

État de l'art associé au projet tuteuré

Interception passive d'informations sur le réseau GSM

Geoffrey Calmet-Sanchez : gsanchez@etud.insa-toulouse.fr

Damien Cassu : cassu@etud.insa-toulouse.fr

Axel Chauvin : achauvin@etud.insa-toulouse.fr

Cécile Duthoit : duthoit@etud.insa-toulouse.fr

4^{ème} année Réseaux & Télécoms

INSA Toulouse 2015/2016



Tuteurs : Daniela Dragomirescu, Damien Roque

Résumé du projet

Le but premier de ce projet est de mettre en oeuvre une plate-forme d'interception passive d'informations sur le réseau GSM. Notre système s'appuiera sur une station de base déjà développée à l'aide de technologies open source. Pour préparer cette réalisation technique nous avons réalisé une étude bibliographique résumant les techniques et les outils utilisés aujourd'hui pour contourner les procédures d'authentification du standard GSM.

Points abordés dans ce rapport :

- Principes généraux du fonctionnement du réseau GSM
- Qu'est-ce qui a déjà été fait dans le domaine de l'interception ?
- Jusqu'où peut-on aller (simple captation de messages, déchiffrement ...) ?
- Quelles sont les solutions techniques possibles ?

Sommaire

1 Introduction	2
2 Les réseaux GSM	3
2.1 Principe de fonctionnement.....	4
2.1.1 Architecture du réseau GSM	4
2.1.2 Les bandes de fréquence GSM.....	5
2.1.3 Modulation GSM et couverture du signal	5
2.2 Système de sécurité du réseau GSM	6
2.2.1 Vue d'ensemble du système de sécurité GSM	6
2.2.2 Authentification des utilisateurs du réseau.....	6
2.2.3 Chiffrement des données	7
3 Les faiblesses du système de sécurité GSM.....	8
3.1 État des lieux des faiblesses du réseau GSM	8
3.2 Les attaques possibles	9
3.3 Exemple de réalisation d'une station d'interception	9
3.3.1 IMSI catcher	9
3.3.2 Contourner le chiffrement des communications	14
3.3.3 Intercepter et router appels et messages	15
3.3.4 Attaques diverses.....	16
3.4 Le cas des SMS	16
3.4.1 Principe de fonctionnement.....	17
3.4.2 Les vulnérabilités des SMS	17
3.4.3 Le SMS, un outil de surveillance	18
4 Conclusion.....	20
5 Lexique.....	21
6 Références bibliographiques	24
7 Table des illustrations.....	25

1. Introduction

Le GSM (Groupe Spécial Mobile puis Global System for Mobile Communication) est une norme de téléphonie mobile de seconde génération standardisée par l'ETSI¹¹ (European Telecommunications Standards Institute) au cours des années 80. Depuis le début de son déploiement au début des années 90, le nombre de terminaux mobiles compatibles n'a cessé d'augmenter. En 2011 plus de 6 milliards de connexions mobiles sont recensées à travers le monde.



Fig. 1.1 - Logo de la norme GSM

Les coûts élevés des équipements d'interception ont permis pendant longtemps d'éviter tout problème relatif à la sécurité des réseaux GSM. Mais les outils technologiques logiciel et hardware étant de plus en plus accessibles au fil des années, les failles du système GSM ont commencé à être progressivement exploitées.

Considérant la popularité de ce moyen de communication et le nombre d'utilisateurs vulnérables, il nous a semblé nécessaire de nous intéresser aux techniques d'interception et aux moyens de les mettre en oeuvre. Afin de concevoir une plate-forme d'interception passive d'informations sur le réseau GSM, nous avons réalisé la présente étude bibliographique. Son rôle est de faire un état des lieux des connaissances et techniques actuelles. Dans un premier temps, nous nous intéresserons au standard GSM pour identifier et comprendre ses faiblesses. Ensuite nous étudierons dans le détail différents types d'attaques ainsi que les outils disponibles pour les mettre en oeuvre.

2. Les réseaux GSM

Depuis leurs débuts, les communications mobiles ont connu nombre d'évolutions. On peut globalement considérer qu'une nouvelle génération de système de communication mobile apparaît chaque décennie. La deuxième génération de technologie mobile (2G) a été développée au début des années 90. Elle est une évolution de la première génération (1G) de technologie mobile qui s'appuyait sur un système analogique, développé au début des années 80. La 2G, aussi connue sous le nom de technologie GSM, s'appuie sur un standard qui décrivait à l'origine un réseau digital, optimisé pour des communications téléphoniques (voix) en full-duplex. Le développement de la 2G, grâce à son système digital, marque notamment le début des SMS (Short Message Service).

Au cours des années 90, le réseau 2G a été étendu pour inclure les communications par paquets de données, d'abord par le transport à commutation de circuits, puis par le transport de paquets de données via GPRS¹³ (General Packet Radio Services), aussi connu sous le nom 2.5G, et via EDGE¹⁰ (Enhanced Data rates for GSM Evolution or EGPRS), ou 2.75G. Ces évolutions ont permis d'atteindre de meilleurs débits de données (d'environ 9.05 Kb/s pour la première 2G à un débit théorique de 384 Kb/s pour la 2.75G). La 2.5G a aussi marqué le début des MMS (Multimedia Messaging Service).

Au début des années 2000, la troisième génération (3G) de réseaux cellulaires est développée. Elle est aussi connue sous le nom d'UMTS³³ (Universal Mobile Telecommunications System). Ce système est basé sur le standard GSM. Il a été développé et est encore maintenu par le 3GPP¹ (3rd Generation Partnership Project). Plus tard, il a évolué vers la 3.5G (ou 3G+), en utilisant les standards HSDPA¹⁵ (High-Speed Downlink Packet Access) ou HSUPA¹⁸ (High-Speed Uplink Packet Access), puis vers la 3.75G avec les standards HSPA+¹⁷ (Evolved High-Speed Packet Access) et DC-HSPA+⁹ (Dual Carrier/Channel High-Speed Packet Access) pour atteindre des débits jusqu'à 42 Mb/s. Cette dernière évolution a annoncé la 4G.

Dans les années 2010, la 3.9G est développée, aussi connue sous le nom de Long Term Evolution (LTE)²³, avec des débits théoriques pouvant atteindre 300 Mb/s. Bien que cette technologie ne respecte pas encore tous les critères décidés pour définir la 4G, l'appellation commerciale "4G" est tolérée.

Aujourd'hui, la 4G LTE Advanced²⁴, la seconde génération de 4G LTE qui répond aux critères du standard, est en développement et promet des débits pouvant atteindre 1Gb/s.

2.1. Principe de fonctionnement

2.1.1. Architecture du réseau GSM

Le réseau GSM est un réseau cellulaire, ce qui signifie que les téléphones mobiles s'y connectent en recherchant les antennes relais les plus proches. Une antenne est une partie d'une station de base (BS aka Base Station) et plusieurs BS forment le réseau cellulaire.

Typiquement, un réseau GSM contient des BS, un concentrateur de BS (BSC aka Base Station Controller), différentes bases de données (VLR, HLR), des commutateurs (MSC) et des terminaux. Cette partie du réseau GSM est présentée figure 2.1.

Le système mobile (MS²⁵ aka Mobile Station) inclut l'équipement mobile (ME aka Mobile Equipment) et la carte SIM pour identifier l'utilisateur (SIM aka Subscriber Identity Module). Cette carte SIM contient l'identifiant de l'utilisateur IMSI¹⁹ (International Mobile Subscriber Identity) qui renseigne différents types d'informations tels que le code de la zone (area code), le code du pays (country code), l'identité de l'utilisateur, etc.

La BTS⁷ (Base Transceiver Station), en pratique un récepteur radio, assure des fonctions relatives à la communication avec le téléphone mobile. Chaque BTS couvre une zone d'accès radio appelée cellule. On appelle cluster un ensemble de cellule qui utilise la totalité des canaux attribués au système.

