Unité Communications mobiles

Institut Eurécom
2229 route des Crêtes
BP 193
06904 Sophia Antipolis Cedex
France

WINES : Wireless Network Simulation
Plateforme de simulation du réseau GSM

Véronique Devernay, Christian Bonnet

Juin 1994

Technical Report : RR94-010 bis

E-mail : bonnet@eurecom.fr, devernay@eurecom.fr

Introduction

La plateforme WINES modélise un réseau GSM complet, avec sa partie fixe (stations de base, commutateurs, bases de données du système) et ses éléments mobiles.

Seule la couche 3 –la couche protocole– est simulée : tous les échanges de messages sont en conformité avec la norme GSM. Les fonctionalités de base du GSM sont disponibles, en ce qui concerne la voix : appels mobile demandé et mobile demandeur, handover, mais sans le cryptage et l'authentification. La mobilité est également gérée (mises jour de localisation).

L'implémentation de ces fonctionalités correspond toujours au cas nominal, c'est à dire au cas o aucun message n'est perdu : aucune temporisation n'est prévue pour vérifier que tel message attendu arrive effectivement.

Au sein de l'Institut Eurécom, la plateforme est utilisée dans un projet de recherche sur la détection d'intrusion dans les réseaux mobiles.

1 Description des objets modélisés

1.1 Description générale

Chaque objet du réseau se compose de deux couples d'émetteurs-récepteurs, l'un dirigé vers le niveau inférieur dans la hiérarchie du réseau, l'autre vers le niveau supérieur, et d'un ou plusieurs processus chargé(s) de traiter les messages arrivant (voir figure 1)

Cette description ne vaut pas pour les"extrémité" du réseaux : la station mobile, qui n'est pourvue que d'une couple d'émetteur-recepteur radio, et les MSC, qui sont reliées à plus de deux entités du réseau.

Les messages échangés portent les noms exacts des messages spécifiés dans la norme, les champs qui les composent forment un sous-ensemble des champs normalisés : par exemple le message LOCATION UPDATING REQUEST du protocole RIL3-MM, est composé des champs obligatoires suivants (GSM 04.08 - v. 3.13.0 - page 230) :

