسمى با IMEI
تعريف جهاز المتحرك العالمي International Mobile Equipment Identity
وهذا السجل يتوي على ثلاث اقسم او قوائم , القائمة البيضاء او ما يعرف بال White list و هي الاجهزة المصرحه باستخدام الشبكة و القائمه السوداء Black List و هي الاجهزة الغير مصرح لها بإستخدام الشبكه و القائمه الرماديهGray List وهي التي ليست من القوائم الاخرى

لمحة عن IMEI :
هو رقم خاص لكل جهاز موبايل (جوال) ME يوضع بواسطة المصنع , هذاالرقم يرسل مع كل اتصال يعمله الموبايل (الجوال) الى الشبكه و هو عادة يكتب خلف بطارية الجهاز و يتكون من النمط التالي

X X X X X X - X X - X X X X X X - X

TAC - FAC - SNR - CD
TAC: type approval code
FAC : final assembly code
SNR: serial number
CD: check digit
ولكن تم تغيير النمط الحالي من قبل اتحاد الاتصالات العالمي ITU الى التالي

X
TAC - SNR - CD

ويمكن ان نجده ايضا بهذا النمط IMEISV و ال SV software version تعني نسخة البرنامج

X X X X X X X X X - X X X X X X - X - X X
TAC - SNR - CD -SVN
SVN software version noumber

لمحة عن تعريف المشترك IMSI International Mobile Subscriber Identity

هو عبارة عن رقم خاص لكل بطاقة (شريحه) و هو ليس رقم الموبايل (الجوال) الذي يتم الاتصال بواسطته , هو رقم اقرب الى رقم الشبكه و هو يحتوي غالبا على 15 خانه كالنمط التالي

X X X - X X - X X X X X X X X X
MCC - MNC - MSIN

MCC: mobile country code كود الدوله
MNC : mobile network code كود الشبكه التي اشتريت منها بطاقتك (شريحتك)
بعض الاحيان يكون من ثلاث ارقام خاصه في امريكا الشماليه
MSIN: mobile station identification numbe رقم تعريف المحطة المتحركة (الموبايل)

هذا الرقم نحتاجه من اجل ان اى شبكة هاتف متحرك ارضيه PLMN Public land mobile network تستطيع به ان تتعرف على الموبايل و اذا كان خاصة غير مشترك معها بحيث تقدم له الخدمات التي يكون مخول بها من قبل شبكته الام .

التواصل بين الشبكات :-

عندما نشغل جهاز الموبايل (الجوال)MS فإنه يحاول ان يتصل بالشبكه , على امل ان تسمح له او تخوله الشبكة من استخدام مواردها . هذا يمكن ان يحدث بالنسبه لشبكتك الام او حتى اذا كنت في حالة تجوال roaming و تستخدم خدمات شبكه غير شبكتك الام.
ان جهاز الموبايل (الجوال) MS يعمل هذا الشى بالاتصال مع ال BTS الموجود في نفس المكان او بمعنى اخر الBTS المغطي لهذه المنطقه المتواجد بها الموبايل .

تقوم ال BTS's بشكل اعتيادي ببث (ارسال) الترددات و ذلك لتمكين الموبايل MS من التقاط الاشارة الاقوى .

و هذا التغيير في ال BTS لا يحدث هكذا و انما الموبايل MS يقيس قوة الاشارة فاذا وجد اشارة افضل من التي هو عليها يرسل القياس الى ال BTS و ال BTS بدوره يرسلها الى ال BSC الذي هو مراقب لل BTS's ويرى اذا كان هذا التغيير في ال BTS ممكن يحوله او يسلم الموبايل الى ال BTS الجديدو هذه الطريقه تسمى ال Handover .و لكن اذا ال BTS الجديد لا يتبع ال BSC الحالي فانه يرفع الامر الى MSC لأخذ الاجراء المناسب و هو بالاتصال بال BSC الجديد وتسليم الموبايل ال BTS الجديد لان ال BSC لا يستطيع التحدث BSC اخر, اذا الموبايل غيرBSC وغير ال BTS و هذه عادة تحصل عندما نكون في وسيله من وسائل النقل كالسياره فنغير الاثنين معا .