Le BSC⁶ (Base Station Controller) décharge le MSC des éléments de gestion radio tels que le RCS (Radio Call Setup), l'administration des canaux, et le passage d'une antenne à une autre (handover, roaming).

Le MSC²⁸ (Mobile Switching Center) agit tel un commutateur et permet le switching entre les canaux de 64 Kbps. Il est aussi responsable de la gestion et de l'enregistrement des appels.

Le VLR³⁴ (Visitor Location Register) est une base de données localisée dans le MSC qui gère la liste des utilisateurs du réseau mobile présents dans la zone de couverture de la MSC.

Le HLR¹⁴ (Home Location Register) est la principale base de données, gérant la liste de tous les clients de l'opérateur considéré. Le HLR assure aussi différentes fonctions relatives au maintien et à l'administration des services mobiles.

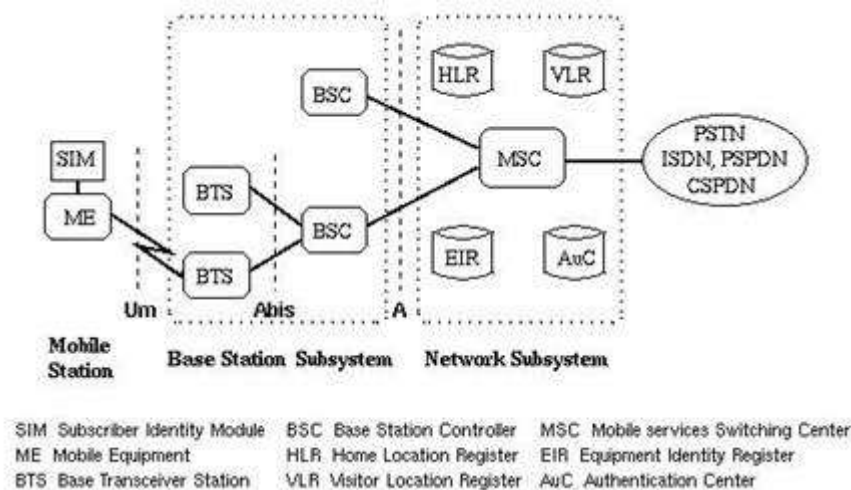


Fig. 2.1 : schéma de l'architecture du réseau GSM

2.1.2. Les bandes de fréquence GSM

Le standard GSM définit des bandes de fréquences pour les différentes allocations de spectre de fréquences dans le monde. L'interface sans fil fonctionne généralement sur quatre principales bandes de fréquences standardisées, mais dans le cas de certaines applications spécifiques ou dans des pays où ces bandes sont déjà utilisées, d'autres allocations de spectre peuvent être nécessaires.

Il existe en tout quatorze bandes de fréquences reconnues pour le réseau GSM, allant de 380 MHz à 1900 MHz. Ces bandes sont définies par le standard 3GG TS 45.005. Le choix des bandes à utiliser dépend du pays considéré et de la région ITU (International Telecommunications Union) à laquelle ce pays appartient. Par exemple, l'Europe, le Moyen-Orient, l'Afrique et l'Asie ont tendance à globalement utiliser les bandes de fréquences 900 MHz et 1800 MHz tandis que les Etats-Unis utilisent plutôt les bandes 850 MHz et 1900 MHz.

C'est la raison pour laquelle de nos jours, la plupart des téléphones portables supportent les opérations multibandes. La majorité des téléphones portables actuellement sur le marché fonctionne sur deux standards, on les appelle « dual-band phones ». Cette diversité permet notamment aux utilisateurs de conserver leur propre téléphone quand ils se déplacent dans d'autres pays. A titre d'exemple, les européens se rendant au Japon dans les années 90 devaient louer un téléphone compatible sur place à cause de la différence de standards utilisés.

2.1.3. Modulation GSM et couverture du signal

La technologie GSM diffère de la première génération de technologie mobile (1G), qui n'utilisait que la division de fréquence FDMA¹² (Frequency Division Multiple Access), en cela qu'elle combine les modulations par division de fréquence (FDMA) et de temps (TDMA³¹ aka Time Division Multiple Access) pour partager la bande passante entre les utilisateurs. Avec cette technique de modulation, la FDMA divise la bande passante de 25 MHz en 124 canaux

de 200 kHz chacun, et la TDMA divise à nouveau chacune de ces porteuses en 8 time-slots. Le partage de la bande passante est donc à la fois fréquentiel et temporel, ce qui permet de maximiser le nombre d'utilisateurs.

La couverture du signal GSM d'une BTS est généralement limitée à une zone de rayon 35 km, mais peut s'étendre jusqu'à 70 km dans certaines zones dotées d'équipements spéciaux.

2.2. Système de sécurité du réseau GSM

2.2.1. Vue d'ensemble du système de sécurité GSM

Le réseau GSM est longtemps resté à l'abri des intrusions, notamment à cause du coût élevé des équipements d'interception. Cependant, du fait de la démocratisation des outils technologiques logiciel et hardware, cet obstacle financier n'est plus, rendant exploitables les failles du système GSM. L'utilisation de transmission sans fil pour les communications rend le paysage GSM (PLMN aka GSM Public Land Mobile Networks) plus sensible à tout type d'attaque.

En effet, les pirates n'ont pas besoin de localiser les câbles du réseau pour interférer dans ses communications. Ainsi, étant donné sa popularité et son nombre d'utilisateurs, le réseau GSM demeure une cible intéressante pour de potentielles attaques. C'est pourquoi la sécurité est un point fondamental du système GSM. Ses caractéristiques sont implémentées de façon à protéger l'accès aux services mobiles pour les utilisateurs, à garantir l'intégrité du réseau et à assurer la confidentialité des données utilisateur.

Dans le but d'assurer cette confidentialité, différentes fonctions sont implémentées dans le système de sécurité GSM. Tout d'abord, il est indispensable de s'identifier avant de pouvoir accéder au réseau. Ensuite, les données sont systématiquement chiffrées avant d'être transmises (du moins sur une partie du réseau). Enfin, l'identité des utilisateurs est protégée et une carte SIM, dont la duplication est interdite, est nécessaire pour accéder au réseau. Ces différentes fonctions sont expliquées ci-dessous.

2.2.2. Authentification des utilisateurs du réseau

L'identifiant international IMSI (International Mobile Subscriber Identity) a été conçu dans le but de protéger le réseau des accès non autorisés en y empêchant les intrusions. Pour cela, l'algorithme A3² est implémenté pour authentifier l'utilisateur. L'authentification se fait en plusieurs étapes.

Tout d'abord, la station mobile (MS) envoie son identité via l'IMSI au réseau GSM. A sa réception, le réseau cherche la clé KI²¹ correspondant à cet identifiant. La KI est une clé de 128 bits spécifique à chaque utilisateur, et est utilisée en tant que clé secrète entre la MS et le HLR (Home Location Register) du réseau de l'utilisateur (home network). Dès lors, le réseau, à

travers son HLR, génère un nombre aléatoire sur 128 bits, le RAND²⁹ et l'envoie au MS par l'interface sans fil. Le MS calcule ensuite le SRES³⁰, un entier signé de 32 bits généré par l'algorithme A3 à partir du RAND et de la KI enregistrée dans la carte SIM. Cet entier est aussi simultanément calculé par le MSC²⁸ (Mobile services Switching Center) à partir du même A3 et des mêmes entrées. Lorsque le MS envoie le code SRES au réseau, celui-ci le compare avec le SRES calculé pour tester sa validité. Si les deux correspondent, l'utilisateur est authentifié.

L'authentification IMSI est basée sur le partage d'une même clef secrète (la KI) entre l'utilisateur (via sa carte SIM) et le réseau.