- Protocol Discriminator
- Transaction Identifier
- Message Type

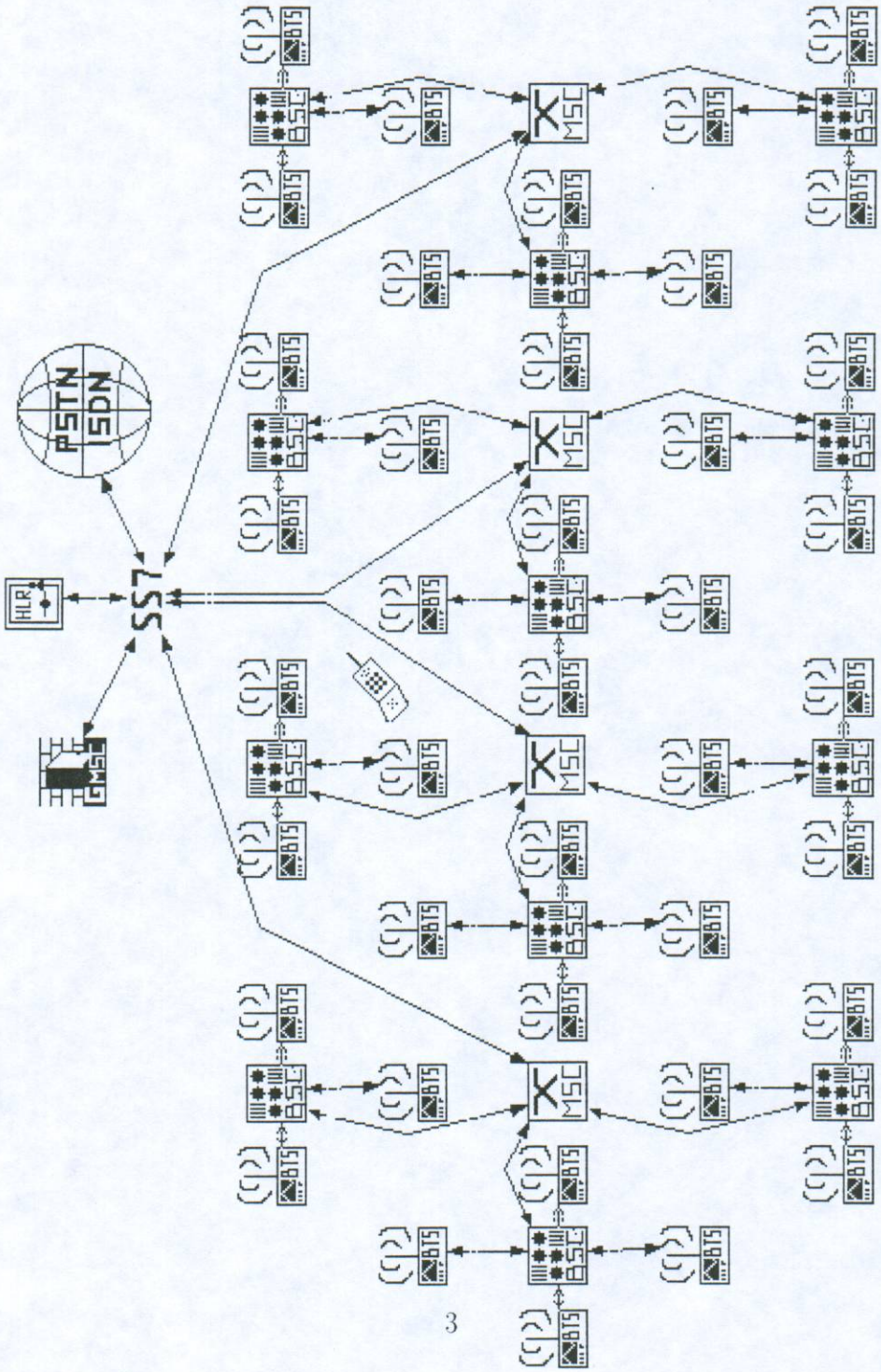

FIG. 1 - *Structure générale d'un élément du réseau*

- Location Update Type
- Cyphering key sequence number
- Location area identification
- Mobile station classmark 1
- Mobile identity

Dans la plateforme le format de ce message reprend exactement 8 de ces 9 champs (le champ 5 est omis puisqu'on ne fait pas de cryptage).

1.2 Parties fixes du réseau

La partie fixe d'un PLMN (Public Land Mobile Network) comprend les éléments suivants :

- des BTS (Base Transceiver Station), ou stations de base,
- des BSC (Base Station Control), ou stations de contrôle,
- des MSC-VLR (Mobile Switching Center - Visitor Location Register), c'est-à-dire des commutateurs associés à des bases de données locales,
- un HLR (Home Location Register), qui est la base de données principale du réseau,
- un ou plusieurs GMSC (Gateway MSC), qui permettent l'interconnexion avec d'autres réseaux et le routage des appels.

La plateforme de simulation comprend en plus un objet chargé de modéliser un réseau fixe de type PSTN (Public Switched Telephone Network) ou ISDN (Integrated Service Digital Network) dans ses relations avec le réseau mobile.

Les paragraphes suivants rappellent les rôles de ces différents éléments au niveau protocole et précisent leurs fonctionalités dans la plateforme de simulation.

1.2.1 BTS

La BTS est l'émetteur radio qui permet d'entrer en contact avec les stations mobiles : située au centre d'une cellule, elle est entiérement commandée à distance par la BSC (activation des canaux) et ne posséde un peu d'autonomie qu'en ce qui concerne les mesures.

En effet la station mobile comme la BTS mesurent en permanence la qualité de la transmission : ces mesures peuvent être partiellement traitées dans la BTS avant d'être remontées vers la BSC.

Dans la plateforme les mesures sont envoyées la BSC sans ê tre traitées.

1.2.2 BSC

La BSC gére les ressources radio, relaie les messages concernant le contrôle d'appel (couche CC) et la mobilité (couche MM) entre la station mobile et la MSC, exploite les mesures et déclenche les handovers en conséquence.

