N=° d'ordre : 03/2003-M/IN

Université des Sciences et de la Technologie Houari Boumedienne
(U.S.T.H.B.) Alger

Faculté d'Electronique et d'Informatique
Département Informatique

THESE

Présentée à l'U.S.T.H.B. en vue de l'obtention du diplôme de

MAGISTER

En Informatique
Spécialité : Programmation et Systèmes

Par
Mme Souad Benmeziane

Sujet

POUR UN ANONYMAT COMPLET EN ENVIRONNEMENT MOBILE

Soutenue le 09 Juin 2003, devant le jury composé de :

Mr M. Ahmed Nacer	Maitre de Conférences (USTHB)	*Président*
Mr H.M. Khelalfa	Chargé de Recherche, University of Wollogong, Dubai, UAE	*Directeur de thèse*
Mme Z. Ali-Mazighi	Maitre de Conférences (USTHB)	*Examinateur*
Mr N. Badache	Maitre de Conférences (USTHB)	*Examinateur*
Mme M. Boukala	Maitre de Conférences (USTHB)	*Examinateur*

A la mémoire de mon père

"Il n'y a pas de problèmes; il n'y a que des solutions. L'esprit de l'homme invente ensuite le problème."

A. Gide

Remerciements

L'accomplissement du travail effectué dans cette thèse est certainement le fruit de nombreux efforts et du soutien de nombreuses personnes.

Evidemment, la première personne à laquelle j'adresse mes vifs remerciements est certainement mon Directeur de Thèse : Mr Halim Khelalfa. Ma reconnaissance envers lui est inestimable. Je le remercie de m'avoir dirigée dans mes recherches et pour l'aide constante qu'il m'a prodiguée tout au long de ces années. Ses conseils avisés, sa disponibilité malgré son emploi du temps très chargé et surtout ses encouragements ont été pour moi un soutien capital.

Je remercie également, Monsieur M. Benhamadi, Directeur du C.E.R.I.S.T., pour m'avoir autorisée à entamer cette thèse et m'avoir encouragée à mener à bien ce travail.

Je tiens à remercier vivement Monsieur M. Ahmed Nacer, Maître de Conférences au Département Informatique de l'USTHB, pour m'avoir fait l'honneur d'accepter la présidence du Jury.

Je remercie Mme M. Boukala,chef du Département Informatique de l'USTHB pour m'avoir accueillie dans son département et pour avoir accepté de faire partie du jury.

Je remercie Mme Z. Ali Mazighi, Maitre de conférences au Département Informatique de l'USTHB, pour l'honneur qu'elle me fait en participant au jury.

Je suis très honorée de la présence dans le jury de Monsieur N. Badache, Maître de Conférences au Département Informatique de l'USTHB. Je le remercie d'avoir accepté de faire partie du jury. Je lui exprime également ma gratitude pour son soutien et pour tous ses encouragements.

J'ai grand plaisir de remercier tous les membres du laboratoire des logiciels de Base, du service Formation ainsi que le personnel de la bibliothèque du CERIST.

Mes sincères remerciements s'adressent également à ma chère amie Aliane Hassina, qui a dû supporter ma présence dans le même bureau durant toutes ces années. Je la remercie pour son soutien, sa collaboration scientifique et pour la bonne humeur qu'elle a fait régner tout au long de cette phase.

Je remercie également Sakina, Nadia, Omar et Djamel de m'avoir soutenu pour l'accomplissement de ce travail.

Enfin, Je ne saurai trouver les mots appropriés pour remercier ma famille particulièrement Djamel et mes trois perles : Sara, Hadjer et Hind de m'avoir supportée jusqu'au bout. Qu'ils trouvent dans ce travail, l'expression de toute ma reconnaissance et ma gratitude pour leur sacrifice et leur immense soutien.

Sommaire

Introduction Générale

Chapitre 1 : Introduction aux Environnements Mobiles

Chapitre 2 : La sécurité informatique : Concepts de Base

Chapitre 3 : La sécurité dans Les environnements Mobiles

Chapitre 4 : Anonymat dans les Réseaux Mobiles

Introduction générale

1. Problématique

L'apparition de la mobilité a changé la nature des systèmes distribués à grande échelle. De nouveaux services ont dû être développés pour les réseaux fixes afin d'offrir une disponibilité globale aux utilisateurs. Ces derniers, autrement dit les utilisateurs mobiles doivent pouvoir accéder à des services à partir d'un ensemble de situations différentes. L'extension de ces services aux réseaux sans fil a engendré de nouveaux problèmes spécifiques à ces réseaux ; la sécurité étant un problème majeur. En effet, la sécurité des communications sans fil peut être compromise plus facilement que celle des communications avec fils, en particulier lorsque les transmissions s'établissent sur de grandes distances et lorsque les utilisateurs sont autorisés à traverser des domaines de différents pays.
Les vulnérabilités des réseaux sans fil sont dûes essentiellement au manque de protection physique au niveau de l'interface d'accès et au médium de transmission entre l'unité mobile et l'unité de raccordement qui est accessible à tous. Les problèmes rencontrés concernent l'usurpation d'identité, le refus de service, l'écoute et la surveillance des déplacement des mobiles. Il est donc nécessaire d'identifier les faiblesses propres à un tel environnement et d'y inclure les mécanismes sécuritaires aux réseaux sans fil.
En fait, le grand défi pour les concepteurs d'architectures mobiles est d'adapter les conceptions qui ont si bien fonctionné dans les environnements fixes aux environnements mobiles. Nous noterons, donc que dans le domaine de la sécurité, c'est rajouter une incertitude à l'équation [Curtis 01].
Le premier mécanisme de sécurité introduit dans les environnements mobiles est l'authentification. Néanmoins, la mise en place de ce mécanisme dans un réseau mobile a introduit un nouveau besoin par rapport aux réseaux fixes traditionnels, celui de l'anonymat. Un besoin, qui jusque là, n'a pas été considéré comme besoin potentiel dans des environnements fixes tel qu'Internet.
Dans le contexte mobile, l'anonymat consiste à protéger les informations secondaires telles que l'identité des entités impliquées dans une transaction mais aussi à protéger les méta-informations qui découlent des interactions entre entités d'un système. Dans un réseau mobile, si aucune précaution n'est prise, un ennemi peut avoir accès à des informations secondaires concernant la localisation et les déplacements des utilisateurs. Les messages échangés durant la procédure d'authentification peuvent révéler des informations privées à des ennemis écoutant le médium de communication. Il devient alors possible de pister l'usager.
Préserver l'anonymat est de plus grande importance dans les environnements mobiles car ils sont plus vulnérables à l'écoute, comparés aux réseaux fixes. Il est donc plus facile d'accéder à l'information de l'utilisateur dans les canaux de communication. Dans ce cas, un nouveau type d'information devient de valeur importante c'est à dire l'information détaillée sur les mouvements et la location de l'utilisateur. Traverser des domaines étrangers accroît le risque de révélation d'informations relatives aux utilisateurs.
Dans ce contexte, différents besoins d'anonymat pour les systèmes mobiles ont été proposés. Ils concernent principalement, la prévention contre la révélation de l'identité réelle d'un utilisateur mobile, son domaine de résidence et les domaines visités.

2. Objectifs De la Thèse

L'objet de cette thèse est d'étudier en détail le problème de l'anonymat, de critiquer les solutions existantes et de proposer une solution garantissant un anonymat complet en environnement mobile.
Pour cela, nous avons eu à étudier :

- Les environnements mobiles
- La sécurité informatique : particulièrement les mécanismes cryptographiques et les mécanismes d'authentification.
- La sécurité dans les environnements mobiles ; en particulier les vulnérabilités propres aux systèmes mobiles.
- Les mécanismes d'authentification dans les environnements mobiles : que ce soit dans les infrastructures mobiles existantes tels que GSM ou les solutions proposées dans la littérature.
- Le problème de l'anonymat : d'abord tel que pris en compte dans les environnements statiques tels que Internet ou dans le domaine bancaire, puis dans les environnements mobiles.

A l'issue de cette étape, nous avons effectué une synthèse où une classification des degrés d'anonymat est présentée. Ce qui nous a permis d'associer un degré d'anonymat assuré par chaque solution.
Nous avons orienté notre étude sur les systèmes existants tels que GSM, et étudié les protocoles d'authentification proposés dans la littérature en vue de garantir l'anonymat. La critique et la comparaison des différentes solutions existantes nous a permis de conclure qu'auncune n'offrait un anonymat complet. Dans ce contexte, nous avons proposé une solution basée sur la signature en aveugle pour pallier aux problèmes des solutions existantes permettant ainsi de garantir un anonymat complet nécessaire dans certaines situations. En effet, l'emergence et le développement d'applications telles que le commerce électronique ou le vote électronique exigent un anonymat complet.
L'avancée technologique des mobiles en termes de performances et les progrés réalisés dans le domaine de la cryprographie, nous ont permis de proposer une solution jusque là, abondonnée pour son inadéquation dans le contexte mobile. En effet notre solution tient compte des derniers developpemnts technologiques en milieu mobile, qui permettent certains traitements impossibles à prendre en compte par le passé.

3. Organisation du document

- Le chapitre 1 propose un état de l'art en matière d'environnements mobiles : Il s'agit de présenter les différentes architectures de réseaux mobiles, les divers types de mobilité et surtout les problèmes engendrés par la mobilité.

- Au chapitre 2, nous définissons les différents concepts de la sécurité informatique, et détaillons un peu plus les mécanismes cryptographiques et les mécanismes d'authentification.

- Dans le chapitre 3, nous abordons la sécurité dans les environnements mobiles en explicitant les vulnérabilités de ces systèmes par rapport aux systèmes fixes. Nous abordons également les différents protocoles d'authentification proposés pour les réseaux mobiles.

- Dans le chapitre 4, nous discutons la problématique de notre étude à savoir l'anonymat dans les evironnements mobiles. Nous définissons le contexte de l'anonymat dans les environnments fixes tel que Internet et résumons certaines solutions proposées dans ce sens. Puis nous définissons la notion d'anonymat dans le contexte mobile en mettant en lumière une classification des différents degrés d'anonymat, et enfin, nous détaillons les solutions proposées dans la littérature pour concilier l'authentification et l'anonymat.
  Le chapitre est clôturé par une synthèse où les différentes solutions sont comparées puis critiquées.

- Dans le chapitre 5, nous proposons un protocole d'authentification pour les environnements mobiles garantissant un anonymat complet tel que défini par les degrés d'anonymat.

- Enfin, nous achéverons cette thèse par une conclusion résumant les principales étapes et résultats ainsi que les futures extentions et perspéctives de ce travail.

Résumé

Domaine de recherche relativement sensible, la protection de la vie privée et particulièrement l'anonymat constitue un axe de recherche crucial en sécurité dans les environnements mobiles.
L'anonymat consiste à protéger les informations secondaires telles que l'identité des entités impliquées dans une transaction mais aussi à protéger les méta-informations qui découlent des interactions entre entités d'un système. Etant donné que les réseaux mobiles sont plus vulnérables à l'écoute, un intrus peut avoir accès à des informations sensibles concernant la vie privée des utilisateurs. Les messages échangés durant la procédure d'authentification peuvent révéler des informations privées à des ennemis écoutant le médium de communication. Il devient alors possible de pister l'usager.
En nous intéressant au problème d'anonymat, nous nous sommes confrontés à un domaine sensible. En effet, d'un point de vue social, les communications anonymes semblent être désirées seulement par une minorité de gens concernés par le problème de préserver confidentielles les informations privées et souvent non acceptées par les gouvernements ou organisations. C'est pourquoi, les solutions pour les communications anonymes ne sont pas intégrées dans des produits existants ou infrastructures. Notons que l'anonymat assuré par GSM n'est que partiel et à ce jour les travaux de UMTS ne considèrent pas un anonymat complet. Il est également important de noter que même les travaux de recherche ne considèrent pas un anonymat complet.

Dans ce contexte, nous proposons un protocole d'authentification dans un environnement mobile qui assure l'anonymat complet. Le protocole est basé sur la technique de signature aveugle pour assurer l'intraçabilité de l'utilisateur mobile même par son domaine d'affiliation. Ce dernier ne pourra pas connaître les différents déplacements de son abonné. Le protocole, ainsi défini, garantit la confidentialité des messages échangés durant l'authentification et permet de résister aux attaques par rejeu.
L'anonymat complet peut sembler contradictoire avec la tarification des services demandés. Pour cela, nous intégrons un moyen de paiement électronique sans compromettre l'anonymat.

Mots clés : Authentification, Anonymat, Intraçabilité, Signature aveugle, Mobilité.

Abstract

Anonymity consists in protecting secondary information such as identity from the entities implied in a transaction but also protecting meta-information which rises from the interactions between entities. Given that mobile networks are more vulnerable to eavesdropping, an intruder can have access to significant information relating to the privacy of the users. The messages exchanged during the authentication procedure can reveal information to intruders listening to the medium of communication. It then becomes possible to track the user.

By interesting us in the problem of anonymity, we are confronted ourselves with a significant field. Indeed, in a social point of view, the anonymous communications seem to be only desired by a minority of people concerned with the problem to preserve confidential the private information and often not accepted by the governments or organizations. Thus, the solutions for the anonymous communications are not integrated in existing products or infrastructures. Let us note that anonymity assured by GSM is partial and to date of work, UMTS does not consider a complete anonymity. It is also significant to note that even the research tasks do not consider a complete anonymity. In this context, we propose an authentication protocol in a mobile environment which ensures complete anonymity.

The protocol is based on the blind signature technique to ensure untraceability of a mobile user even by his affiliation domain. This latter will not be able to know various displacements of its subscriber. The protocol, such defined, guarantees the confidentiality of the messages exchanged during the authentication and makes it possible to resist to replay attacks. Complete anonymity can seem contradictory with the accountancy of the required services. For that, we integrate an electronic means of without compromising anonymity.

Key words: Authentication, Anonymity, untraceability, blind signatures, wireless.

1.1 Introduction

Actuellement, les réseaux mobiles sont de plus en plus répandus et ils vont le devenir encore plus dans les prochaines décennies. En effet, l'informatique mobile permet aux utilisateurs de se déplacer tout en restant connectés au réseau, il leur devient donc possible d'accéder à leur environnement de travail et de continuer à communiquer. En fait, le but de l'informatique mobile est de permettre à un utilisateur l'accès à un réseau sans se préoccuper de la localisation et de la mobilité. L'idée principale est de conserver des connexions réseaux au cours des déplacements de l'utilisateur et de sa machine [Baggio 95].
L'informatique mobile a pris récemment un essor très important dû aux avancées techniques qui y sont liées. En effet, des développements considérables ont été effectués conjointement dans le domaine des composants (qui permettent de concevoir des ordinateurs portables de plus en plus petits et puissants), des médias de communication sans fil (qui offrent des débits de plus en plus élevés) et des protocoles (qui gèrent la mobilité de manière plus ou moins satisfaisante) [LeGrand 98].
Néanmoins, la mobilité a fait apparaître de nouveaux problèmes qui doivent être résolus tant du point de vue matériel (déconnexion, faible largeur de bande, limitation en énergie, stockage et puissance…), que réseau (nommage, routage), localisation des ressources ou de sites mobiles, gestion des données. En plus de ces problèmes, la mobilité a introduit de nouveaux besoins de sécurité en comparaison aux réseaux fixes traditionnels.

1.2 Architecture d'un environnement mobile

Dans un environnement mobile, on distingue deux ensembles distincts d'entités: les sites (ou unités) fixes d'un réseau de communication filaire **(wired network)** et les sites (ou unités) mobiles **(wireless network)** [Pitoura 93]. Les sites fixes appelés stations de base (base stations) ou station support mobile SSM (Mobile Support Station) sont dotés d'interfaces de communication sans fil pour pouvoir communiquer avec les sites mobiles. Chaque site mobile communique avec une seule station de base. L'aire géographique couverte par une station de base est appelée : cellule.

L'architecture cellulaire, illustrée par la figure 1.1, est vue comme une agrégation de trois principaux éléments [Badache 98]:

1. Les stations de base (**SB**)
2. Les stations mobiles (**SM**)
3. L'interface air (**IA**)

Les Stations de Base (SB)

Les stations de base sont chargées d'assurer l'interface entre le réseau sans fil et le réseau filaire auquel il est relié. Elles sont munies d'une interface de communication sans fil pour la communication directe avec les sites mobiles localisés dans une cellule. Elles sont généralement composées d'un concentrateur et d'un émetteur-récepteur. Le concentrateur garantit une fonction de tampon car les débits peuvent être différents entre le réseau sans fil et le réseau filaire. A chaque SB correspond une cellule à partir de laquelle les mobiles peuvent émettre et recevoir des signaux. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées.

Les Stations Mobiles (SM)

Une station mobile peut échanger des informations avec les stations fixes disposant ou non d'interfaces de communication sans fil et ce quelque soit leur position à l'intérieur des cellules. A un instant donné, une station mobile ne peut directement être connectée qu'à une seule SB. Elle communique avec les autres sites à travers la station à laquelle elle est directement rattachée. Pour communiquer, une SM dispose des composants classiques d'un ordinateur et d'un émetteur-récepteur jouant le rôle d'interface pour les communications sans fil.
A un instant donné, une unité mobile ne peut appartenir qu'à une seule cellule. Lorsqu'une unité mobile se déplace de sa cellule courante à une cellule voisine, une migration a donc lieu et une procédure spécifique de déconnexion/reconnexion appelée **handoff** est utilisée [Badache 98].
Les unités mobiles qui se trouvent dans une même cellule sont considérées locales à la SB, par conséquent, elle partagent la bande passante attribuée par la SB.
Le réseau sans fil (Wirelless Network) est composé de la SB et des unités mobiles qui lui sont locales.

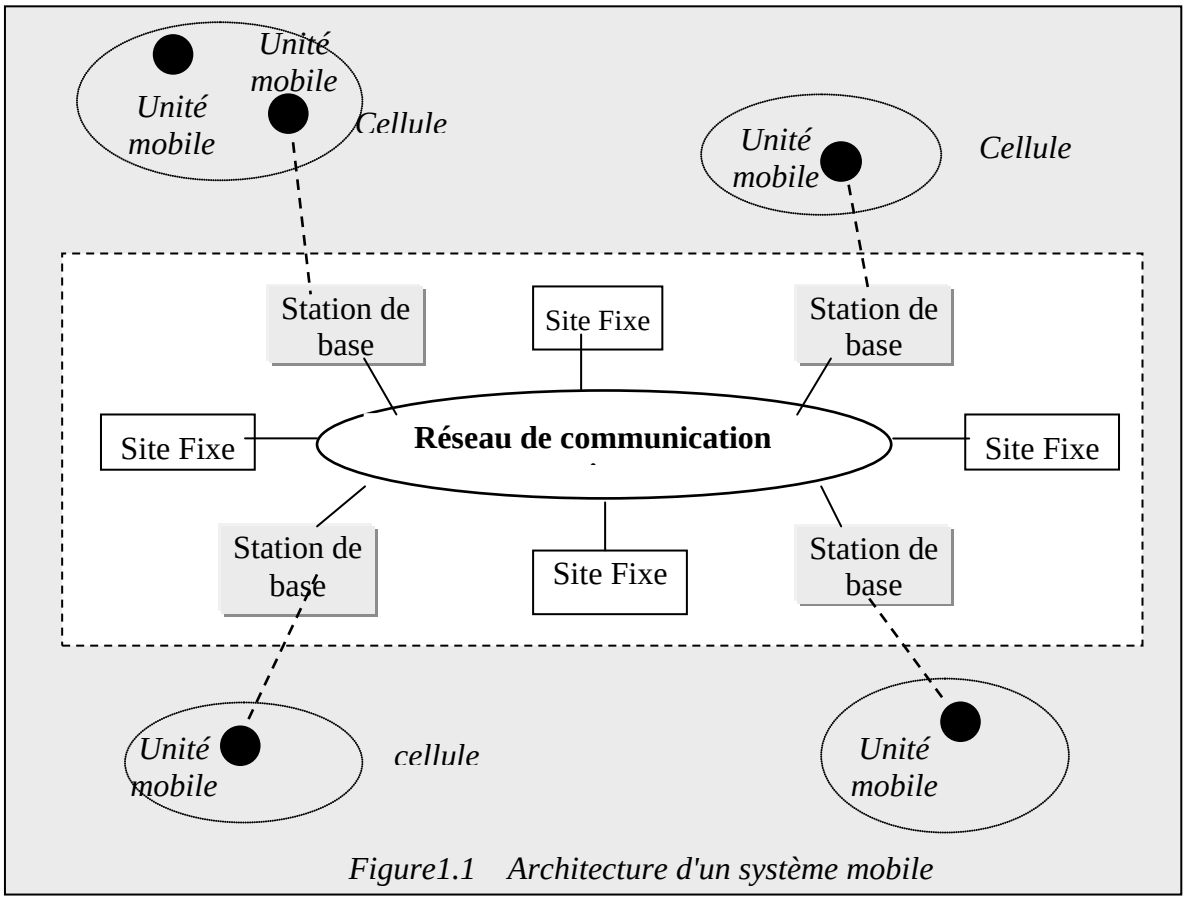

Figure1.1 Architecture d'un système mobile

L'interface air (IA)

Cette interface représente la liaison qui s'établit entre une station fixe et un site mobile par l'intermédiaire de techniques de communication sans fil (ondes radio, micro-ondes, infrarouge, laser). L'interface air est une liaison caractérisée par :

- son caractère instable vu qu'elle peut être rompue à tout moment.
- sa qualité variable dépendant des conditions extérieures.

- Son débit limité.

Une liaison sans fil ne peut s'établir que lorsque le mobile entre dans la cellule de communication de la station, comprise dans sa zone d'émission, et qu'il est suffisamment proche de la station pour que celle-ci soit dans sa propre zone d'émission (figure 1.2).

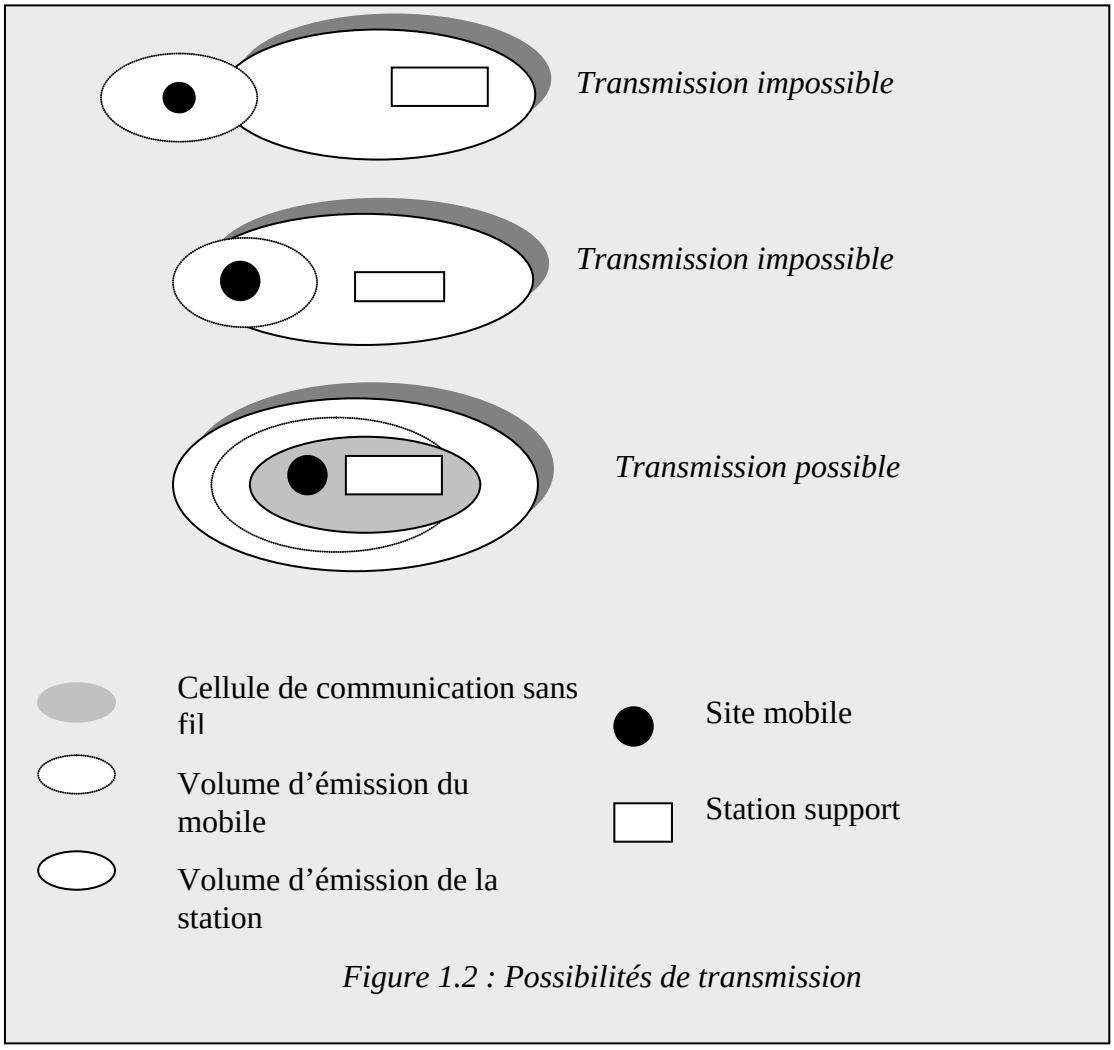

Figure 1.2 : Possibilités de transmission

Nous distinguons donc comme le montre la figure 2, trois cas de figure possibles :

- Dans le premier cas, le mobile est en dehors de la zone d'émission de la station et de plus, la station n'est pas à portée du mobile, aucune transmission n'est donc possible.
- Dans le deuxième cas, le mobile est entré dans la zone d'émission de la station, mais sa portée est trop faible pour lui permettre d'entamer une communication. Il peut malgré tout recevoir des informations en provenance de la station.
- Enfin, pour le troisième cas, toutes les conditions sont réunies pour autoriser une transmission : le mobile et la station sont à portée d'émission l'un de l'autre, et le mobile se trouve dans la cellule de communication qui a été définie pour la station.

1.3 Types de Mobilité

L'informatique mobile est un terme très vague pour désigner tout ce qui a trait à la mobilité. D'après [Baggio 95], il existe trois contextes utiliser l'informatique mobile : la mobilité du matériel, la mobilité des utilisateurs et la mobilité des applications.

1.3.1 Mobilité du matériel

La mobilité du matériel conjointe à la mobilité de l'utilisateur constitue pour le moment le problème le plus étudié en informatique mobile. En fait, ce type de mobilité présente la limitation qu'une identification est associée à un terminal particulier et non pas à un abonné qui possède souvent plusieurs terminaux. Les problèmes rencontrés sont essentiellement dûs aux besoins de changement d'adresse réseau des machines au fur et à mesure qu'elles se déplacent, ce sont en particulier des problèmes de routage, de localisation et d'acquisition d'informations dépendantes de cette localisation [Baggio 95].

1.3.2 Mobilité des utilisateurs

La caractéristique principale de type de mobilité est l'identification personnelle de l'abonné matérialisé par un numéro d'identité. Dans ce type de mobilité, il n'y a plus de problème d'adresse des machines puisque celles-ci restent fixes. Néanmoins, on doit obtenir les profils des utilisateurs. Parmi les problèmes rencontrés, citons: la facturation et l'optimisation des chemins de localisation.

1.3.3 Mobilité des applications

La mobilité des applications permet à l'utilisateur de disposer de ses applications actives quelque soit sa nouvelle localisation. Dans ce cas, un certain nombre de problèmes est posé à savoir : la sécurité et l'authentification des utilisateurs, la localisation des utilisateurs…

1.4 Modes de fonctionnement des mobiles

Dans un système distribué sans ordinateur mobile, une machine ne peut travailler que dans deux modes différents : connecté ou déconnecté. Par contre, en environnement mobile, les unités mobiles disposent de modes de fonctionnement qui leurs sont propres. En fait, il existe des degrés variés de déconnexion qui dépendent de la bande passante attribuée au unités mobiles [Pitoura 93].
Actuellement, il existe quatre modes de fonctionnement (figure 1.3) . Nous allons dans ce qui suit, définir chacun de ces modes ainsi que les différentes transitions entre ces états.

a. *Le mode connecté*: Dans ce cas, le mobile dispose d'une connexion normale au réseau. La connexion peut alors être réalisée soit par une liaison filaire, soit par une interface de communication sans fil.
b. *Le mode partiellement connecté*: Dans ce cas de figure, le mobile ne dispose que d'un lien à faible largeur de bande (connexion faible ou déconnexion partielle). Cette situation peut être provoquée par des perturbations dues à des surcharges de la station de base qui gère les communications des mobiles se trouvant dans sa cellule.
c. *Le mode veille*: Ce mode est invoqué par le mobile pour préserver ses ressources énergétiques. Les exécutions des applications de l'utilisateur sont suspendues.

Néanmoins, la liaison avec le réseau est maintenue, le mobile n'envoie plus de messages mais peut en recevoir et passer ainsi au mode connecté.

d. *Le mode déconnecté*: Un mobile peut être totalement déconnecté du réseau à la fois parce qu'il n'y est plus physiquement relié ou parce qu'il est impossible de maintenir une connexion sans fil.

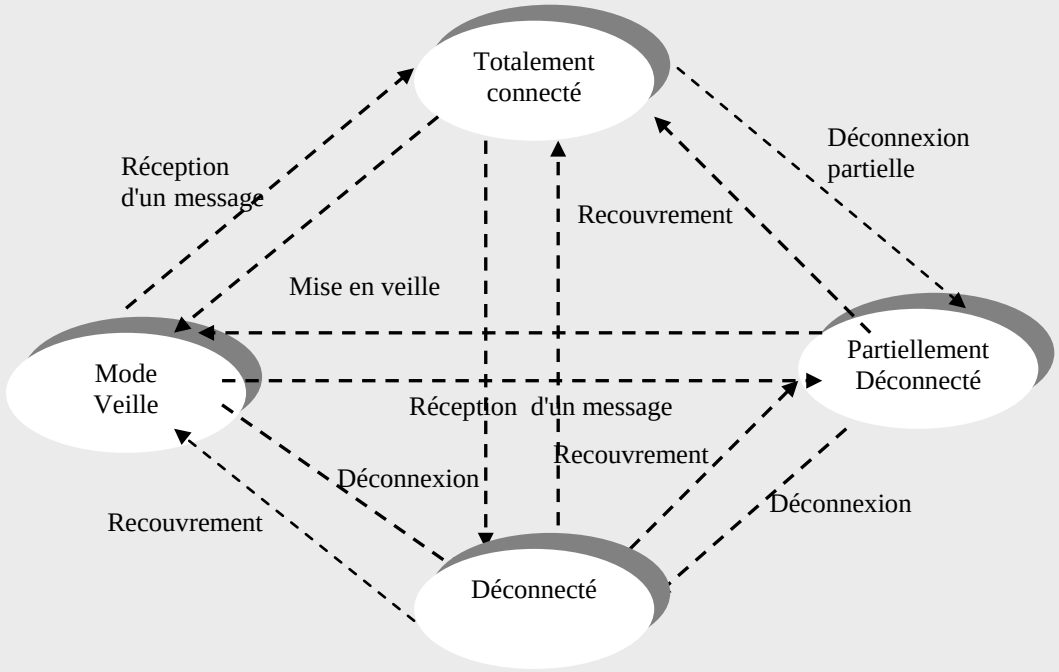

Figure 1.3 : Différents modes d'opération des mobiles [Pitoura 93]

Une caractéristique essentielle des modes d'opération des sites mobiles est qu'ils sont prévisibles. En effet, les déconnexions peuvent être le plus souvent détectées et un protocole spécifique est mis en œuvre pour les prendre en compte [Pitoura 93].

- Le protocole de déconnexion doit être exécuté avant que la machine ne soit physiquement détachée du réseau fixe.
- Le protocole de déconnexion partielle a pour objectif de préparer le mobile à exécuter des opérations dans un mode où toutes les communications avec le réseau fixe sont réduites.
- Le protocole de recouvrement, quant à lui, permet de rétablir les connexions avec le réseau fixe pour passer à l'état totalement connecté.
- Enfin, le protocole de handoff permet de sortir des bornes d'une cellule pour entrer dans une autre tout en conservant la connexion et en mettant à jour certaines informations telles que : la localisation du mobile sur le réseau fixe et le nom de la

station support locale sur le mobile. Des informations d'états se référant au mobile peuvent être ainsi transférées vers la station support de la nouvelle cellule.

1.5 Aperçu de quelques réseaux mobiles

1.5.1 GSM : Global System For Mobile Communications

GSM est un système cellulaire, c'est à dire que la couverture radio est assurée par de multiples sites d'émission réception. La couverture d'une antenne est appelée cellule. Les cellules sont groupées en clusters. Le spectre radio disponible est réparti entre les cellules d'un même cluster. Les objectifs de GSM est de fournir un service de téléphonie mobile de voix et de données compatible avec les réseaux fixes (analogique et données par paquets) [Rahnemma 93].