في كلتا الحالتين الموبايل MS و ال BSC/MSC يعملون مع بعض لعمل التسليم Handover بشكل سلس, الشبكه تعمل على حجز قناة في ال BTS الجديد لتمكين التسليم Handover و حتى ان كنا اثناء مكالمه .

للاتصال القادم علينا بمعنى اذا اراد احد ان يتصل عليك من الضروري ان تعرف الشبكة اين يتواجد الموبايل (الجوال) MS و تحت اى MSC و اى BSC و اى BTS لكى تتمكن الشبكة من ايصال المكالمه اليك , هنا نتعرف على اهمية ال HLR سجل الموطن , VLR سجل الزوار .
ان ال HLR يخبرنا عن ال VLR و ماذا يعرف ؟ اين الموبايل (الجوال) MS ؟ أن ال VLR يحتوي على ما يسمى بال LAC Location Area Code كود المناطق و هو عباره عن كود للمناطق التي تغطيها كل خليه او مجموعه من الخلايا . ال VLR ينشأ صفحة تحتوي معلومات عن الموبايل MS ويرسلها الى MSC و هذا يحدث عندما يغير الموبايل موقعه من مكان الى اخر و ال MSC يحدث ال HLR بأخر موقع للموبايل . الموبايل دائما يكون على اتصال مع ال PCH Paging channel لذلك الموبايل دائما يحصل على مكالمات ويستقبلها .
اذا الاتصال القادم الى الموبايل MS يبدأ دائما من عند HLR هذا الاتصال يحدث بسهوله لان كل شبكه تعرف اينHLR الخاص بها و ايضا تعرف رقم الموبايل المشترك لديها MS و لهذا لانهتم الابهم فالاتصال يذهب اليهم اولا و لايهتم في البدايه بموقع الموبايل MS الحالي لان التبديل او تحويل المكالمه سوف يتم عن طريق MSC مثال على ذلك : شخص يتصل من الصين على رقم موبايل في هولندا و هذا الموبايل حاليا ليس في هولندا بل هو متواجد في اسبانيا كيف يتم الاتصال .؟؟؟؟ كالتالي :-
الشخص الذي في الصين سوف يتصل على رقم الموبايلفي هولندا الاتصال سوف يذهب ال شبكة الموبايل في هولندا وبالتحديد الى MSC و ال MSC سوف يخاطب ال HLR ماهو اخر تحديث لديك عن موقع الموبايل

ال HLR سوف يخبره ان اخر معلومات لديه انه متواجد في اسبانيا على الشبكه الابانيه

ياترى كيف عرف ال HLR ??? لان ال VLR اسبانيا التقط إشارة الموبايل الهولندي و حولها الى ال MSC الى الاسباني و بدوره حول المعلومات عن موقع الموبايل الى شبكته الام في هولندا و الشبكه حفظت المعلومات الجديده في ال HLR .... ال MSC سوف يحول الاتصال الى الشبكة الاسبانيه وفي الشبكة الاسبانيه سوف يستلم ال MSC الاتصال و يحوله الى الموبايل الهولندي المتواجد في اسبانيا . اذا من هنا اتضح لنا فائدة ال HLR و ال VLR هو عندما نقوم بإغلاق الموبايل MS , الشبكه سوف تتذكر اخر موقع كان متواجد فيه الموبايل MS

اذا لم تتلقى الشبكه اى اشارة بأنالموبايل MS أُغلق فأنها تستمر بالاعتقاد ان الموبايل يتصل على قناة تحديد الموقعPCH و للتاكد من ذلك تقوم الشبكه بتحديد وقت يقوم فيه الموبايل MS بأرسل فيه رساله بانه متواجد على الشبكه .