Le problème qui peut cependant être mis en avant est le risque d'écoute (interception passive) lors de l'authentification de l'utilisateur et la récupération de son identifiant IMSI. Pour répondre à ce problème, un système d'identité temporaire a été inventé. Quand un utilisateur achète une nouvelle carte SIM et allume son téléphone pour la première fois, son identifiant IMSI est transmis au centre d'authentification (AuC aka Authentication Center). Dès cette première authentification, un identifiant temporaire, le TMSI³² (Temporary Mobile Subscriber Identity) est assigné à l'utilisateur et sauvegardé sur le réseau avec son IMSI. L'IMSI sera alors très rarement utilisé, sauf extrême nécessité, et les authentifications se feront systématiquement à l'aide du TMSI, qui est mis à jour à chaque fois que les caractéristiques du MS, telles que sa position, sont elles-mêmes modifiées. Le TMSI est aussi sauvegardé sur la carte SIM de façon à le rendre disponible pour la prochaine authentification.

2.2.3. Chiffrement des données

Pour assurer la protection des données envoyées et reçues par les utilisateurs, ces données sont systématiquement chiffrées. Elles ne peuvent alors être déchiffrées que par le destinataire.

Ce chiffrement est assuré par l'algorithme A8⁴, implémenté dans la carte SIM. Après l'authentification de l'utilisateur, le RAND et la clé KI servent tous deux d'entrée pour l'algorithme de génération de clé de chiffrement, pour créer la clé KC²⁰. Cette clé est ensuite utilisée par l'algorithme A5³ pour chiffrer ou déchiffrer les données.

La requête de chiffrement des données est initialisée par le réseau GSM. Le MS exécute alors l'algorithme A5, à partir de la clé de chiffrement KC et le nombre de trames à envoyer. Chaque trame sera alors chiffrée avec une key-stream (clé de chiffrement) différente. Le chiffrement est effectué sur le téléphone en raison de la faible capacité de stockage de la carte SIM. La même KC est utilisée tant que le MS ne se réauthentifie pas, et si une nouvelle authentification est nécessaire, du fait du déplacement de l'utilisateur par exemple, une nouvelle KC sera générée. En pratique, s'il n'y a pas d'importante évolution dans l'état du MS, le même KC peut être utilisé pendant plusieurs jours.

Ces trois algorithmes A3, A8 et A5 forment l'algorithme COMP128⁸, dont le fonctionnement est confidentiel. Il est utilisé par la presque totalité des opérateurs GSM pour

l'authentification de l'utilisateur, la génération de la clef, le chiffrement et le déchiffrement des données.

3. Les faiblesses du système de sécurité GSM

3.1. État des lieux des faiblesses du réseau GSM

Il y a plusieurs failles dans le système de sécurité GSM qui peuvent potentiellement être utilisées par des pirates.

Tout d'abord, la sécurité des algorithmes utilisés est basée sur le concept de sécurité par l'obscurité, ce qui signifie que le code est gardé secret dans le but de le protéger des lectures indésirables.

Le système GSM ne procure qu'une sécurité partielle dans son utilisation du chiffrement. En effet, toutes les communications sans fil entre les utilisateurs (MS) et les BTS sont systématiquement chiffrées, mais les communications à travers le réseau fixe sont transmises en texte clair. Cela signifie que seule la partie sans fil est indéchiffrable et que l'interception des transmissions dans le réseau filaire (entre les BTS et le centre du réseau) permet la lecture en clair de toutes les données.

Une des plus importantes faiblesses du système de sécurité GSM est le fait que l'authentification est unidirectionnelle : l'utilisateur doit s'authentifier auprès de la BTS, comme expliqué précédemment, mais la BTS ne s'authentifie jamais auprès de l'utilisateur. Elle peut donc facilement être dupliquée et il sera alors difficile pour le MS de différencier la véritable BTS de la fausse. Un pirate peut alors simuler une BTS au moyen de dispositifs relativement accessibles, et récupérer les identifiants de l'utilisateur. La confidentialité et l'anonymat de l'utilisateur ne sont alors plus assurés.

Enfin, les algorithmes utilisés présentent certaines failles utilisables par les pirates. L'une d'entre elles a notamment été découverte dans l'algorithme COMP128 par la SDA (Smartcard Developer Association) et le groupe de recherche ISAAC. Cette faille leur a permis de retrouver la clef secrète KI à partir de la carte SIM. En effet, l'algorithme COMP128 a été conçu de façon pouvoir à révéler des informations concernant la KI lorsque le RAND est donné en argument à l'algorithme A8. Retrouver la clef KI à partir de la carte SIM est considéré comme l'attaque la plus dangereuse.

Dans cette étude nous ne nous intéresserons qu'à l'exploitation des vulnérabilités de la partie sans fil des réseaux GSM.

3.2. Les attaques possibles

On distingue plusieurs types d'attaques :

- **L'écoute (eavesdropping) :** L'attaquant est capable de capter la phase de signalisation et les données d'un utilisateur.
- **Usurpation de l'identité de l'utilisateur :** L'attaquant est capable d'envoyer des données de signalisation ou des données utilisateur au réseau en lui faisant croire qu'elles proviennent du mobile de l'utilisateur.
- **Usurpation de l'identité du réseau :** L'attaquant est capable d'envoyer des données de signalisation ou des données utilisateur au mobile de la cible en lui faisant croire qu'elles proviennent du réseau officiel.
- **Man-in-the-middle :** L'attaquant s'intercale entre le mobile de l'utilisateur et le réseau. Il est alors capable d'écouter, de modifier, de supprimer, de réordonner et de renvoyer les données de signalisation et utilisateur échangées entre les deux entités.

3.3. Exemple de réalisation d'une station d'interception

3.3.1. IMSI catcher

Obtenir l'IMSI d'un mobile permet d'usurper l'identité d'un utilisateur ou de le suivre à la trace. L'interception de cette information sensible se fait au moyen d'une fausse BTS sur laquelle le mobile se connectera, pensant qu'il s'agit d'une BTS légitime. C'est une attaque de type Man-in-the-Middle. Deux implémentations sont possibles : la fausse BTS usurpe l'identité d'une vraie BTS de la zone ou la fausse BTS brouille les signaux des vraies BTS.

Principe :

a. Usurpation d'identité de BTS

Lorsqu'un mobile cherche à se connecter à une BTS, il reçoit une liste recensant les BTS de la zone avec la force de leur signal via le canal BCCH⁵. Il se connecte à celle dont le signal est le plus fort. La fausse BTS doit analyser les fréquences utilisées et émettre sur celle dont la puissance reçue est la plus faible. Deux étapes sont alors nécessaires pour usurper l'identité de la BTS qui émet sur le canal choisi :

- Émettre avec un signal plus puissant que la vraie BTS pour masquer cette dernière au mobile. Pour cela, il suffit d'ajuster les interférences co-canal entre la vraie et la fausse BTS pour que le rapport canal sur interférence C/I soit supérieur à 9 dB.

- Présenter la fausse BTS comme la vraie. La fausse BTS doit donc utiliser le même Mobile Code Country (MCC²⁶) et le même Mobile Network Code (MNC²⁷) que la vraie BTS.

Il faut ensuite contraindre le mobile à effectuer un handover pour qu'il se connecte à la fausse BTS. Le paramètre de Path Loss C2 de la fausse BTS doit alors être supérieur à celui de la BTS courante du mobile. Une solution simple consiste à augmenter la puissance d'émission de la fausse BTS.