Dans la plateforme la zone couverte par chaque BSC définit une aire de localisation, c'est dire qu'à chaque fois qu'une station mobile quitte une telle aire, elle procéde une mise à jour de localisation (la définition de l'aire de localisation est laissée par la norme GSM au libre choix de l'opérateur).

1.2.3 MSC-VLR

La MSC est le commutateur du réseau, permettant de relier le monde extérieur aux stations mobiles du PLMN. Elle gére tous les aspects du contrôle d'appel et de la mobilité pour les mobiles qui se trouvent dans sa zone. Elle est en contact avec le HLR pour les mises à jour de localisation, avec les autres MSC pour les handovers, et avec la gateway MSC pour le routage des appels entrants.

La VLR est une base de donnée locale qui reprend les informations de la base de donnée globale (le HLR) pour une station mobile tant que celle-ci se trouve dans la zone qu'elle couvre.

Dans la plateforme une VLR est associé chaque MSC et les deux sont confondues en un même objet.

1.2.4 GMSC

La gateway MSC porte un nom trompeur puisqu'elle n'a rien d'une MSC: elle est une passerelle entre le PLMN et d'autres réseaux. Pour le routage des

appels entrants en particulier, c'est elle qui interroge le HLR pour connaître la localisation d'une station mobile, puis redirige l'appel vers la bonne MSC.

1.2.5 PSTN/ISDN

Cet objet, sensé représenter le reste du monde dans la plateforme de simulation, répond aux appels émanant des stations mobiles et simule des appels adressés aux stations mobiles. Dans ce dernier cas il s'adresse à la GMSC pour obtenir des informations sur le routage.

1.2.6 SS7

Dans un PLMN tous les éléments fixes sont reliés par le réseau international de signalisation Sémaphore 7 : dans la plateforme il est modélisé d'une part par des liens fixes entre les BTS, BSC et l'objet qui se situe juste au dessus, d'autre part par un noeud auquel sont reliés toutes les MSC, la GMSC, le HLR et le reste du monde. Ce noeud appelé SS7 se contente d'assurer le routage des paquets entre ces différentes entités.

2 La station mobile

La station mobile a fait l'objet d'une implémentation détaillée suivant autant que possible les recommandations du GSM. On y retrouve les 3 couches RR (Radio Management), MM (Mobility Management) et CC (Call Control).

Sont également modélisés à l'intérieur du même objet la carte SIM nécessaire au fonctionnement du téléphone mobile, et l'utilisateur dont le comportement est paramétrable.

3 Procédures

Les procédures simulées par la plateforme sont résumées dans les paragraphes qui suivent, puis l'une d'elles, la procédure de handover, est entiérement détaillée.

3.1 Mise jour de localisation

Cette procédure est déclenchée par la station mobile à chaque fois qu'elle s'aperçoit qu'elle a changé d'aire de localisation (informations reçues sur la voie balise de chaque cellule). Elle a pour buts d'une part de mettre à jour dans le HLR l'information"MSC courante", d'autre part d'inscrire la station mobile dans la VLR de la MSC courante.