مصطلحات :-

MS mobile station(الشريحه) و هو الجهاز مع البطاقه

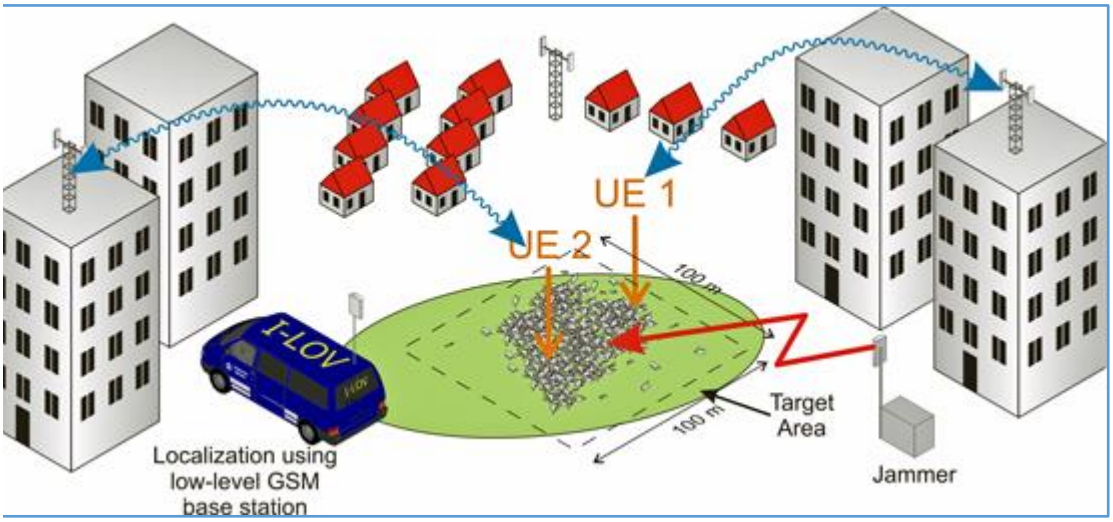
BTS base terminal station و هي المحطة الطرفيه التي تحتوي على الهوائي

BSC Base station Controller وهو المراقب لعدة محطات طرفيه

MSC mobile switching center و هو بدالة الموبايل

Security GSM

عمليات الحماية والتشفير فى شبكات الموبايل



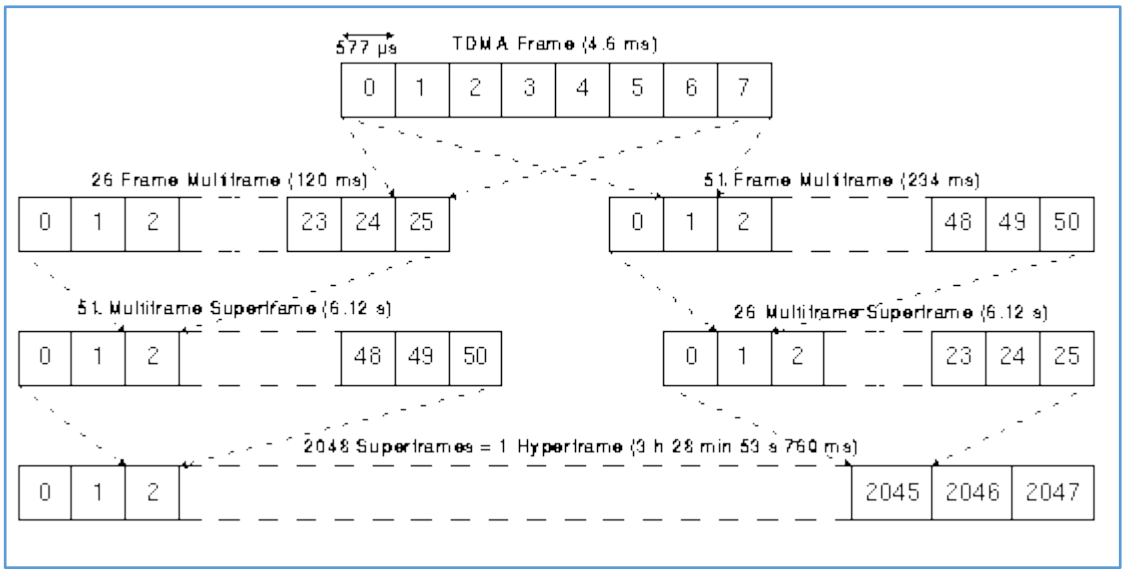
عملية اعتراض على احدى المناطق المستهدفة داخل احدى شبكات الموبايل