La fausse BTS doit ensuite contraindre le mobile à s'enregistrer à nouveau pour qu'il lui envoie son IMSI. Ceci implique l'utilisation par la BTS d'un Location Area Code (LAC²²) différent de celui diffusé par la BTS courante du mobile ciblé.

b. Brouillage

Pour cette méthode il faut utiliser un brouilleur qui bloque les voies descendantes des BTS de la zone cible afin que seule la fausse BTS soit disponible. Cette méthode est bien plus risquée que la précédente car l'utilisateur peut détecter la perte de connexion subite et donc penser à une attaque.

Réalisation (version a):

Nous allons maintenant présenter l'attaque expérimentale d'un mobile par IMSI catcher détaillée dans l'article « An approach to analyse security of GSM network » [5].

Matériel requis :

- Plate-forme radio USRP (Universal Software Radio Peripheral) capable d'émettre et de recevoir sur une large bande de fréquence (50MHz à 2.2GHz) connectée en Ethernet à un ordinateur. Cette plate-forme programmable permet de réaliser facilement tous types d'émetteurs récepteurs.
- Deux antennes VERT900 opérant dans la bande GSM.

Logiciels requis :

- GNU Radio, outil open source qui permet de créer un ou plusieurs systèmes radio sur un même USRP. L'analyseur de spectre intégré sera particulièrement utilisé pour détecter les fréquences des BTS voisines.
- OpenBTS qui contient une implémentation d'un système GSM (commutation, contrôle de connexion, gestion de la mobilité, SMS, etc.).

Étape 1: analyser l'environnement

En utilisant l'analyseur de spectre de GNU Radio, il faut déterminer les fréquences d'émission des BTS de la zone ciblée et les opérateurs présents. L'attaque détaillée ici a lieu en Bosnie Herzégovine et vise un mobile possédant une carte SIM de l'opérateur BH Télécom. L'analyse de la zone au moment de l'expérience donne les résultats suivants :

Operator	Allocated spectrum
BH Telecom	932.1 – 935.1 MHz 951.1 – 959.1 MHz 959.1 – 959.5 MHz 1805.1 – 1817.1 MHz
Telekom Srpske	925.3 – 928.7 MHz 935.1 – 943.1 MHz 1842.7 – 1854.7 MHz
HT Mostar	928.7 – 932.1 MHz

Fig 3.1 - Fréquences allouées pour la voie descendante

Étape 2 : trouver la BTS courante du mobile ciblé et les informations associées.

Considérant les capacités limitées en puissance d'une solution à base d'USRP, il faudra être proche du mobile ciblé. Par conséquent, trouver sa BTS courante revient à trouver celle dont le signal reçu est le plus fort. En utilisant l'analyseur de spectre de GNU Radio pour cette expérience, le plus fort signal reçu est capté sur le canal 111 (957.2MHz). La BTS qui émet à cette fréquence est donc celle à laquelle le mobile ciblé est rattaché. Après cette étape, il faut utiliser l'outil AirProbe (intégré à GNU Radio) pour obtenir plus d'informations sur cette BTS. On obtient alors les résultats de la figure 3.2.

```
Location Area Identification (LAI)
  Location Area Identification (LAI) - 218/90/7
    Mobile Country Code (MCC): Bosnia and Herzegovina (218)
    Mobile Network Code (MNC): GSM218 (90)
    Location Area Code (LAC): 0x0007 (7)
  Cell Selection Parameters
    011. .... = Cell Reselection Hysteresis: 3
    ...0 0101 = MS TXPower MAX cch: 5
    0... .... = ACS: False
    .1.. .... = NECT: 1
    ..00 0110 = RXLEV-ACCESS-MIN: -105 <= x < -104 dBm (6)
  Neighbour Cell Description - BCCH Frequency List
    ..0. .... = EXT-IND: the information element carries the complete BA (0)
    ...0 .... = BA-IND: 0
    00...000 = Format Identifier: bit map 0 (0x00)
    List of ARFCNs = 121 120 116 115 110 105 103 102 99 98 97 95 94 93 89 85 84 83 81
```

Fig.3.2 - Paramètres de la BTS du mobile cible

A la fin de cette étape, on connaît donc la liste des BTS adjacentes, le MCC (218), le MNC (90) et le LAC (7) de la BTS à laquelle le mobile à attaquer est connecté.

Étape 3 : Trouver une BTS dont l'identité va être usurpée.

Il faut donc mesurer le signal de réception des BTS listées dans la figure 3.2 et choisir l'un des plus faibles : la BTS qui émet le signal correspondant va être imitée. Une fois encore, l'analyseur de spectre va donc être nécessaire pour l'expérience et on obtient les résultats de la figure 3.3.

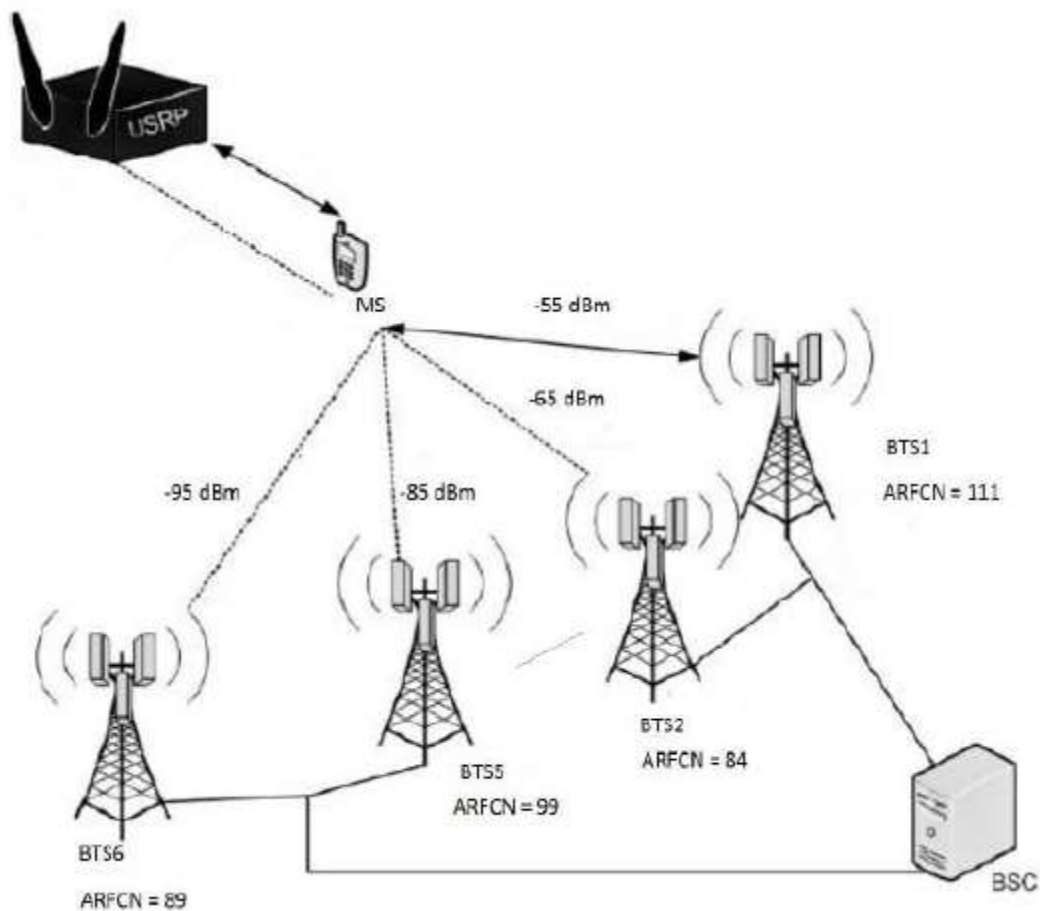


Fig.3.3 - BTS de la zone avec le niveau de réception de leur signal

Avec les résultats de la figure 3.3, on en déduit que l'USRP doit transmettre sur le canal 89. De plus, pour déclencher un handover du mobile ciblé entre sa vraie BTS courante à la fausse BTS, il faut que le signal reçu par le mobile soit supérieur à -55 dBm.