Plusieurs niveaux de hiérarchie sont présents dans le système GSM (figure 1.4):

- Base Tranceiver Station : BTS, responsables de la gestion de la transmission radio, de la gestion de la couche physique, de la gestion de la couche liaison de données et de la mesure de la qualité du signal reçu. Une BTS est associée à une cellule.

- Base Station Controller : les BSC gèrent la ressource radio (allocation de canaux, utilisation des mesures de la BTS et contrôle de puissance du mobile, handoff,…). Une BSC peut gérer jusqu'à 40 BTS.

- Mobile-services Switching Center : les MSC gèrent les communications entre les mobiles et le réseau fixe, ainsi que les mobiles en visite sur le VLR (voir ci-dessous).

- Visitor Location Register : les VLR maintiennent une base de données des abonnés mobiles présents sous le MSC. Cette base de données comprend :

    - IMSI : International Mobile Subscriber Identity qui représente l'identité globale de l'abonné.
    - MSISDN : Mobile Integrated Services Digital Network Number), le numéro d'appel du mobile.
    - TMSI : (temporary Mobile Station Identity), l'identité temporaire du mobile.
    - Le type d'abonnement.
    - La zone de localisation.

- Les HLR (home location Register sont chargés) de la gestion de la base de données des abonnés mobiles , c'est à dire :
    - Des informations sur les abonnés (IMSI, MSISDN, type d'abonnement)
    - Des informations de localisation (identité du VLR où se trouve l'abonné).

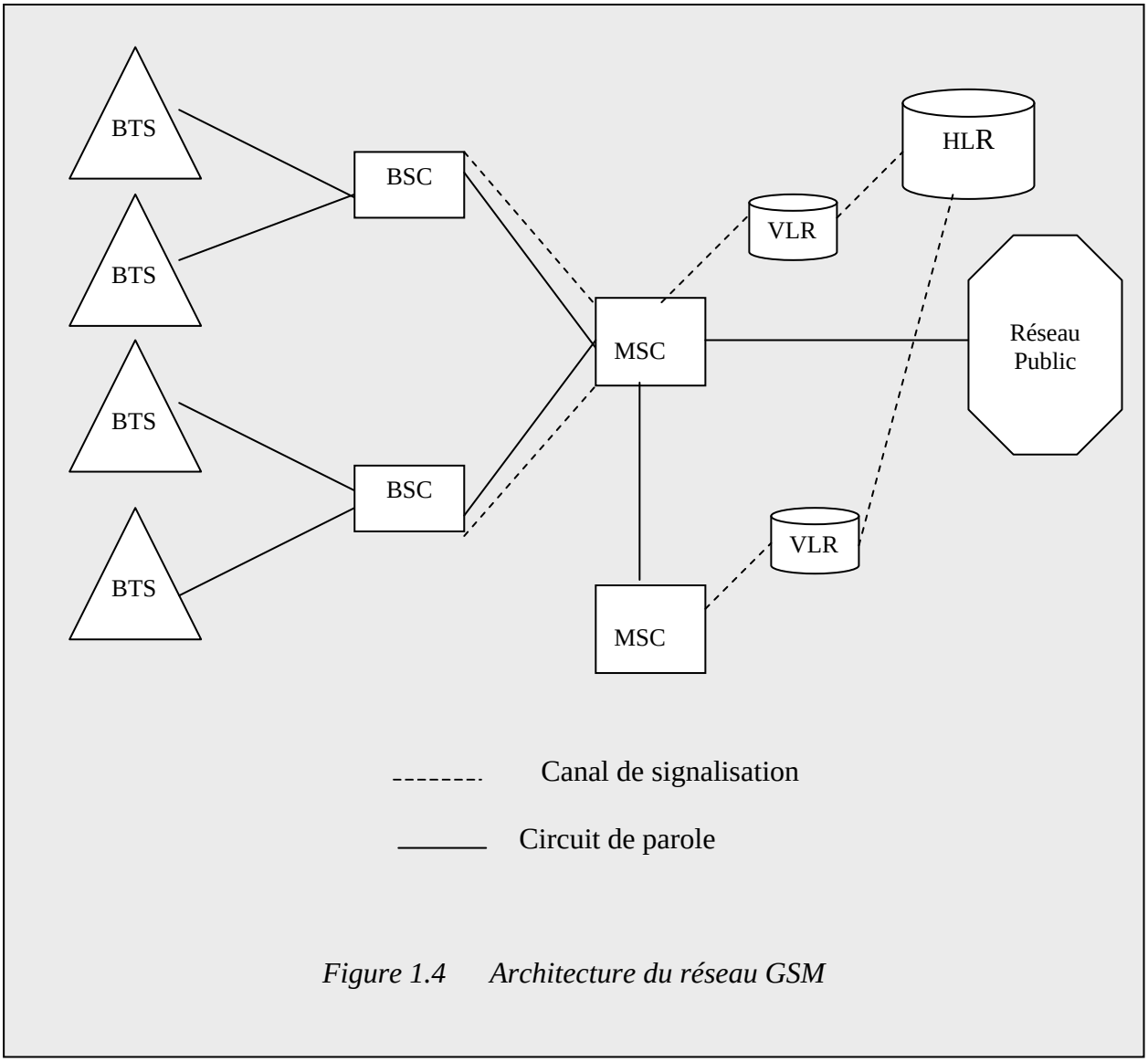

Figure 1.4 Architecture du réseau GSM

GSM fournit un service de mobilité globale dans un réseau, c'est à dire qu'un utilisateur ayant commencé une communication dans une cellule n'est pas contraint de rester dans cette cellule.
Il existe deux types de handoff : inter-cellulaire et intra-cellulaire. Le premier s'effectue lorsque le mobile s'éloigne de sa station de base pour transférer un appel établi sur une cellule vers une autre cellule. Le second est réalisé lorsque la communication est brouillée malgré un champ reçu correct.

1.5.2 CDPD : Cellular Digital Packet Data

Le CDPD a été développé par un consortium d'entreprises américaines. CDPD est un réseau mobile à grande échelle orienté vers le trafic de données. Il propose une connectivité sur des zones géographiques très étendues. Ces zones sont de la taille d'une ville ou d'un pays. CDPD exploite les slots libres, disponibles dans les communications cellulaires vocales pour transmettre les données. Il supporte plusieurs protocoles de niveau réseau IP et le protocole CLNP (Connectionless Network protocol) [Badr 95].

1.5.3 UMTS (Universal Mobile Telecommunications Systems)

La scène actuelle du monde mobile et de celui des communications personnelles est composée de différents systèmes incompatibles. Ces systèmes englobent les systèmes cellulaires, les systèmes téléphoniques, et les systèmes satellitaires. Il est à noter que non seulement, les bandes de fréquence utilisées par ces systèmes sont différentes mais ces derniers sont basés sur des standards nationaux et régionaux différents : c'est pourquoi l'interconnexion et l'interfonctionnement de ces systèmes est parfois impossible. Les acteurs dans le domaine des télécommunications ont déjà commencé à préparer la génération suivante, sous la nomination en Europe de UMTS. Le but de ce standard est de développer une troisième génération de systèmes issue de la convergence des différentes familles de systèmes mobiles [Curtis 01].

1.6 Problèmes liés à la mobilité

L'informatique mobile entraîne de nouveaux problèmes [Pitoura 93]. Ces problèmes affectent d'une part le réseau statique et les réseaux sans fil qui lui sont rattachés d'autre part. En effet, les divers déplacements des sites mobiles impliquent une modification de la topologie physique du réseau avec des systèmes hautement hétérogènes. De plus, la mobilité fait de la localisation une donnée variable [Pitoura 93]. Par conséquent, différentes questions se posent: Comment seront localisées les unités mobiles? Comment effectuer la distribution de données…
Ainsi, dans un environnement mobile, il est nécessaire de nommer les unités mobiles, de les localiser, de router les messages d'autres unités mobiles, d'accéder aux ressources des réseaux locaux qu'elles visitent, et enfin d'assurer la sécurité.
Dans ce qui suit, nous essayons de caractériser certains problèmes introduits par la mobilité.

1.6.1 Hétérogénéité du matériel et des réseaux

Contrairement aux systèmes fixes où les machines sont connectées une fois pour toutes à un réseau donné, en informatique mobile on rencontre non seulement une multitude de sites mobiles mais également un grand nombre de réseaux à la fois avec ou sans fil [Baggio 95]. Les mobiles se retrouvent donc à naviguer dans un environnement hautement hétérogène et de même, les réseaux risquent de voir passer un grand nombre de machines de tout ordre et d'utiliser un nombre important de protocoles d'accès différents.
Les interfaces de communication sans fil risquent également de changer lors des déplacements entre l'intérieur et l'extérieur.
De plus à l'hétérogénéité des systèmes, se rajoutent l'hétérogénéité des performances et de la disponibilité dûes aux spécificités du matériel utilisé.

De nouvelles techniques sont donc nécessaires pour maximiser à la fois les performances et la disponibilité des sites mobiles.
La gestion de cette hétérogénéité implique donc des traitements beaucoup plus complexes qu'en informatique fixe [Baggio 95].

1.6.2 Le nommage des sites mobiles

L'allocation des noms est un problème clef en Informatique mobile. En effet, un mobile doit disposer d'un nom s'il veut utiliser des services, envoyer ou recevoir des informations. Ce nom permettra aux serveurs locaux de communiquer avec le mobile, de l'authentifier et de lui fournir une note de frais.

1.6.3 Le routage dans les réseaux mobiles

Tout comme l'adressage, le routage doit être dynamique. Il est essentiel que lorsqu'un mobile se déplace, les paquets qui lui sont destinés ne soient plus dirigés vers l'ancienne localisation du mobile, mais vers la nouvelle, tout en utilisant le routage le plus optimal possible.
Il arrive que les protocoles de routage limitent le nombre de sites mobiles qu'ils peuvent supporter dans un sous-réseau donné. Malheureusement, avec une telle méthode, le nombre de mobiles dans un sous réseau est alors borné par le nombre d'adresses disponibles et non par la largeur de bande passante utilisable.

1.6.4 La localisation des ressources

Lorsqu'ils se déplacent, les ordinateurs doivent être capables de situer les ressources présentes sur le réseau visité, comme par exemple les imprimantes disponibles. Ces requêtes concernent des informations sur l'environnement dont la localisation est statique (en général) ou mobile. L'objectif est donc de réaliser et d'intégrer un protocole de localisation de ressources et de le faire fonctionner de façon complètement transparente avec les applications existantes.

1.6.5 La localisation des sites mobiles

En environnement mobile, les mouvements fréquents des machines impliquent à la fois une gestion appropriée des informations de localisation et des mécanismes de recherche de sites mobiles de manière à mettre à jour leur position. En effet, lorsqu'une information est destinée à un mobile, il est important de pouvoir la délivrer à la localisation courante du mobile, et non à son réseau de rattachement [Koch 93].

1.6.6 La gestion de données

L'informatique mobile engendre des problèmes de récupération de données, de dépendance à la localisation, de diffusion de données, de gestion des déconnexions et d’accès efficace aux données [Duchamp 92].
Les utilisateurs se déplaçant, il est nécessaire de connaître leur position. Du point de vue de la gestion de données, il va falloir stocker ces informations dans une base de données En fait, il est plus intéressant [Baggio 95] de considérer l'ensemble des utilisateurs avec leurs caractéristiques comme une base de données répartie entre les différents serveurs de localisation.

L'environnement mobile a donc introduit un nouveau type de requêtes qui manipulent des informations dépendantes de la localisation actuelle de l'unité mobile. Par exemple, répondre à la requête: Quelle est la route la plus courte à l'hôpital le plus proche? Implique l'acquisition de données pendant l'exécution même de cette requête si la localisation contenue dans la base de données est incomplète.
D'autre part, la mobilité des utilisateurs nécessite souvent la réplication de données couramment utilisées. En effet, lors du déplacement d'un utilisateur, il doit retrouver son ancien environnement : à sa nouvelle position, il doit pouvoir accéder aux fichiers, applications ou services utilisés auparavant.
De plus, les sites mobiles, pouvant être déconnectés, il est nécessaire de gérer sur les mobiles des mécanismes de cache. [Baggio 95]

1.6.7 La sécurité

La sécurité des communications sans fil peut être compromise plus facilement que celle des communications avec fils, particulièrement lorsque les transmissions s'établissent sur de grandes distances et lorsque les utilisateurs sont autorisés à traverser des domaines de différents pays [Asokan 95].
En effet, les réseaux mobiles de par leur structure sont plus sensibles que les réseaux fixes traditionnels du fait que l'interface air ne bénéficie pas de protection physique et le médium de transmission reste accessible à tous.
Les problèmes rencontrés concernent l'usurpation d'identité, le refus de service, l'écoute ou encore la surveillance des déplacements des mobiles. Il est donc nécessaire d'inclure des mécanismes de sécurité dans les réseaux sans fil.

Dans le cadre de cette thèse, nous allons étudier plus en détail la sécurité dans les environnements mobiles. Néanmoins, avant d'étudier la sécurité dans les environnements mobiles, il est important de présenter certains concepts de base de la sécurité informatique et les mécanismes de sécurité employés dans les environnements statiques.

Ce Chapitre introduit les différents concepts de base de la sécurité informatique. Dans une première étape, nous présentons les objectifs de la sécurité informatique, les menaces et les services de sécurité. Dans une seconde étape, nous définissons les mécanismes de sécurité et présentons de manière plus détaillée les mécanismes de cryptographie et d'authentification.

2.1 Introduction

La croissance des systèmes informatiques et l'expansion du nombre de réseaux interconnectés rend la question de sécurité informatique de plus en plus importante. Dans un système informatique, les éléments qu'il faut prendre en compte sont [Khelalfa 00]:

- Les sujets ou entités : Une entité ou sujet est un composant actif qui permet aux informations de circuler entre les objets ou qui cause un changement de l'état du système. Par exemple, un utilisateur, un processus,…
- Les objets : Un objet est un composant passif dans un système. Ce sont les informations et les ressources du système. Par exemple, les programmes, les disques,…

Le terme « sécurité » [ISO 89] est utilisé dans le sens de minimiser les vulnérabilités d'actifs et de ressources. Un actif est tout élément de valeur. Une vulnérabilité est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient. Une menace est une violation potentielle de sécurité.

2.2 Les objectifs de la sécurité

L'objectif de la sécurité informatique est la mise en œuvre de mécanismes de protection permettant d'assurer les propriétés suivantes [ISO 89] :

La *confidentialité* : assurer qu'une information n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

L'*Intégrité* : assurer que l'information contenue dans les objets n'est ni créée, ni altérée, ni détruite de manière non autorisée.

La *Disponibilité* : assurer qu'un objet est accessible et utilisable sur demande par une entité autorisée.

L'*Utilisation légitime* : assurer que les ressources ne sont pas utilisées par des personnes non autorisées ou de manière non autorisée.

2.3 Menaces

Les menaces peuvent être considérées comme *une violation potentielle du système de sécurité utilisant les vulnérabilités de ce dernier.*
Il existe deux types fondamentaux de menaces :

- Les menaces accidentelles.
- Les menaces intentionnelles (les attaques).

- Les menaces accidentelles surviennent sans aucune préméditation, par exemple, défaillance d'un système ou bugs de logiciels.
- Les menaces intentionnelles utilisent des connaissances spécifiques du système et leur concrétisation est considérée comme une attaque. Une attaque est une action exécutée par une entité pour violer la sécurité.

Le résultat des attaques est la désorganisation des informations, la violation de la confidentialité, la révélation d'informations secrètes, la modification des objets ou la violation de l'intégrité des objets.

Les attaques peuvent être directes ou indirectes [Olovsson 92]:
- les attaques directes aux objets sont destinées directement vers un objet. Plusieurs composants d'un système peuvent être attaqués avant que l'objet en question ne le soit.
- Dans l'attaque indirecte les informations concernant l'objet sont reçues sans attaquer l'objet lui-même.

Les attaques peuvent être classées en attaques passives et attaques actives [Olovsson 92].
- Attaques passives : elles ne produisent aucune modification d'informations contenues dans le système, et par conséquent, il n'y a aucun changement dans son état et dans son fonctionnement. En général il est très difficile de détecter une attaque passive car elle n'agit pas sur le fonctionnement du système. L'écoute via une ligne de communication pour la collecte d'informations est une attaque passive.
    - Attaques actives : elles altèrent les informations contenues dans un système entraînant ainsi des changements d'état et de fonctionnement de ce dernier. Un exemple d'attaque active est la modification de la table de routage d'un système par un utilisateur non autorisé.

Des exemples d'attaques sont présentés dans [Olovsson 92] et [Khelalfa 00].

2.4 Services de sécurité d'un système de communication

Les services de sécurité sont les propriétés que l'on souhaite obtenir du système de communication. L'ISO a défini cinq types de services de sécurité [ISO 89] : l'authentification, la confidentialité des données, l'intégrité des données, la non répudiation et le contrôle d'accès.

2.4.1 L'Authentification

Dans le cas d'un simple message, le service d'authentification assure que le message provient de l'endroit d'où il prétend venir. Dans le cas d'un échange bidirectionnel, deux aspects sont présents. Il faut assurer que les deux entités sont bien ce qu'elles affirment être. De plus, le service d'authentification doit montrer que la connexion ne peut être brouillée par une troisième entité essayant de se faire passer pour un des deux correspondants.
Ce service permet d'authentifier les entités qui communiquent entre elles, préalablement à tout échange de données. Il a pour but de garantir l'identité des correspondants. On peut distinguer deux types:

- l'authentification de l'entité homologue qui assure que l'entité réceptrice qui est connectée est bien celle annoncée. Son principal objectif est la lutte contre le déguisement.
- l'authentification de l'origine qui assure que l'entité émettrice est bien celle prétendue.

2.4.2 La Confidentialité des données

Ce service assure la protection des informations contre toute divulgation non autorisée [ISO 89]. Il s'agit de s'assurer que les informations sont inaccessibles (ou incompréhensibles) pour les utilisateurs non désignés comme autorisés à y accéder. Le terme information recouvre non seulement les données mais aussi le flux d'informations et la connaissance de l'existence des données ou des communications. Par exemple :

- Observer l'existence ou la non existence d'une donnée (quelle que soit sa valeur)
- Observer la taille d'une donnée
- Observer les variations dynamiques des caractéristiques de la donnée

L'idéal serait de pouvoir protéger l'information contre les divulgations et révélations. Cela a mené vers deux types de services de confidentialité :

a. Le service de confidentialité des données : L'objectif de ce service est d'empêcher des données d'être compréhensibles par une entité tierce non autorisée, le plus souvent en état de fraude passive, c'est-à-dire en écoute de l'information sur le réseau.
   On distingue:
   - la confidentialité intégrale où l'ensemble des données transmises doit être protégé;
   - la confidentialité d'un champ spécifique où la protection est assurée pour quelques données inclues dans une transmission.

b. Le service de confidentialité du flux du trafic : ce service assure la protection des informations qui pourraient être dérivées de l'observation des flux de données. En fait, ce service fournit une protection contre l'analyse de trafic.
   Notons que l'analyse de trafic est un exemple d'attaque passive consistant en la déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence).

2.4.3 L'Intégrité des données

Ces services contrecarrent les menaces actives c'est à dire font en sorte que l'information ne puisse être modifiée que par les personnes autorisées ou seulement par les moyens autorisés.
Modifier une information inclut [Khelalfa 00]:

- L'insertion d'autres données.
- L'effacement de données.
- La modification de données.
- Le réarrangement d'une partie des données.
- Changer l'existence d'une donnée (la créer ou l'effacer).

2.4.4 La Non répudiation

La non répudiation est la propriété qui assure que l'auteur d'un acte ne puisse ensuite nier l'avoir effectué [Khelalfa 00].
Ce service peut prendre l'une des deux formes suivantes :

- Non répudiation avec preuve de l'origine : le destinataire reçoit la preuve de l'origine des données. Cela le protégera de toute tentative de l'expéditeur de nier le fait d'avoir reçu les données ou leur contenu.
- Non répudiation avec preuve de la remise : l'expéditeur de données reçoit la preuve de la remise des données. Cela le protégera contre toute tentative ultérieure du destinataire de nier le fait d'avoir reçu les données ou leur contenu.

2.4.5 Le contrôle d'accès

Ce service assure une protection contre toute utilisation non autorisée des ressources [Khelalfa 00]. Il représente la capacité de limiter et de contrôler les accès aux systèmes et applications via les liens de communication. Pour cela, chaque entité demandant un accès se voit identifiée ou authentifiée afin de lui adapter ses droits d'accès.

2.5 Politique de Sécurité

Olovsson définit une politique de sécurité comme étant l'ensemble des règles qui régissent ce qui est permis et ce qui n'est pas permis dans un système, dans les conditions normales d'opérations [Olovsson 92].
En fait, la politique de sécurité régule la manière avec laquelle les entités peuvent accéder aux objets dans un système (figure 2.1). L'analyse du risque est primordiale dans la définition d'une politique de sécurité. L'analyse du risque est un processus qui identifie toutes les menaces possibles du système. Lorsque la politique de sécurité est définie, elle peut être utilisée pour sélectionner les mécanismes de sécurité qui représentent les mécanismes de base utilisés pour implémenter la sécurité dans un système.

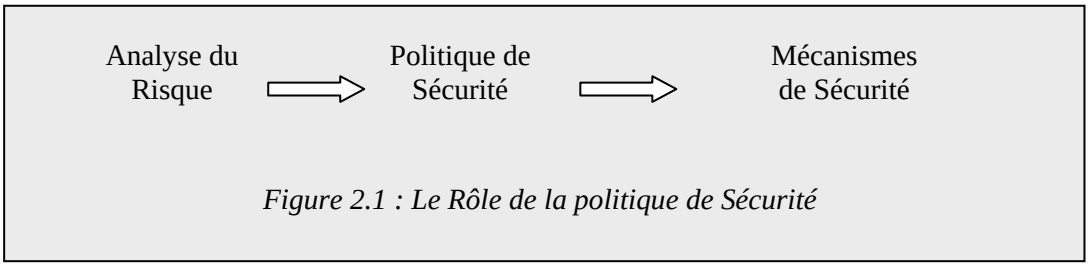

Figure 2.1 : Le Rôle de la politique de Sécurité

2.6 Mécanismes de sécurité

Les mécanismes de sécurité sont employés pour mettre en application les règles indiquées dans la politique de sécurité. Ils peuvent être divisés en trois classes [ISO 89] :

- Mécanismes de prévention : Un mécanisme de prévention est un mécanisme qui empêche une violation de sécurité de se produire avant l'exécution d'un système.

- Mécanismes de Détection : Un mécanisme de détection est employé pour détecter les tentatives de violation de la sécurité et les violations réussies de sécurité, pendant ou après qu'elles se soient produites dans un système.
- Mécanismes de recouvrement : Un mécanisme de recouvrement est un mécanisme utilisé pour restaurer l'état d'avant la violation de la sécurité.

Chaque classe comporte plusieurs mécanismes de sécurité associés à la réalisation des services de sécurité énumérés au point 2.4. Les mécanismes de sécurité appropriés pour un environnement de communication de données sont présentés dans [ISO 89].
Nous abordons dans les sections suivantes les principaux mécanismes de cryptographie et d'authentification importants dans le cadre de cette thèse.

2.7 Les Systèmes Cryptographiques

Avec l'apparition des moyens informatiques, les besoins concernant les informations sensibles sont restés les mêmes : la confidentialité et l'intégrité des données manipulées et stockées. Une technique triviale pour préserver la confidentialité des données consiste à rendre illisible le contenu de l'information. Les techniques de chiffrement permettent de chiffrer le contenu de l'information à toute personne accédant à l'information.
Pour garantir l'intégrité des données, il faut utiliser une technique similaire à celle de la signature manuelle : la signature digitale ou numérique.
Donc, la mise en œuvre de la sécurité au sein d'un système informatique nécessite l'utilisation de mécanismes cryptographiques, qui permettent le chiffrement, le déchiffrement, la signature digitale et la vérification de signature digitale.

2.7.1 Principes de Base

Messages et chiffrement : Un message est appelé texte en clair. Le processus de transformation d'un message de telle manière à le rendre incompréhensible est appelé chiffrement. Le résultat de ce processus de chiffrement est appelé texte chiffré (ou cryptogramme). Le processus de reconstruction du texte en clair à partir du texte chiffré est appelé déchiffrement (figure 2.2).

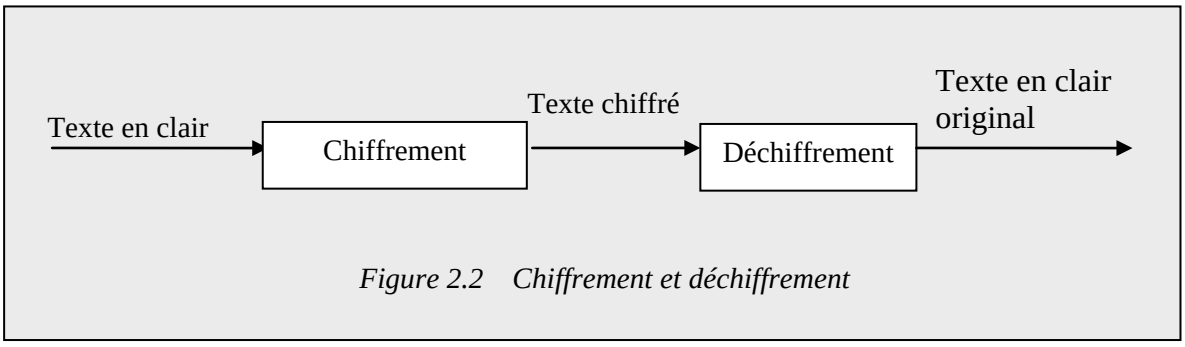

Figure 2.2 Chiffrement et déchiffrement

Le texte en clair est noté M. Ce peut être une suite de bits, un fichier de texte, une image, ….
Du point de vue machine, M n'est rien d'autre que de l'information binaire. Le message chiffré est noté C. La fonction de chiffrement notée E transforme M en C :

$$E(M) = C$$

La fonction de déchiffrement notée D, transforme C en M :

$$D(C)= M$$

Algorithmes Cryptographiques : Un algorithme cryptographique est une fonction mathématique utilisée pour le chiffrement et le déchiffrement. Pour chiffrer un message en clair, on applique un algorithme de chiffrement au texte de ce message. Pour déchiffrer un texte chiffré, on applique un algorithme de déchiffrement au texte chiffré.

On parle d'algorithme restreint si la sécurité de l'algorithme est basée sur le fait que celui-ci est tenu secret. De nos jours, de tels algorithmes ne sont plus adaptés car ils sont faciles à casser.

Les algorithmes modernes de chiffrement utilisent une clef notée k. Cette clef peut prendre une des valeurs parmi un grand nombre de valeurs possibles. L'ensemble des valeurs d'une clef est appelé espace de clefs. La valeur de la clef affecte les algorithmes de chiffrement et de déchiffrement et donc les fonctions de chiffrement et de déchiffrement.

2.7.2 Algorithmes à clef secrète et algorithmes à clef publique

Il y a deux types principaux d'algorithmes à base de clefs : algorithmes symètriques ou à clef secrète et algorithmes asymétriques ou à clef publique.

2.7.2.1 Le Chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrment à clé privée ou chiffrment à clé secrète) consiste à utiliser la même clef pour le chiffrement que pour le déchiffrement. Les algorithmes à clef secrète sont des algorithmes où la clef de chiffrement peut être calculée à partir de la clef de déchiffrement ou vice versa. Dans la plupart des cas, la clé de chiffrement et la clef de déchiffrement sont identiques.

Le chiffrement consiste (figure 2.3) alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles. Ainsi, le moindre algorithme (tel qu'un OU exclusif) peut rendre le système quasiment inviolable quoique la sécurité absolue n'existe pas.

Pour de tels algorithmes, l'émetteur et le destinataire doivent se mettre d'accord sur une clef à utiliser avant d'échanger des messages. Cette clef doit être gardée secrète : la sécurité de l'algorithme repose sur cette clef.

Le principal inconvénient d'un cryptosystème symétrique provient donc de l'échange de clés. Se pose ainsi le problème de la distribution des clés : Pour un groupe de n personnes utilisant un cryptosystème à clés secrètes, il est nécessaire de distribuer n*(n-1)/2 clés.

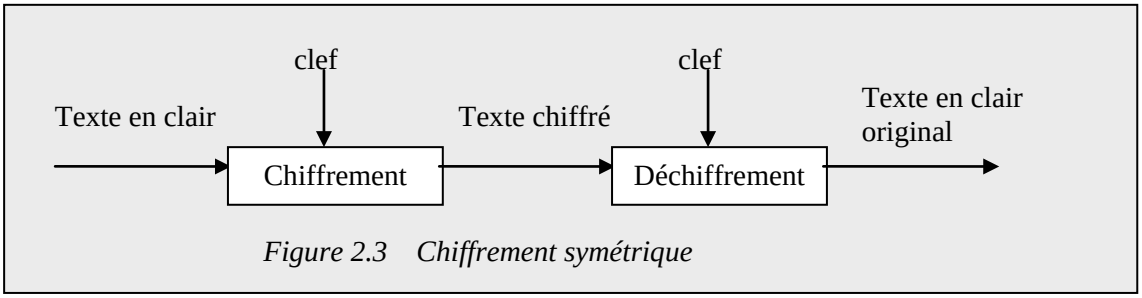

Figure 2.3 Chiffrement symétrique

2.7.2.2 Le Chiffrement Asymétrique

a. Principe du Chiffrement à clé publique

Le paradigme de chiffrement à clés publiques est apparu en 1976 [Diffie 96]. Dans un cryptosystème asymétrique, les clés existent par paires :

- Une clé publique pour le chiffrement
- Une clé secrète pour le déchiffrement

Les algorithmes à clef publique sont différents : ils sont conçus de telle manière que la clef de chiffrement soit différente de la clef de déchiffrement (figure 2.4).

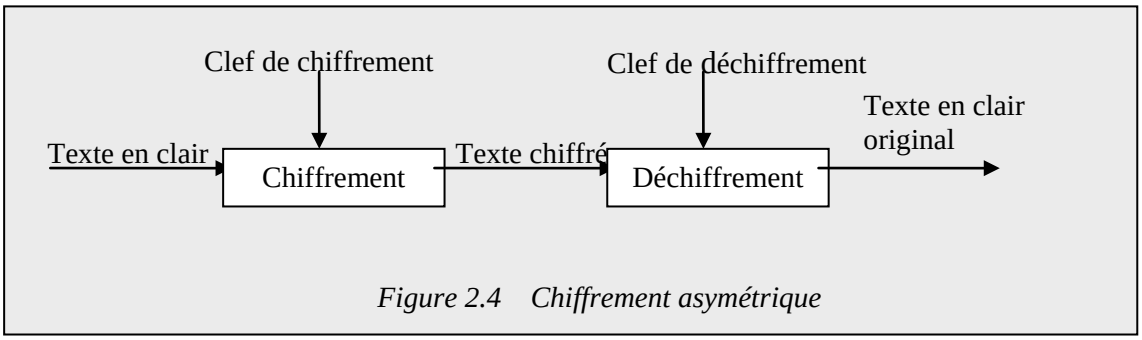

Figure 2.4 Chiffrement asymétrique

De plus, la clef de déchiffrement ne peut pas être calculée (du moins en un temps raisonnable) à partir de la clef de chiffrement. De tels algorithmes sont appelés « à clef publique » car la clef de chiffrement peut être rendue publique. Ainsi, n'importe qui peut utiliser la clef de chiffrement pour chiffrer un message mais seul celui qui possède la clef de déchiffrement peut déchiffrer le message chiffré résultant. Dans de tels systèmes, la clef de chiffrement est appelée clef publique et la clef de déchiffrement est appelée clef privée.

Ce type de systèmes présente les avantages fondamentaux suivants [Meot 93]:

- Confidentialité
- Authenticité

Le premier avantage est la confidentialité car soit Ks *(les clés secrètes)*, et Kp *(les clés publiques)* possédées par un utilisateur, l'une peut être rendue publique et l'autre secrète. Connaissant la clef publique de l'utilisateur A, que l'on peut appeler Kpa, chaque utilisateur peut chiffrer sans cette clef, et seulement A peut déchiffrer grâce à sa clef secrète Ksa.

Le deuxième avantage est l'authenticité : si l'on considère un message qui a été chiffré par un utilisateur avec la clef secrète de A, Ksa, alors chacun peut le déchiffrer avec Kpa, mais seul l'utilisateur A est capable de l'avoir chiffré, car il est le seul à connaître Ksa (figure 2 .5).