كلنا يعرف متى واين بدأ العمل بنظام الاتصالات الخلوية GSM ولكن كان دائما مشاكل وقلق من كيفية الحد من التشويش او التجسس على الشبكة مما كان يؤدى الى تسرب المكالمات الشخصية او ايضا المكالمات التى تخص الامن القومى لكل دولة.

تم التغلب على هذه المشاكل بطرق كثير من توثيق للمستخدم Authentication وتشفير للبيانات وغيرها من الطرق التى تمنع عمل jamming على الشبكة او قنوات الاتصال.

كلنا نعلم ان الجيل الثانى للموبايل تعمل على ترددات من 890 ميجاهرتز حتى 915 ميجاهرتز فى uplink وتعمل على ترددات من 935 ميجاهرتز حتى 960 ميجاهرتز فى downlink مقسكة الى عدة قنات بحيث ان يكون حيز كل قناة 200 كيلوهرتز. كما نعلم ان الجيل الثانى يستخدم GMSK وايضا يعتمد على hopping .

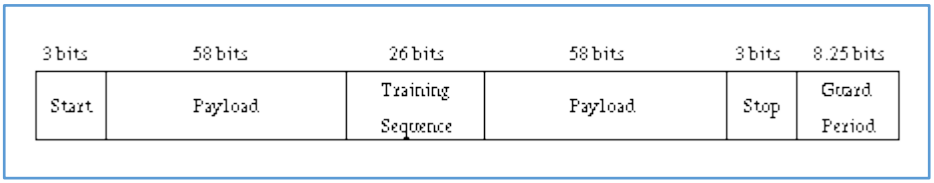
ونعلم جميعا ان الجيل الثانى يعتمد بالدرجة الاولى على TDMAحيث يقوم بتقسيم كل قناة الى عدة فريمات frames ويحتوى كل فريم على 8 Ts وكل 26 او 51 فريم يتم جمعهم فى فريم اكبر يسمى multiframes وهو يحتوى على مجموع 120 او 235 مللى ثانية . ثم يتمم جمع كل 26 او 51 ملتى فريم الى فريم اكبر يسمى superframe ويحتوى على 6.12 ثانية.



يتم تجميع القنوات التى يعتمد عليها عمل TDMA فى قنوات traffic channels (TCHs) والتى تستخدم لنقل الصوت والداتا وايضا الى قنوات control channels (CCHs) والتى تستخدم لنقل بيانات الاشارة والتحكم .

نعلم ايضا من الدروس السابقة ان كل Ts تسمى burst ويوجد فى شبكات الموبايل 5 انواع منها وهم (normal, frequency correction, synchronization, dummy, and access bursts)

والشكل التالى يوضح مما يتكون النوع الاول normal burst



ماهو التشفير Cryptography ؟

لكى نفهم التشفير علينا ان نعلم كيفية عمله اولا وماهى الخوارزميات المستخدمة

1- الخوارزميات المتناظرة

فى هذا النوع يتم استخدام نفس المفتاح فى التشفير وفك التشفير فمثلا لو عندنا رسالة بها حرف A وتم تشفيره الى نص وليكن B وتم استخدام المفتاح X فى التشفير encryption باستخدام الدالة Ex( ) وفى فك التشفير decryption باستخدام الدالة Dx( ) فسوف تصبح معادلات التشفير كالتالى :

C=Ex(P)
P=Dx(C)
P=Dx(Ex(P))

ولكى نحافظ على سرية التشفير يجب علينا الحفاظ على سرية مفتاح التشفير وفكه لأن لو استطاع اى مخترق ان يعرفه فسوف يستطيع فك النص المشفر ومعرفة الرسالة الحقيقة ولعمل ذلك سيتم عمل التالى :