Étape 4 : Paramétrer la fausse BTS

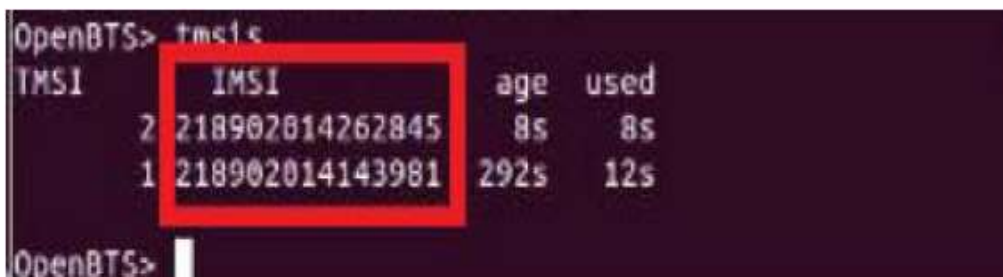
Enfin, il faut paramétrer OpenBTS pour qu'il imite la BTS déterminée à l'étape 3 en tenant compte de toutes les mesures réalisées. Ainsi il faut donc que :

- Le MCC soit égal à 218
- Le MNC soit égal à 90
- Le LAC soit différent de 7 (pour forcer le mobile à se réenregistrer)
- Nommer la BTS "BH Mobile"
- Mettre l'atténuation de puissance à 0 pour émettre à la puissance maximale
- Émettre sur le canal 89
- Que la fausse BTS accepte tous les utilisateurs sans authentification de leur IMSI

La fausse BTS fait ainsi partie du même réseau que celui de l'opérateur du mobile ciblé. Elle imite une vraie BTS, elle est par conséquent listée par la BTS à laquelle est connecté le mobile. La détection de l'attaque est donc difficile. La puissance du signal émis est supérieure à celle du signal de la BTS courante du mobile. Par conséquent une procédure de handover va être initiée par le mobile qui va alors se connecter à la fausse BTS à qui il va communiquer son IMSI car le LAC est différent.

Étape 5 : Tester le système

Pour finir, il suffit de démarrer le système et de patienter quelques secondes, le temps que le mobile ciblé exécute la procédure de handover. L'IMSI du ou des mobiles cible(s) peut ainsi être lu dans la console d'OpenBTS comme le montre la figure 3.4.



```
OpenBTS> tmsic
TMSI      IMSI      age  used
2 218902014262845   8s   8s
1 218902014143981 292s  12s
OpenBTS>
```

Fig.3.4 - Liste des IMSI interceptés

Le système d'IMSI catcher peut être amélioré pour intercepter les SMS et les appels des mobiles attaqués. Ainsi, si l'on se reporte au processus d'authentification GSM :

- La fausse BTS se connecte au vrai réseau de l'opérateur du mobile ciblé en utilisant l'IMSI intercepté
- Le réseau envoie un RAND à la fausse BTS qui le fait ensuite suivre au mobile cible toujours connecté à cette dernière.
- Le mobile calcule le SRES et l'envoie à la fausse BTS qui fait suivre au réseau. La fausse BTS est donc authentifiée auprès du réseau comme étant le mobile cible. Par conséquent tous les appels et SMS entrant à destination du mobile attaqué passent par

la fausse BTS (qui peut les relayer ou pas). Les messages et appels sortant sont tous interceptés par la fausse BTS.

Cependant les messages et appels interceptés via cette méthode ne sont pas exploitables en l'état. En effet la BTS légitime activera le chiffrement des communications dès que l'authentification du mobile sera terminée. Si notre BTS d'attaque ne relaie pas cette demande au mobile, l'attaque sera détectée et la communication coupée.

3.3.2. Contourner le chiffrement des communications

Comme expliqué en 2.2.3, les communications GSM sont en théorie protégées par chiffrement au moyen de l'algorithme A5. Au fil des évolutions technologiques, différentes versions de cet algorithme ont été développées : A5/2, A5/1 et A5/3, listées par force de chiffrement croissante.

Ces techniques de chiffrement ne sont cependant pas infaillibles et peuvent être supplantées de deux façons différentes.

a. Briser l'algorithme de chiffrement

Diverses études ont montré qu'il était possible de retrouver la clef de chiffrement Kc utilisée par un mobile à partir de l'enregistrement de communications chiffrées. Par exemple en 2003 trois chercheurs Israéliens ont réussi à trouver la clef Kc générée par l'algorithme A5/2 en moins d'une seconde grâce à un ordinateur personnel et une douzaine de millisecondes d'enregistrement de données chiffrées (voir bibliographie [6]). Les failles de cette version sont tellement importantes que la 3GPP, coopération des organismes de standardisation des télécommunications, a interdit en 2007 l'implémentation de A5/2 dans les nouveaux portables.

L'algorithme A5/1, bien que plus robuste, est également vulnérable. En effet, son fonctionnement a été découvert en 1999 par rétro-ingénierie. Depuis, plusieurs attaques ont été publiées. Le projet Kraken, publié en 2010, est une des implémentations les plus récentes. Cet outil se base sur un ensemble de tables précalculées (représentant près de 1,7To de données). Il cherche ensuite des correspondances entre les tables et les données chiffrées interceptées. Si la captation est effectuée dans de bonnes conditions, alors il existe une chance de trouver la clef de chiffrement utilisée par le mobile.

Ces techniques s'appuyant sur des notions cryptographiques complexes, nous ne les détaillerons pas dans ce rapport.

b. Désactiver le chiffrement

Dans un souci de compatibilité, les mobiles implémentent toutes les versions de l'algorithme A5. Le choix de l'algorithme utilisé est imposé par la BTS après que le mobile se soit authentifié auprès du réseau. Or il existe une autre version de l'algorithme A5, l'A5/0, qui ne chiffre pas les données. Par conséquent si nous voulons pouvoir déchiffrer les informations captées, il faut que notre BTS d'attaque impose cet algorithme aux mobiles cibles.

Il existe alors un risque que l'utilisateur se rende compte de l'attaque. En effet, depuis 1997, le standard GSM indique qu'un utilisateur doit être notifié lorsque ses communications sont transmises en clair. En pratique le risque de détection est très faible. En effet, dans une étude publiée en 2012 (voir bibliographie [7]), trois chercheurs mettent en lumière des faits surprenants :

- Malgré les recommandations du standard GSM, de nombreux constructeurs/opérateurs n'implémentent pas ces mécanismes d'avertissement dans leurs produits/services.
- Les solutions déployées ne sont pas uniformes, ainsi certains constructeurs affichent un message d'avertissement, d'autres utilisent une icône (différente d'un constructeur à l'autre), etc.
- La grande majorité des utilisateurs ne connaissent pas cette fonctionnalité qui, même lorsqu'elle est implémentée, est rarement documentée par les notices des appareils.

3.3.3 Intercepter et router appels et messages

En utilisant la fausse BTS et la méthode de contournement du chiffrement expliquée précédemment, nous allons voir qu'il est possible d'intercepter, en clair, tous les messages et appels passés par un mobile tout en les relayant au réseau légitime. Pour cela l'attaquant doit posséder un mobile et un abonnement légitime à un opérateur mobile. Ce mobile doit ensuite être relié à la fausse BTS. La première étape est de capturer le mobile cible en le forçant à s'authentifier auprès de notre fausse BTS en suivant la méthode détaillée en 3.3.1. Ensuite la fausse BTS doit imiter la procédure d'authentification du mobile cible. Pour cela, elle doit envoyer un RAND au mobile et accepter le SRES reçu quel qu'il soit (la fausse BTS ne connaissant pas la clef Ki elle est incapable de vérifier le SRES renvoyé par le mobile). La fausse BTS ne connaissant pas la clef Kc pour le chiffrement, elle désactive ce dernier en demandant au mobile d'utiliser l'algorithme A5/0. Pour la connexion avec le réseau légitime, on utilise le mobile de l'attaquant qui s'authentifiera directement auprès du réseau légitime et qui supportera le chiffrement imposé (l'attaquant étant propriétaire de ce mobile et de l'abonnement correspondant, il dispose d'une carte SIM légitime et donc de toutes les clefs nécessaires). L'infrastructure d'interception est désormais en place.