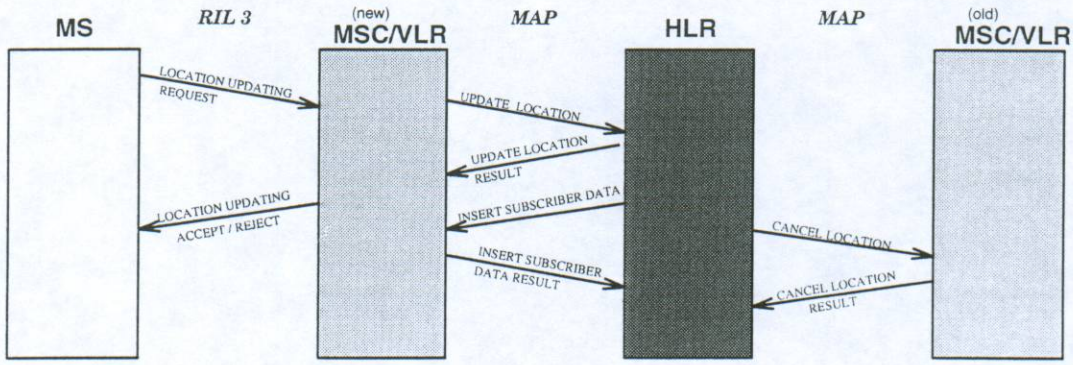

FIG. 2 - *Mise à jour de localisation*

La demande de mise jour est traitée par la MSC: si la nouvelle localisation concerne toujours la même MSC (on parle d'inter-BSC locup), elle se contente d'une mise à jour de la VLR. Si par contre la station mobile a changé de MSC en même temps que d'aire de localisation (inter-MSC locup), elle doit le signaler au HLR: il y a alors mise à jour du HLR et de la VLR de l'ancienne MSC. Voir figure 2.

3.2 Appel mobile demandeur

L'utilisateur du poste mobile peut déclencher un appel vers un abonné d'un autre réseau: la demande est relayée par la MSC vers le module PSTN/ISDN, qui y répond. Les ressources radio sont allouées et la communication établie (le traffic lui-mme n'est pas simulé).

L'appel pourra être interrompu par l'utilisateur du téléphone mobile ou par le PSTN/ISDN, ceci en fonction de paramétres définis pour la simulation.

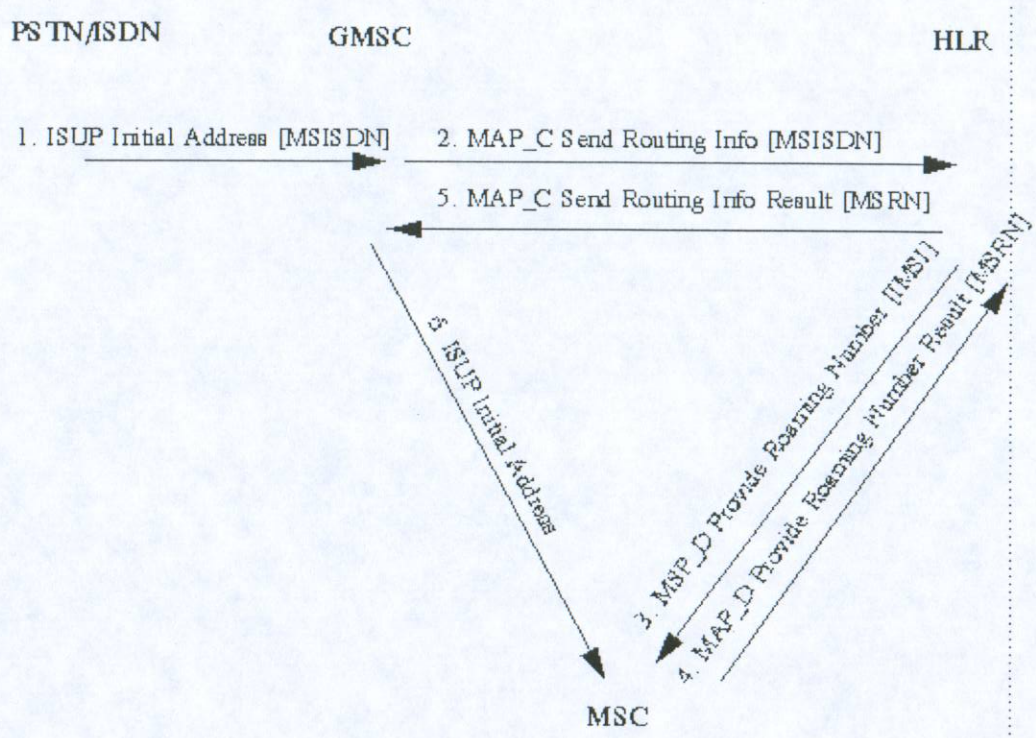

FIG. 3 - *Routage de l'appel*

3.3 Appel mobile demandé - Paging

De même les appels peuvent être initiés par le module PSTN/ISDN, qui, muni d'un numéro téléphonique classique (MSISDN = Mobile Station ISDN Number), s'adresse la GMSC pour obtenir des informations sur le routage. La GMSC interroge le HLR, qui connaît l'identité de la station mobile appelée (IMSI = International Mobile Subscriber Identity), ainsi que la VLR dont elle dépend. Le HLR à son tour interroge cette VLR et obtient un numéro de routage (MSRN = Mobile Station Roaming Number), qui retourne par le même chemin parcouru en sens inverse jusqu'à la GMSC. Celle-ci peut alors re-router l'appel vers la bonne MSC.(Figure 3)