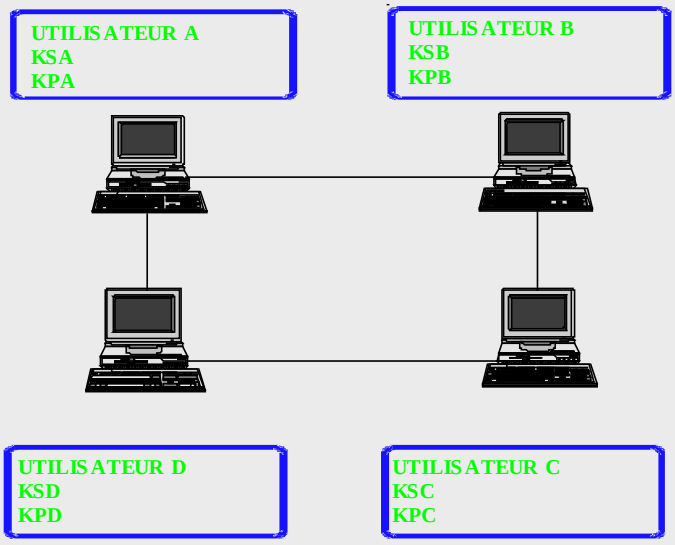

Figure 2.5 Schéma d'explication des avantages d'un système à clé publique

2.7.3 Exemples d'algorithmes de chiffrement

Nous présentons les algorithmes de chiffrement les plus couramment utilisés [Meot 93].

2.7.3.1 Le D.E.S

Le Data Encryption Standard, mis au point dans les laboratoires d'IBM en 1977, a été formalisé au sein de l'ISO et proposé sous le nom de Data Encipherment Algorithm. C'est un algorithme très répandu dans le monde industriel et bancaire. Il est notamment implémenté pour le contrôle des codes liés aux cartes bancaires.
Le principe le plus couramment utilisé consiste à découper un message M en clair (suite binaire codée dans un alphabet quelconque) en un ensemble de blocs U de 64 bits; chacun d'eux sera crypté à l'émission et décrypté à la réception indépendamment des autres blocs, grâce à une clé. Le même algorithme est utilisé pour chiffrer et déchiffrer les données. La clé de chiffrement est identique à la clé de déchiffrement, c'est un algorithme symétrique.
Comme pour les techniques traditionnelles, la difficulté du DES réside dans la communication des clés de cryptage et de décryptage.
Il existe une version du DES assez connue sous le nom de Triple DES, noté aussi 3DES, car il utilise une clé de longueur triple en entrée, soit de 3*64 = 192 bits.

2.7.3.2 L'algorithme R.S.A

L'algorithme RSA (expliqué en Annexe), du nom de ses trois concepteurs américains R. Rivest, A. Shamir et L. Adleman, a été proposé en 1977, puis mis au point en février 1988. RSA est un exemple type d'algorithme asymétrique. C'est une méthode fondée sur la théorie des nombres et permettant de rendre les clés publiques.

La sécurité de cette technique réside dans le choix de très grands nombres de plus de 512 bits et dont la décomposition en facteurs premiers est longue et difficile.
L'inconvénient essentiel de l'algorithme RSA est son temps d'exécution, ce qui rend ce chiffrement inutilisable pour des applications financières dont le temps de réponse doit être instantané. RSA sera donc d'abord utilisé pour la gestion des clés, puis pour la signature des messages.

2.7.4 La Signature électronique

Il est généralement admis que la signature manuscrite d'un document signifie que le signataire convient du contenu et qu'il identifie le document par rapport à une copie. Une signature doit pouvoir jouer un rôle similaire pour les documents électroniques. Elle doit assurer la personne qui reçoit le document électronique de l'identité de l'émetteur et de l'authenticité du document.
La production d'une signature est obtenue par l'application d'un algorithme au message transmis, qui devient signé. Le plus souvent, cette signature sera le résultat d'une transformation cryptographique du message, indépendante de la taille de ce dernier; elle sera de plus de taille réduite [Meot 93].
Le propre de la signature est qu'elle peut être vérifiée par tous les détenteurs de la clé, mais ne pourra être imitée par personne. A première vue, les algorithmes les plus adaptés en matière de signature électronique sont asymétriques (clés publiques).
En transposant les notions de signature et de notaire dans le monde électronique, une garantie supplémentaire peut être apportée par la notarisation: les entités font confiance à un tiers qui assure l'intégrité, l'origine, la date et la destination des données. Le processus sous-entend que ce tiers doit acquérir les informations par des voies de communication très protégées. Ainsi, chaque message émis est envoyé au notaire N qui effectuera un certain nombre d'authentifications afin de s'assurer de l'origine et du contenu; le message sera alors daté et enregistré par N puis envoyé avec un certificat au récepteur.

2.7.5 Fonction de Hachage

Une fonction de hachage (ou fonction de condensation) est une fonction permettant d'obtenir un condensé (haché) d'un texte, c'est à dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé.
Ainsi, le haché représente en quelque sorte l'empreinte digitale (finger print) du document.

Les algorithmes de hachage les plus utilisés actuellement sont :
MD5 : (Message Digest) : créant une empreinte digitale de 128 bits.
SHA (Secure Hash Algorithm) : créant des empreintes d'une longueur de 160 bits.

2.7.5.1 Utilité d'une fonction de hachage

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est à dire que le destinataire peut vérifier que le message n'a pas été altéré durant la communication. Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et le comparer avec le haché accompagnat le document. Si le message

(ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondent pas.

2.7.6 Le Scellement des données

L'utilisation d'une fonction de hachage permet de vérifier que l'empreinte correpond bien au message reçu, mais rien ne prouve que le message a bien été envoyé par celui que l'on croit être l'expéditeur. Ainsi, pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer le condensé à l'aide de sa clé privée (le haché signé est appelé sceau) et d'envoyer le sceau au destinataire. A la réception du message, il suffit au destinataire de déchiffrer le sceau avec la clé publique de l'expéditeur, puis de comparer le haché obtenu avec la fonction de hachage au haché reçu en pièce jointe. Ce mécanisme de création de sceau est appelé scellement.

2.8 Mécanismes d'authentification

Dés l'apparition des systèmes informatiques multi-utilisateurs, le problème de l'authentification des utilisateurs s'est posé, l'accès au système doit être autorisé uniquement aux sujets habilités [Bidan 95][Benmeziane 01a].
La phase d'authentification de l'utilisateur consiste à associer à chaque utilisateur un unique identifiant qui est en général un nom connu par tout le monde, que personne ne peut changer ou créer. La phase d'authentification est divisée en deux parties :

1. L'identification : lors de laquelle l'utilisateur présente son identifiant (il dit qui il est).
2. L'authentification : où l'utilisateur prouve son identité (il prouve qu'il est bien celui qu'il prétend être)

Informellement, l'authentification consiste, pour un sujet donné, à prouver à une entité que son identité est correcte. Autrement dit, les deux entités appelées prouveur et vérifieur vont communiquer pour vérifier que l'identité du prouveur est correcte (la phase d'authentification se termine correctement) ou non (la phase d'authentification échoue).
De manière plus formelle, ISO définit l'authentification en termes de deux services [ISO 89]: authentification de l'entité homologue et authentification de l'origine des données.

a. Authentification de l'entité homologue : Ce service est prévu pour être utilisé pour confirmer les identités d'une ou plusieurs entités connectées à une ou plusieurs autres entités. Il garantit qu'une entité n'essaye pas de se déguiser ou de rejouer une ancienne connexion de façon non autorisée. Deux schémas d'authentification sont possibles dans ce cas :
Authentification unilatérale : seulement une partie s'authentifie à l'autre.
Authentification mutuelle : les deux parties (entités) s'authentifient l'une à l'autre.

b. Authentification de l'origine des données : Ce service confirme la source d'une unité de données. Il n'assure pas de protection contre la duplication ou la modification des unités de données.

Différentes méthodes existent pour assurer l'authentification. Certaines dépendent des techniques cryptographiques et d'autres non. Dans ce qui suit, nous allons décrire ces méthodes en ressortant à chaque fois leurs vulnérabilités.

2.8.1 Mécanismes d'authentification non cryptographiques

2.8.1.1 Mots de passe

Le mot de passe ou PIN (personal identification number) est un mécanisme sur lequel beaucoup de systèmes d'authentification sont basés. Cependant, ces systèmes sont vulnérables. Tout d'abord, les mots de passe peuvent être révélés ou devinés. Plusieurs mesures et recommandations sont établies pour le choix des mots de passe [Ford 94]. En plus de ces vulnérabilités, l'écoute de la ligne peut révéler les mots de passe. Pour éviter ceci, des mécanismes de protection de mots de passe sont mis en œuvre, sans avoir recours à la cryptographie, la protection peut être assurée en utilisant des fonctions à sens unique.

Rappelons qu'une fonction à sens unique f(x) = y comporte les propriétés suivantes :

- Etant donné x, il est facile de calculer y= f(x).
- Etant donné y, il est difficile de calculer x

Supposons que le mot de passe correct de l'identité id est p. Au niveau du terminal où un processus d'authentification prend place (figure 2.6), l'identité id et un mot de passe p' sont entrés. La valeur q'=f(p') est calculée et est envoyée au vérifieur avec l'identité id.
Le vérifieur tient pour chaque id la valeur q générée pour le mot de passe correct p. Si q=q' alors le bon mot de passe est entré et l'identité authentifiée.

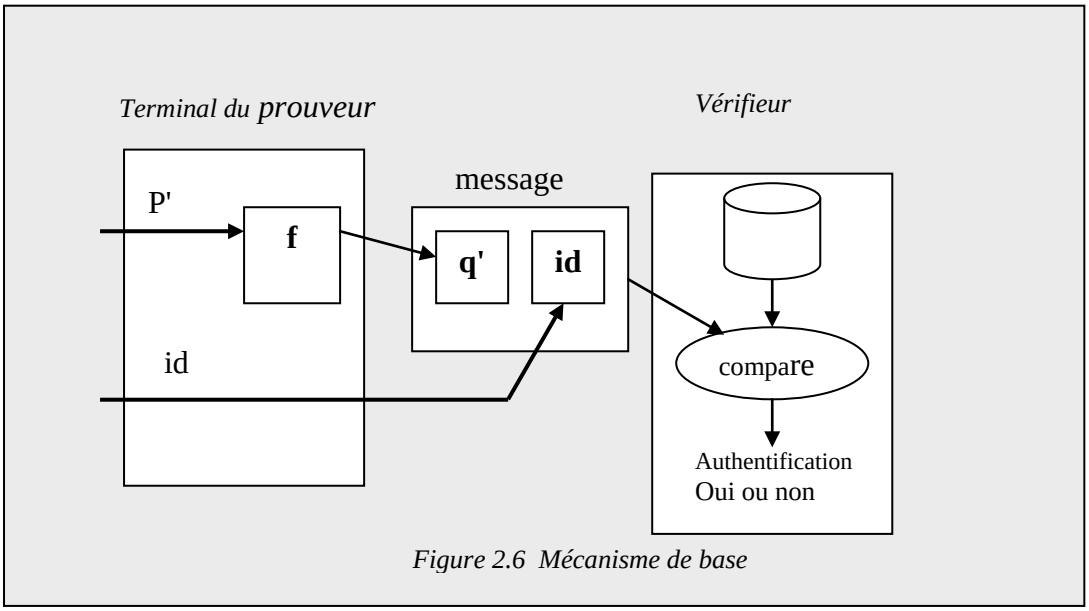

Figure 2.6 Mécanisme de base

Ce schéma simpliste a un inconvénient: il est facile pour un attaquant de construire une table de valeurs de q correspondant aux valeurs de p en s'assurant que la table contient les valeurs les plus probables de p. Ainsi, en construisant une table significative, un attaquant peut contrôler passivement des tentatives d'authentification et obtenir quelques mots de passe associés à des usagers. Cet inconvénient peut être contourné avec une simple modification. Il suffit d'appliquer la fonction à sens unique à une chaîne contenant la concaténation de l'identité et du mot de passe.

a. Prévenir la compromission du vérifieur

Une autre menace potentielle des mécanismes des mots de passe est la compromission du fichier de mots de passe du vérifieur à travers une attaque interne. Le mécanisme de mots de passe décrit précédemment offre une certaine mesure de protection contre de telles attaques. Du moment que les valeurs stockées dans la base de données sont générées à partir de fonction à sens unique. Connaître la valeur de q ne donne pas à un attaquant la possibilité de connaître la valeur de p. Cependant, la connaissance de q permet à un attaquant de générer un message d'authentification qu'il présentera au vérifieur.
Pour prévenir cette attaque, on peut appliquer la fonction à sens unique au niveau du vérifieur (figure 2.7).

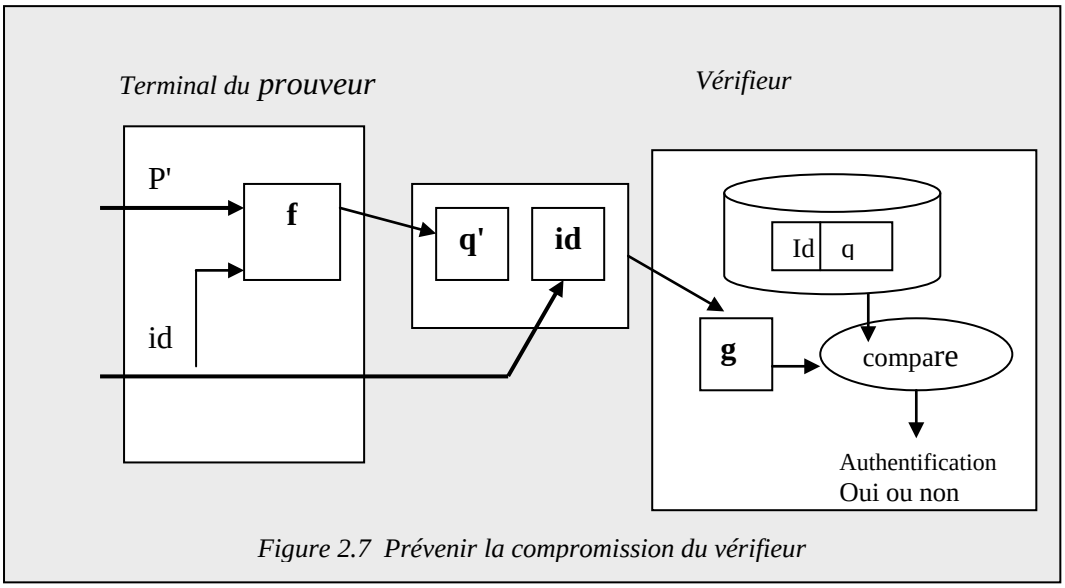

Figure 2.7 Prévenir la compromission du vérifieur

b. Prévenir le rejeu : Replay

Lorsqu'une communication chiffrée est établie entre deux sites reliés par un réseau non-sûr, il est possible qu'un intrus intercepte des messages, et puisse renvoyer certains de ces messages tel quels à des moments où ceux-ci pourraient être mal interprétés par le destinataire, et ceci peut être fait alors que le pirate ne connaît pas le contenu du message ni aucune des méthodes cryptographiques utilisées dans le protocole de communication.
Le mécanisme de mots de passe protégés peut être étendu pour prévenir de telles attaques. L'idée est d'introduire une valeur nrv non répétitive. Le vérifieur doit examiner si nrv n'a pas déjà été utilisée. Dans le cas positif, la requête d'authentification est rejetée et considérée comme rejeu. (plus de détails sont donnés dans le point 2.3)

2.8.1.2 One Time Password

Dans les mécanismes one time password, un mot de passe différent est utilisé à chaque authentification dans le but de prévenir les attaques de rejeu.
Un exemple de mécanisme basé sur OTP est illustré dans la figure 2.8. Un utilisateur a un périphérique personnel d'authentification. Une valeur secrète dsv est stockée dans le

périphérique. Pour s'authentifier au vérifieur, l'utilisateur donne un mot de passe p' au périphérique. Le périphérique affiche une valeur r' calculée en appliquant les fonctions à sens

unique f et g respectivement à p' et à dsv et ts (estampille courante). La valeur r' et l'identité sont ainsi envoyées au vérifieur. Ce dernier, garde pour chaque id, la valeur dsv et la valeur q=f(p,dsv). A l'arrivée de la requête d'authentification, le vérifieur calcule r = g(q, dsv, ts). La comparaison de r et r' déterminent si l'authentification est acceptée.

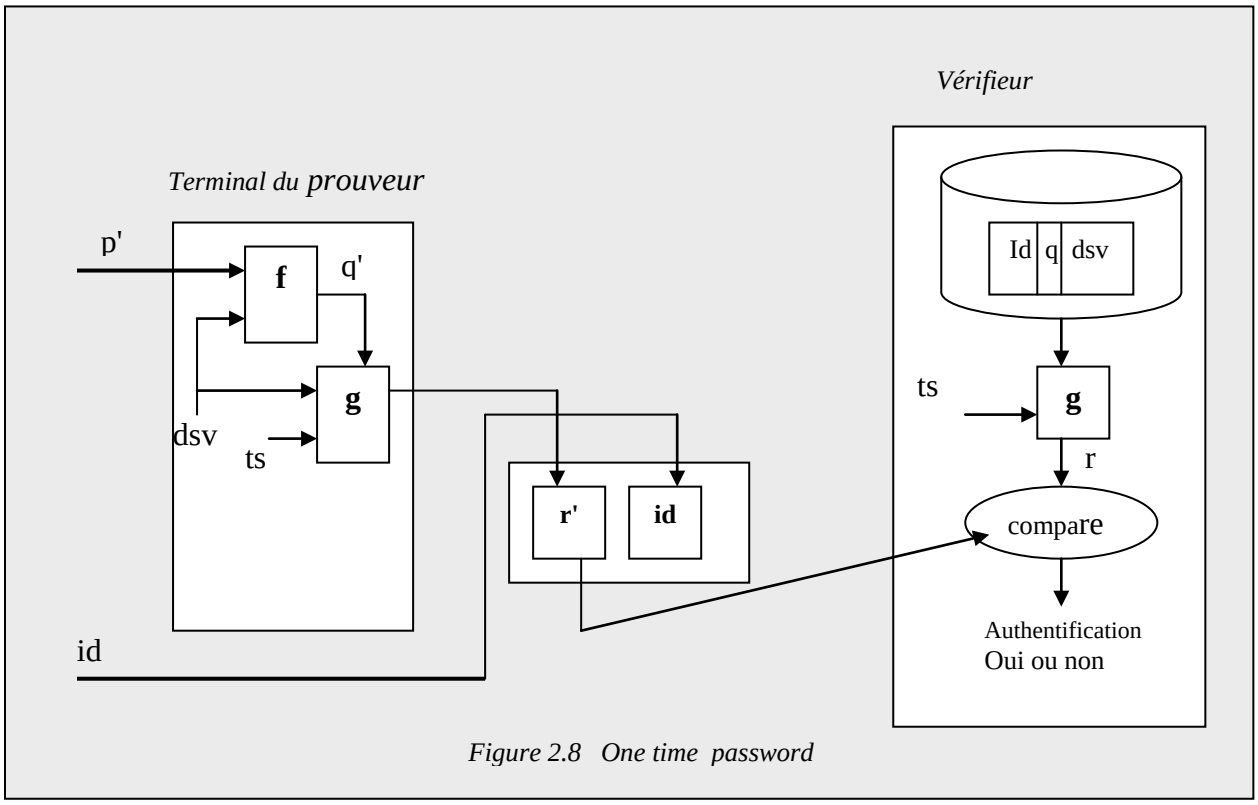

Figure 2.8 One time password

2.8.1.3 Challenge-Response

Les schémas basés sur les mots de passe peuvent être augmentés du principe <challenge response> qui est également employé dans les mécanismes d'authentification basés sur la cryptographie. Ce principe peut améliorer la résistance aux attaques par rejeu, mais toujours en augmentant la compléxité du protocole d'authentification. Notons que dans le mécanisme de mots de passe protégés, il y a deux problèmes significatifs :

- Le premier est la nécessité de maintenir une synchronisation pour connaître les valeurs nrv.
- Le second problème est la difficulté pour le vérifieur de vérifier que la valeur nrv est répétée.

L'approche challenge-réponse remédie à ces problèmes. En effet, le vérifieur envoie au prouveur un nrv spécifique pour une tentative d'authentification donnée à l'avance (figure 2.9 et figure 2.10). Le nrv est connue comme challenge.

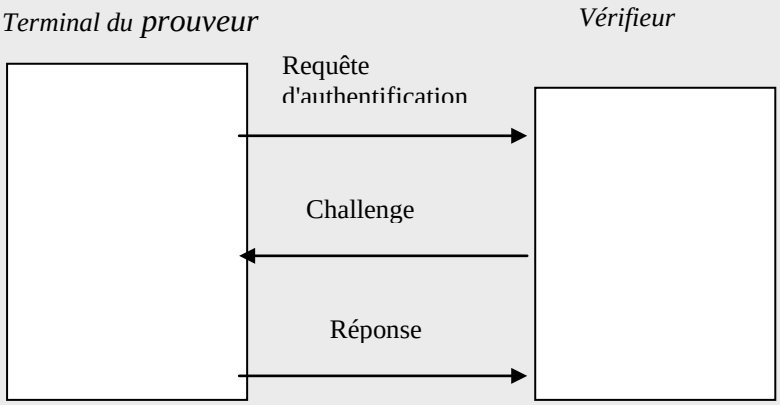

Figure 2.9 Challenge - Response

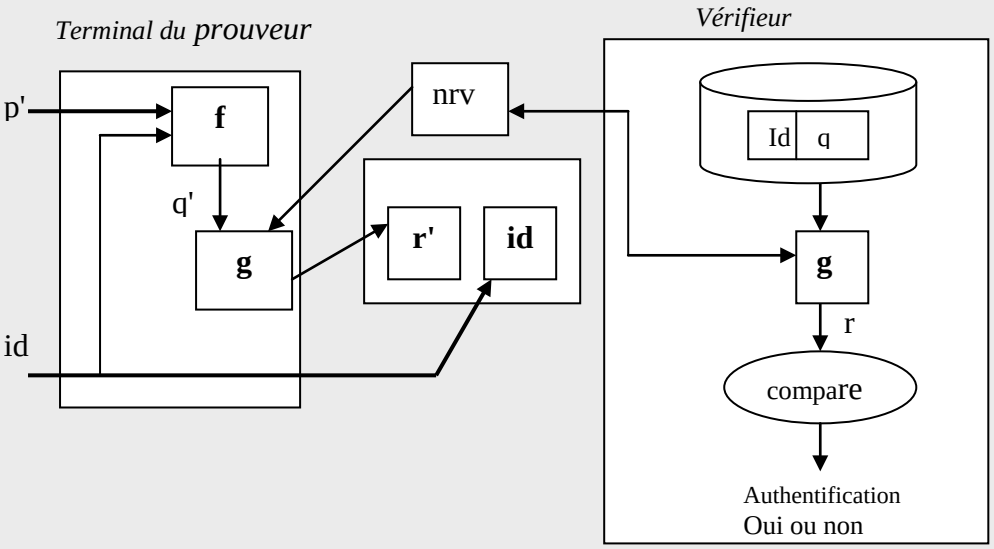

Figure 2.10 Mécanisme challenge - Response

2.8.2 Utilisation des techniques cryptographiques dans les mécanismes d'authentification

Les mécanismes d'authentification qui utilisent des techniques cryptographiques sont basés sur le principe de convaincre le vérifieur que puisqu'un prouveur connaît un certain secret alors il a prouvé qui il est. Dans les mécanismes d'authentification, les techniques à clé symétrique ou à clé publique peuvent être employées.

2.8.2.1 Techniques symétriques

Dans l'approche la plus simple, le vérifieur et le prouveur partagent une clé symétrique. Le prouveur crypte ou scelle un message en utilisant cette clé. Si le vérifieur réussit à décrypter le message ou à vérifier que le sceau est correct alors le vérifieur peut être sûr que le message

provient du prouveur. Le contenu du message crypté doit inclure une valeur non répétitive comme protection contre le rejeu.
L'approche basée sur les algorithmes symétriques n'est pas pratique dans un réseau large, car il est nécessaire que chaque vérifieur maintienne une clé secrète avec chaque prouveur. Le problème d'explosion de clés est évité en introduisant un serveur d'authentification on-line digne de confiance avec lequel chaque vérifieur et chaque prouveur partagent une clé.

2.8.2.2 Techniques basées sur la clé publique

L'approche est similaire, le prouveur signe un message en utilisant sa clé privée. Le vérifieur vérifie la signature en utilisant la clé publique du prouveur. Si la signature est correcte alors le vérifieur peut s'assurer de l'identité du prouveur. De même, le message doit contenir une valeur non répétitive comme prévention aux rejeux. Ce type de mécanisme est illustré dans la figure suivante :

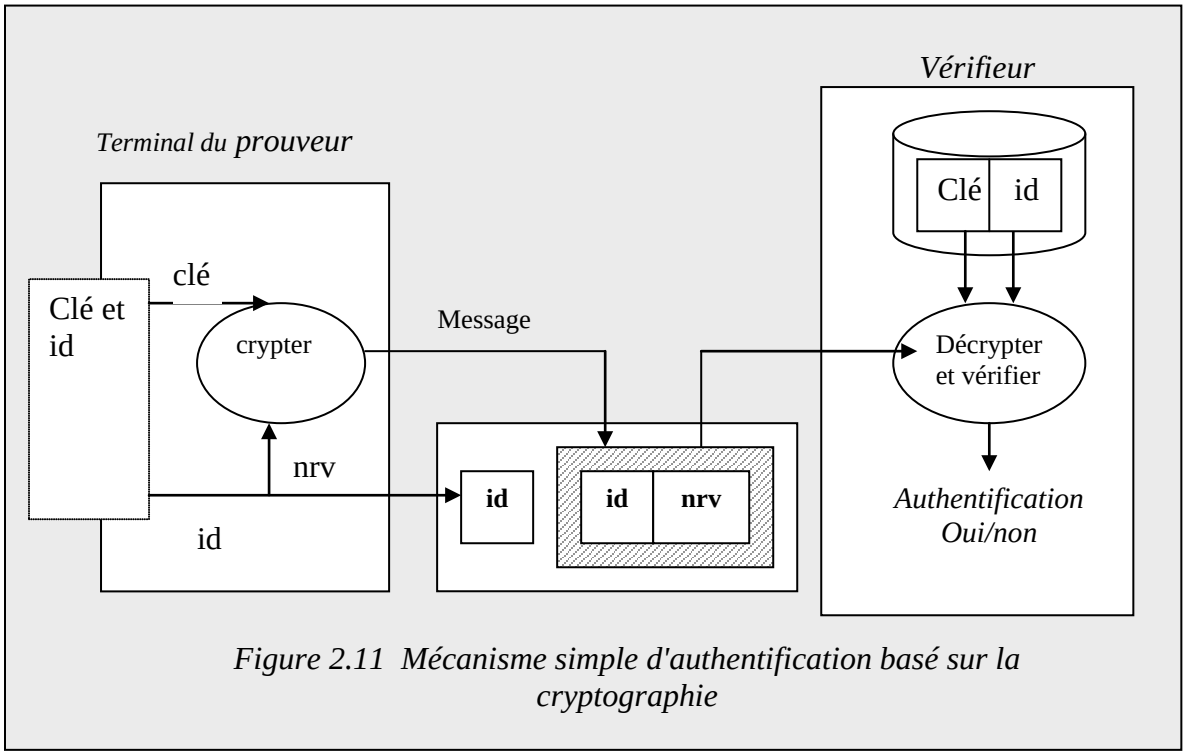

Figure 2.11 Mécanisme simple d'authentification basé sur la cryptographie

Avec les cryptosystèmes à clé publique, il n'est pas nécessaire de disposer de serveurs d'authentification on-line, car les caractéristiques des systèmes à clé publique évitent le problème d'explosion de clés. Néanmoins, il est nécessaire pour les vérifieurs d'obtenir des clés publiques certifiées des prouveurs. Ces certificats sont obtenus de serveurs appelés: serveur d'authentification off-line. Ces derniers présentent divers avantages par rapport aux serveurs on-line:

- Les délais de réponse associés à l'accès au serveur on-line sont évités.
- Le serveur a besoin de moins de capacité de communications.
- Les entités peuvent s'authentifier même si le serveur n'est pas disponible.

2.8.3 Utilisation des valeurs non répétitives

Les valeurs non répétitives sont utilisées dans les messages d'authentification pour assurer qu'une tentative de rejeu va être détectée. Les sources potentielles de telles valeurs sont:

- Un numéro de séquence maintenue entre le prouveur et le vérifieur.
- Estampilles.
- Une valeur envoyée précédemment au vérifieur (challenge).

1. avec les numéros de séquence, le prouveur et le vérifieur s'entendent en avance sur la politique de numérotation des messages. L'approche générale est qu'un message avec un numéro particulier n'est accepté qu'une seule fois (ou seulement une fois pendant une période de temps). Les messages reçus par le vérifieur sont contrôlés et toute tentative d'authentification est rejetée si la politique est violée. L'utilisation de numéros de séquence cause néanmoins un temps de déperdition (overhead). Le vérifieur doit maintenir les informations d'état de chaque prouveur.

2. Le champ d'authentification est estampillé avec la date courante (timestamp), en supposant que les différentes horloges locales sont bien synchronisées. Dans ce cas, tout message rejoué sera détecté car il sera trop vieux. On peut améliorer ce mécanisme en mémorisant un historique des signatures récemment envoyées et de vérifier que toute nouvelle signature n'est pas déjà présente dans l'historique. Ce système permet de détecter le rejeu même si les horloges sont désynchronisées.

3. Valeurs aléatoires émises à travers les challenges : méthode très puissante car elle offre au vérifieur un contrôle direct à travers les messages d'authentification. La caractéristique principale est que ces valeurs sont imprévisibles, avec une probabilité suffisamment grande, non répétitive. Cette méthode évite le problème de gestion des numéros de séquence et les vulnérabilités des estampilles mais le principal inconvénient est qu'elle requiert plus de messages dans le protocole.

2.8.4 Exemples de Protocoles d'authentification : Kerberos

Kerberos est un protocole d'authentification à tierce partie digne de confiance conçu pour les réseaux Tcp/Ip. Il est basé sur la cryptographie à clé secrète. Le serveur d'authentification appelé par convention Kerberos partage une clé secrète différente avec chaque entité du réseau qu'elle soit client ou serveur.
Kerberos a été initialement développé au MIT et son modèle est basé sur le protocole à tierce partie de confiance de Needham et Schroeder [Schneier 96].
Kerberos offre les services suivants:

1. Authentification
Kerberos fournit aux principaux un moyen sûr de s'identifier vis à vis des autres principaux du réseau. Il maintient une base de données de sécurité.

2. Confidentialité
Kerberos peut fournir des clés de session à deux principaux qui désirent communiquer de façon secrète. Ces clés sont à durée de vie limitée et peuvent être utilisées par les principaux selon leur gré.

L'authentification dans kerberos est fondée sur le modèle de distribution de clés. Pour s'authentifier, le principal dispose de deux types de preuves d'identité : le ticket et l'authentifieur.

Un ticket est utilisé pour passer au serveur, de manière sûre, l'identité du client pour qui le ticket a été émis. Il contient également des informations que le serveur peut utiliser pour s'assurer que le client qui utilise le ticket est bien celui à qui le ticket a été délivré. Le ticket de kerberos a la forme suivante:

{ serveur S, client C, adresse du client, durée de vie, Ks,c clé de session entre C et S }Ks

Un ticket est valable pour un seul serveur et un seul client. Il contient le nom du client, le nom du serveur, l'adresse réseau du client, une datation et une clé de session. Cette information est chiffrée avec la clé secrète du serveur. Une fois que le client obtiend ce ticket, il peut l'utiliser plusieurs fois pour avoir accès au serveur, jusqu'à ce que le ticket expire. Le client ne peut pas déchiffrer le ticket (il ne connaît pas la clé secrète du serveur), mais il peut le présenter au serveur sous sa forme chiffrée. Personne ne peut espionner le réseau pour lire ou modifier les tickets qui passent.

Un authentifiant est une accréditation supplémentaire présentée avec ce ticket.
L'authentifiant est une pièce d'identité provisoire engendrée par le client dans le but de signer son message. Il contient le nom et l'adresse du client, ainsi qu'une date d'émission afin d'éviter le rejeu. Le tout est chiffré avec la clé de session entre C et S:

{C, adresse, date}Ksc

A l'inverse des tickets, le client peut créer des authentifiants tant qu'il veut puisqu'il possède la clé Ksc, mais cette clé étant réservée à l'utilisation entre lui et le serveur S, lui seul est censé l'avoir en dehors de S et il ne peut donc pas l'utiliser pour se faire passer pour un autre principal.
Le fonctionnement de kerberos est décrit en détail dans [Schneier 96].

2.9 Conclusion

La sécurité informatique est un axe crucial et complexe. Ce chapitre a introduit les concepts de base et a présenté les principaux mécanismes de sécurité employés notamment ceux relatifs à la cryptographie et à l'authentification. Le chapitre suivant est consacré à l'étude de la sécurité dans les environnements mobiles en insistant sur les nouvelles menaces que posent ces systèmes.