Lorsque le mobile cible passe un appel, la fausse BTS est capable de lire le numéro destinataire (transmis en clair car le chiffrement est inactif) et le compose automatiquement sur le mobile de l'attaquant qui va alors passer l'appel auprès du réseau légitime. La fausse BTS

État de l'art associé au projet tuteuré

relaie ensuite la voie montante du mobile cible sur le mobile de l'attaquant et la voie descendante du mobile de l'attaquant vers le mobile cible. La communication est ainsi établie et l'attaquant capte en clair la communication. Le même principe peut s'appliquer pour l'envoi de messages.

Là encore l'utilisateur peut détecter l'attaque. En effet, les appels effectifs ne sont pas passés par sa ligne. Ainsi les communications ne lui sont pas facturées et n'apparaissent pas sur sa facture, c'est l'attaquant qui paie. Cependant rares sont les clients à lire le détail de leur communication, surtout à l'heure des forfaits voix illimités. Il y a également un risque, assez faible (voir 3.3.2 - b) que l'utilisateur soit notifié de la désactivation du chiffrement. Enfin le destinataire de l'appel et/ou des messages voit un numéro inconnu s'afficher (celui du mobile de l'attaquant car c'est ce dernier qui passe l'appel au réseau légitime), il peut donc en avvertir l'utilisateur ciblé. Pour la même raison, durant toute la durée de l'attaque, le mobile cible ne peut pas recevoir d'appel car il n'est pas directement connecté au réseau, seul le mobile de l'attaquant l'est.

3.3.4. Attaques diverses

Pour intercepter des informations émises par un mobile capturé par une fausse BTS, il n'est pas nécessaire de maintenir la communication entre la BTS d'attaque et le réseau légitime. Ainsi diverses attaques sont possibles une fois le chiffrement désactivé :

- **Lister les numéros appelés par la cible** : A chaque fois que le mobile attaqué essaie de passer un appel, la BTS capture le numéro de téléphone appelé (l'appel ne sera pas routé sur le réseau). Ainsi l'attaquant peut obtenir une liste de correspondant de sa cible.
- **Répondre à un appel** : L'opérateur de la fausse BTS peut répondre à un appel passé par le mobile cible et ainsi se faire facilement passer pour quelqu'un d'autre (institution financière, service d'urgence, etc.).
- **Usurper l'identité d'un appelant** : L'opérateur de la fausse BTS peut passer des appels à destination d'un mobile cible en utilisant le numéro source de son choix.

3.4. Le cas des SMS

Les SMS (Short Message Service) permettent aux utilisateurs de communiquer par l'envoi de messages textes. Aujourd'hui de plus en plus de services (commerces électroniques, banques, réseaux sociaux, etc.) utilisent les SMS comme méthode de sécurité pour authentifier les utilisateurs, généralement par l'envoi d'un code à usage unique après une authentification classique sur un portail web.

L'intérêt pour un attaquant d'intercepter ces messages est donc énorme.

3.4.1. Principe de fonctionnement

Les SMS constituent un des services les plus utilisés de la téléphonie mobile. Le premier message, “Merry Christmas”, fut envoyé en Angleterre en 1992. Malgré le fait que la téléphonie mobile fut conçue et commercialisée pour la transmission d’une communication vocale, l’utilisation du SMS s’est intensifiée rapidement au fil des années. Rien qu’aux États-Unis, plus de mille milliards de messages furent envoyés en 2008, rapportant ainsi plusieurs millions de dollars aux opérateurs téléphoniques.

L’envoi d’un SMS est basé sur un service de transmission en différé par lequel les messages reçus sont préalablement stockés sur des serveurs internes de messagerie avant d’être réexpédiés vers leur destinataire final. Le stockage est nécessaire afin que le message puisse être envoyé même si le téléphone du destinataire est éteint ou hors-ligne. Les messages sont transférés vers les nœuds de l’opérateur selon différents formats propres aux constructeurs tels que SMPP, EMI/CUP, TAP...

Le mode de fonctionnement et les différentes spécifications relatives à l’envoi des messages sont décrits dans le standard GSM. Le Short Message Center (SMC) se charge de recevoir, stocker et envoyer les messages entre deux Short Message Entities (SME). Ces dernières peuvent être des téléphones portables, des ordinateurs ou bien d’autres réseaux de services. Ensuite, la passerelle SMS (GMSC - SMS gateway MSC) joue le rôle d’interface entre le reste du réseau et les autres opérateurs. En recevant un SMS depuis le SMC, le GMSC utilise le réseau SS7 pour trouver la position de la station mobile destinataire à partir du HLR et ainsi retransmettre le message.

3.4.2. Les vulnérabilités des SMS

- **Un chiffrement perfectible**

Comme mentionné dans les chapitres précédents, le chiffrement (s’il a lieu) des communications vocales, tout comme celui des messages, s’arrête habituellement lorsque la donnée arrive sur le réseau interne de l’opérateur. A partir de là, les messages sont majoritairement retransmis en clair au sein du réseau. Ainsi, les salariés de l’opérateur qui ont accès aux systèmes de messagerie peuvent lire à leur guise le contenu des messages et accéder aux informations personnelles de l’expéditeur et du destinataire.

- **Une interception aisée**

La fausse station de base décrite au chapitre 3.3.1 a la capacité d’intercepter n’importe quel message que l’utilisateur essaie d’envoyer, ainsi que le numéro de son destinataire.

Ainsi selon le type de BTS d’attaque utilisé il est possible de bloquer, relayer ou modifier n’importe quel message émis par un mobile ciblé.

3.4.3. Le SMS, un outil de surveillance

Dans tous les cas, les SMS, en dehors du contenu lui-même, peuvent dévoiler des informations relatives au comportement de l'utilisateur. En effet, rien qu'avec les accusés de réception, un simple utilisateur (n'ayant aucun accès au réseau interne de l'opérateur) peut être informé sur l'état, allumé ou éteint, de l'autre téléphone et sera averti au moment exact où l'utilisateur le rallumera. Ceci est rendu possible par le fait que les accusés de réception sont délivrés à l'expéditeur dès que le mobile se rallume et qu'ils restent en attente tant que le téléphone du destinataire est éteint.

Cependant les messages, même vides, envoyés au mobile ciblé seront affichés, l'utilisateur peut donc se rendre compte de l'attaque. Des techniques intelligentes rendent cependant possible l'implémentation de cette attaque sans éveiller les soupçons de la victime. Il est en effet possible d'envoyer des messages "invisibles" qui seront délivrés sur l'appareil de la victime sans faire apparaître de notifications sur l'écran du téléphone. De tels messages peuvent être envoyés par un simple utilisateur n'ayant aucun accès au réseau interne de l'opérateur. L'enregistrement des temps d'arrivées des accusés de réception permet à l'attaquant dans le même temps de surveiller le comportement de l'utilisateur du téléphone portable. Il peut alors, sur le long terme, en déduire les habitudes de vie de l'utilisateur et ainsi repérer les situations exceptionnelles. Par exemple, il pourrait savoir si une matinée, la victime a dormi plus que d'habitude (elle aurait allumé son téléphone plus tard que d'habitude) ou si elle est toujours endormie (puisque son téléphone est normalement toujours allumé à cette heure-là). Dans la figure 3.5, des SMS discrets sont envoyés chaque demi-heure. Les accusés de réception sont indiqués par des points bleus. La ligne rouge montre le temps qui s'est écoulé depuis le dernier accusé de réception et donne une estimation de la période pendant laquelle le téléphone de la victime est resté éteint. Dans cet exemple, le téléphone s'est éteint la première nuit entre 23h33 et 00h03 et a été rallumé à 8h07 le matin d'après. On observe des périodes d'extinction similaires sur les autres jours de la semaine, excepté le week-end.