اولا: تجزئة الشفرات الى بلوكات Block Ciphers

نقوم هنا بتشفير او فك تشفير البيانات عبر تقسيمها على مجموعات من البيتات bits ومثال على هذا النوع هو نظام DES حيث يقوم باستخدام 56 بيت --> 56-bit كمفتاح للتشفير ثم يقوم بتقسيم الداتا الى 64- bit كمجموعات او لوكات blocks ثم تحويل الداتا الى 64-bits داتا مشفرة جديدة وهكذا...

يتم تمييز هذا النوع بنوع العملية المستخدمة فى هذا الاجراء وهناك عدة انواع منها

---> Electronic code book (ECB)

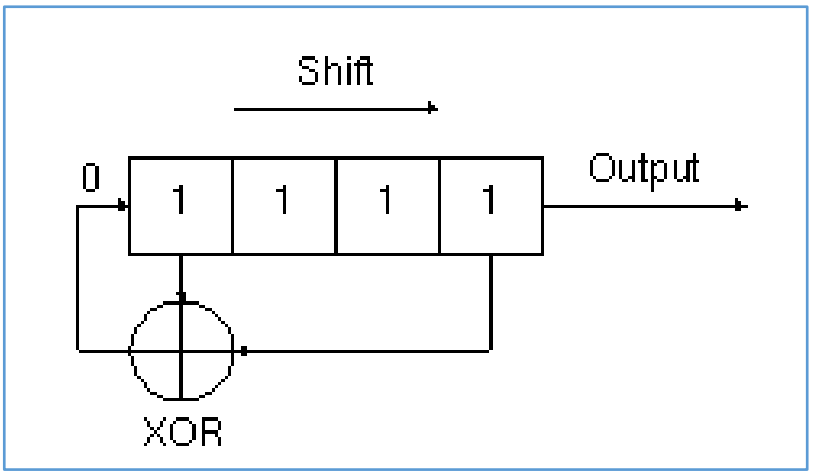
---> Cipher block chaining (CBC)

---> Cipher feedback (CFB)

ثانيا: تحويل الشفرات الى استريم Stream Ciphers

ويقوم هذا النوع بتشفير بيت وراء الاخرى bit-by-bit على الترتيب مما ينتج bit مشفرة ويعتمد هذا النوع على استخدام XOR للتشفير وهى من الانواع القوية فى التشفير وتعتمد خصائص الملف المشفر على الاستريم الخاص بمفتاح التشفير keystream والخاص بكل bit

يتم الاعتماد على Linear Feedback Shift Registers (LFSRs) كأداة اساسية فعمل مفتاح التشفير حيث يتم ازاحة كل bit ثم تشفيره باستخدام XOR ثم ازاحته مرة اخرى وتشفير bit الذى يليه كما بالشكل



وهنا نلاحظ انه يقوم بعمل نفس الشـــىء الذى يقوم به اى مولد لـــــــرقم pseudo-random ويوجد ميزة فى هذا النوع حيث ان به امكانية اعادة تصـــحيح الخطأ فى الداتا المرسلة

أقصى طول لأى تشفير يمكن الحصول عليه يساوى n-12 حيث n هى درجة ريجستر الازاحة shift register وكمثال على ذلك اذا نظرنا الى الرسم بالأعلى نستطيع ان نعرف الاستريم الناتج من هذا الريجستر وهو كالتالى

1111, 0111, 1011, 0101, 1010, 1101, 0110, 0011, 1001, 0100, 0010, 0001, 1000, 1100, 1110

وهنا نلاحظ انه فى البداية تم خروج 1111 ثم تم عمل ازاحة من اخر رقم وعمل XOR مع اول رقم لينتج رقم جديد يتم ازاحة الريجستر به وهكذا ...

معلومة :

يتم استخدام هذا النوع من التشفير فى تشفير الداتا للثوت المرسل فى شبكة الجيل الثانى GSM