3.1 Introduction

L'apparition de la mobilité a changé la nature des systèmes distribués à grande échelle. De nouveaux services ont dû être développés pour les réseaux fixes afin d'offrir une disponibilité globale aux utilisateurs [Samfat 94]. Autrement dit, les utilisateurs mobiles doivent pouvoir accéder à des services à partir d'un ensemble de situations différentes. Ce phénomène a introduit de nouveaux besoins en sécurité en comparaison aux réseaux fixes traditionnels. En effet, la sécurité des communications sans fil peut être compromise plus facilement que celle des communications avec fils, particulièrement lorsque les transmissions s'établissent sur de grandes distances et lorsque les utilisateurs sont autorisés à traverser des domaines de différents pays [Horlait 01].
Par conséquent, la mobilité a crée de nouveaux besoins en sécurité pour les réseaux mobiles par rapport aux problèmes connus et relatifs aux réseaux fixes. Il est donc nécessaire d'identifier les faiblesses propres à un tel environnement.

Dans ce chapitre, nous allons d'abord introduire les menaces et les brèches de sécurité relatives aux réseaux cellulaires. Nous étudierons par la suite les challenges que posent ces réseaux au concepteurs d'architectures de sécurité. Nous citerons les approches de sécurité adoptées dans les environnements mobiles et présenterons dans plus de détails les mécanismes d'authentification.

3.2 Types de menaces affectant les communications mobiles

Dans cette section, nous nous intéressons aux menaces qui affectent les communications dans le contexte mobile [Cox 96]. Néanmoins, avant de relater les faiblesses des réseaux mobiles et les malveillances qui s'y rapportent, rappelons brièvement l'architecture des réseaux mobiles. L'architecture présentée (figure 3.1) ci-dessous sera l'architecture de référence dans la suite du document.

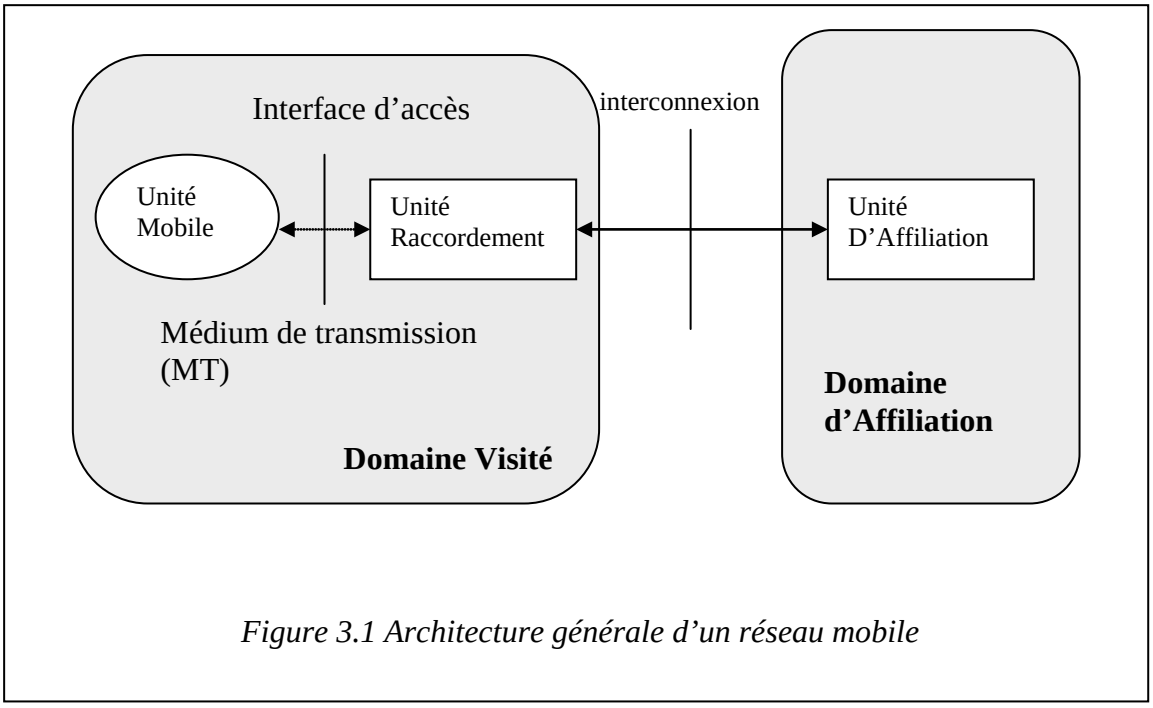

Figure 3.1 Architecture générale d'un réseau mobile

Notons que du point de vue de la sécurité, l'UA (unité d'affiliation) peut être vue comme l'autorité administrative responsable d'un domaine auquel est rattaché le mobile durant une longue période. Pendant ses déplacements, le mobile pourrait avoir à traverser des domaines différents, il serait donc amené à se connecter à une UR (unité de raccordement) qui peut appartenir au domaine d'affiliation comme à un autre domaine visité.

Dans [Ford 94], nous retrouvons une classification des exigences en sécurité pour les réseaux de communication. En effet, sécuriser un système requiert les besoins fondamentaux définis précédemment, à savoir :

- La confidentialité,
- L'intégrité,
- La disponibilité,
- La Légitimité.

Les réseaux mobiles de part leurs structures sont plus sensibles à ces besoins que les réseaux fixes traditionnels [Cox 96]. Ceci est du essentiellement au manque de protection physique au niveau de l'interface d'accès et au médium de transmission entre l'unité mobile et l'unité de raccordement qui est accessible à tous. Dans ce qui suit, nous allons décrire comment ces vulnérabilités favorisent certains types de menaces.

3.2.1 Manque de protection physique

Dans les réseaux fixes, chaque équipement de terminaison ou équipement terminal (terminal, modem, téléphone) est connecté physiquement à un port unique relié à un commutateur. La connexion se fait à travers un câble dédié. Comme l'installation du câble est généralement assurée par le fournisseur de service (par exemple l'opérateur du réseau téléphonique), ce dernier est alors pratiquement certain que la transmission provient réellement de l'abonné légitime.
Cependant, dans le contexte mobile, cette hypothèse n'est plus fondée, l'authentification de l'utilisateur dans un réseau mobile devient incertaine [Samfat 96]. Les malveillances qui exploitent le manque de protection physique portent atteinte essentiellement à la légitimité de service, et peuvent être résumés comme suit :

- *Le déguisement (ou mascarade)* : Dans ce cas, l'attaquant se substitue à l'utilisateur légitime et obtient ainsi un accès illicite au réseau [Cox 96].
  L'attaquant tente de se faire passer pour une personne ou une machine qu'il n'est pas. Par exemple, un site mobile peut tenter de se faire passer pour un serveur du site qu'il visite. Le mobile risque donc en cas de succès de pouvoir accéder à des services réservés aux machines appartenant au domaine en question. De plus, la facturation de ces services se fera au détriment de l'utilisateur piraté.

- *Le vol de l'équipement d'accès au réseau mobile* : Un attaquant ayant volé l'unité mobile de l'utilisateur (par exemple, la carte SIM dans le cas de GSM) peut avoir accès au réseau.

- *La fraude* : cette attaque concerne particulièrement la fraude à l'abonnement. En effet, dans le cas des réseaux fixes, la solvabilité de l'utilisateur est garantie par le lieu

physique du raccordement au réseau. La facture relative aux services utilisés est automatiquement envoyée à l'adresse ou a été installée la ligne câblée. Cependant, un utilisateur mobile malveillant peut lors de la phase d'abonnement donner une fausse identité et une fausse adresse. Ces dernières informations n'étant pas solvables, la facture sera impayée.

3.2.2 Transmission sur la voie radio

Dans les réseaux cellulaires, les données transitent par la voie radio et sont donc susceptibles d'être captées et écoutées par une tierce personne munie d'un récepteur radio adéquat [Samfat 96]. Les menaces qui en découlent sont :

- L'écoute : peut être réalisée indifféremment par des sites mobiles ou par des sites fixes, simplement en réceptionnant et en copiant des paquets de données, ce qui est particulièrement facile avec la majeure partie des médiums sans fil [Baggio 95]. Cette attaque porte atteinte à la confidentialité des données de l'utilisateur.

- La modification : Un tiers peut capter des données, les modifier et les retransmettre au destinataire. Cette attaque active porte atteinte à l'intégrité des messages transférés.

- Le « hijaking » : un utilisateur frauduleux peut capturer le signal émis par la station mobile de l'utilisateur et en même temps accroître sa puissance d 'émission. L'attaquant peut ainsi prendre le contrôle du canal alloué privant l'abonné de la disponibilité de service [Samfat 95]

Nous pouvons récapituler les différentes attaques qui exploitent les faiblesses propres à un environnement mobile par la table suivante [Samfat 96]:

	Confidentialité	Intégrité	Disponibilité	Légitimité	Comptabilité
Manque de Sécurité physique	---	---	---	Mascarade	Fraude
Médium accessible par tous	Ecoute des données	Modification des données	hijacking	hijacking	---

3.3 Challenges

Les réseaux sans fil étendent la flexibilité des communications et du calcul. Cependant, l'environnement sans fil est plus dynamique, moins robuste et plus ouvert aux intrusions et à la fraude que tout réseau filaire. Cet ensemble de facteurs pose des challenges aux concepteurs d'architectures de sécurité.
Dans un article intitulé : « The Challenges of Mobile Computing » [Forman 94] qui récapitule les différences entre les environnements filaires et sans fil et les problèmes que les réseaux sans fil posent aux développeurs de logiciels. Forman et Zahorjan ont distingué trois besoins essentiels : l'utilisation des réseaux sans fil, la possibilité de changer de location et le besoin d'une portabilité non encombrante. Les remarques et conclusions des auteurs quoique

énoncées en 1994, demeurent valables de nos jours [Curtis 01]. Les auteurs insistent sur le fait que le plus grand défi pour les concepteurs est d'adapter les conceptions qui ont si bien fonctionné dans les environnements fixes aux environnements mobiles. Néanmoins, nous noterons que dans le domaine de la sécurité, c'est donc rajouter une incertitude à l'équation [Curtis 01].
Dans ce qui suit, nous allons identifier les premiers challenges des environnements mobiles pour la sécurité et l'authentification en utilisant les trois catégories proposées par Forman et Zahorjan.

3.3.1 Challenge 1 : Utilisation des liaisons sans fil

A plusieurs égards, l'utilisation des liaisons sans fil dans un réseau pose des problèmes qu'on résumera ci-dessous :

Faible largeur de bande passante : La vitesse à laquelle les réseaux sans fil opèrent augmente avec l'évolution de la technologie, en général. Cependant, les débits de transfert de données restent plus faibles que ceux offerts par les infrastructures fixes.

Transmission des données : Lorsque dans un réseau sans fil, les données sont transmises en utilisant les ondes radio, quiconque peut écouter et espionner la communication en utilisant un équipement de moindre coût [Curtis 01]. De plus, ces intrusions sont passives et donc difficiles à détecter.

3.3.2 Challenge 2 : La mobilité de l'utilisateur

Comme mentionné précédemment, dans les environnements mobiles, l'utilisateur est libre de se déplacer tout en maintenant un lien au réseau. Les contraintes liées à cet avantage, décrites au chapitre 1, peuvent être résumées :

- *Déconnexions et Reconnexion*
- *Connexions aux réseaux hétérogènes*
- *Migration d'adresses*
- *Informations dépendantes de la la localisation* : Dans un réseau filaire conventionnel, les emplacements des périphériques est relativement statique et connues par l'administrateur du système. Dans un environnement sans fil, les emplacements changent fréquemment. L'infrastructure du réseau sans fil doit non seulement répondre aux besoins de changement dans le but d'offrir des services aux utilisateurs, mais également fournir des services de sécurité qui protègent les informations de location.

3.3.3 Challenge 3 : Portabilité :

En vue d'exploiter les potentialités des réseaux sans fil, les utilisateurs exigent des périphériques de communication qu'ils peuvent porter aisément. Une implication directe pour la sécurité est le vol. La forme portable impose d'autres limitations aux concepteurs qui, de leur coté, posent aussi des limitations aux solutions de sécurité et d'authentification.

Vitesse du processeur : La puissance de traitement délivrée par les circuits intégrés utilisés dans les mobiles, quoique augmentant de plus en plus, ne peuvent pas approcher les machines

fixes traditionnelles. Les algorithmes de chiffrement et d'authentification nécessitent beaucoup de traitements. Par conséquent, la puissance de traitement disponible dans les mobiles contraint le choix des concepteurs de sécurité pour les environnements sans fil [Asokan 94].

Capacité de stockage limitée : Pour des raisons similaires, le volume de données pouvant être stocké dans un mobile est limité comparé à celui offert par une machine traditionnelle. Ce facteur influe également sur les choix des solutions de sécurité pour les réseaux sans fil.

Capacité de traitement : Tout mobile opère sur une batterie. Tout traitement du processeur réduit la durée de vie de la batterie. D'un point de vue de l'utilisateur, bien que la sécurité est d'une grande importance. Son implémentation représente un temps de déperdition (overhead).

A l'issue de cette section, nous pouvons conclure que les concepteurs d'architectures de sécurité pour les réseaux sans fil doivent relever les challenges posés par ces derniers.

3.4 Approches de sécurité dans les environnements mobiles

Pour pallier aux vulnérabilités des environnements mobiles, deux types d'approches pour élaborer une architecture de sécurité sont possibles [Samfat 96] : l'approche préventive et l'approche analytique.
L'approche préventive se base sur des mécanismes d'authentification : dans ce cas, l'utilisateur doit fournir une identification et la prouver par le biais d'un secret qu'il est le seul à partager avec une entité mandatée capable de vérifier la solvabilité de ce dernier.
Dans l'approche analytique, les actions effectuées sur le système sont enregistrées puis analysées à posteriori afin de détecter les auteurs d'actions litigieuses. Dans ce qui suit, nous allons décrire ces deux approches.

3.4.1 Approche préventive

Dans cette approche, il est nécessaire de mettre en œuvre des protocoles d'authentification [Curtis 01] qui assurent que les entités communicantes sont vraiment ce qu'elles prétendent être. Dans les réseaux fixes, plusieurs protocoles d'authentification ont été développés. La plupart utilisent les clés secrètes partagées nécessitant un serveur d'authentification. Dans le cas général, il est nécessaire d'avoir une autorité en laquelle les utilisateurs puissent avoir confiance. C'est sur cette approche que sont basés les protocoles connus tels que Kerberos [Shneier 96] et Kryptoknight [Bird 95].
Dans les réseaux mobiles, le principe d'authentification est relativement nouveau. En fait, dans les premiers réseaux cellulaires il n'y a pas d'authentification mais une identification. L'unité mobile, désirant se connecter au réseau, transmet à la station de base une identification composée d'un numéro de téléphone et d'un numéro de série de fabrication de mobile. Donc, aucune preuve de cette identification n'est fournie par le mobile [Uskela 97]. Actuellement, le développement des réseaux cellulaires a connu l'introduction des mécanismes d'authentification que nous décrirons dans la partie 3.5.

3.4.2 Approche analytique

Dans cette approche, l'utilisateur mobile est constamment surveillé. Le système de sécurité vérifie que l'activité de l'utilisateur est bien conforme aux règles de sécurité prédéfinies et une action sera entreprise lorsque le comportement de l'individu dévie de la normale [Zimmerman 02]. Lorsque cette analyse est effectuée en temps réel on parlera de détection d'intrusions. Les premiers systèmes de détection d'intrusion ont été développés pour les réseaux fixes. Contrairement aux réseaux fixes, très peu de systèmes de détection d'intrusion ont été développés pour les réseaux mobiles [Molva 97].

Dans le contexte de notre étude, nous nous intéressons à l'approche préventive et particulièrement à l'authentification.

3.5 Authentification dans les environnements mobiles

La mobilité à travers un réseau n'est pas sans rappeler la mobilité dans le monde réel ; lorsqu'une personne voyage d'un pays à l'autre, elle doit souvent effectuer des démarches administratives afin d'obtenir une accréditation pour pouvoir rester temporairement dans le pays visité. Ces démarches peuvent être des procédures pour l'obtention d'un visa ou d'une carte de séjour et elles varient d'un pays à l'autre. Par analogie, nous retrouvons les mêmes procédures dans les réseaux mobiles partagés en domaines.
Une variété de protocoles ont été proposés pour l'authentification dans les réseaux sans fil. Certains ont été proposés pour les intégrer dans les services de sécurité des systèmes mobiles de seconde génération existants et d'autres pour l'utilisation dans les systèmes de Troisième génération. Par rapport aux systèmes cryptographiques de base appliqués, certains protocoles utilisent les cryptosystèmes à clé secrète et d'autres utilisent des cryptosystèmes à clé publique ou encore se basent sur un système hybride.
Nous allons adopter cette classification pour présenter les protocoles d'authentification proposés dans la littérature sans oublier d'étudier, à titre d'exemple, les protocoles d'authentification adoptés par certains systèmes de seconde génération tel GSM et de troisième génération tel que UMTS.

3.5.1 Protocoles d'authentification basés sur les clés secrètes

La majorité des protocoles d'authentification proposés dans la littérature ou intégrés dans les systèmes existant se basent sur un cryptosystème à clé secrète [Curtis 01].
Dans cette section, nous commençons par présenter l'authentification dans GSM et CDPD. Puis, nous présenterons les travaux de Refik et Molva qui ont conduit à une série de protocoles d'authentification basés sur les clés secrètes.

3.5.1.1 Etude de cas : Sécurité et authentification dans GSM

Avant d'aborder l'authentification dans GSM, essayons d'expliquer comment la question de sécurité est traitée dans ce réseau.

En fait, Il existe trois niveaux de sécurité dans le GSM :

- Pour l'usager (confidentialité des informations utilisateur)
- Pour l'usager et l'opérateur (confidentialité de l'identité de l'utilisateur)
- Pour l'opérateur (authentification de l'abonné)

L'introduction de la mobilité dans les réseaux GSM a nécessité la création de nouvelles fonctions par rapport aux réseaux fixes classiques. Le système doit pouvoir connaître à tout moment la localisation d'un abonné. En effet, dans un réseau fixe, à un numéro correspond une adresse physique fixe (une prise de téléphone), alors que pour le réseau GSM, le numéro d'un terminal mobile est une adresse logique constante à laquelle il faut associer une adresse physique qui varie au gré des déplacements de l'usager du terminal.
De plus, l'emploi d'un canal radio rend les communications vulnérables aux écoutes et aux utilisations frauduleuses. Le système GSM a donc recours aux procédés suivants :

- authentification de chaque abonné avant de lui autoriser l'accès à un service,
- utilisation d'une identité temporaire,
- chiffrement des communications.

Pour réaliser ces opérations, le système GSM utilise deux types d'adressage liés à l'abonné :
- L'IMSI : identité invariante de l'abonné, qui n'est connue qu'à l'intérieur du réseau GSM; cette identité doit rester secrète autant que possible. Pour cela, GSM a recours au TMSI,
- Le TMSI est une identité temporaire utilisée pour identifier le mobile lors des interactions Station Mobile / Réseau.
A l'intérieur d'une zone gérée par un VLR, un abonné dispose d'une identité temporaire. Le TMSI, codé sur 4 octets, est attribué au mobile de façon locale, c'est-à-dire uniquement pour la zone gérée par le VLR courant du mobile. Le TMSI est utilisé pour identifier le mobile appelé ou appelant lors de l'établissement d'une communication.

3.5.1.1.1 Authentification

L'utilisation du canal radioélectrique pour transporter les informations rend les abonnés particulièrement vulnérables :

- à la possibilité d'utilisation frauduleuse de leur compte par des personnes disposant de mobiles "pirates", qui se présentent avec l'identité d'abonnés autorisés,
- à la possibilité de voir leurs communications écoutées lors du transit des informations sur le canal radio.

Le système GSM intègre donc des fonctions de sécurité visant à protéger à la fois les abonnés et les opérateurs :

- confidentialité de l'IMSI,
- authentification d'un abonné pour protéger l'accès aux services,
- confidentialité des données usager,
- confidentialité des informations de signalisation.

3.5.1.1.2 Confidentialité de l'identité de l'abonné

Il s'agit d'éviter l'interception de l'IMSI lors de son transfert sur la voie radio par des entités non autorisées. Ainsi, il devient difficile de suivre un abonné mobile en interceptant les messages de signalisation échangés.

Le meilleur moyen d'éviter l'interception de l'IMSI est de la transmettre le plus rarement possible. C'est pourquoi le système GSM a recours au TMSI et c'est le réseau qui gère des bases de données et établit la correspondance entre IMSI et TMSI. En général, l'IMSI est transmise lors de la mise sous tension du mobile et ensuite les TMSIs successives du mobile seront transmises.

Ce n'est qu'en cas de perte du TMSI ou lorsque le VLR courant ne la reconnaît pas (par exemple après une panne) que l'IMSI peut être transmise.

L'allocation d'une nouvelle TMSI est faite au minimum à chaque changement de VLR, et suivant le choix de l'opérateur, à chaque intervention du mobile. Son envoi à la station mobile a lieu en mode chiffré.

Pour mettre en œuvre les fonctions d'authentification et de chiffrement des informations transmises sur la voie radio, GSM utilise les éléments suivants:

- des nombres aléatoires RAND,
- une clé Ki pour l'authentification et la détermination de la clé Kc,
- un algorithme A3 fournissant un nombre SRES à partir des arguments d'entrée RAND et de la clé Ki,
- un algorithme A8 pour la détermination de la clé Kc à partir des arguments d'entrée RAND et Ki,
- un algorithme A5 pour le chiffrement / déchiffrement des données à partir de la clé Kc.

A chaque abonné est attribuée une clé Ki propre. Les algorithmes A3, A5 et A8 sont quant à eux les mêmes pour tous les abonnés d'un même réseau.
La figure 3.2 schématise l'utilisation de ces différents éléments pour la mise en œuvre des fonctions de sécurité.

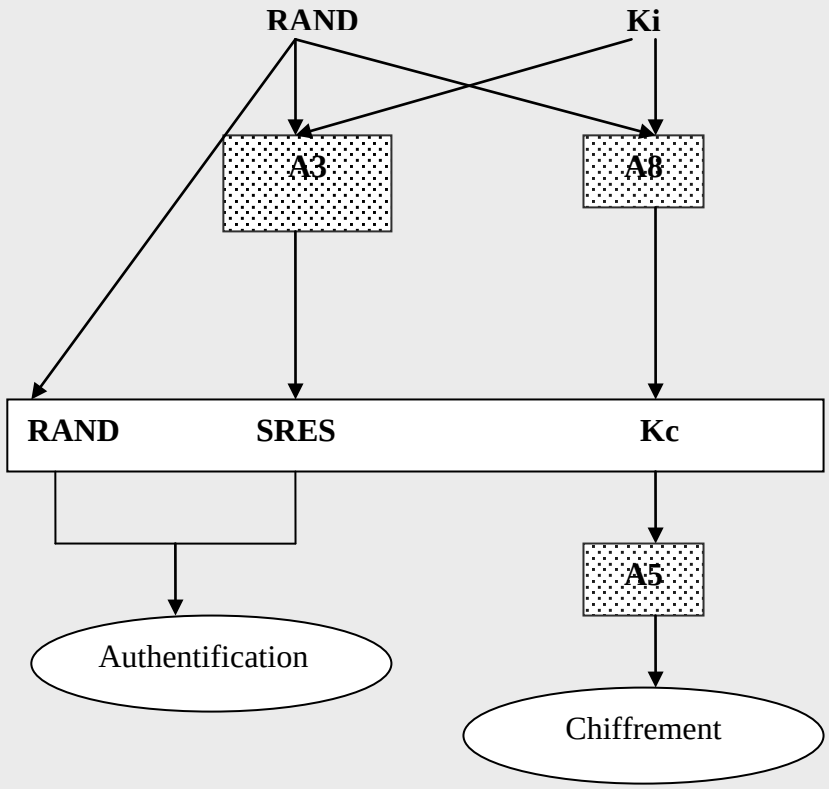

Figure 3.2 : Les différents éléments pour la mise en œuvre de la sécurité dans GSM

3.5.1.1.3 Authentification de l'identité de l'abonné

L'authentification de l'identité de l'abonné peut être exigée du mobile par le réseau à chaque mise à jour de localisation, à chaque établissement d'appel et avant d'activer ou de désactiver certains services supplémentaires. Dans le cas où la procédure d'authentification de l'abonné échouerait, l'accès au réseau est refusé au mobile.
Chaque abonné possède dans sa carte SIM, une clé secrète Ki, connue seulement du HLR. Lorsque l'unité mobile indique sa présence dans un domaine donné, le VLR local contacte le HLR de l'abonné pour lui transmettre sa propre identification, celle du mobile (l'IMSI) ainsi que la position de ce dernier. Le HLR demande alors à l'Autorité chargée d'appliquer la politique de sécurité de l'opérateur, un ensemble de triplets contenant un challenge (RAND), une réponse signée SRES et la clé de session correspondante Kc. Ces triplets sont ensuite communiqués au VLR. Chaque triplet ne sera utilisé qu'une seule fois pour chaque authentification du mobile.

La carte SIM du mobile calcule la signature de RAND grâce à l'algorithme A3 et la clé Ki. Le résultat calculé, noté SRES, est envoyé par le mobile au réseau.

Le réseau compare SRES au résultat calculé de son coté. Si les deux résultats sont identiques, l'abonné est identifié (Figure 3.3).

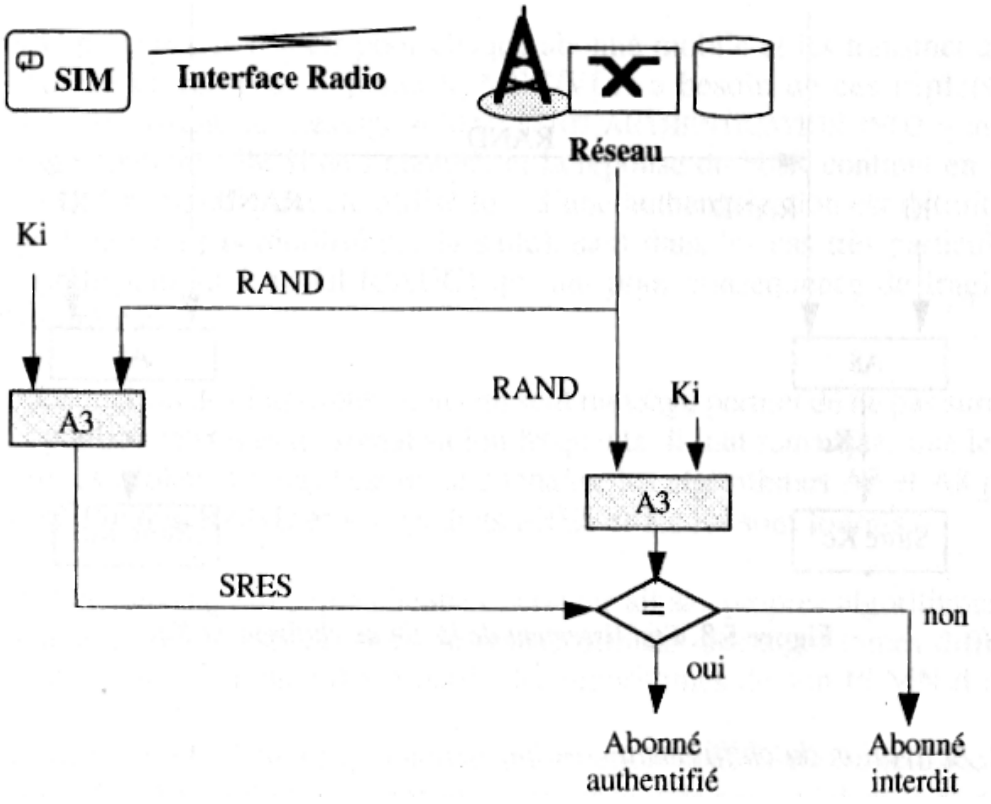

Figure 3.3 : Authentification de l'unité mobile dans GSM

La confidentialité des données transmises est assurée en chiffrant les données avec Kc. L'algorithme cryptographique A5 est utilisé pour le chiffrement de la voix et des messages de signalisation.

3.5.1.2 L'authentification dans le CDPD: Cellular Digital Packet Data

CDPD est une architecture développée par un consortium de compagnies aux états unis. Comme dans GSM, chaque mobile a un unique nom et appartient à un domaine de résidence spécifique. Pour s'authentifier à H, M doit présenter un triplet <M, ARN, ASN> où ARN (Authentication Random Number) et ASN (Authentication Sequence Number).
Le protocole d'authentification procède comme suit: Quand M accède à un domaine étranger, il engage un protocole Diffie-hellman [Shneier 96] d'échange de clés avec R. Ce protocole permet aux deux parties d'une connexion à travers un canal non sécurisé de négocier une clé secrète Ks de telle sorte qu'un observateur ne puisse pas déterminer la clé. Une fois la clé établie, M présente ses crédits sous forme < M, ARN, ASN>.

R déchiffre l'accréditation reçue et la transmet en texte clair à H. Ce dernier valide l'accréditation et envoie un message de confirmation à R. optionnellement, H peut envoyer un nouveau triplet avec de nouvelles valeurs pour ARN et ASN.
La figure 3.4 illustre cet échange de messages. La notation suivante est utilisée:
M-ES : Mobile Equipment System
MD-IS : Mobile Data Intermediate System. Le MD-IS peut être soit une unité de raccordement dans un domaine visité soit l'autorité d'affiliation du mobile. Par analogie, le MD-IS peut être considéré comme un serveur d'authentification ou sont stockés les données de l'abonné.

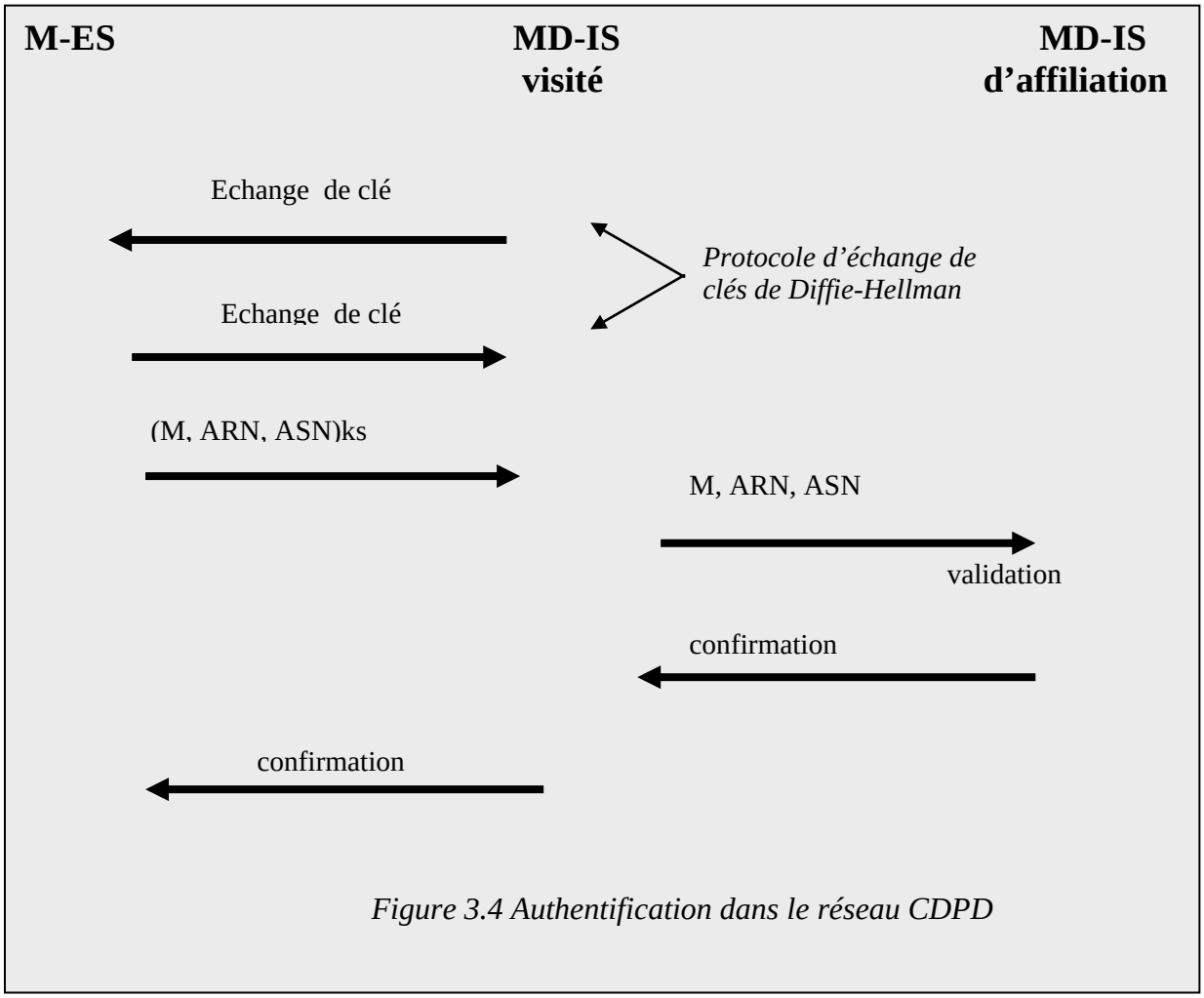

Figure 3.4 Authentification dans le réseau CDPD

3.5.1.3 Critiques des protocoles d'authentification de GSM et CDPD :

GSM est l'un des premiers réseaux mobiles à inclure les mécanismes d'authentification dans son système. Néanmoins, le problème réside dans l'hypothèse que le réseau fixe intermédiaire est physiquement sécurisé [Curtis 01]. Les principales critiques de GSM se résument à :

- Les triplets SRES, RAND et Ki sont transmis en clair entre HLR et VLR.
- Le HLR doit générer un ensemble de paires de RAND et SRES que le VLR utilisera lors des échanges successifs pour authentifier l'abonné. Cette solution n'est pas optimale car le HLR doit gérer des millions d'utilisateurs.