Fig. 3.5 - Habitudes d'un utilisateur déduites des périodes d'extinction de son téléphone et révélées par l'utilisation de SMS silencieux

Dans une configuration différente, comme le montre la figure 3.6, des SMS du même type sont envoyés de manière continue. Dès que l'utilisateur entre dans une zone non couverte par le réseau (un ascenseur ou un tunnel par exemple), on peut observer des retards au niveau des accusés de réception. Si la victime suit la même route pour se rendre au travail tous les jours, l'attaquant est en mesure de savoir si un jour la victime s'est écartée de son chemin habituel.

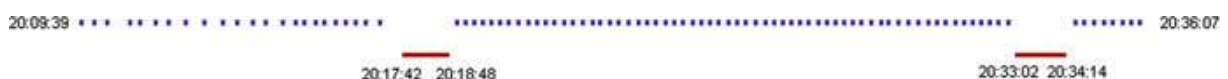


Fig. 3.6 - Les écarts par rapport au chemin emprunté habituellement par un utilisateur peuvent être déduits des périodes d'extinction de son téléphone et révélés par l'utilisation de SMS silencieux

Enfin, cette technique peut aussi être utilisée par les forces de police avant un assaut dans la maison d'un suspect ou pour forcer le mobile de celui-ci à émettre et ainsi faciliter son identification parmi les autres téléphones dans le cas où un IMSI catcher, tel qu'il est décrit dans le chapitre 3.3.1, serait utilisé.

4. Conclusion

En conclusion, nous pouvons donc dire que le réseau GSM, bien que disposant de mécanismes de sécurité, est aujourd'hui vulnérable à de nombreuses attaques. Cette vulnérabilité est notamment due à l'absence d'authentification du réseau par le mobile et aux mécanismes de chiffrement qui ne sont plus suffisamment robustes de nos jours. Des attaques actives, hors du champ d'étude de ce rapport, sont également possibles si l'attaquant peut accéder physiquement au mobile (clonage de carte SIM, installation de logiciels malveillants, etc.) et peuvent compromettre davantage la sécurité des échanges.

Ces problèmes de sécurité ont en partie été comblés par les standards plus récents comme l'UMTS qui offre une authentification bidirectionnelle mobile-réseau. Cependant, d'autres failles existent dans ces technologies. De plus, les réseaux et mobiles actuels étant multibandes, il est toujours possible de forcer un mobile à utiliser le réseau GSM (car les autres technologies ne sont pas disponibles dans certaines zones géographiques ou si un attaquant brouille les fréquences correspondantes).

Malgré les points soulevés par ce rapport, il est toutefois nécessaire de remettre en perspective nos conclusions. En effet, l'interception d'information n'est pas à la portée de n'importe quel individu et nécessite un matériel spécifique. La réglementation est de plus en faveur des utilisateurs. En effet le cadre légal permettant aux autorités l'utilisation de telles techniques est extrêmement strict et nécessite l'accord des tribunaux.

5. Lexique

- ¹ 3GPP (3rd Generation Partnership Project) : regroupement d'organismes de standardisation qui établit les spécifications techniques des principales technologies de télécommunications (GSM, GPRS, EDGE, UMTS, LTE).
- ² A3 : algorithme utilisé pour authentifier le MS auprès du réseau.
- ³ A5 : algorithme utilisé pour chiffrer et déchiffrer les données.
- ⁴ A8 : algorithme utilisé pour générer la clé KC, elle-même utilisée par l'algorithme A5.
- ⁵ BCCH (Broadcast Control Channel) : canal sur lequel sont diffusées régulièrement des informations de la cellule (identité du réseau, caractéristiques d'accès...) vers le MS.
- ⁶ BSC (Base Station Controller) : station commandant un certain nombre de BTS (jusqu'à plusieurs centaines), gérant l'allocation des canaux, interprétant les mesures de puissance et déclenchant le handover.
- ⁷ BTS (Base Transceiver Station) : regroupe tout le matériel permettant l'émission et la réception. Connu aussi sous le nom d'antenne relais, une BTS prend en charge la couche physique (multiplexage, chiffrement...) et la transmission radio (modulation, démodulation, codage ...). Elle fait le lien entre le mobile et le réseau de l'opérateur.
- ⁸ COMP128 : ensemble confidentiel d'algorithmes (A3, A5 et A8) définis dans le standard GSM et utilisés pour l'authentification et le chiffrement des données.
- ⁹ DC-HSPA+ (Dual Carrier/Channel High-Speed Packet Access) : mode particulier d'un mobile qui lui permet d'utiliser simultanément deux porteuses en mode HSPA+. L'agrégation de deux canaux permet d'augmenter les débits par rapport au HSPA+ classique.
- ¹⁰ EDGE (Enhanced Data Rates for GSM Evolution) : évolution du GPRS, cette technologie offre de meilleurs débits que le GPRS (jusqu'à 332 kbits/s), notamment grâce à une modulation plus efficace.
- ¹¹ ETSI (European Telecommunications Standards Institute) : organisme de standardisation européen des télécommunications.
- ¹² FDMA (Frequency Division Multiple Access) : technique de partage des ressources spectrales. Le spectre est découpé en bandes de fréquences permettant ainsi à plusieurs utilisateurs (un par bande) de communiquer simultanément.
- ¹³ GPRS (General Packet Radio Services) : connu aussi sous l'appellation 2.5G, c'est le premier protocole qui permet aux mobiles compatibles de se connecter à internet. C'est la version paquet du GSM avec un débit supérieur.
- ¹⁴ HLR (Home Location Register) : base de données contenant les informations (IMSI, localisation approximative, ...) de tous les abonnés d'un opérateur.
- ¹⁵ HSDPA (High Speed Downlink Packet Access) : version améliorée de l'UMTS offrant des débits plus importants sur la voie descendante (jusqu'à 14.4 Mbps).
- ¹⁶ HSPA (High Speed Packet Access) : connu aussi sous l'appellation 3G+, combinaison des protocoles HSDPA et HSUPA.