Commence alors la procédure de paging qui permet de retrouver la station mobile appelée : des messages sont effets diffusés dans les zones où elle est susceptible de se trouver. Le choix de ces zones est laissé à l'opérateur, dans notre cas l'appel est diffusé dans l'aire de localisation o la station mobile s'est enregistrée pour la dernière fois.

La station mobile répond au paging et alors peut commencer l'établissement de l'appel.

3.4 Handover

Le handover consiste pour la station mobile à changer de cellule courante en cours de communication sans que celle-ci soit interrompue.(Figure 4)

Le changement peut avoir lieu entre deux cellules dépendant de la même BSC (internal handover), ou entre deux cellules dépendant de la même MSC mais de BSC différentes (inter-BSC handover), ou entre deux cellules dépendant de MSC différentes (inter-MSC handover).

On distingue de plus les cas ou la MSC est celle qui a établit l'appel (anchor-MSC) ou bien une autre (relay-MSC). Tout au long d'une communication c'est la anchor-MSC qui gére tous les handovers, puis la fin de l'appel, car c'est la seule à posséder dans la VLR associée les informations concernant la station mobile.

Les différents types de handover sont décrits en détail dans les paragraphes suivants.

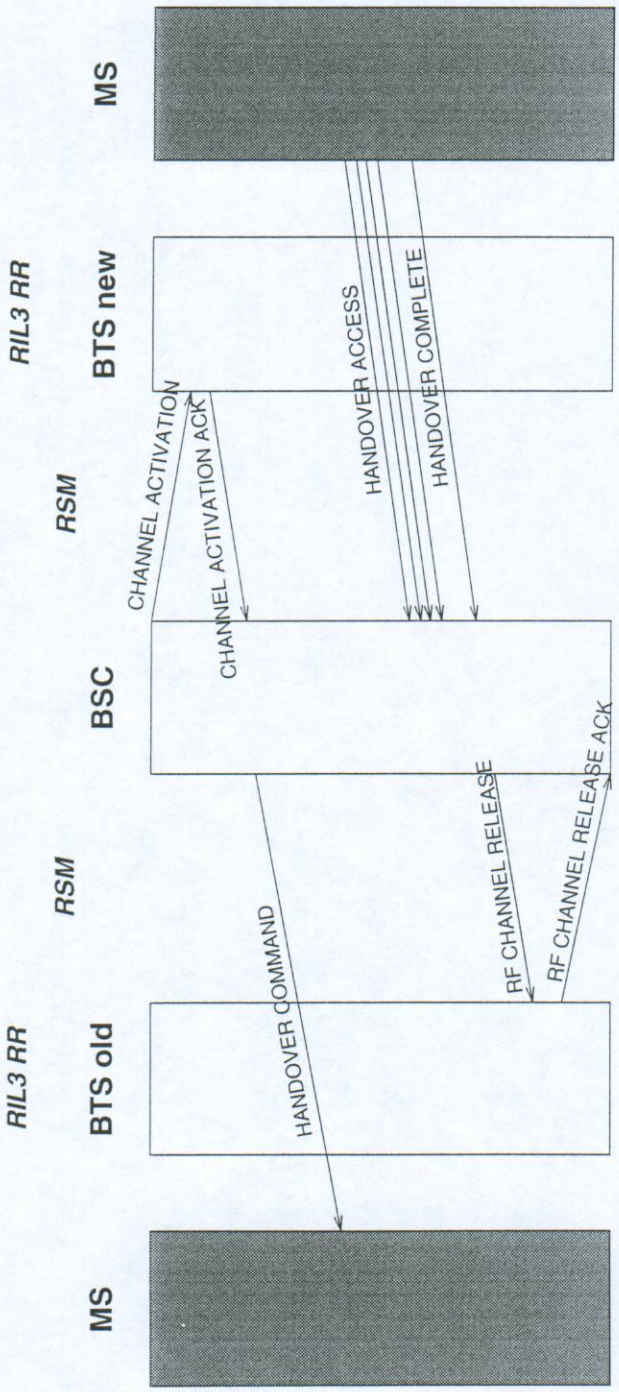

FIG. 4 - *Echange de messages de l'internal handover*

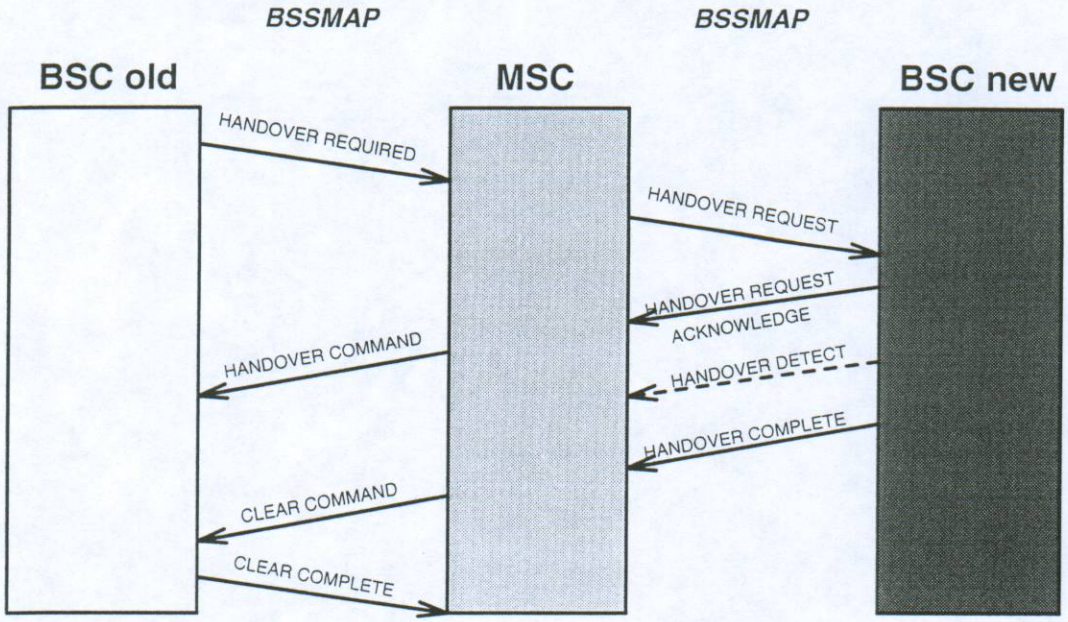

FIG. 5 - *Echanges de messages de l'inter-BSC handover*

3.4.1 Internal handover

On voit sur la figure 2 les échanges qui ont lieu lors d'un handover (quel qu'en soit le type) entre la BSC et la BTS d'une part (protocole RSM), la BSC et la station mobile (MS) d'autre part (protocole RIL3).

Pour un "internal handover" le reste du réseau n'est pas sollicité. (Les shémas suivants ne reprendront plus cette partie de la procédure).

3.4.2 Inter-BSC handover

Ce type de handover nécessite des échanges de messages entre la MSC et les deux BSC concernées, l'ancienne et la nouvelle (protocole BSSMAP, figure 5).

C'est toujours la BSC courante (BSC old) qui prend au vu des mesures la décision de demander un handover à la MSC courante, qui le traite entiérement.