- L'utilisation d'algorithmes de chiffrement qui n'ont pas été publiés ne fournit pas à un utilisateur un sentiment de sécurité.

Comme dans GSM, CDPD adopte l'hypothèse que le réseau fixe est sûr car les messages qui contiennent les informations secrètes des utilisateurs sont transmis en clair.

3.5.1.4 Protocoles d'authentification de Molva et Samfat

Dans la littérature, les travaux de Molva et Samfat [Molva 92] [Samfat 95] ont mené à une série de protocoles d'authentification pour les réseaux mobiles que nous pouvons classer en : protocole d'authentification faible et protocoles d'authentification forte. Dans le premier cas, l'authentification est basée sur un mot de passe. L'authentification forte, elle est basée sur une clé cryptographique.
Nous allons décrire directement le protocole d'authentification forte. L'approche proposée, contrairement à GSM et CDPD, permet d'optimiser la procédure d'authentification en terme de nombre de messages échangés entre autorités administratives. De plus, le domaine d'affiliation peut déléguer ses pouvoirs au domaine visité afin que la procédure correspondant à la création de la base d'accréditation n'ait lieu qu'une seule fois. Comme le domaine visité et le domaine d'affiliation peuvent être séparés par de longues distances géographiques, ce passage de responsabilité permet de diminuer les coûts des communications inter-domaines et de minimiser les ressources allouées pour l'authentification [Samfat 94].
Pour expliquer ces protocoles, nous utiliserons un schéma de notation uniforme, par conséquent, la notation d'une solution spécifique peut être différente de celle utilisée dans le document original.

Notation
U: identification de l'utilisateur mobile
ASv, ASl: identification du serveur d'authentification respectivement dans le domaine visité et dans le domaine d'affiliation.
Ku : clé partagée par U et ASl
Kuv : clé locale utilisée par U dans le domaine visité
Kvl : clé secrète partagée par ASv et ASl.
Ks : clé de session partagée par U et ASv
Nu : nombre aléatoire généré par U
Tu : estampille temporelle générée par U
Nv : nombre aléatoire généré par ASv
AUTHk(X Y Z) : authentificateur calculé avec la clé K et prenant en entrée X, Y et Z.
TICKk(A, [Ks], B, C) : certificat émis par A, scellé avec la clé k contenant une clé secrète [Ks] qui sera utilisée par B pour communiquer avec C.

Les différentes étapes du protocole se résument en l'échange de messages suivant (figure 3.5) :

1. Lorsque le mobile se connecte au réseau, il reçoit l'identification du domaine visité ASv. Le mobile calcule K_{ut} la clé locale dépendante du temps comme suit :

$$K_{ut} = F(U, Asv, Tu, Ku)$$

Cette clé est dérivée de la clé Ku que l'utilisateur partage avec son domaine d'affiliation. Cette clé temporaire est à usage unique et ne servira pas à l'authentification de U lors de ses accès futurs dans le domaine visité. Ayant K_{ut}, l'utilisateur choisit un nombre aléatoire Nu, et calcule le jeton d'authentification $AUTH_{Kut}(Nu, Tu, U)$ et le transmet à ASv.
$AUTH_{Kut}(Nu, Tu, U)$: l'authentificateur ou le jeton d'authentification est un message cryptographique généré par U. C'est le résultat d'une fonction de chiffrement E avec la clé K_{ut} prenant entrée Nu (nombre aléatoire généré par U), Tu ou temps courant est une estampille temporelle utilisée dans le but de garantir la fraîcheur du message et empêche toute répétition de ce message ultérieurement par un ennemi (attaque par rejeu).

2. A la réception du message, ASv reconnaît que l'utilisateur appartient à un autre domaine. Il doit donc obtenir une preuve de l'identité revendiquée. ASv doit formuler une requête qui lui permet à la fois de s'authentifier et d'authentifier U à ASl. Une solution évidente serait de transmettre séparément les deux jetons d'authentification. Cependant, dans le cas où l'utilisateur possède une clé faible, le jeton d'authentification calculé avec cette clé risque d'être révélé. De ce fait, une technique de chaînage de jetons est appliquée. L'idée est donc d'utiliser le jeton généré par U comme paramètre d'entrée dans le jeton d'authentification généré par V.

3. Lorsque ASl reçoit le message, il procède de la manière suivante :
    a. Il cherche dans sa base de données la clé Ku correspondant à l'utilisateur U.
    b. Il valide Tu en le comparant au temps courant. Une marge de tolérance et un seuil maximal doivent être définis pour éviter toute tentative de rejeu.
    c. ASl recalcule Kut après avoir obtenu U, Ku et ASv et Tu.
    d. Il utilise Kut pour recalculer l'expression $AUTH_{kut}(Nu, Tu, U)$
    e. ASl recalcule $AUTH_{Kvl}()$ et compare le résultat avec le jeton contenu dans le second message.

    Si l'égalité est vérifiée, ASl authentifie à la fois U et ASv. Ensuite, ASl génère un ticket pour confirmer l'identité de U permettant à ce dernier d'opérer dans le domaine de ASv.

4. A la réception du ticket, ASv récupère la clé Kut, puis génère une clé forte Kuv qui sera la clé d'authentification de U dans le domaine visité.
   ASv vérifie l'intégrité de la clé en recalculant $AUTH_{kut}$ (contenu dans le message) et génère et transmet à U les deux tickets suivants :
    - $TICK_{Kut}$ qui contient Kuv scellé avec K_{ut}.
    - $TICK_{Kuv}$ qui contient la clé de session de travail Ks.

5. Lorsque U reçoit ce dernier message, il récupère la clé Kuv et la sauvegarde dans une zone mémoire de son équipement. La clé Ks peut être ensuite utilisée pour chiffrer les données de la communication courante.

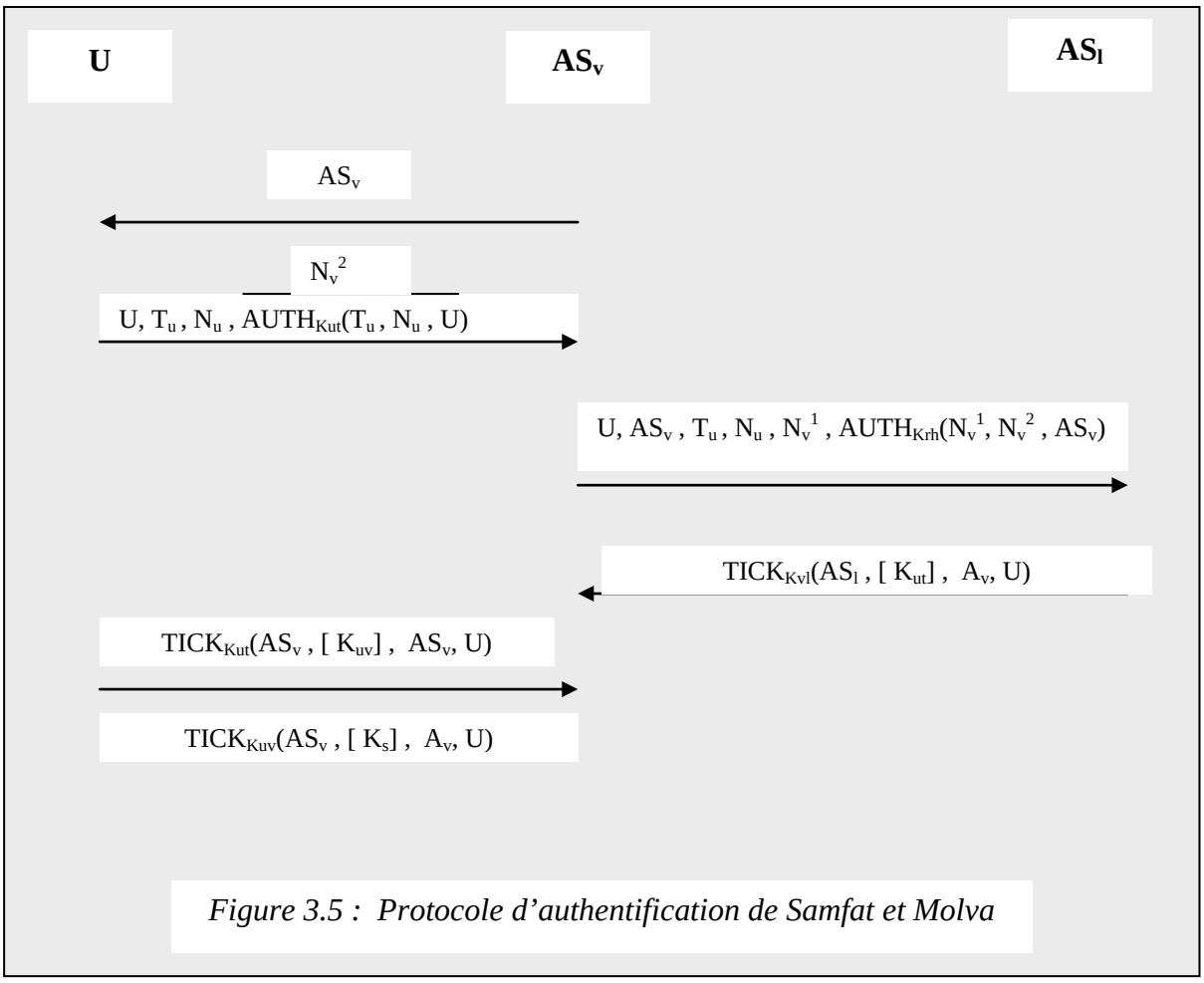

Figure 3.5 : Protocole d'authentification de Samfat et Molva

Rappelons que dans un environnement dynamique tel que les réseaux cellulaires, les utilisateurs sont amenés à traverser des frontières administratives séparant des domaines adjacents au cours d'une même communication. Il est alors important de transférer les informations de vérification de sécurité entre domaines de manière transparente à l'utilisateur. Samfat et Molva ont décrit dans la figure 3.6 un transfert rapide des informations d'authentification durant un handoff, évitant à Asb de contacter Asl. Les deux premiers messages représentent l'authentification unidirectionnelle de l'utilisateur dans le domaine A, et la distribution de la clé de session Ks. Par la suite, l'utilisateur traverse la frontière séparant le domaine A du domaine adjacent B. Au lieu de contacter immédiatement Asl, Asa transmet à Asb la même clé de session Ks . Connaissant Ks, Asb est alors capable d'authentifier l'utilisateur directement. Toutefois, ce protocole est une solution temporaire car lors d'une prochaine tentative d'accès au réseau dans le domaine B, la procédure d'authentification impliquant Asl devra être effectuée.

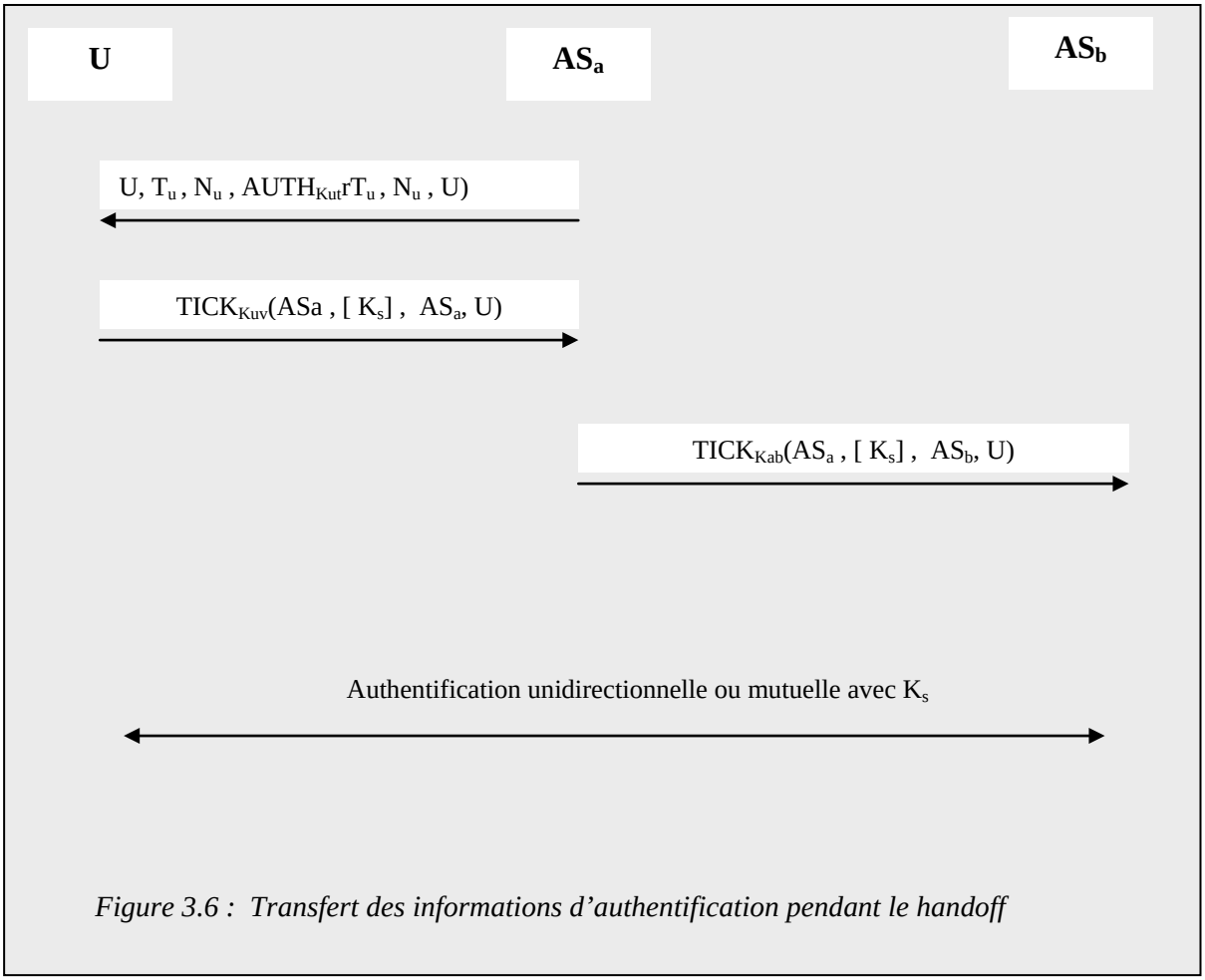

Figure 3.6 : Transfert des informations d'authentification pendant le handoff

Le protocole décrit précédemment apporte une nouveauté par rapport à celui adopté dans GSM, dans le sens où le domaine d'affiliation peut déléguer ses pouvoirs au domaine visité en communiquant à ce dernier une accréditation qui permettra d'authentifier l'utilisateur dans le nouveau domaine. Néanmoins, tous les protocoles décrits dans cette section sont basés sur un cryptosystème à clé secrète et présentent donc tous les inconvénients d'une architecture de sécurité basé sur les clés secrètes.

3.5.2 L'utilisation de la cryptographie à clé publique dans les environnements sans fil

L'utilisation des algorithmes cryptographiques à clé publique [Go 2001] dans l'authentification peut résoudre un grand nombre de problèmes posés par les algorithmes à clé secrète, à savoir :

- La gestion des Clés : Les algorithmes à clé symétrique nécessitent des relations de confiance entre le réseau et tous ses abonnés. Plus le nombre de réseaux est grand, plus la configuration du réseau évolue et il est donc plus difficile de gérer toute relation de confiance entre eux dans tout le réseau. En utilisant les clés publiques, ceci est évité puisque les clés publiques peuvent être distribuées librement à toutes les

entités qui en ont besoin. L'utilisation des clés publiques peut réduire le temps de déperdition (overhead) de la gestion des clés. [Lee 99]

- La non Répudiation de l'utilisation d'un service : La non répudiation de l'utilisation d'un service ne peut être possible que par l'utilisation d'algorithmes cryptographiques à clé publique c'est à dire les signatures digitales [Go 2001].

Néanmoins, durant les années 80, lorsque les protocoles de sécurité pour le GSM ont été développés, le choix d'une solution basée sur un cryptosystème à clé publique a été vite abandonné dans les réseaux sans fil car ces protocoles nécessitent beaucoup de traitements. Par exemple, RSA est estimé nécessiter 1000 fois plus de temps de calcul qu'un cryptosystème à clé secrète [Schafer 01]. Connaissant les limitations des mobiles, en terme de vitesse de processeur et durée de vie de la batterie, les concepteurs ont considéré que le prix est trop cher à payer.
Plus récemment, les chercheurs ont identifié un ensemble d'algorithmes à clé publique nécessitant moins de puissance de traitement qui peuvent être appliqués dans l'authentification et la sécurité dans les environnements sans fil. Parmi ces algorithmes, nous citons le Modular Square Root Algorithm et l'Elliptic Curve Cryptography [Shneier 96].

3.5.2.1 Le Modular Square Algorithm :

Comme la plupart des algorithmes cryptographiques, l'approche est basée sur l'arithmétique modulaire et dépend de la difficulté de factoriser les nombres premiers (voir Annexe).
En bref, Le Modular Square Algorith ou MSR opère comme suit :
La clé publique est un modulo N qui est le produit de deux grands nombres premiers, p et q (en pratique, p et q sont des nombres binaires de 75 à 100 bits de taille). La combinaison de p et q constitue un élément de clé privée de l'algorithme.

Si un principal A envoie un message M à B, il chiffre ce message comme suit :

$$C= M^2 \bmod N$$

Pour retrouver M, B déchiffre le message et a :

$$M= \text{Racine } (C) \bmod N$$

L'application de MSR dans les environnements sans fil présente certains avantages :
- Calculer le carré modulaire nécessaire pour le chiffrement nécessite moins de temps (le temps d'une multiplication modulaire) que le calcul de l'extraction d'une racine carrée modulaire (une exponentiation). De ce fait, si la fonction de chiffrement est placée dans la station mobile et la fonction de déchiffrement dans la station de base. MSR répond donc aux contraintes imposées par le mobile qui ont des processeurs lents et des réserves de batteries limitées.
Dans ce qui suit, nous allons décrire le protocole d'authentification de Beller, Chang et Yacobi [Beller 92]. Pour cela, adoptons la notation ci-dessous :

Notation

ID_{BS} : Identificateur de la station de base
ID_{MS} : Identificateur de la station mobile (équivalent à IMSI dans GSM)
N_{BS} : clé publique de la station mobile obtenue par le produit de nombres premiers p_{BS} et q_{BS} connus uniquement de la station de base et de l'autorité de certification.
N_{CA} : clé publique de l'autorité de certification obtenue par le produit de nombres premiers p_{CA} et q_{CA} connus uniquement de l'autorité de certification.
K_S : clé de session pour le cryptage durant une session de communication.
RANDX : nombre aléatoire choisi par la station mobile pour déterminer Ks
h,g : fonctions de hachage.
$CERT_{BS}$: certificat de la station de base qui prend la forme : SQRT(h(ID_{BS} , N_{BS}) mod N_{CA}
$CERT_{MS}$: certificat de la station mobile qui prend la forme : SQRT(g(ID_{MS}) mod N_{CA} . Ce certificat est intégré dans le mobile de l'abonné .

Déroulement du protocole d'authentification :
1. La station mobile signale à la station de base du réseau visité qu'elle désire ouvrir une session de communication.
2. La station de base envoie une copie de son certificat SQRT(h(ID_{BS} , N_{BS}) mod N_{CA}
3. La station mobile vérifie la validité de ce certificat en calculant le carré du certificat et le compare à la valeur (h(ID_{BS} , N_{BS}) calculée indépendamment. Si les valeurs sont identiques, alors la station mobile continue sinon la session est rompue.
4. La station mobile choisit un nombre aléatoire RANDX qui servira de clé de session et calcule une valeur a = $RANDX^2$mod N_{BS}. Elle envoie a à la station de base.
5. La station de base calcule la racine carrée de a et retrouve RANDX qui représente la clé de session K_S .
6. La station mobile calcule b et le transmet à la station de base tel que b = f(K_S ,m) ou m est la concaténation de ID_{MS} et $CERT_{MS}$.
7. Connaissant K_S , la station de base décrypte b et extrait m. Elle calcule $CERT_{MS}^2$mod N_{CA} . Cette valeur est donc comparée à g(ID_{MS}) mod N_{CA} . Si les deux valeurs sont identiques alors la station de base authentifie ainsi la station mobile.

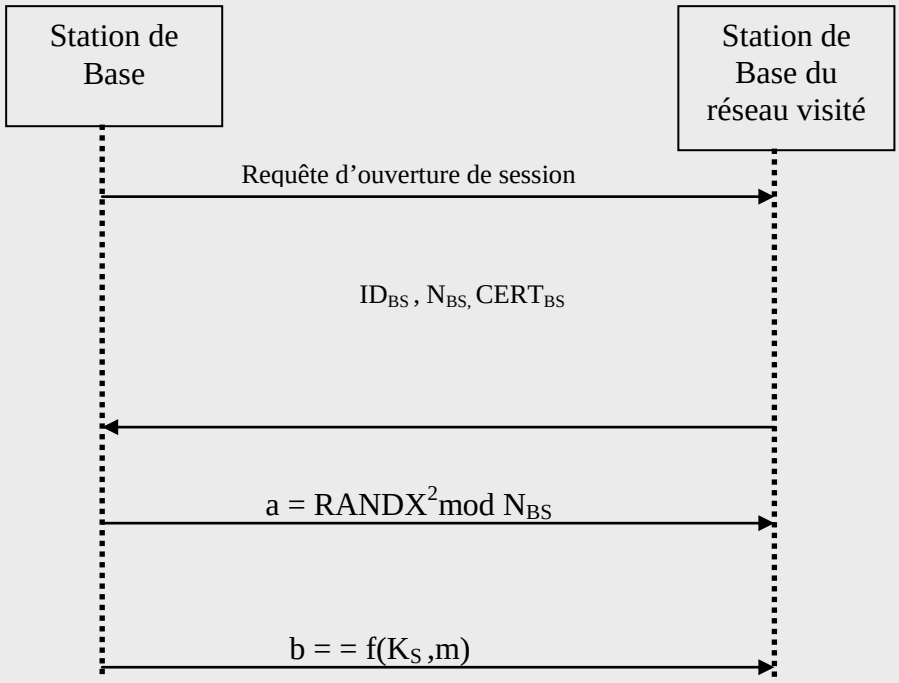

Figure 3.7 Protocole d'authentification de Beller, Chang et Yacobi

Dans le protocole décrit (figure 3.7), seulement deux multiplications modulaires sont effectuées par la station mobile (carrés) et ce traitement est envisageable avec les équipements actuels. [Curtis 01]

3.5.2.2 Protocole de Aziz et Diffie

Ashar Aziz et Whitfield Diffie [Aziz 94] ont proposé un protocole pour les réseaux sans fil qui utilise un protocole à clé publique pour l'authentification et la génération de clé de session, et une approche à clé privée pour le chiffrement des données dans une session de communication. Comme le protocole décrit précédemment, celui ci utilise les certificats numériques et une autorité de certification. Une caractéristique qui le distingue est qu'il fournit un support explicite pour la station mobile et la station de base pour négocier quel algorithme cryptographique symétrique utiliser pour le cryptage des données.
Le protocole de Aziz-Diffie supporte l'authentification mutuelle [Aziz 94].

3.6 L'authentification dans UMTS

Les premiers travaux sur l'architecture de sécurité de UMTS ont conduit à un ensemble de projets de recherche qui incluent ASPECT (Advanced Security for Personal Communications Technology, MONET et 3GS3 (Third Generation Mobile Communications) [Gunter 99]. Ces derniers ont défini un ensemble de protocoles et procédures pour l'environnement UMTS.
Néanmoins, tous ces travaux ont adopté trois principes de base :

- l'architecture de sécurité de UMTS est construite sur les caractéristiques de sécurité des systèmes de seconde génération.
- La sécurité de UMTS améliorera la sécurité des systèmes de seconde génération en éliminant les failles de ces derniers.
- La sécurité de UMTS offrira de nouveaux services de sécurité non disponibles dans les systèmes de seconde génération.

Le concept est donc, de créer un environnement meilleur que GSM mais pas nécessairement radicalement différent. L'objectif d'une conception d'une architecture de sécurité dans UMTS est de créer un framework qui pourra évoluer à travers le temps.
A cette date, les concepteurs de UMTS ont choisi d'adopter un schéma d'authentification qui ressemble étroitement à celui de GSM avec des extensions. Même si les chercheurs ont pensé à une solution utilisant les clés publiques, une fois encore, les approches basées sur les clés secrètes ont gagné du terrain.
Le protocole UMTS utilise une approche basée sur un cryptosystème à clé secrète dans laquelle le centre d'authentification du réseau de résidence de l'abonné et la carte USIM de l'utilisateur partagent une clé secrète.

Nous noterons les principales améliorations apportées à UMTS [Gunter 00]:

- L'USIM et le centre d'authentification partagent un numéro de séquence en plus d'une clé secrète ; ce numéro n'est pas une valeur constante.
- La station de base du réseau visité est authentifiée à la station mobile.
- Durant la phase d'authentification, l'UMTS établit une clé de session pour le chiffrement des données et une autre clé pour garantir l'intégrité des données.
- Les algorithmes cryptographiques de UMTS ne sont plus propriétaires et vont être placés dans le domaine publique pour analyse.

Les différentes étapes du protocole d'authentification sont résumées ci-dessous :

1. Le serving node (SN) qui abrite le VLR fait une requête d'authentification au Home Environment (HE) qui supporte le HLR et le centre d'authentification AuC
2. L'environnement de résidence envoie un vecteur d'authentification AV au noeud visité. Chaque vecteur est utilisé pour garantir une seule authentification et un accord pour une clé de session entre le SN et l'USIM de la station mobile. Ce vecteur correspond au triplet de GSM et comprend :
    - Un nombre aléatoire RAND (challenge)
    - Une réponse XRES
    - Une clé de session CK
    - Une clé pour l'intégrité IK
    - Et un jeton d'authentification AUTN
3. SN envoie un challenge RAND et un jeton d'authentification AUTN à la station mobile.
4. L'USIM confirme que AUTN est acceptable (authentifie le réseau à l'unité mobile). Dans ce cas, elle génère une réponse RES, et la transmets à SN
5. L'USIM calcule ses propres copies de CK et IK en utilisant RAND, sa clé secrète et le numéro de séquence contenu dans AUTN.
6. SN compare RES qu'il a reçu de l'unité mobile et la compare à XRES. Si les valeurs sont égales, alors l'unité mobile est authentifiée.

Le protocole d'authentification de UMTS (figure 3.8) utilise cinq fonctions cryptographiques F1…F5 pour générer les valeurs de AUTN et AV [Curtis 01].

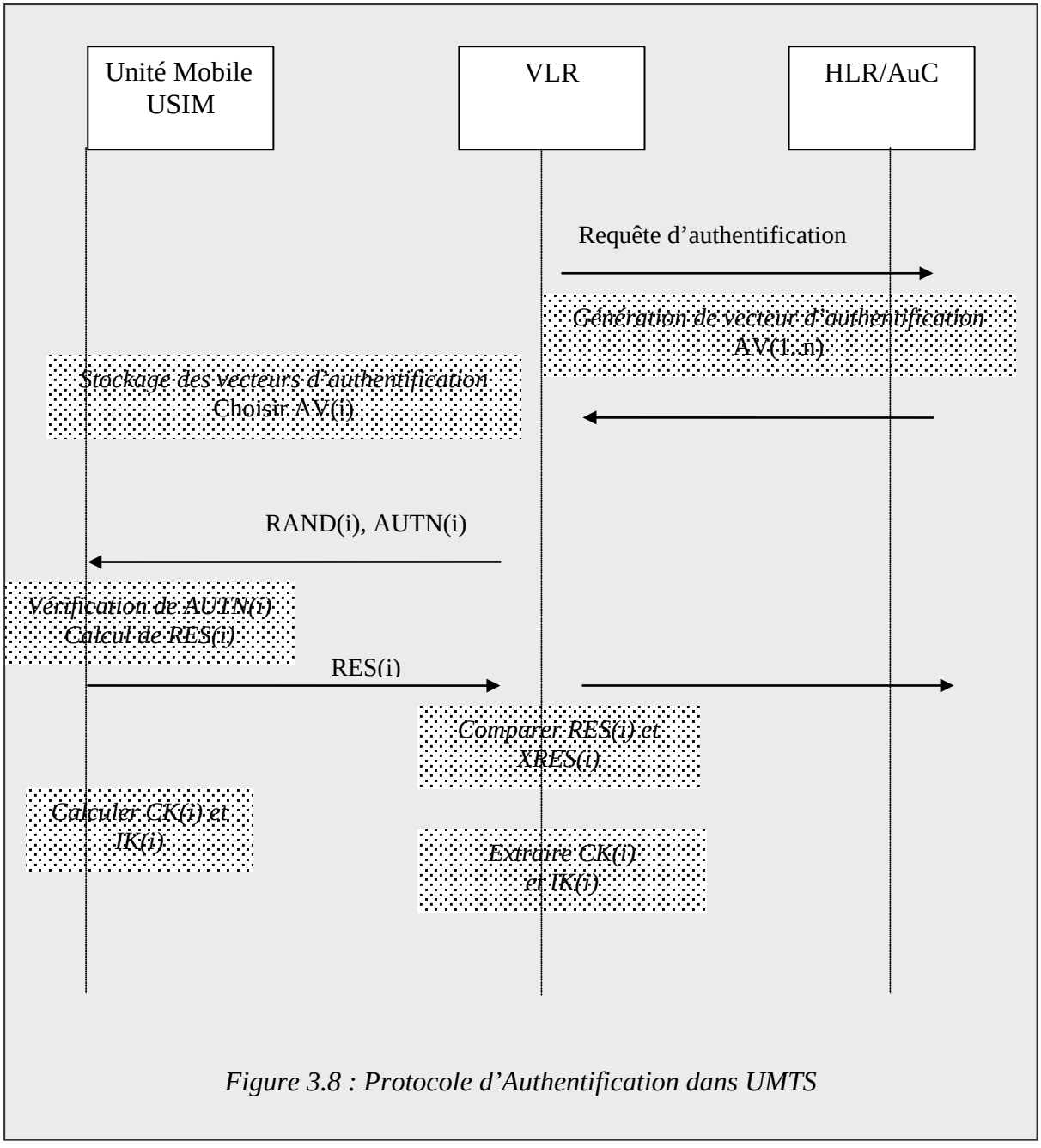

Figure 3.8 : Protocole d'Authentification dans UMTS

La mise en place d'un protocole d'authentification dans la première phase d'implémentation d'UMTS a été un long processus qui a pris beaucoup de tournures. En effet, quelques uns des premiers travaux de recherche précurseurs de UMTS dans les programmes européens ont

adopté une solution basé sur un cryptosystème à clé publique. En phase finale, il est impératif de construire une architecture autour de GSM en vue d'assurer l'interopérabilité avec ce dernier.
Par conséquent, UMTS a adopté un schéma d'authentification basé sur les clés secrètes. Cependant, les extensions apportées offrent une meilleure sécurité.

3.6 La Confidentialité

Un autre aspect de la sécurité passe par la protection des données qui circulent sur le réseau, c'est à dire le contenu des trames en lui même, ou encore le trafic. Pour garantir la sécurité des données elles mêmes, une technique couramment employée dans les réseaux fixes correspond au chiffrement. Bien que le chiffrement soit une méthode assurant relativement bien la confidentialité des données, son emploi reste problématique avec les machines mobiles. Les algorithmes de déchiffrement sont, en effet, très souvent complexes. Ils exigent donc une puissance de calcul notable et impliquent une consommation d'énergie supplémentaire lors de chaque envoi de message si les données sont sensibles. De ce fait, la confidentialité des données a été résolue par la clé de session déduite du protocole d'authentification. En effet, cette clé permet d'offrir un canal sécurisé entre le mobile et le réseau.

3.7 Conclusion

Dans ce chapitre, nous avons introduit la sécurité dans les réseaux cellulaires. Le description des différents menaces que présentent ces réseaux et leurs spécificités imposent aux concepteurs d'architectures de sécurité de concevoir des solutions propres à ces environnement. L'introduction de mécanismes d'authentification constitue une première défense contre les tiers malveillants. Les travaux dans ce domaine ont engendré une panoplie de protocoles d'authentification. Toutefois, le fait d'introduire des mécanismes d'authentification dans un réseau mobile, introduit un nouveau besoin, l'anonymat.