- ¹⁷ HSPA+ (High Speed Packet Access+) : connu aussi sous l'appellation H+, version améliorée de HSPA permettant des débits plus élevés (42 Mbps en downlink, 11 Mbps en uplink).
- ¹⁸ HSUPA (High Speed Uplink Packet Access) : version améliorée de l'UMTS offrant des débits plus importants sur la voie montante (jusqu'à 5.7 Mbps).
- ¹⁹ IMSI (International Mobile Subscriber Identity) : numéro unique permettant à un réseau mobile GSM, UMTS ou LTE d'identifier un utilisateur. Il est stocké dans la carte SIM.
- ²⁰ KC : clé de 64 bits générée par le MS à partir du RAND et de la KI, et utilisée par l'algorithme A5 pour chiffrer et déchiffrer les données.
- ²¹ KI : clé de 128 bits spécifique à chaque utilisateur utilisée en tant que clé secrète entre la MS et le HLR du réseau de l'utilisateur.
- ²² LAC (Location Area Code) : code de la zone dans laquelle se situe le MS, faisant partie, avec d'autres identifiants, du LAI (Location Area Identification).
- ²³ LTE (Long Term Evolution) : évolution de l'UMTS, connue sous le nom commercial de 4G bien que ne respectant pas entièrement les spécifications de la norme définie par l'ITU (International Telecommunication Union)
- ²⁴ LTE Advanced : future évolution de la 4G actuelle, cette norme permettra d'atteindre des débits très élevés, jusqu'à 1 Gbps.
- ²⁵ MS (Mobile station) : terme qui désigne un terminal mobile authentifié et autorisé à accéder au réseau GSM, comportant le terminal physique, appelé Mobile Equipment (ME), et une carte SIM représentant l'abonnement souscrit et qui contient les paramètres clés le concernant.
- ²⁶ MCC (Mobile Country Code) : code pays sur trois chiffres standardisé par l'ITU (208 pour la France par exemple). Il est diffusé par la voie balise des BTS pour indiquer le pays d'appartenance.
- ²⁷ MNC (Mobile Network Code) : code utilisé en combinaison avec le MCC. Également diffusé par les BTS, il permet de différencier les opérateurs (chacun a un code unique, 01 pour Orange par exemple).
- ²⁸ MSC (Mobile services Switching Center) : commutateur qui supervise plusieurs BSC, il donne accès aux principales bases de données d'un opérateur (HLR, VLR, etc.). Certains MSC (les GMSC) permettent de communiquer avec les autres réseaux d'opérateurs.
- ²⁹ RAND : nombre de 128 bits généré aléatoirement par le HLR et utilisé dans le cadre de l'authentification de l'utilisateur du réseau.
- ³⁰ SRES : entier signé de 32 bits calculé via l'algorithme A3, à partir du RAND et de la clé KI, par le MS (Mobile Station) et par le MSC en parallèle, afin de comparer les deux résultats et d'authentifier l'utilisateur du réseau.
- ³¹ TDMA (Time Division Multiple Access) : technique de partage de ressource permettant de répartir temporellement l'accès au médium de communication entre plusieurs utilisateurs.
- ³² TMSI (Temporary Mobile Subscriber Identity) : identifiant temporaire assigné à l'utilisateur, mis à jour à chaque modification des caractéristiques du MS et sauvegardé

sur la carte SIM, permettant d'authentifier l'utilisateur tout en évitant d'exposer son IMSI.

- ³³ UMTS (Universal Mobile Telecommunications System : connu aussi sous l'appellation 3G, c'est un standard de télécommunication offrant de meilleurs débits que le GSM, jusqu'à 2 Mbps, et supportant plus d'utilisateurs grâce notamment à l'utilisation d'une technique de multiplexage supplémentaire (le W-CDMA).
- ³⁴ VLR (Visitor Location Register) : base de données contenant des informations sur tous les utilisateurs (Mobile Stations) d'une zone de localisation. Un VLR est associé à un MSC.
- ³⁵ W-CDMA (Wideband Code Division Multiple Access) : variante du CDMA ; technique de codage utilisée dans la partie radio (UTRAN) des réseaux de téléphonie mobile UMTS (3G) qui, combinée au FDMA et TDMA, permet d'accroître encore le nombre d'utilisateurs.

6. Références bibliographiques

- [1] Francisco J. González-Castaño, Javier Vales-Alonso, José M. Pousada-Carballo, Fernando Isasi de Vicente, et Manuel J. Fernández-Iglesias, « Real-Time Interception Systems for the GSM Protocol », *IEEE Transactions on vehicular technology*, vol. 51, no. 5, septembre 2002. [Online]. Disponible sur: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1105930&newsearch=true&queryText=Real-Time%20Interception%20Systems%20for%20the%20GSM%20Protocol> [Consulté le: 10-dec-2015]
- [2] Kan Zhou, Aiqun Hu, Yubo Song, « A No-jamming Selective Interception System of the GSM Terminals », 2010 *IEEE*, 2010. [Online]. Disponible sur: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5601273&newsearch=true&queryText=%20A%20No-jamming%20Selective%20Interception%20System%20of%20the%20GSM%20Terminals%20> [Consulté le: 10-dec-2015]
- [3] Constantin Daniel Oancea, « GSM Infrastructure Used for Data Transmission », *The 7th International Symposium on Advanced Topics in Electrical Engineering*, mai 2011. [Online]. Disponible sur: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5952239&newsearch=true&queryText=GSM%20Infrastructure%20Used%20for%20Data%20Transmission> [Consulté le: 10-dec-2015]
- [4] Luka Perkovic, Ana Klisura et Nikola Pavkovic, « Recent advances in GSM insecurities », 2011 *Proceedings of the 34th International Convention MIPRO*, mai 2011. [Online]. Disponible sur: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5967298&newsearch=true&queryText=Recent%20advances%20in%20GSM%20insecurities%20> [Consulté le: 10-dec-2015]
- [5] M. Hadzialic, M. Skrbic, K. Huseinovic, I. Kocan, J. Musovic, A. Hebibovic, et L. Kasumagic, « An approach to analyze security of GSM network », in *Telecommunications Forum Telfor (TEFOR)*, 2014 22nd, Belgrade, Serbie, 2014, p. 99–102 [Online]. Disponible sur: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7034366. [Consulté le: 08-nov-2015]
- [6] E. Barkan, E. Biham, et N. Keller, « Instant ciphertext-only cryptanalysis of GSM encrypted communication », in *Advances in Cryptology-CRYPTO 2003*, vol. 2729, Springer, 2003, p. 600–616 [Online]. Disponible sur: http://link.springer.com/chapter/10.1007/978-3-540-45146-4_35. [Consulté le: 21-janv-2016]
- [7] I. Androulidakis, D. Pylarinos, et G. Kandus, « Ciphering Indicator approaches and user awareness », *Maejo International Journal of Science and Technology*, vol. 6, p. 514- 527, 2012. [Online]. Disponible sur: <http://www.mijst.mju.ac.th/vol6/514-527.pdf>. [Consulté le: 21-janv-2016]
- [8] I. Androulidakis, *Mobile phone security and forensics*. New York: Springer, 2012.
- [9] C. J. Mitchell, « The security of the GSM air interface protocol », Royal Holloway, University of London, Rapport technique RHUL-MA-2001-3, août 2001 [Online]. Disponible sur: https://www.researchgate.net/publication/48602714_The_security_of_the_GSM_air_interface_protocol. [Consulté le: 24-janv-2016]
- [10] D. Dragomirescu, « Réseaux mobiles terrestres ». Publication INSA, 2014-2015

7. Table des illustrations

Fig. 1.1 - *Logo GSM*. [Online]. Disponible sur:

<https://upload.wikimedia.org/wikipedia/commons/thumb/5/5d/GSMLogo.svg/250px-GSMLogo.svg.png>. [Consulté le: 08-nov-2015]

Fig. 2.1 *Schéma de l'architecture du réseau GSM*. [Online]. Disponible sur :

http://www.polarsat.com/en/index.php?option=com_content&view=category&layout=blog&id=7&Itemid=17&lang=fr [Consulté le : 25-jan-2016]

Fig. 3.1 - *Allocated spectrum in Bosnia and Herzegovina*. Novembre 2014 [Online].

Disponible sur : http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7034366 [Consulté le : 08-nov-2015]

Fig. 3.2 - *BTS parameters*. Novembre 2014 [Online]. Disponible sur :

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7034366 [Consulté le : 08-nov-2015]

Fig. 3.3 - *BTSS with received signals levels*. Novembre 2014 [Online]. Disponible sur :

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7034366 [Consulté le : 08-nov-2015]

Fig. 3.4 - *Caught IMSI numbers*. Novembre 2014 [Online]. Disponible sur :

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7034366 [Consulté le : 08-nov-2015]

Fig. 3.5. - I. Androulidakis. *User's behavior deduced from switch on/off time as portrayed by silent SMSs*. 2012.

Fig. 3.6. - I. Androulidakis. *Deviations from user's everyday route can be deduced from switch on/off time as portrayed by silent SMSs*. 2012.