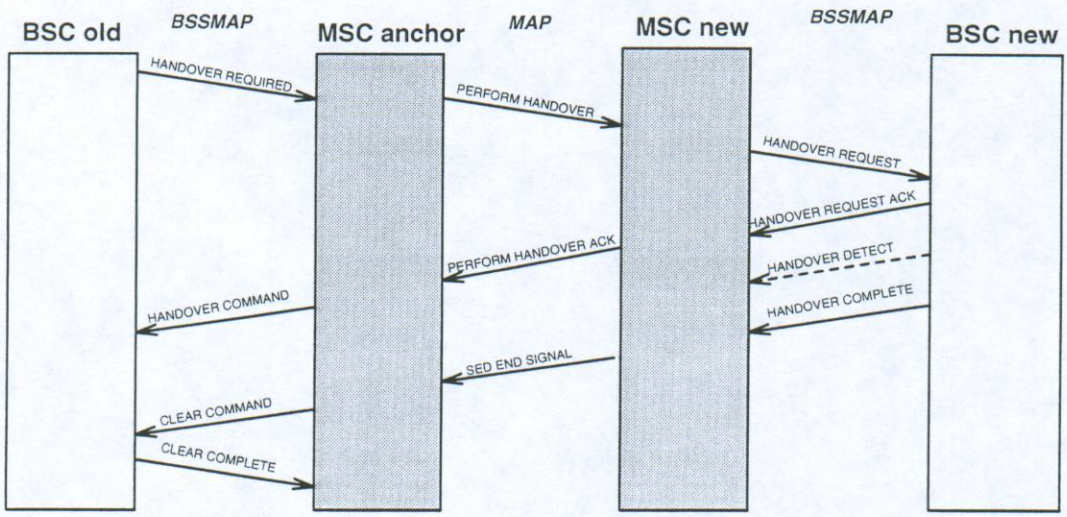

FIG. 6 - *Echanges de messages de l'inter-MSC handover*

3.4.3 Inter-MSC handover

Dans ce cas deux MSC sont concernées, et on suppose que la MSC courante est l'anchor-MSC, c'est donc elle qui gére les différentes phases du handover. Elle demande à la nouvelle MSC (protocole MAP, figure 6) de provoquer l'allocation des ressources radio dans la cellule cible, et déclenche la procédure de handover chez la station mobile.

3.4.4 Subsequent handover

Enfin dans ce cas le mobile souhaite passer d'une MSC à une autre (figure 7), et aucune des deux n'est la anchor-MSC ; celle-ci intervient pourtant pour commander toute l'opération, à la demande de la MSC courante. Elle relaie tous les messages entre les deux MSC.

4 Utilisation de la plateforme au sein de l'Institut Eurécom

La plateforme est utilisée dans le cadre d'un projet de recherche sur la détection d'intrusion dans les réseaux mobiles. Des modules spécifiques ont été ajoutés afin d'étudier le comportement des utilisateurs (fréquence, durée

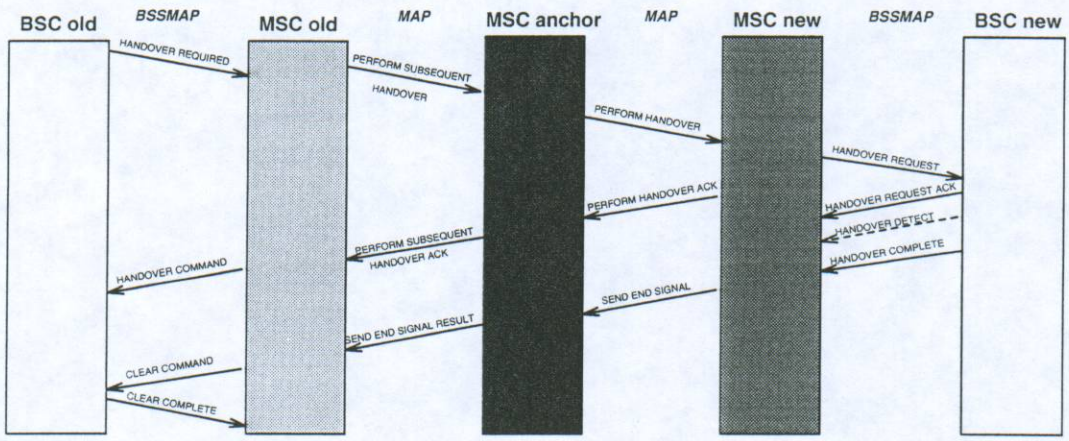

FIG. 7 - *Echanges de messages du subsequent handover*

et distance des appels notamment) : on souhaite ainsi repérer des utilisateurs fraudeurs qui auraient par exemple volé le téléphone mobile ou la carte SIM d'autres personnes.