4.1 Introduction au problème

Dans les systèmes où la mobilité est possible (réseaux sans fil ou avec fil mais supportant la mobilité), l'information sur la location et la migration des utilisateurs est vulnérable d'une certaine manière. Typiquement, quand un utilisateur enregistré dans son domaine de résidence, arrive à un autre domaine, il est nécessaire de prouver son identité au domaine visité dans le but d'obtenir des services. Le domaine de résidence doit être contacté durant ce processus. Les messages échangés peuvent révéler une information privée aux espions qui peuvent se trouver sur le réseau. De plus, la protection des informations de mouvements ou intraçabilité est aussi une issue dont il faudra tenir compte [Hellberg 98].
En général, il existe différents aspects pour la confidentialité d'un utilisateur dans les systèmes distribués. Traditionnellement, le caractère privé du contenu d'un message est souvent la seule issue de sécurité prise en compte dans la conception de systèmes distribués. Le chiffrement est une technique communément utilisée pour préserver le caractère privé des contenus des messages.
L'anonymat consiste à protéger les informations secondaires telles que l'identité des entités impliquées dans une transaction mais aussi à protéger les méta-informations qui découlent des interactions entre entités d'un système distribué. Dans un réseau mobile, si aucune précaution n'est prise, un intrus peut avoir accès à des informations secondaires concernant la localisation et les déplacements des utilisateurs. Les messages échangés durant la procédure d'authentification peuvent révéler des informations privées à des ennemis écoutant le médium de communication. Il devient alors possible de pister l'usager. Cet intrus, pourra donc utiliser ces données de manière à porter préjudice à l'utilisateur mobile. Nous estimons, que l'accès illicite à ces informations privées, sans le consentement de l'utilisateur, constitue une véritable atteinte à sa vie privée [Dix 02]. D'où l'intérêt de réclamer le droit à l'intimité numérique (privacy).
De plus, l'anonymat est essentiel pour prévenir le déni de service sélectif dans les réseaux de communication. En effet, couper le canal de communication entre un client et un serveur ou saturer (flooding) le réseau au maximum de telle sorte qu'il n'y ait plus de bande passante disponible pour l'utilisation rend le réseau effectivement non opérationnel. L'anonymat semble être une solution évidente à ce problème.
Dans cette thèse, nous nous intéressons à la protection d'informations secondaires. Ceci inclut l'information sur les identités des entités impliquées dans la transaction ou la méta-information (exemple, le nombre de fois qu'une unité mobile a visité un certain magasin durant une certaine période de temps).

Dans ce chapitre, nous allons donc étudier le problème de l'anonymat de manière détaillée. Tout d'abord, dans une première partie, nous allons commencer par présenter l'anonymat dans les environnements fixes tel que Internet : nous présenterons les solutions apportées dans ce contexte.
Dans une seconde partie, nous définirons de manière formelle l'anonymat dans les environnements sans fil, et présenterons les solutions adoptées dans certaines infrastructures existantes ou celles décrites dans la littérature. Nous critiquerons chaque solution en la classifiant selon le degré d'anonymat garanti.

4.2 L'Anonymat dans les systèmes traditionnels tels qu'Internet.

Les lettres envoyées par la poste sont généralement dans une enveloppe avec les adresses de l'émetteur et du destinataire. Nous avons confiance en la poste qui ne verra pas ce qu'il y a à

l'intérieur, car il est admis que le contenu d'une lettre a un caractère privé, et que ce caractère privé est respecté par tous, et protégé par la loi. Nous avons également confiance que la poste ne contrôlera pas qui envoie à qui, car cette information est également d'ordre privé.

Ces deux types d'information : le contenu d'une enveloppe et son adresse s'appliquent également à la communication électronique. Le développement rapide des transactions électroniques et la possibilité de collecte d'informations personnelles sur le Web ont contribué à accroître l'intérêt des utilisateurs à conserver le caractère privé d'une communication et à réclamer le droit à l'intimité numérique (privacy). En effet, Les parties communicantes s'identifient l'une à l'autre : il n'y a pas de raison de divulguer à tous les autres qui parle à qui et de quoi ils parlent. Le premier point peut être révélé par **l'analyse de trafic** (traffic analysis) et le second par **l'espionnage** (eavesdropping).

4.2.1 Confidentialité et Anonymat

Sur Internet, les paquets sont constitués d'une entête et d'un message. L'entête, utilisée pour le routage, révèle la source et la destination du message. Rappelons que la confidentialité consiste à garder le contenu du message confidentiel et non compréhensible par une tierce non autorisée. Les mécanismes de cryptographie existant peuvent protéger les contenus des communications basées IP, assurant ainsi la confidentialité du message et empêchant les espions du réseau de déduire le but du trafic observé. Cependant, vu que le trafic lui même n'est pas caché, l'émetteur et le destinataire de chaque paquet sont clairement visibles sur le réseau (et aux observateurs du réseau) dans les entêtes des paquets même si le paquet est crypté de bout en bout [Syverson 98].
En effet, dans un réseau cryptographique conventionnel, une partie A décide d'envoyer un message M à une autre partie B. Pour procéder, A protège M avec une clef secrète k, produisant un texte chiffré k(M). Les noms A et B et la direction de la communication sont généralement explicites, alors le message apparaît comme :

$$A \rightarrow B : k(M)$$

Notons que l'entête du message A→B n'est pas cryptée. Par conséquent, les points finaux de la communication sont visibles pour tous les observateurs. L'anonymat consiste donc à garantir de telles entêtes de messages secrètes [Mart 98].
De manière générale, l'objectif de l'anonymat est de préserver ces informations confidentielles et d'éviter aux observateurs d'inférer l'information « qui communique avec qui » [Mart 99].
Enfin, l'anonymat consiste essentiellement en la séparation entre la fonction d'identification et la fonction de routage [Mart 99].

4.2.2 Caractéristiques de l'anonymat

Nous définissons un service d'anonymat comme étant un service assurant la propriété d'anonymat. C'est un service qui restreint les capacités d'un adversaire à inférer les vrais points finaux d'une communication réseau [Mart 99]. Un réseau « Anonyme » est un réseau de nœuds qui communiquent en utilisant la propriété d'anonymat. Nous distinguons plusieurs types d'anonymat. Par exemple, supposons que A décide d'envoyer un message à B :

- Si un adversaire potentiel est incapable de déduire que la source du message est A alors le service d'anonymat offre l'anonymat de l'émetteur (sender anonymity).
- Si un adversaire potentiel est incapable de déduire la destination du message alors le service d'anonymat garantit l'anonymat du destinataire (receiver anonymity).
- Etant données de multiples messages anonymes envoyés de A à B, si un adversaire potentiel est incapable de déterminer si les messages se réfèrent à la même source et à la même destination alors le service garantit une indépendance émetteur destinataire (sender or receiver unlikability). Ce dernier est plus fort que les deux premiers, car dans ce cas l'adversaire est non seulement incapable d'identifier correctement le point final d'une communication mais il est incapable de déterminer un renommage des points finaux consistant avec la séquence de messages observés [Pfitzmann 00].

De manière générale, l'anonymat est qualifié [Dingledin 00] de :

- Anonymat faible : assure l'intraçabilité c'est à dire qu'il est impossible de faire le lien entre l'origine d'un objet et son destinataire, même si on a des soupçons;

- Anonymat fort : à l'intraçabilité, est ajoutée l'indépendance où il est impossible de lier deux actions d'un même individu.

4.2.3 Services d'anonymat

Les solutions pour les communications anonymes ne sont pas intégrées dans des produits existants ou infrastructures, mais sont offertes comme services indépendants pour lesquels un effort supplémentaire doit être accompli pour pouvoir les utiliser. Mis à part l'intérêt à offrir des services de connexions anonymes en général, nous distinguons trois types de services Web pour lesquels des solutions d'anonymat ont été apportées : la messagerie électronique, la navigation et la publication.

4.2.3.1 Cas de la messagerie électronique

Il existe des services implémentés pour cacher la location et les identités de l'émetteur et du destinataire d'un message.
Une solution triviale pour cacher son identité est de créer un compte pseudonyme anon@wissal.dz. Cependant, un observateur peut avoir une trace du message dans le réseau, particulièrement si l'adresse IP de l'émetteur est visible dans le message. D'autres services existent qui peuvent offrir un plus haut degré d'anonymat pour la messagerie électronique. Ce sont les réexpéditeurs anonymes. Il existe différents types :

- Les plus simples réexpéditeurs de type 0 se présentent sous forme de serveurs de messagerie qui utilisent une tiers de confiance appelé : Réexpéditeur. Son rôle est de maintenir une base de données qui associe les adresses réelles aux adresses pseudonymes associées. Il permet ainsi d'assurer l'anonymat de l'émetteur. L'exemple le plus connu est celui de Anon.penet.fi. Ces type de réexpéditeur offre un Anonymat traçable [Dingledin 00]: Dans ce cas, un réexpéditeur ne donne au destinataire du message aucun indice sur l'identité de l'émetteur, mais garde cette information entre les mains d'un intermédiaire. *Un exemple simple : A envoie un message non crypté à un réexpéditeur dont l'opérateur est T avec des instructions pour réexpédier le message à B. Le réexpéditeur efface l'adresse de retour pouvant identifier A et émet le message à B. A n'a aucun moyen de savoir si T a tracé le message (fichiers logs), gardant ainsi un enregistrement des*

adresses de B et de A ou alors le message en entier. Si l'opérateur a gardé ces traces alors B pourra trouver qui lui a envoyé le message en persuadant T de lui révéler l'identité de A.
Bien que l'anonymat traçable offre un bas niveau de sécurité, il peut suffire dans certains cas. Cependant tout repose sur la confiance accordée à l'opérateur.

- Un plus haut degré d'anonymat est obtenu avec les réexpéditeurs de type 1. Dans ce système, un message e-mail consiste en un ensemble chaîné de messages cryptés et utilise une chaîne de réexpéditeurs. L'idée repose sur la technique de base des mix de Chaum [Chaum 81]. L'utilisation de deux ou plus de nœuds intermédiaires préserve l'émetteur anonyme à chaque noeud sauf pour le premier et le destinataire anonyme à chaque noeud sauf pour le dernier
  La figure 4.1 représente graphiquement un message qui va être envoyé à travers 3 réexpéditeurs A, B et C et finalement à Ali. Les boites représentent les encryptions avec le nom de la personne pour laquelle le message est crypté écrit au coin gauche de la boite. Chaque réexpéditeur a sa clef publique et utilise PGP pour le cryptage. Le message ainsi chiffré est envoyé à chaque réexpéditeur. Le message consiste en fait :
  - en une requête pour réémettre à un autre réexpediteur
  - et un message chiffré avec la clef publique du prochain réexpéditeur.

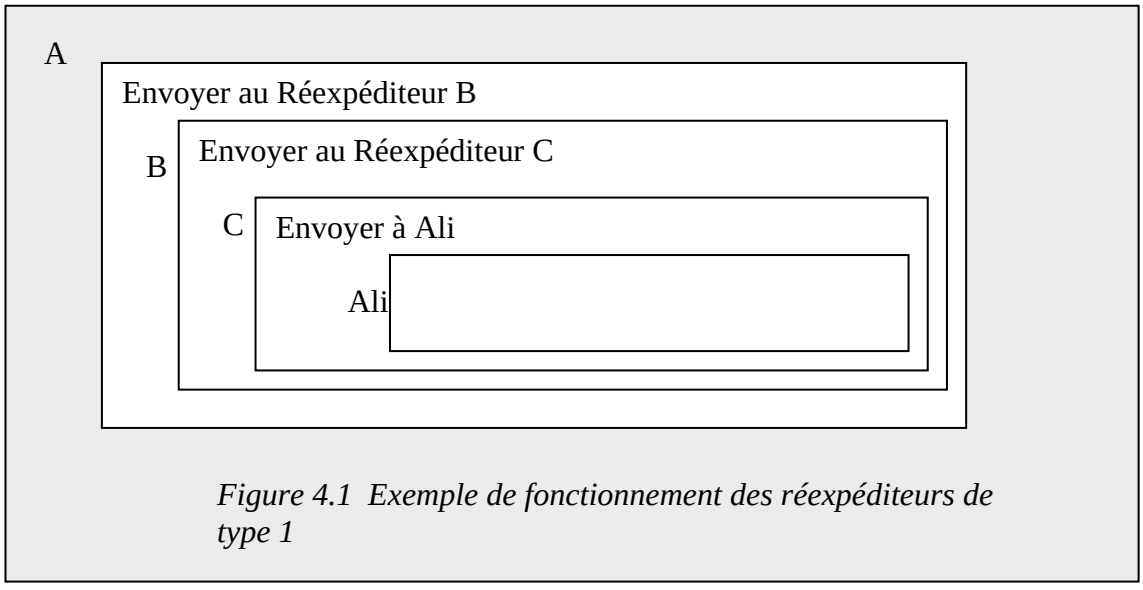

Figure 4.1 Exemple de fonctionnement des réexpéditeurs de type 1

Cette solution permet d'assurer un anonymat intraçable : Dans ce cas, l'auteur de la communication est simplement non identifiable.
Cependant, ce service ne peut pas garantir l'anonymat dans les cas de figures suivants :
1er cas : Les réexpéditeurs peuvent être corrompus, les opérateurs peuvent coopérer pour révéler l'identité de l'émetteur.

2ème cas : Un espion (eavesdropper) qui est capable de traquer les messages en entrée et en sortie des multiples réexpéditeurs pour une période de temps, peut inférer

certaines informations. Ce type de serveurs demeure très vulnérable aux attaques par reproduction de messages et à l'analyse de trafic qui peut exploiter les informations temps et taille.

- Le mixmaster est probablement la technologie de réexpédition de messages la plus intraçable à ce jour. C'est une pure implémentation des Mix de Chaum en incluant la notion de chemins de retour [Dingledin 00]. Ils remédient aux problèmes des réexpéditeurs de type 1 en [Loki 99]:
  - réordonnant les messages en les différant pour agir sur le temps
  - utilisant le mécanisme de bourrage pour agir sur la taille:
  - insérant un identificateur de paquet pour résoudre le problème des attaques par reproduction de paquets

4.2.3.2 Cas de la navigation anonyme

Contrairement aux services de messagerie anonyme, il y a très peu de services pour la navigation anonyme sur le web. De plus, les leçons tirées des services de réexpédition anonyme ne peuvent pas être supportées par les applications Web, du fait que les caractéristiques des e-mail et des applications basées sur le Web sont différentes [Pfitzman 86] :

- Le Web est un médium interactif contrairement aux e-mail qui sont de type store-and-forward.
- Dans la messagerie, l'émetteur initie le transfert de données. Il est même possible de le faire sans le consentement du destinataire. Mais, sur le Web, le destinataire doit explicitement demander des données de l'émetteur.

Malgré cela, les solutions proposées dans la littérature se basent sur les mêmes techniques [Benmeziane 01].

4.2.3.3 Connexions Anonymes : Onion Routing

Plus récemment, un groupe de chercheurs de la NRL (US Naval Research Laboratory) ont adopté l'idée d'utiliser les mix de Chaum pour implémenter les connexions anonymes [Reed 98][Goldschlag 99].
L'idée est d'établir des connexions anonymes similaires aux connexions TCP/IP mais qui doivent être résistantes à l'analyse de trafic. Les connections anonymes sont bidirectionnelles et peuvent être utilisées là où une connexion TCP/IP peut être utilisée.
Pour mettre en œuvre cette idée, Les chercheurs du NRL ont construit un prototype appelé Onion Routing [Reed 99]. L'objectif de onion Routing n'est pas de fournir des communications anonymes, les parties communiquantes sont libres de s'identifier dans les contenus de leurs messages. Mais l'utilisation d'un réseau public ne doit pas automatiquement révéler les identités des parties communiquantes.
Dans la description de ce système, le terme onion désigne un message avec des niveaux d'encryption. Le terme routeur onion (onion router) est utilisé pour désigner le mix qui agit comme un nœud dans le réseau.
Dans un tel réseau, au lieu d'avoir des connexions TCP/IP directes à une machine de destination, une application initiale ou initiatrice établit une connexion anonyme à travers une séquence de routeurs onion. Bien que la technologie est appelée onion routing, le routage s'effectue au niveau de la couche application. Pour toute connexion anonyme, la séquence

d'onion routeurs est une route strictement définie dans la configuration de la connexion et chaque onion routeur peut seulement identifier le précédent et le suivant dans la route.
Dans onion routing, l'application ne peut pas communiquer directement avec un routeur ou un onion routeur. Ceci est réalisée grâce à des interfaces proxy entre l'application et le réseau de routage. Ainsi, pour accéder à un site Web, l'utilisateur doit configurer son proxy http à un point d'entrée du réseau onion appelée : application proxy.

Pour débuter une session entre un initiateur et un destinataire, le proxy de l'initiateur identifie une série de nœuds formant une route à travers le réseau et construit un onion qui encapsule cette route. La figure 4.2 illustre un onion construit par le proxy ou nœud initiateur W pour une route anonyme au proxy du nœud destinataire Z à travers les nœuds intermédiaires X et Y. Le proxy initiateur envoie l'onion à travers une route pour établir un circuit virtuel entre W et Z.

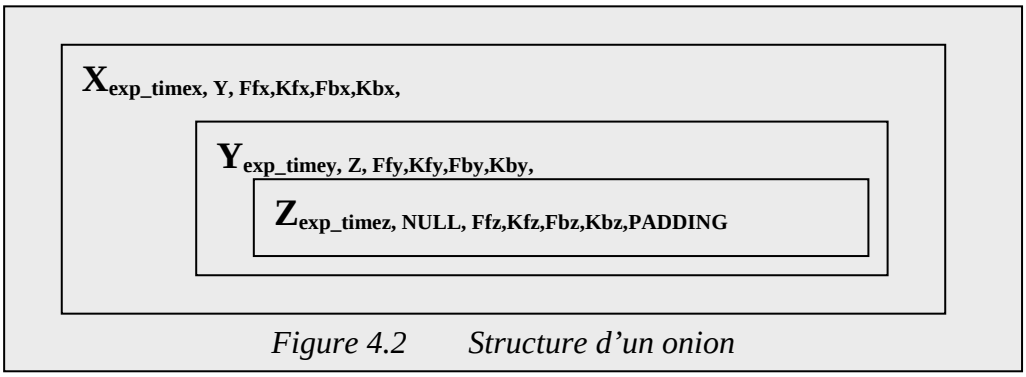

Figure 4.2 Structure d'un onion

La structure de donnée de l'onion est composée d'une succession de niveaux d'encryption. La structure de base est basée sur la route vers le destinataire, choisie par le proxy initiateur. Quand un onion est reçu, chaque nœud sait qui le lui a envoyé et à qui il doit le transmettre. Cependant, il n'a aucune idée des autres nœuds, ou encore le nombre de nœuds dans la chaîne ou sa place dans cette chaîne (à moins que ce ne soit le dernier). Un nœud Px reçoit la forme suivante :

(exp_time, next-hop, Ff, Kf, Fb,kb,payload) pkx

pkx est la clé publique d'encryption du nœud px, il est supposé avoir la clé de décryptage correspondante). Le message contient un temps d'expiration pour l'onion, le prochain nœud pour lequel l'onion doit être envoyé et deux fonctions respectivement deux clés spécifiant les opérations cryptographiques et les clés à appliquer aux données qui vont être émises à travers le circuit virtuel. La paire (Ff, Kf) est appliquée aux données circulant en chaînage avant sur la route de l'onion et la paire (Fb, kb) est appliquée aux données circulant dans la direction inverse. Si le nœud est le proxy destinataire alors next-hop est à null. Pour chaque nœud intermédiaire, le payload est un autre onion.
Le temps d'expiration est utilisé pour détecter les reproductions, chaque nœud garde une copie de l'onion jusqu'à exp_time. S'il reçoit une copie du même onion avant ce temps ou après il l'ignore.
A chaque onion routeur, l'onion est diminué d'une couche jusqu'à arriver à destination. Onion routing utilise la technique de circuits virtuels décrite précédemment.

Onion routing semble être la solution la plus efficace contre l'analyse de trafic [Goldschlag 96]. D'autres attaques dépendent de la compromission des serveurs proxy et des nœuds de routage. Si le proxy initiateur est compromis alors toute l'information est révélée. En général, un seul nœud de routage non compromis est suffisant pour compliquer l'analyse de trafic. Néanmoins, un seul nœud compromis peut détruire la connexion et ainsi provoquer une attaque de déni de service [Reiter 98].

4.2.4 Exemples d'applications nécessitant l'anonymat

Dans les points précédents, nous avons montré les techniques de base pour intégrer l'anonymat et nous avons exposé certains services pour assurer des communications anonymes. Néanmoins, il est important de montrer comment assurer la propriété d'anonymat pour deux applications de haut niveau pour lesquelles cette propriété est d'un grand intérêt : le payement et le vote électronique.

4.2.4.1 L'Anonymat et le Commerce électronique

Avec l'importance grandissante d'Internet, le commerce électronique devient un service nécessaire qu'aucun opérateur ne peut se permettre de négliger. Cependant, une grande crainte du tout électronique est la traçabilité des dépenses qui constitue un viol manifeste du respect de la vie privée des utilisateurs.
On voit à l'heure actuelle fleurir de nombreuses solutions pour le commerce électronique. La plupart ont recours à la cryptographie pour sécuriser les échanges. On peut classer les différents systèmes de paiement en trois grandes catégories [Mé 99]:

- L'argent électronique : transposition de la monnaie réelle au monde virtuel.
- Les transactions directes client-marchand : transposition sur l'Internet des opérations classiques effectuées lors d'un achat par carte bancaire ou par virement,
    - L'intermédiation : présence de sociétés qui jouent le rôle d'intermédiaire entre clients, marchands et banque. Ces sociétés gèrent des identifiants, garantissent l'identité des acteurs et l'intégrité des données.

Nous nous intéressons dans cette section au premier mode de paiement c'est à dire l'argent électronique pour lequel la notion d'anonymat est de première importance. En effet, l'argent électronique est au moins un cas d'école fort intéressant car il pose la question de l'anonymat dans les transactions électroniques en général [Mé 99]. Contrairement au métal et au papier, les bits ont la particularité d'être facilement copiables, à la perfection et à l'infini. Si l'argent électronique sous une forme non anonyme se généralise, tout organisme pourrait potentiellement espionner la vie privée des utilisateurs et de dresser des profils de consommation.

4.2.4.1.1 L'argent électronique

L'idée de départ est de transposer la monnaie réelle au monde virtuel. L'argent électronique ou e-cash se veut donc aussi simple et anonyme que l'argent liquide.
Un système d'argent électronique idéal devrait satisfaire la propriété d'anonymat telle que définie dans : [Menzus 96] l'objectif est d'assurer que personne ne peut retrouver les liens entre les utilisateurs et les achats.

Les systèmes d'argent électronique sont fondés sur la notion de pièces. Chaque pièce se présente sous la forme d'une série unique de nombres, validée par une banque et à laquelle une valeur monétaire est donnée. Les pièces (séries de nombres) sont stockées sur le disque dur du client ou sur une carte à puce. Les séries de nombres déjà utilisées seraient stockées dans une base de donnée accessible à toutes les banques. Seules les banques sont habilitées à émettre de l'argent électronique aux titulaires de comptes classiques. En fait, l'argent électronique n'est qu'un moyen de paiement supplémentaire.

Pour acheter, le client transfère les pièces à travers le réseau vers l'ordinateur du marchand. Ces données sont chiffrées et authentifiées par la signature électronique de la banque du client. On peut également envoyer de l'argent électronique à n'importe quel utilisateur privé, qui peut à son tour dépenser cet argent ou le déposer sur son compte en banque. Cependant, les pièces électroniques ne sont utilisées qu'une seule fois : le destinataire de l'argent électronique ne peut le transmettre à quelqu'un d'autre sans passer par la banque, qui lui donnera de nouvelles pièces.

La circulation de l'argent est réglée logiciellement, les procédures sont transparentes aux yeux des clients et des marchands. L'argent électronique est ainsi d'une grande simplicité d'utilisation. De plus, cela évite la transmission de coordonnées bancaires (numéros de carte par exemple) sur le réseau.
Grâce à l'automatisation offerte par les logiciels et en raison du nombre réduit d'opérations pour chaque transaction, le coût de l'argent électronique est très faible. Il est donc tout à fait adapté au règlement de petits montants.

Il n'existe pour l'instant qu'un seul projet « viable » d'argent électronique : l'E-Cash inventé par David Chaum, dirigeant de la société DigiCash. Nous détaillons ce système dans la section suivante.

Exemple : E-Cash

Il s'agit en fait de garantir l'anonymat des paiements. Ainsi, de la même façon qu'une banque sait qu'un client à retiré 100 U (unités) auprès d'un distributeur mais ne peut savoir ce qu'il est advenu de ce billet, personne ne peut connaître l'utilisation qui est faite des pièces de David Chaum.
Pour préserver l'anonymat, Chaum utilise le mécanisme de signature aveugle [Chaum 83]. Rappelons que Chaum avait introduit ce mécanisme par analogie avec une enveloppe-carbone où il s'agit de suivre le scénario suivant :

1. Le client envoie à sa banque une enveloppe scellée contenant une feuille de papier vierge et un carbone.
2. La banque, après vérification de la signature du client, signe l'enveloppe : le sceau est imprimé sur la feuille de papier grâce au carbone. Le sceau de la banque vaut une certaine somme qui est retirée du compte du client.
3. La banque retourne l'enveloppe au client. Ce dernier vérifie que le sceau de la banque est correct et décachette l'enveloppe. Il retire ainsi la feuille marquée qui vaut la somme indiquée.
4. Pour acheter un objet chez un commerçant, le client lui donne la feuille marquée. Le commerçant vérifie que la feuille est bien marquée par le sceau de la banque avant de l'accepter.

5. Le commerçant transmet la feuille marquée à la banque. Cette dernière vérifie que la marque correspond bien à son sceau et crédite le compte du commerçant.

Il est important de remarquer que la feuille marquée ne permet en aucun cas de remonter à l'identité du client : l'anonymat est donc bien préservé.
Plus concrètement, Digicash utilise RSA pour le chiffrement. Chaque acteur possède une et une seule paire de clés. Lorsqu'un client désire retirer de l'argent électronique de son compte bancaire, son logiciel Digicash construit un message M contenant un nombre N. Ce message est caché en le combinant avec un nombre aléatoire r chiffré avec la clé publique de la banque P_{banque}. Le tout est signé avec la clé privée du client S_{client}. :

Client → Banque :{ $M * r^{Pbanque}$}

La banque vérifie la signature du client puis que son compte est créditeur. Si c'est le cas, elle appose sa signature électronique grâce à sa clé privée S_{banque} :
$\{M * r^{Pbanque}\}^{Sbanque} = M^{Sbanque} * r$, cette signature confère à la pièce sa valeur monétaire. La banque envoie le résultat au client :

Banque → Client : $M^{Sbanque} * r$

M est bien signé par la banque : c'est la signature aveugle.

Le client vérifie la signature de la banque puis récupère la pièce en divisant simplement ce qu'il vient de recevoir par r. Il dispose ainsi d'une pièce anonyme et peut payer un marchand avec cette pièce :

Client → Marchand : $M^{Sbanque}$

Le marchand à qui on remet cette pièce, vérifie qu'elle est bien émise par la banque. Si la correspondance est obtenue, le marchand transmet la pièce à la banque.
Marchand → Banque : $M^{Sbanque}$

La banque vérifie que c'est bien elle qui a émis cette pièce, puis crédite le compte du marchand de la somme correspondante. Afin que cette pièce ne puisse pas être déposée une seconde fois, la banque garde une trace du nombre aléatoire N.

L'argent électronique reste encore très controversé. Pour ses partisans, il est le moyen de paiement de l'avenir, un aboutissement inévitable. Par contre, les détracteurs de l'argent électronique anonyme y voient une menace : ils craignent que les criminels s'en servent pour transférer anonymement des fonds, faire du marché noir, blanchir de l'argent ou échapper au fisc.

4.2.4.2 Vote électronique

Généralement, la procédure de vote nécessite également la vérification de la propriété d'anonymat : chacun veut conserver le secret de son vote [Menzus 96].
L'idée pour aboutir à un anonymat fort est de pouvoir dissocier le vote du votant tout en maintenant l'authentification. C'est exactement ce que réalise le protocole de signature en aveugle, appliqué au vote électronique, décrit au chapitre 1.

Le protocole appliqué suit les étapes suivantes :

Tous les votants engendrent un ensemble de messages, où :

- chaque ensemble contient un vote valide pour chaque vote possible.
- chaque message contient un numéro de série engendré aléatoirement.

1. Tous les votants camouflent individuellement tous les messages et envoient le résultat à une autorité centrale AC.
2. L'AC vérifie d'abord, si le votant n'a pas déjà soumis un vote camouflé puis signe chaque message et enregistre le nom du votant dans sa base de donnée.
3. Les votants chiffrent leurs votes avec la clé publique de l'AC.
4. Les votants envoient leur vote.
5. L'AC déchiffre les votes, vérifie les signatures, et décompte les voix.

4.2.5 Anonymat sur Internet : Synthèse

D'un point de vue social, les communications anonymes semblent être désirées seulement par une minorité de gens concernées par le problème de préserver confidentielles les informations privées et souvent non acceptées par les gouvernements ou organisations. C'est pourquoi, les solutions pour les communications anonymes ne sont pas intégrées dans des produits existants ou infrastructure, mais sont offerts comme services indépendants pour lesquels un effort supplémentaire doit être accompli pour pouvoir les utiliser.

Du point de vue technique, l'étude du problème de l'anonymat a montré qu'il y a déjà plusieurs solutions pratiques pour fournir des communications anonymes pour les applications Internet. Ces solutions restent toutes basées sur les mêmes principes.

Dans cette section, nous avons passé en revue les différentes solutions existantes pour l'anonymat sur Internet.
Que ce soit pour la messagerie électronique, la navigation ou la publication, nous pouvons déduire que les schémas de solutions présentées se basent essentiellement sur deux types de conceptions : Serveurs-Proxy ou Réseaux-basés-Mix. Les serveurs proxy ont été très populaires pendant longtemps notamment pour la messagerie électronique (anon.pipenet.fi) et la navigation (Anonymizer). La facilité de mise au point de tels systèmes justifie leur grande disponibilité. Cependant, ils assurent un anonymat qualifié de traçable et par conséquent faible de par ses points de vulnérabilités.
Les réseaux-basés-mix remédient aux problèmes des serveurs proxy en introduisant la notion de chaîne de réexpéditeurs et niveaux d'encryption. Plusieurs conceptions ont été proposées allant de la plus simple (réexpéditeurs de type 1) jusqu'aux système sophistiqués incluant toutes les fonctions complexes pour agir contre l'analyse de trafic (onion routing). Néanmoins, la disponibilité de ces derniers demeure limitée vu le coût de ces fonctions. De plus, l'efficacité de ces systèmes dépend étroitement des outils cryptographiques sur lesquels ils reposent.
En ce qui concerne les applications de haut niveau pour lesquelles il est important d'assurer la propriété d'anonymat, telle que le commerce électronique, les solutions ne sont pas très utilisées et restent controversées. En fait, l'anonymat est donc un bel objectif en soi, mais il nécessite un contrôle, notamment la possibilité de le lever en cas de besoin, comme dans le cas d'un constat de fraude. C'est pourquoi, depuis quelques années, les travaux sur la monnaie électronique ont migré de l'anonymat parfait vers l'anonymat révocable, où une institution possède une convention secrète permettant de lever l'anonymat en cas de besoin, lors d'un constat établi de fraude.

En conclusion, nous avons décrit dans cette section la problématique de l'anonymat dans un environnement filaire tel qu'Internet. Cette section nous a permis de cerner le problème de l'anonymat dans un environnement fixe. Nous allons voir dans la suite de ce chapitre que le problème de l'anonymat est posé différemment dans les environnements sans fil.

4.3 Anonymat dans les environnements mobiles

La définition de l'anonymat dans les environnements mobiles diffère de celle adoptée dans les environnements filaires. En effet, dans les environnements mobiles, l'anonymat couvre plusieurs aspects prenant en compte la confidentialité de l'identité de l'utilisateur, la confidentialité de la location de l'utilisateur et la confidentialité des mouvements de l'utilisateur.
L'anonymat consiste à protéger les informations secondaires telles que l'identité des entités impliquées dans une transaction mais aussi à protéger les méta-informations qui découlent des interactions entre entités d'un système distribué. Dans un réseau mobile, si aucune précaution n'est prise, un ennemi potentiel peut avoir accès à des informations secondaires concernant la localisation et les déplacements des utilisateurs. Les messages échangés durant la procédure d'authentification peuvent révéler des informations privées à des ennemis écoutant le médium de communication. Il devient alors possible de pister l'usager.

4.3.1. Classification des degrés d'anonymat dans les environnements mobiles

De manière formelle, Les besoins en confidentialité peuvent être représentés sous forme d'une matrice à deux dimensions [Asokan 95], les lignes correspondent aux objets c'est à dire à l'information qui peut constituer un viol de la vie privée des utilisateurs si elle est divulguée.
Les colonnes représentent les sujets qui consistent en entités dont l'accès à l'information privée doit être permis ou non selon les besoins. Si un sujet représenté par une colonne de la matrice peut être privé d'accès à une information particulière représenté par une ligne de la matrice, alors l'entrée correspondante dans la matrice prend la valeur 0. Si le sujet peut accéder à toute l'information privée alors l'entrée vaut 1. Enfin, si le sujet peut accéder à une partie de l'information alors l'entrée prend la valeur s.

Dans le contexte mobile, les sujets sont:

U : utilisateur ou unité mobile.
H : domaine de résidence.
R : domaine distant (remote domaine)
L : entité réseau légitime (autorisée).
X : espion ou tiers non autorisé.

Les objets sont :

u : identité complète de l'utilisateur.
h : identité du domaine de résidence.
r : identité du domaine distant.

Selon cette représentation, Nous identifions cinq classes particulières :

Classe C1 : Cacher l'identité de l'utilisateur vis à vis d'un tiers non autorisé

La plupart des solutions existantes offrent ce minimum de sécurité.
Dans GSM, les TMSI sont utilisés dans ce sens. Quand l'utilisateur apparaît pour la première fois dans un domaine étranger, il doit établir une résidence temporaire avec l'autorité administrative étrangère. A ce stade, un alias de longue durée est assigné à l'utilisateur pour la durée de son séjour. Le problème principal avec cette approche est que toute l'activité de l'utilisateur dans ce domaine distant peut être lié à cet alias. Après un certain temps, la

relation entre cet alias et le domaine de résidence de l'utilisateur peut être révélée par une analyse de trafic.
Une alternative plus sécurisée est d'assigner un alias différent à chaque fois qu'un utilisateur accède à un service dans le domaine visité. Ceci évite la divulgation de la relation entre l'utilisateur et l'autorité étrangère (Sujet R).

	H	**R**	**L**	**X**
u	**1**	**1**	**1**	**0**
H	**1**	**1**	**1**	**1**
R	**1**	**1**	**1**	**1**

Classe C2 : Cacher l'identité de l'utilisateur vis à vis de l'autorité visitée

Dans un environnement où le degré de confidentialité est de classe C1, le domaine visité garde trace des mouvements de l'utilisateur.
Dans certaines situations, il est nécessaire pour l'autorité étrangère de connaître l'identité de l'utilisateur. Dans ce cas, il suffit de prouver sa solvabilité et un minimum d'informations pour payer son autorité de résidence.

	H	**R**	**L**	**X**
u	**1**	**0**	**0**	**0**
H	**1**	**1**	**1**	**1**
R	**1**	**1**	**1**	**1**

Classe C3 : Cacher les relations entres utilisateurs et autorités

Un niveau plus élevé d'anonymat, consiste à dissimuler la relation entre l'utilisateur mobile et son domaine de résidence des intrus dans le but de prévenir la divulgation de l'identité de l'utilisateur par inférence.
Par exemple, si un utilisateur dont l'alias est x visite un domaine distant en France et veut s'authentifier à son domaine de résidence presidence.dz et un intrus croit savoir que les seuls utilisateurs de presidence.dz, actuellement en France, sont president@presidence.dz et vicepresident@presidence.dz. L'intrus peut donc conclure que x correspond en fait à l'une de ces deux identités.

	H	R	L	X
u	**1**	**0**	**0**	**0**
h	**1**	**1**	**0**	**0**
r	**1**	**1**	**s**	**s**

Classe C4 : Cacher l'identité du domaine de résidence vis à vis de l'autorité visitée

Quand l'utilisateur mobile a besoin d'être authentifié dans un domaine étranger, l'autorité étrangère a besoin de contacter l'autorité du domaine de résidence dans le but de confirmer la bonne volonté de l'utilisateur. Si le nombre d'utilisateurs potentiels traversant le domaine de résidence est petit dans le domaine visité. L'autorité étrangère peut deviner l'identité de l'utilisateur tel que décrit dans le paragraphe précédent. Néanmoins, dans les environnements où il y a d'autres moyens pour établir la solvabilité, un plus haut degré d'intraçabilité est possible en évitant que l'autorité étrangère connaisse l'identité de l'autorité de résidence. La politique correspond donc à la table ci-dessous.

	H	R	L	X
u	**1**	**0**	**0**	**0**
h	**1**	**0**	**0**	**0**
r	**1**	**1**	**s**	**s**

Classe C5 : Cacher le comportement de l'utilisateur de son domaine de résidence

Dans certains cas, il est important à un utilisateur mobile de dissimuler sa migration à son autorité de résidence. Ce besoin est spécifiquement important dans le cas où le système doit garantir que le comportement de l'utilisateur soit gardé parfaitement secret. Cette politique est formulée comme suit :

	H	R	L	X
u	**0**	**0**	**0**	**0**
h	**1**	**0**	**0**	**0**
r	**s**	**1**	**s**	**s**

Notons que chaque classe Ci est un sous ensemble de la classe Ci+1 car la classe Ci+1 est obtenue en augmentant les contraintes de la classe Ci. Dans ce qui suit, nous allons décrire les solutions aux problèmes d'anonymat adoptés dans les architectures de réseaux cellulaires ou celles décrites dans la littérature. Pour chaque solution, nous situerons le degré d'anonymat assuré.

4.3.2 Anonymat : Solutions

Intuitivement, dans un environnement mobile, la technique de base pour protéger une identité est l'utilisation d'alias ou d'une identité temporaire [Asokan 95]. Dans un tel environnement, l'alias choisi devra être une chaîne de caractères facilement mémorisable. La seule condition lors de la génération d'un tel alias est qu'il n'y ait aucune relation entre l'alias et l'identification réelle de l'usager dans son domaine d'affiliation. De ce fait, le choix d'un alias n'est plus sujet aux mêmes contraintes que lors de la génération d'un mot de passe.
Les méthodes de calcul et de génération d'alias ont fait l'objet de plusieurs travaux de recherche. Dans la section suivante, nous allons décrire les schémas proposés.

4.3.3 Utilisation d'une liste d'alias préalablement calculée

Cette approche est basée sur une liste d'alias préalablement calculée par le domaine d'affiliation et sauvegardée au niveau de l'unité mobile. Notons, que seules ces deux entités connaissent la correspondance entre l'alias et l'identité réelle. Les alias sont partagés entre l'utilisateur et le domaine d'affiliation à court ou à long terme. Nous distinguons donc :
Alias de longue durée de vie et alias de courte durée de vie.

a. Alias de longue durée de vie

Molva et al [Molva 95] suggèrent qu'une entité mobile doit utiliser un alias de parcours (traveling alias) quand elle traverse différents domaines. Seule l'unité mobile et son domaine d'affiliation connaissent la correspondance entre l'alias de parcours *Mt* qui change à des intervalles réguliers et l'identité réelle *M*. Néanmoins, en absence de protocole de changement d'alias de parcours dans un canal non sécurisé, les entités peuvent changer leurs alias de parcours seulement lorsqu'elles retournent à leur domaine de résidence. Pourtant, de tels alias avec des durées de vie assez longues peuvent être source de problèmes dans certaines circonstances. Par exemple, supposons que l'entité mobile doit être appelée à révéler (ou prouver) son identité réelle *M* avant de lui offrir certains services dans les domaines étrangers. Avec le temps, l'ensemble des entités qui connaissent la correspondance entre *Mt* et *M* va

croître. De plus, un observateur sera capable de tracer les différentes activités de *M* pendant la période durant laquelle l'alias est maintenu.

b. Alias de Courte durée de vie

Une alternative est l'utilisation des alias de courte durée de vie. L'alias est modifié par un accord mutuel entre l'entité mobile et le serveur du domaine de résidence. Ceci implique, que le mobile et son domaine d'affiliation restent synchronisés. Si la synchronisation est perdue, un sous protocole est nécessaire pour la re-synchronisation. Maintenir une re-synchronisation de manière sécurisée est un grand défi. En effet, l'entité mobile peut être emmenée à envoyer

son identité en clair pour rétablir la synchronisation. Ce schéma de calcul d'alias est adopté dans GSM que nous décrirons la section suivante.

Critique de la méthode (liste d'alias précalculée) :

- *Cette approche exige que le domaine d'affiliation et l'unité mobile partagent un même état afin qu'ils aient recours aux même alias.*
- *Un autre problème survient lorsque tous les alias d'une liste ont été utilisés : dans ce cas, le domaine d'affiliation doit générer en temps réel une nouvelle liste d'alias et la communiquer à l'unité mobile. Ceci nécessite soit un canal de communication sécurisé entre l'utilisateur et son domaine d'affiliation, soit un protocole additionnel de transfert fiable d'alias. De telles fonctionnalités ne sont pas toujours disponibles dans les environnements mobiles.*
- *Une dernière remarque concerne la synchronisation constante que l'unité mobile et son autorité administrative doivent maintenir dans le but de choisir le même alias au même moment. En effet, lorsqu'un décalage survient, un mécanisme additionnel est alors nécessaire pour permettre aux deux entités de se synchroniser à nouveau.*

4.3.3.1 Anonymat dans GSM

Une unité mobile active (téléphone cellulaire) dans GSM est souvent sous le contrôle d'une station de base locale BS. Quand le mobile accède à la cellule, une BS différente prend en charge cette unité.

Chaque unité mobile, une fois enregistrée dans une BS a une identité temporaire TMSI. L'utilisateur utilise cette identité pour communiquer avec la BS. En se déplaçant vers d'autres BS, l'unité mobile envoie l'ancien TMSI et LAI (Location Area Identifier) de la station de base précédente. La nouvelle BS reçoit l'identité actuelle de l'unité mobile et la résidence de la part de la station de base précédente. Si la BS n'est pas joignable, alors la station de base courante demande au mobile de révéler son identité et sa résidence. Donc, ce processus peut être exploité par un attaquant actif qui en se déguisant en station de base peut demander au mobile de révéler son identité sous prétexte qu'il ne peut avoir de contact avec la station de base précédente. Cette attaque de type man-in-the-middle, consistant à s'intercaler entre le mobile et la station, permet de prendre connaissance des IMSI d'une cellule. Ce type d'attaque, connu sous le nom de IMSI-Catcher, est réalisable par exemple à l'aide de produits destinés au test et permettant d'une part la simulation d'une station de base, d'autre part l'enregistrement des données numériques de l'interface air pour une analyse ultérieure.

D'autres possibilités pour traquer existent au niveau inter-domaines. Quand une unité mobile traverse les frontières d'un domaine, un processus d'enregistrement prend place. Son but est

d'établir (au niveau domaine) l'état nécessaire pour l'unité mobile. Au cours de son enregistrement, l'unité mobile est authentifiée avec une aide directe de sa location de résidence et un TMSI lui est assigné. Néanmoins, l'authentification du mobile implique la communication de l'identité réelle du mobile en clair (IMSI).

La conception de GSM n'offre pas d'anonymat pour les stations de base. En fait, chaque station de base découvre en plus de l'identité réelle de l'unité mobile, la précédente et la prochaine station de base visitées. De plus, toute information entre les stations de base voyage en clair. Donc, un attaquant peut facilement découvrir les identités et les locations simplement en espionnant la communication inter stations de base.

Dans GSM, l'anonymat de classe C1 n'est que partiellement assuré.

4.3.3.2 Anonymat dans UMTS

Dans le nouveau modèle de sécurité proposé dans UMTS, la protection de l'identité de l'utilisateur a été amélioré par rapport à GSM [Gunter 00]. En effet, lorsque le mobile se trouve en situation où il doit transmettre son identité réelle, dans UMTS, le mobile envoie IMUI (International Mobile User Identity) chiffré avec une clé de groupe notée GK, et l'identifiant de GK. L'autorité visitée (SN) renvoie cette information à l'autorité d'affiliation (HE). En se basant sur l'identifiant de GK, HE déchiffre le message et retrouve l'identité de l'utilisateur qu'il renvoie à SN.
En fait, le groupe qui partage cette clé GK doit être choisi assez grand pour qu'aucune information sur l'identité de l'utilisateur ne puisse être inféré de l'identifiant de GK. De plus, il doit être assez petit, pour qu'il y ait un minimum d'information divulgué si cette clé est révélée.

Il est clair que même dans la conception de UMTS, la question d'anonymat de degré élevé n'a pas été considérée. L'implémentation actuelle propose d'améliorer celle de GSM en évitant surtout le type d'attaques décrits précédemment

.

Dans UMTS, l'anonymat de classe C2 est assuré.

4.3.3.3 Alias basés sur l'Horodatage

Cette approche se base sur l'utilisation d'une base de temps commune à l'ensemble du système distribué. Herzberg et al. [Herzberg 94] ont proposé une méthode où les alias sont fonctions de l'horodatage et de la clé secrète partagée.
Dans cette approche, les auteurs assument que le monde est partitionné en domaines administratifs. Chaque utilisateur a une résidence permanente dans au moins un domaine et chaque domaine a au moins un serveur d'authentification : une entité qui se charge de l'authentification, de la distribution de clés et de la résolution d'alias.
Soit un utilisateur *A* enregistré dans un domaine de résidence *X*, avec un centre d'authentification *AuCx*. Il lui a été alloué une référence unique *IMSIA* qui contient son identité et son domaine de résidence. *A* est un mobile et en traverse un domaine *Y*. Si un service est demandé alors il est nécessaire qu'un processus d'authentification prenne place dans ce nouveau domaine entre le service provider et l'utilisateur *A*. Au cours de l'authentification, l'identité de *A*, *IMSIA* doit être transmise à *AuCx* via l'autorité étrangère *AuCy* du domaine *Y*. Time-based aliasing offre un moyen de protéger cette identité. Dans ce schéma proposé par Herzberg, un alias *TMSIA* est généré au niveau du terminal mobile :

$$TMSIA = E\ (IMSIA, T, K_A)$$

Où :
E: algorithme de chiffrement symétrique tel que DES.
IMSIA : identité de l'utilisateur.
T : temps courant.
K_A : clé de l'utilisateur.

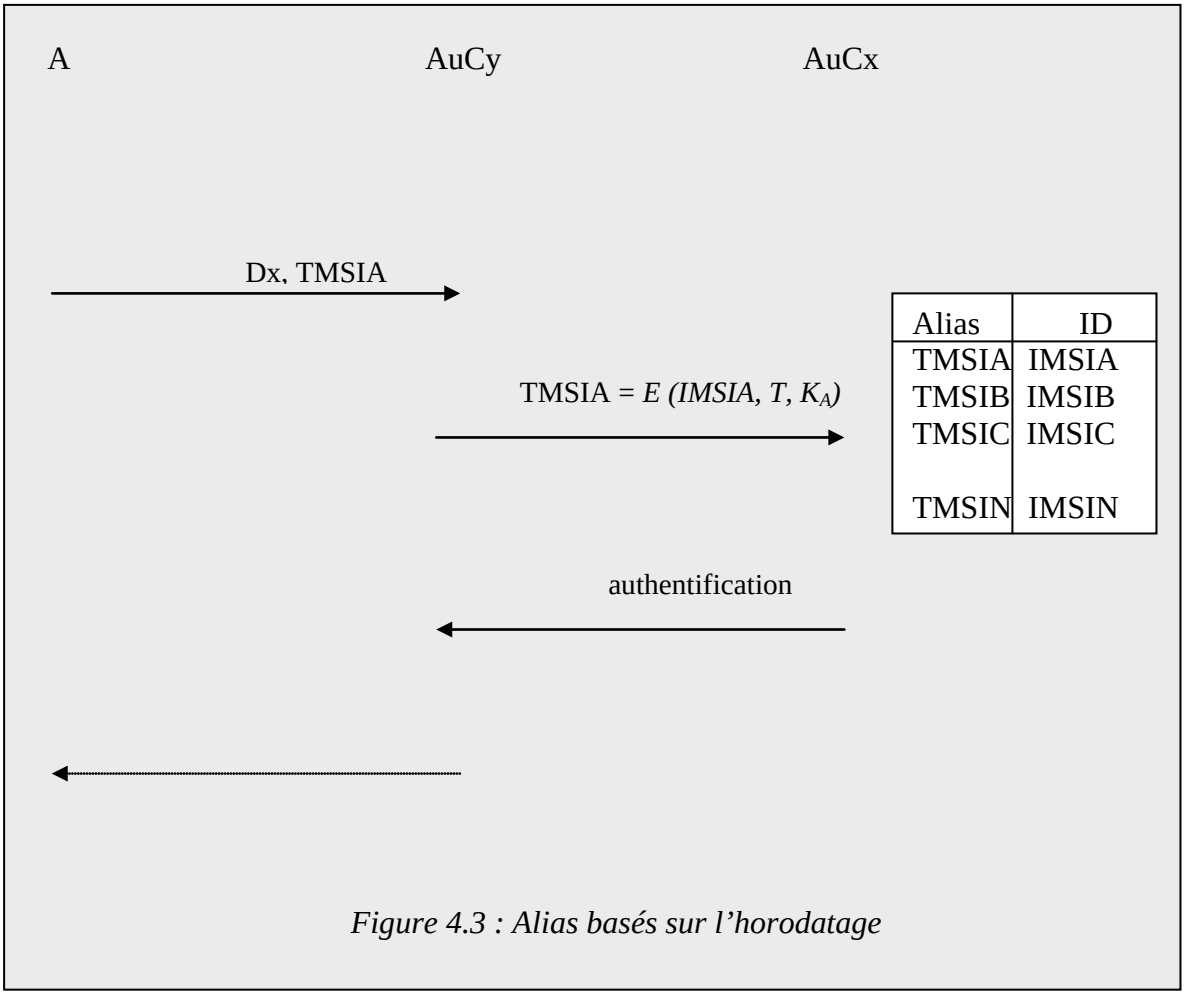

Figure 4.3 : Alias basés sur l'horodatage

Le flux d'authentification allant de l'utilisateur *A* à *AuCy* est connu sous le nom de $AUTH_{AY}$ et consiste en :

$AUTH_{AY} = Dx, TMSIA$

Où *Dx* est l'adresse de *AuCx*. La seule information que *AuCy* est capable d'obtenir est que l'utilisateur mobile est enregistré à *AuCx*.
Au niveau de *AuCx*, une table de correspondance est gérée de telle manière à trouver *IMSIA* en utilisant *TMSIA*. *AuCx* affecte une clé localement à chaque utilisateur. La table est calculée chaque dt (une heure par exemple). Du moment que *TMSI* est indépendante de la location, les tables de translation sont pré-calculées off-line et en avance.

Critique : Les inconvénients de cette méthode sont :

- *La génération et le stockage des tables d'identités demandent un espace et un temps de traitement supplémentaires.*
- *Il est toujours nécessaire à AuCx d'authentifier AuCy comme une entité réseau autorisée.*

Cette méthode (Time-based aliasing) ne fournit qu'un degré d'anonymat de classe C2 vu que chaque domaine connaît l'identité de l'autre.

4.3.3.4 Alias Aléatoires

Avec la disponibilité croissante des puissances de traitement, la station mobile est capable d'effectuer plus de traitements. Dans cette méthode [Herzberg 94], Le mobile s 'identifie par un alias généré et communiqué par le domaine de résidence dans une précédente inscription. Ces alias doivent paraître inintelligibles pour un observateur hostile de la communication. L'autorité de résidence génère chaque fois un alias en chiffrant le nom du mobile en utilisant une clé secrète connue seulement par l'autorité elle même.

$TMSI_i = E_{kx}(IMSIA, N_i)$
Où :
$TMSI_i$ = alias unique valide seulement durant la session i.
E = fonction de chiffrement symétrique tel que DES
Kx : une clé secrète connue seulement par le centre d'authentification de résidence AuCx
IMSIA : identité de l'utilisateur
N_i : sel aléatoire utilisé seulement durant cette session.

Notons que le sel est une chaîne aléatoire qui est jointe à l'identité avant qu'elle ne soit transformée par le chiffrement.

La sécurité est augmentée en rajoutant le nombre aléatoire à IMSI avant le chiffrement. Ceci a plusieurs avantages :

- Les alias du même mobile sont toujours différents.
- Un alias décrypté ne donne aucune information sur l'identité réelle du mobile.
- Une seule unité mobile compromise ne compromet pas les alias et ne révèle pas les précédents alias de la même unité.

L'avantage d'utiliser des alias aléatoires est que du moment que la procédure de calcul des alias est transparente aux utilisateurs mobiles, l'autorité de résidence est capable de changer les clés ou même les méthodes cryptographiques sans aucun impact sur les utilisateurs. L'autorité de résidence doit cependant continuer à reconnaître les anciens alias calculés.

Critique : *Les problèmes qui découlent de cette méthode sont :*

- *Plus de mémoire requise pour stocker les données.*
- *Plus de données de recherche nécessaires pour identifier l'utilisateur.*

Cette méthode (random aliases) ne fournit qu'un degré d'anonymat de classe C2 vu que chaque domaine connaît l'identité de l'autre.

Les méthodes basées sur l'horodatage ou encore les nombres aléatoires offrent, certes, un plus haut degré d'anonymat que GSM. Cependant, pour garantir un anonymat de niveau supérieur, ces méthodes doivent être utilisées en conjonction avec une technique qui permet de dissimuler les identités du domaine d'affiliation et du domaine visité

4.3.4 Chiffrement à clé publique de l'identité réelle

Une autre méthode est le chiffrement à clé publique de l'identité réelle pour générer un alias durant l'exécution du protocole d'authentification. L'unité mobile chiffre son identité réelle avec la clé publique du domaine d'affiliation et d'autres paramètres variables sélectionnés indépendamment dans chaque session, tels que les nombres aléatoires ou des estampilles appelés « nonces ».
Le protocole d'authentification proposé par Samfat et al. [Samfat 96] est basé sur un cryptosystème symétrique (décrit dans le chapitre 3). Cependant, ils ont appliqué un schéma de chiffrement à clé publique pour garantir l'anonymat de l'utilisateur. Pour cela, une identité temporaire TID_M est calculée comme :

$$TID_M = \{r_M, r_M \oplus M\}P_{kh}$$

où $\oplus$ dénote l'opération ou-exclusif.
M : l'identité réelle M.
r_M : un nombre aléatoire.
P_{kh} : la clé publique du domaine d'affiliation H.
r_M est généré indépendamment dans chaque session pour calculer TID_M. Après l'établissement de l'identité temporaire lors du premier protocole d'authentification, l'unité mobile et le domaine visité peuvent calculer une nouvelle identité temporaire TID'_M en utilisant la même technique de calcul c'est à dire :

$$TID'_M = \{r'_M, r'_M \oplus TID\}P_{kv}$$

La méthode de calcul d'alias décrite respecte l'indépendance entre les différents alias. En effet, dans la mesure où le nombre aléatoire r_M est généré par un bon générateur de nombre pseudo-aléatoires, il est impossible de faire une corrélation entre les alias d'un même utilisateur.

Cette méthode (Samfat et Molva) ne fournit qu'un degré d'anonymat de classe C2. L'identité de l'utilisateur est gardée secrète pour le domaine visité.

Néanmoins, Samfat et al. ont décrit une série de protocoles qui améliorent le degré d 'anonymat [Samfat 96]. Dans ce qui suit nous allons décrire ces protocoles.

4.3.4.1 Solution de Samfat et Molva

Dans cette section, la solution présentée montre comment le calcul des alias peut être utilisé pour protéger les différentes parties impliquées dans le processus d'authentification.

a. Hypothèses initiales

Un utilisateur a seulement une résidence qui représente le domaine administratif où il est enregistré à long terme. En accédant au réseau dans chaque domaine visité, l'utilisateur mobile est authentifié selon un mécanisme d'authentification traditionnel tel que Kerberos ou Kryptoknight [Shneier 96]. Les utilisateurs d'un domaine donné sont enregistrés avec le serveur d'authentification de ce domaine AS.
L'utilisateur a un périphérique personnel dans lequel il peut sauvegarder de l'information.
L'utilisateur a une identification universelle dont seul le domaine de résidence peut faire le lien avec les différents alias. L'identification peut être un nombre, une chaîne de caractères assigné à l'utilisateur au moment de l'abonnement. Ceci est particulièrement important pour une autorité centrale, notamment quand il s'agit de comptabilité et de facturation.

b. Critères de conception

Pour assurer une bonne confidentialité de l'utilisateur mobile durant sa migration, la génération d'alias doit tenir compte des critères suivants :

- One-time aliases : Pour dissimuler la relation entre le nom de l'utilisateur actuel et l'alias. Chaque alias doit être utilisé au plus une fois par processus de sécurité. Si le même alias est utilisé dans plusieurs processus de sécurité alors une corrélation peut être établie entre le comportement de l'utilisateur dans son domaine de résidence (identifié par le nom de l'utilisateur) et le comportement dans les domaines distants d'un utilisateur anonyme (identifié par un alias) conduisant ainsi à la divulgation de l'identité de l'utilisateur anonyme.

- Aucune corrélation entre les alias : Dans le but d'éviter la divulgation de l'identité d'un utilisateur basée sur la corrélation entre son nom et son alias, non seulement la réutilisation d'alias doit être évitée mais la relation entre un alias et le nom de l'utilisateur doit être difficile à établir.

- Séparation des Domaines : même en supposant la conspiration de tous les domaines visités (excepté le domaine de résidence), l'identité de l'utilisateur ne doit pas être divulguée.

c. Calcul des alias

La conception est basée sur le protocole d'authentification de Kryptoknight. La raison de ce choix est que Kryptoknight est un ensemble de protocoles d'authentification solide résistant contre un grand nombre d'attaques.
Les protocoles de kryptoknight n'offrent pas l'anonymat du moment que l'émetteur A envoie son identité en clair à B. De cette façon, pour cacher l'identité A des parties non autorisées, la

seule information d'identification qui peut être envoyée à travers le réseau est l'alias dont seul le destinataire B peut reconnaître que c'est une représentation secrète de A. La technique de calcul des alias est basé sur la cryptographie à clé publique.
L'utilisation des secrets partagés pour le calcul d'alias, implique nécessairement qu'une certaine information en clair doit être envoyée

La méthode utilisée pour calculer le one-time alias est :

$$ALIAS\ (A) = Pb(N'a, A)$$

Où Pb() dénote le résultat du chiffrement avec la clé publique du destinataire, ayant deux paramètres en entrée: N'a un nonce (sel aléatoire) et l'identité de l'émetteur A. La virgule entre les paramètres indique la concaténation des différents blocs pour lesquels le chiffrement est appliqué.

Se basant sur cette méthode de calcul d'alias, Molva et co ont développé trois protocoles d'authentification tenant compte des cinq classes décrites précédemment. Ces protocoles sont décrits dans les sections qui suivent.

Protocole 1 : Protocole de base

L'idée principale est de permettre à un utilisateur de modifier son alias à travers les transactions successives en générant un alias aléatoire à chaque fois. La notation suivante est utilisée dans ce protocole (figure 4.3):

Uid : identification universelle de l'utilisateur U dans son domaine de résidence.
Uidx : identification de l'utilisateur dans un domaine X.
Ash, Asr : Serveurs d'authentification dans le domaine de résidence, et le domaine distant respectivement.
Ku : clé partagée par U et Ash.
Krh : clé à long terme partagée entre ASr et ASh.
Kur : clé dépendant de la location calculée à partir de F(Uid, ASr, Ku)
Px, Sx : paire (clé publique, clé privée) de ASx.
Nx : nombre aléatoire généré par l'entité X.

Px(M) : Chiffrement du message M avec la clé publique Px de ASx.
AUTHxy : message d'authentification calculé par X pour être vérifié par Y.

TICKkx(Ks) : un ticket calculé avec la clé Kx et contenant une clé de session Ks
F(M) : fonction de hachage tel que MD5 appliqué au message M.
$\oplus$: ou exclusif (xor).

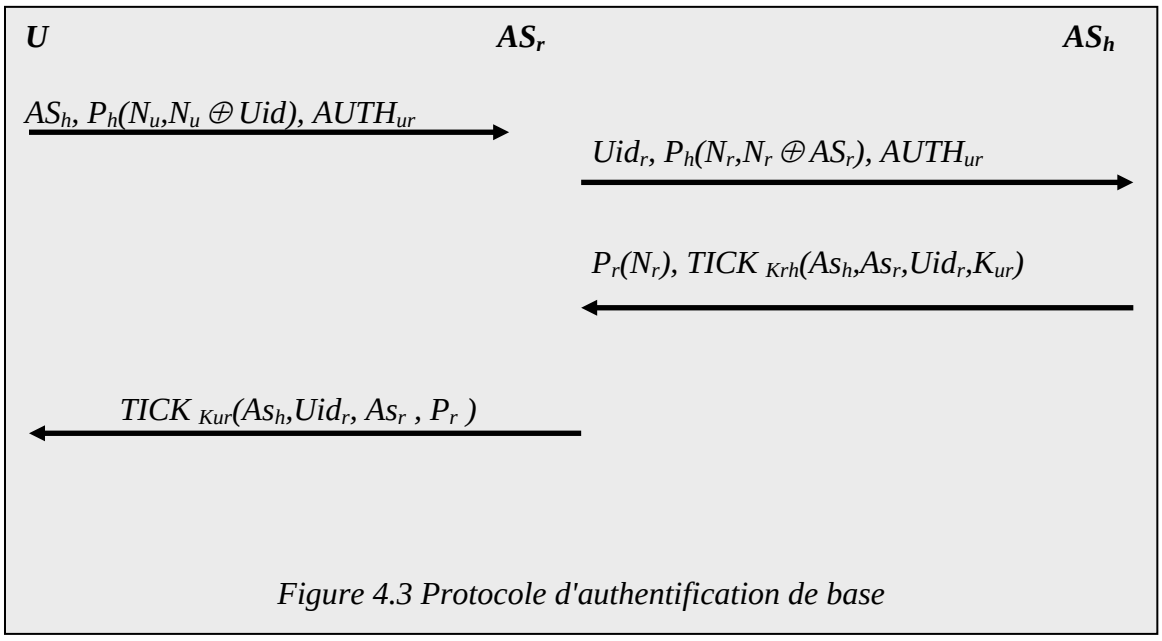

Figure 4.3 Protocole d'authentification de base

Détaillons le protocole :

1. L'utilisateur commence par générer un nonce Nu et sa clé Kur dépendante de sa location et les sauvegarde dans son périphérique. Puis, il calcule son alias Ph(Nu, Nu+Uid) et son message d'authentification en utilisant la clé Kur. Ensuite, il envoie ces messages au serveur local ASr avec l'identité de ASh. Notons qu'à cette étape, la *relation entre l'utilisateur et ASh est révélée*.

2. A la réception de ce message initial, ASr génère un nonce Nr et sauvegarde Pr(Nr) aussi bien que l'identification future de l'utilisateur dans le domaine distant c'est à dire : Uidr = F((Ph(Nu, Nu+Uid)) dans sa base de données. Puis il génère son propre alias Ph(Nr, Nr+ASr) et calcule son message d'authentification.

3. Lorsque ASh reçoit le message de ASr, il procède comme suit:
   a) il déchiffre l'alias de l'utilisateur avec Sh pour obtenir $N_u, N_u \oplus Uid$. Uid est ainsi obtenu en appliquant l'opération xor une fois de plus.
   b) ASh recouvre l'identité de ASr de la même manière.
   c) Ayant Uid et ASr, ASh est capable de retrouver la clé secrète partagée dans la base de données. Puis, Ash génère Kur et recalcule AUTHur et le token AUTHrh.
   d) Une mise en correspondance à ce niveau authentifie l'utilisateur et ASr sans révéler Uid ou ASr à une tierce partie.
   e) Comme ASh a besoin d'un ticket contenant la location dépendante de la clé Kur à ASr, il retourne simplement Nr crypté avec la clé publique de ASr avec le ticket.
4. A la réception d'un message de ASh, ASr recherche Pr(Nr) dans sa base de données et retrouve l'information nécessaire pour lire le ticket arrivant. Ayant Kur, ASr est

   capable de vérifier l'intégrité de la clé en recalculant AUTHur recu. En fait, envoyer Pr(Nr) évite le besoin à ASh de calculer et d'envoyer son alias. Cette valeur peut être

vue comme un nombre de transaction secrète identifiant le processus d'authentification entre l'utilisateur et ASh. En d'autres termes, il permet à Asr de connaître qui envoie le ticket et à qui Kur appartient en assurant un anonymat à la résidence AS et à l'utilisateur.

Critique : Ce protocole offre les propriétés d'anonymat des classes C1 et C2 puisque l'identité de l'utilisateur n'est pas révélée aux observateurs incluant toutes les autorités légitimes excepté ASh. Notons que l'identité de ASr n'est pas révélée à un observateur localisé entre ASh et ASr.

Protocole 2 : Protocole de Samfat et Molva amélioré 1

Le protocole décrit précédemment ne garantit pas le secret de la relation entre l'utilisateur et son domaine de résidence car l'identité de ASh est révélée. Dans le but d'atteindre un degré supérieur de confidentialité, l'utilisateur doit calculer un alias pour ASh en utilisant la clé publique Pr de ASr (figure 4.4). Comme l'utilisateur mobile n'a pas nécessairement Pr avant le commencement du protocole d'authentification, il doit obtenir le certificat de la clé publique dPr de ASr.

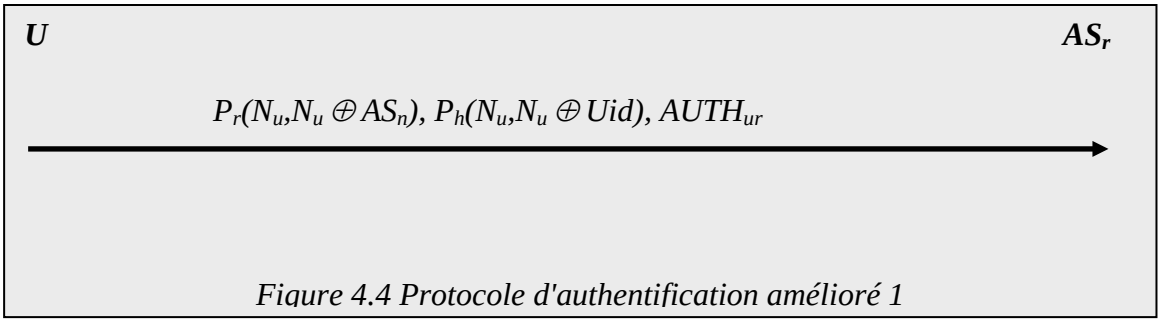

Figure 4.4 Protocole d'authentification amélioré 1

Protocole 3 : Protocole Amélioré 2

Les protocoles décrits ci-dessus obligent l'utilisateur à contacter le domaine de résidence dans le but d'authentification. Le protocole décrit dans la figure 4.5 évite de contacter le domaine de résidence.
Les auteurs [Samfat 96] ont introduit de nouveaux paramètres :

X: alias calculé pour l'identité X en utilisant la technique de clé publique définie précédemment.

Uid_d : authentification/alias de l'utilisateur dans le domaine D.

K_{ua} : clé dépendante du temps utilisée seulement une fois.

$K'_{ua} = F (K_{ua} , T_u, Uid_a)$

L'idée de base de ce protocole est que l'utilisateur a seulement besoin de la connaissance d'un domaine récemment visité D pour garantir sa solvabilité au domaine courant. Nous assumons que l'utilisateur a déjà été authentifié dans le domaine D et partage une clé secrète Kua avec AS

Ce protocole satisfait l'anonymat tel que défini dans la classe C4 puisque la migration du mobile est cachée à son domaine de résidence. Notons, que le premier domaine visité, en exécutant ce protocole, connaîtra la location de résidence de l'utilisateur mobile. Cependant, le domaine de résidence est supposé ne pas être en collaboration avec les autres autorités, donc le domaine étranger ne saura pas qu'il s'agit du domaine de résidence. La seule information qu'il a est que le mobile lui a fourni l'identification d'un serveur digne de confiance qui peut garantir sa solvabilité.

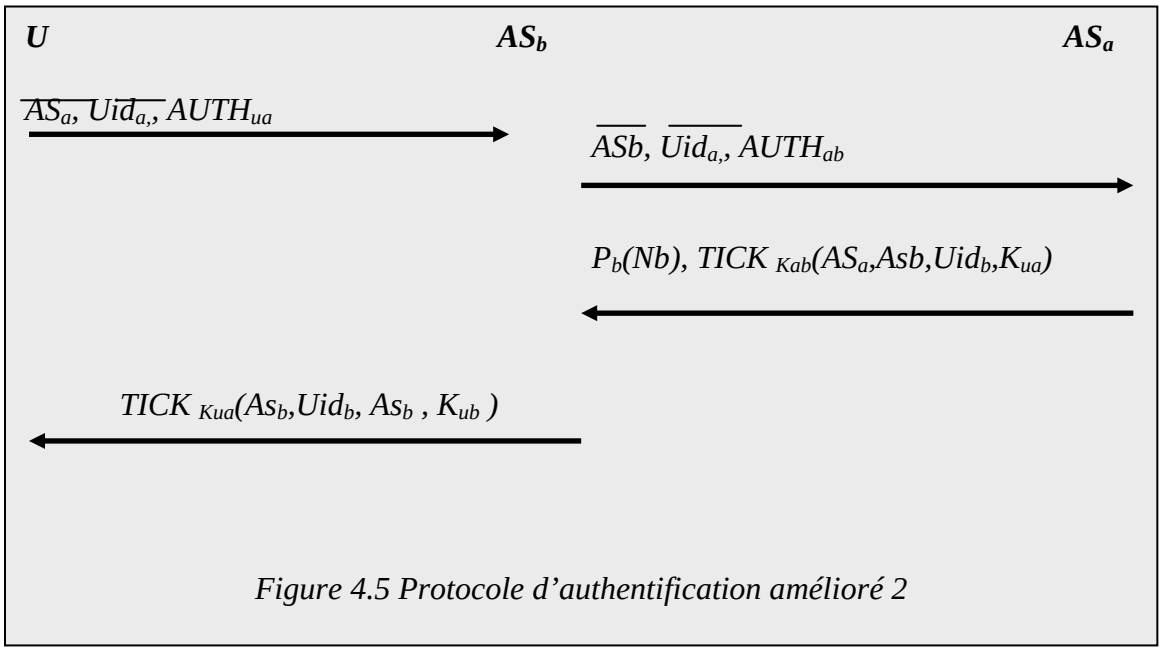

Figure 4.5 Protocole d'authentification amélioré 2

L'intracabilité définie dans la classe C5 est partiellement assurée par ce protocole. En fait, le domaine de résidence connaîtra toujours la première migration de l'utilisateur dans un domaine distant. C'est la seule information que le domaine de résidence puisse avoir dans un temps limité en supposant qu'il n'y a pas de collusion entre les autorités des domaines. Ce protocole est classé en fait entre les classes C4 et C5.

4.4 Synthèse des Solutions présentées

A l'issue de ce chapitre, nous pouvons élaborer une synthèse des solutions apportées à l'anonymat dans les environnements mobiles en se basant sur trois critères de comparaison :

- La politique d'Anonymat
- L'intraçabilité
- L'hypothèse de tiers digne de confiance (Trusted Third party)

4.4.1 Politique d'Anonymat

Une formalisation du problème de la confidentialité des méta-informations définit une classification qui permet d'identifier cinq politiques d'anonymat. Grâce à cette classification, nous avons démontré que les solutions existantes telles que GSM présentent des faiblesses lorsqu'il s'agit de fournir un anonymat même partiel. Néanmoins, toutes les solutions présentées ne peuvent offrir un anonymat complet tel que défini par la politique C5.
Enfin, le tableau ci-dessous récapitule les critiques et permet de comparer les différents protocoles présentés en termes de classes d'anonymat.

	GSM	**UMTS**	**Herzberg et al.**	**Protocole de base de Molva**	**Protocole amélioré de Molva**
Politique d'anonymat	*Partiellement C1*	*C1 et C2*	*C1 et C2*	*C1 et C2*	*C4*

4.4.2 L'intraçabilité

Dans ce qui suit, nous allons comparer les solutions présentées selon le critère d'intraçabilité : la possibilité de pister les déplacements d'une unité mobile. Pour cela, il est important de souligner qu'en général les intrus sont classés en deux classes : les insiders et les outsiders. Un outsider est celui qui peut intercepter la communication à travers les ondes radio par exemple. Un insider est celui qui a accès à l'information et peut la révéler. Dans notre cas, les insiders peuvent être le domaine visité et le domaine d'affiliation. Le tableau ci-dessous résume la protection de l'identité de l'unité mobile vis à vis de ces domaines et vis à vis d'un observateur externe.

	Outsider	Domaine visité	Domaine d'Affiliation
GSM	~oui	non	non
UMTS	oui	non	non
Herzberg	oui	non	non
Samfat	oui	oui	~non

4.4.3 Hypothèse du tiers digne de confiance (Trusted Third party)

Dans la majorité des solutions décrites, les concepteurs adoptent dans les hypothèses initiales : la présence d'une autorité digne de confiance. Cependant, cette hypothèse contredit l'anonymat de classe C5, car dans ce cas l'autorité d'affiliation connaît tous les déplacements de l'utilisateur. Par conséquent, cette autorité peut sous certaines conditions révéler des informations secrètes.
Ce point est très important car il constitue le point fort de la solution que nous allons présenter par la suite.

	Autorité éprouvée
GSM	oui
UMTS	oui
Herzberg	oui
Samfat	oui

4.5 Conclusion

Dans ce chapitre nous avons étudié l'anonymat dans son contexte global. Il nous a permis de constater que le problème d'anonymat est posé dans les environnement mobiles de manière différente que dans les environnements fixes. Nous avons pu critiquer et classer les différentes solutions d'anonymat selon les classes définies dans la formalisation de l'anonymat dans les environnements mobiles. L'objet du chapitre suivant est de présenter une solution qui permet de garantir un anonymat complet.

5.1 Introduction

L'anonymat peut être vu comme un besoin conflictuel avec l'authentification, puisque l'anonymat a pour but de dissimuler l'identité de l'utilisateur alors que l'authentification nécessite la révélation de l'identité dans le but d'être prouvée. Les solutions étudiées ont montré la possibilité de concilier entre l'authentification et l'anonymat. Néanmoins, toutes les solutions qui ont été proposées ne garantissent pas un anonymat complet.
En effet, les solutions intégrées dans les réseaux cellulaires tels que GSM et UMTS n'offrent qu'un anonymat partiel. Les solutions proposées dans les travaux de recherche n'assurent, dans le meilleur des cas, qu'un anonymat de classe C4. Dans ce cas, l'autorité d'affiliation garde trace des différents mouvements de l'utilisateur. Par conséquent, même si les mouvements de l'utilisateur ne peuvent pas être tracés par un intrus, ou par une autorité visitée; il demeure, néanmoins, traçable par son autorité d'affiliation. Cependant, l'intracabilité ou l'anonymat complet de l'utilisateur est indispensable dans des applications telles que le commerce ou le vote électronique ou encore les groupes de discussion anonymes.
L'émergence de ce type d'applications dans les environnements mobiles nécessite de prendre en compte l'anonymat et de préserver l'intimité numérique dans ces environnements.
Nous nous sommes donc fixés comme objectif de définir un protocole d'authentification satisfaisant l'anonymat de classe C5 dont la politique est formulée dans le chapitre précédent par :

	H	**R**	**L**	**X**
u	**0**	**0**	**0**	**0**
h	**1**	**s**	**0**	**0**
r	**s**	**1**	**s**	**S**

où
U : utilisateur ou unité mobile.
H : domaine de résidence.
R : domaine distant (remote domaine)
L : entité réseau légitime (autorisé).
X : espion ou tiers non autorisé.
Les objets sont :
u : identité complète de l'utilisateur.
h : identité du domaine de résidence.
r : identité du domaine distant.

L'identité complète de l'utilisateur U n'est connue ni de l'autorité d'affiliation H, ni de l'autorité visitée R, ni de toute autre entité réseau légitime ou non.
Dans notre solution, le but est donc de dissimuler totalement l'identité de l'entité mobile. Même si les informations concernant respectivement l'identité de l'autorité d'affiliation et l'autorité visitée, sont divulguées, la relation entre l'utilisateur mobile et chacune de ces entités ne pourra jamais être connue.

La solution que l'on propose, contrairement aux solutions précédentes, **garantit** un anonymat complet où le mobile devient intraçable même par son autorité d'affiliation.
Les solutions présentées dans la littérature pour résoudre le problème d'anonymat se basent toutes sur la notion d'alias. Nous avons pu démontrer que les alias ne peuvent pas garantir un anonymat complet. Car dans le meilleur des cas, l'autorité d'affiliation connait la relation entre l'alias et l'identité réelle.
Bien que l'anonymat dans les environnements fixes et dans certaines applications semble différent de l'anonymat dans les environnements mobiles, il n'en demeure pas moins que les techniques utilisées notamment la signature en aveugle proposée par Chaum [Chaum 83] pour la monnaie électronique [Win 01] constituent une solution pour l'anonymat complet dans les environnements mobiles. Pour notre part, nous avons choisi d'utiliser cette technique pour définir un protocole d'anonymat. Avant d'aborder la description de la solution proposée, nous allons expliquer le principe de la signature en aveugle.

5.2 Principe des signatures en aveugle

Une caractéristique essentielle des protocoles de signature numérique est que le signataire d'un document sait toujours ce qu'il signe. Cependant, il y a des situations dans lesquelles les gens signent un document sans jamais en voir le contenu. Ceci est possible grâce à la notion de signature en aveugle inventée par David Chaum [Menzus 96]. Une signature aveugle ou signature en blanc [Pointchaval 96], comme l'indique son nom, par analogie aux chèques en blanc, consiste à faire signer à une personne un document qui lui est inconnu. De plus, on souhaite que cette personne soit ensuite incapable de reconnaître cette signature et/ou d'y relier un message. En d'autres termes, après avoir signé plusieurs documents, le signataire est incapable, à la vue d'un message signé « par sa main » de déterminer à quelle signature en blanc ce message correspond. La notion de signature en blanc introduite par David Chaum, permet donc typiquement d'assurer l'anonymat en monnaie électronique. Reprenons l'exemple cité dans [Menzus 96] pour expliquer cette méthode :

Exemple :

- *B est notaire. A veut qu'il signe un document mais il ne veut pas qu'il ait la moindre idée de ce qu'il signe. B ne s'intéresse pas au contenu du document, il ne fait que certifier que le document a été enregistré devant un notaire à une certaine date.*

- *Voilà ce à quoi il consent :*

  i- *A prend le document et le multiplie par une valeur aléatoire. Cette valeur aléatoire est appelée facteur de camouflage.*
  ii- *A envoie le document camouflé à B.*
  iii- *B signe le document camouflé.*
  iv- *A divise par le facteur de camouflage, retrouvant ainsi le document original signé par B*

- *A ce niveau, on se pose la question : B peut il tricher ? peut-il acquérir de l'information concernant le document qu'il signe ?*

- *Si le facteur de camouflage est vraiment aléatoire , il ne peut pas. Le document camouflé que B signe à l'étape 2 ne ressemble en rien au document original de A.*
- *Le document camouflé avec la signature de B à l'étape 3 ne ressemble en rien au document signé à la fin de l'étape 4.*
- *Même si B met la main sur le document avec sa signature après l'accomplissement du protocole, il ne peut pas prouver (à lui même ou à toute autre personne) qu'il l'a signé dans le cadre de ce protocole-là.*
- *B sait que sa signature est valide. Il sait qu'il (ou quelqu'un d'autre avec sa clef privée) a signé ce document ; il peut, comme n'importe qui d'autre, vérifier la signature.*
- *Toutefois, il ne dispose d'aucun moyen de corréler la moindre information qu'il a reçue durant le protocole avec le document signé. S'il signe un million de documents avec ce protocole, il n'a toujours pas de moyen de savoir dans quel cas il a signé un tel document.*

5.3 Propriétés des signatures en aveugle

Les propriétés des signatures en aveugle total sont :

- La signature de B sur le document est valide. La signature sert de preuve que B a signé le document. B sera convaincu qu'il a signé le document quand on le lui montrera. Les propriétés des signatures numériques présentées précédemment sont aussi valables.

- B ne peut pas faire le lien entre un document signé et l'acte de signature du document. Même s'il garde une trace de toutes les signatures en aveugle qu'il a effectuées, quand on lui présente un document signé, il ne peut pas déterminer quand il l'a signé.

Une personne, assise entre A et B, qui écoute tout le protocole, en sait encore moins que B.

La méthode de David Chaum peur être résumée ainsi (figure 5.1) :

- Les documents camouflés sont dans des enveloppes.
- Le procédé de camouflage consiste à mettre le document dans une enveloppe.
- Le procédé de retrait du facteur de camouflage consiste à ouvrir l'enveloppe.
- Quand le document est dans l'enveloppe, personne ne peut le lire.
- Le document est signé grâce à une feuille de carbone dans l'enveloppe.
- Quand les signataires signent l'enveloppe, leurs signatures passent à travers la feuille de carbone et sont ainsi transférées sur le document.

L'utilisation de la signature aveugle a donc permis de garantir l'anonymat dans des applications telles que [Stadler 95]:
- Le commerce électronique avec l'introduction du concept de monnaie électronique, décrit au chapitre 4.
- Les systèmes de vote électronique pour lesquels l'anonymat constitue la pierre angulaire car il est important de dissocier le bulletin de vote du votant et assurer l'intraçabilité du votant durant tout le processus de vote [Benmeziane 02].

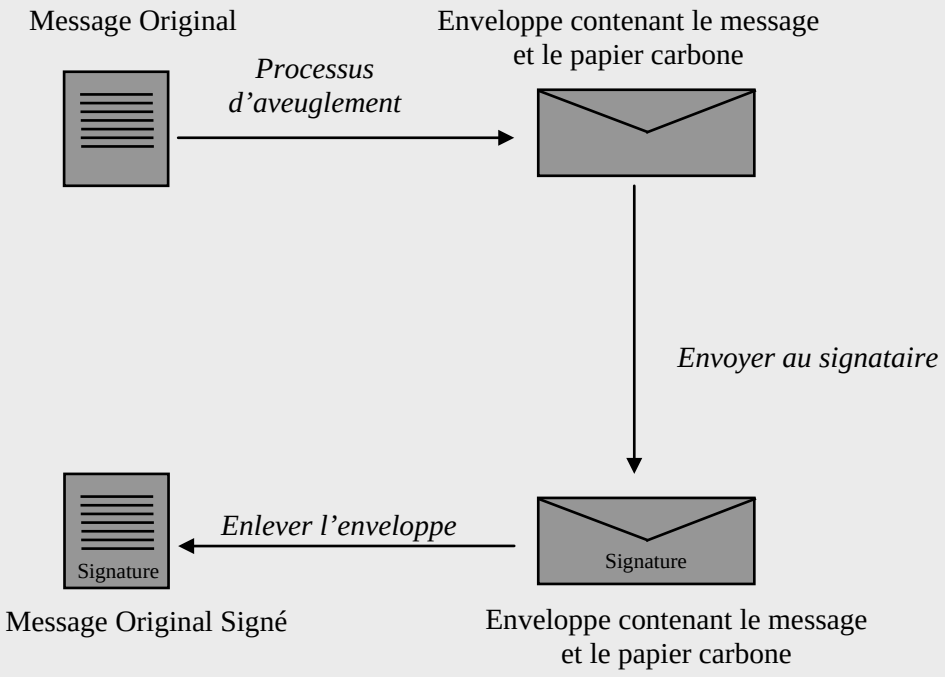

Figure 5.1 Principe de la Signature aveugle

Dans ce qui suit, nous allons expliquer comment réaliser une signature en aveugle en utilisant l'algorithme de chiffrement asymétrique RSA (décrit en annexe), signature que nous utiliserons dans notre solution.

5.4 La signature RSA en Aveugle

Avant de présenter un exemple de signature aveugle avec RSA, expliquons comment on réalise une signature digitale avec RSA. Le principe du Cryptosystème RSA repose sur l'utilisation des fonctions puissance dans le sous ensemble des entiers modulo n (décrit en annexe). La clé publique est la paire (n, e) et la clé secrète est (n,d).

- Pour signer un message m, A doit calculer :

$$S = m^d \bmod n$$

- Pour vérifier que le message a bien été signé par A, on calcule :

$$m = S^e \bmod n \quad (e \text{ étant la clé publique de A})$$

Nous allons expliquer la transformation en blanc du schéma RSA (figure 5.2). Ce fut le schéma utilisé par David Chaum dans les premiers systèmes de monnaie électronique [Chaum 83].

Soient A le signataire et U le détenteur du message m.

- *U veut faire signer le message m en aveugle par A.*
- *U doit d'abord calculer x, puis l'envoyer à A:*

  $x = m\, r^e \bmod n$ *r étant le facteur de camouflage et e la clé publique de A.*
- *A va signer x :*

  $y = x^d \bmod n$
- *U récupére s qui est la signature du message x et le divise par le facteur de camouflage r :*
  $x^d\ r^{-1} \bmod n = m^d\ (r^e)^d\ r^{-1} \bmod n = m^d \bmod n$ *qui est exactement la signature traditionnelle de m par A.*

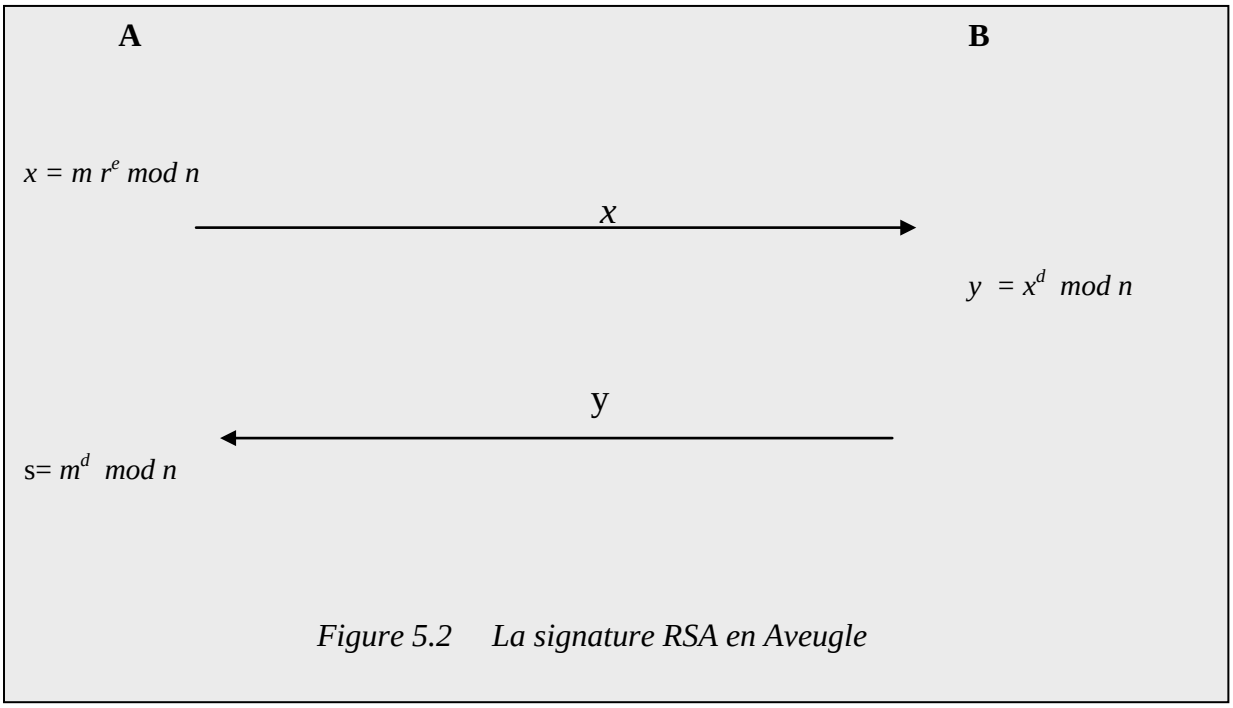

Figure 5.2 La signature RSA en Aveugle

5.5 Motivations pour la signature aveugle et les algorithmes à clé publique dans le milieu mobile

Rappelons que la signature aveugle ou plus généralement la signature digitale repose sur un schéma cryptographique à clé publique. Il est clair que l'implémentation de ces derniers est coûteuse en milieu mobile vu leurs caractéristiques inhérentes.
Néanmoins, les avancées technologiques en termes d'évolution des équipements mobiles (vitesse du processeur) et les développements en cryptographie [Curtis 01] nous ont encouragé à considérer la signature aveugle dans les environnements mobiles.

- En effet, en termes d'équipements mobiles, plusieurs solutions sont actuellement proposées par les grands fabricants de cartes et évolueront dans le temps grâce aux fournisseurs de composants. Récemment cette évolution s'est traduite par l'arrivée sur le marché de circuits à microcontroleurs, puissants et fonctionnellement riches. Des solutions avec cryptoprocesseur ou unité de calcul spécialisée en logique câblée sont proposées, autrement dit, il s'agit de spécialiser une partie significative de la carte du mobile pour y exécuter des calculs arithmétiques. Actuellement, plusieurs produits sont disponibles avec un cryptoprocesseur facilitant le chiffrement asymétrique en intégrant RSA.

- En termes d'algorithmes cryptographiques, plusieurs travaux de recherche actuels ont défini des algorithmes à clé publique avec de meilleurs performances. Nous notons essentiellement les efforts concentrés sur l'amélioration de RSA, notamment les travaux de [Khamitov 03] qui définissent une nouvelle version de la signature aveugle avec RSA adapté aux environnements avec des ressources limitées. Le protocole que nous proposons utilise un schéma de signature aveugle basé sur la version simplifiée de RSA.

5.6 Modèle du Système

Avant de concevoir un protocole d'authentification pour les environnements mobiles, nous commençons par décrire l'environnement de communication et les différentes entités du protocole (figure 5.3).

- Un utilisateur mobile se déplace librement dans les différents domaines du réseau sans fil.
- Les services de communication mobiles peuvent être offerts par divers réseaux sous des domaines administratifs différents.
- Lorsqu'un utilisateur désire s'abonner à un service donné, il choisit un réseau comme étant son réseau de résidence et devient donc un abonné de ce réseau.
- Quand un utilisateur mobile se déplace vers un autre réseau différent de son réseau de résidence, le réseau devient donc le réseau visité.

L'architecture de base schématisée dans la figure 5.3 représente les différentes entités. Les différents composants sont ceux définis dans un réseau cellulaire tel que GSM (défini au chapitre 1).

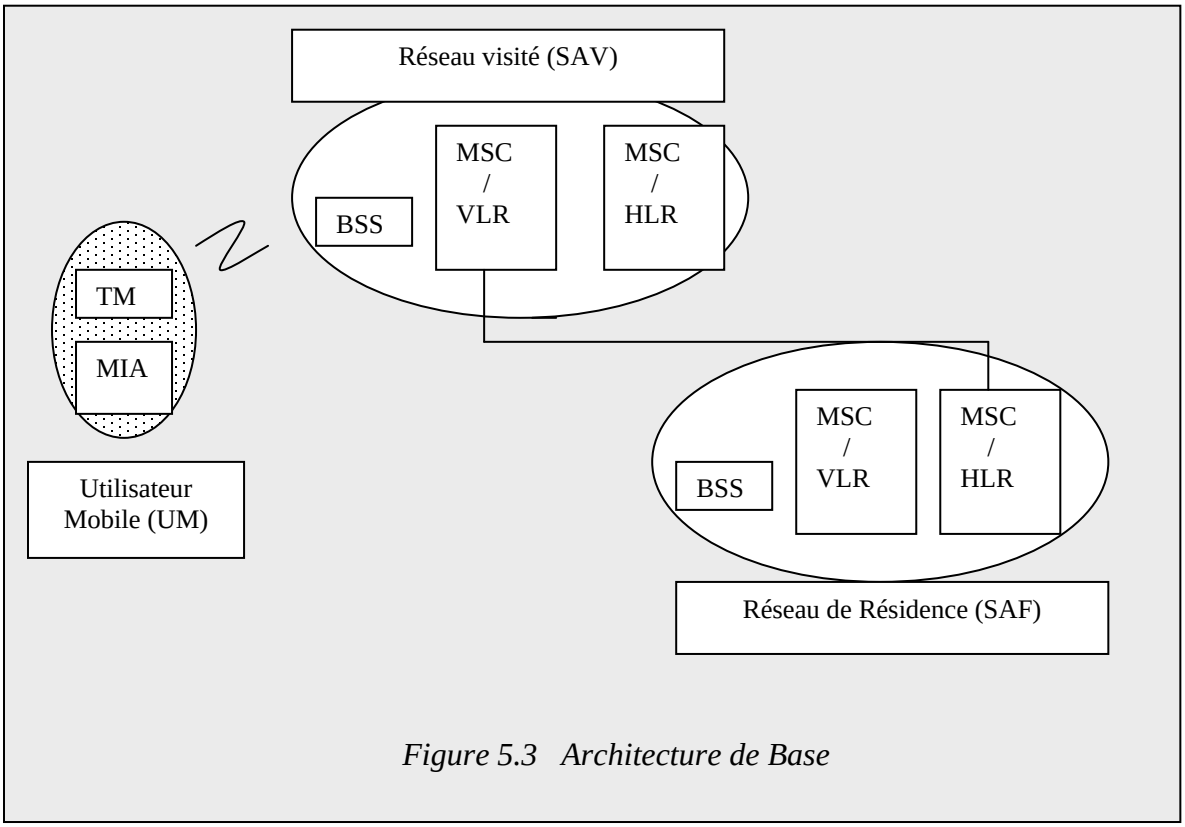

Figure 5.3 Architecture de Base

L'entité mobile contient l'équipement ou le terminal mobile (TM), et le module identité de l'abonné (MIA), similaire à la carte SIM de GSM. Nous considérons que les deux entités TM et MIA sont combinées pour représenter une même entité que nous notons UM dans le protocole.

Nous représentons également le réseau de résidence ou réseau d'affiliation par son serveur d'authentification noté SAF (serveur d'authentification de l'autorité d'affiliation) et par analogie le réseau visité est représenté par son serveur d'authentification SAV (serveur d'authentification du domaine visité).

5.6.1 Hypothèses initiales

Nous supposons que :

- Un utilisateur a un terminal mobile équipé d'un périphérique personnel avec une mémoire non-volatile pour sauvegarder des informations et qui a des capacités de calcul qui supportent des opérations cryptographiques à clé publique.

- Au moment de l'abonnement à un service donné, l'autorité d'affiliation fournit à un utilisateur mobile, son identité réelle stockée dans MIA ainsi que la clé publique de celle-ci. En effet, la clé publique de l'autorité d'affiliation est connue de tous ses abonnés.

- Un réseau visité ne doit fournir des services que si le réseau de résidence confirme l'identité de l'utilisateur mobile. Nous décrirons comment, dans notre protocole, cette vérification est effectuée sans divulguer l'identité réelle.

Dans la solution proposée, nous nous fixons les objectifs suivants :

a. réconcilier les mécanismes d'authentification et d'anonymat
b. prendre en charge l'anonymat complet et éviter la traçabilité
c. garantir la confidentialité des messages échangés.

Pour assurer la confidentialité des messages échangés, nous utilisons un cryptosystème à clé publique. L'adaptation d'un cryptosystème asymétrique permet de garantir un certain nombre d'avantages par rapport aux algorithmes symétriques :

- Les algorithmes à clé symétrique nécessitent des relations de confiance entre le réseau et tous ses abonnés. Plus le nombre de réseaux est grand, plus la configuration du réseau évolue et il est donc plus difficile de gérer toute relation de confiance entre eux dans tout le réseau. En utilisant les clés publiques, ceci est évité puisque les clés publiques peuvent être distribuées librement à toutes les entités qui en ont besoin. L'utilisation des clés publiques peut réduire le temps de déperdition (overhead) de la gestion des clés.
- La non Répudiation de l'utilisation d'un service : La non répudiation de l'utilisation d'un service ne peut être possible que par l'utilisation d'algorithmes cryptographiques à clé publique c'est à dire les signatures digitales.

Pour cela, nous assumons que les différentes entités peuvent exécuter les fonctions cryptographiques suivantes :

- Une fonction de chiffrement asymétrique.
- Un générateur de nombres aléatoires.
- La signature aveugle pour l'autorité d'affiliation.

Dans le contexte de cette thèse, nous supposons que les fonctions cryptographiques considérées sont sures. Autrement dit :

- Il existe un cryptosystème asymétrique sûr [Pointcheval 00].
- Il existe un schéma de signature aveugle sûr [Poitcheval 96]

5.7 Description générale du protocole

Le protocole d'authentification que nous proposons se base sur la notion de ticket d'authentification. En effet, c'est ce ticket qui permettra d'identifier l'utilisateur. Ce ticket est différent de la notion d'alias vu dans le chapitre précèdent. En fait, il n'y a aucune relation entre le ticket et l'identité réelle de l'utilisateur.
Rappelons, qu'un utilisateur est doté d'un terminal mobile équipé d'un périphérique personnel avec une mémoire non-volatile pour sauvegarder des informations et qui possède des capacités de calcul capables de supporter des opérations cryptographiques à clé publique. Au moment de l'enregistrement, un abonné obtient au niveau de son unité mobile, en plus des informations relatives à son identité et l'identité de son autorité de résidence :

- la clé publique de l'autorité d'affiliation pour le chiffrement des messages donc pour garantir la confidentialité.
- et une autre clé publique pour la signature en aveugle.

Notons que nous utilisons deux algorithmes asymétriques : le premier utilisé pour le chiffrement des messages et le second pour la signature en aveugle. D'où les deux clés stockées au niveau du mobile.

Lors de la première authentification, l'unité mobile transmet :

- son identité réelle et le ticket d'authentification (généré aléatoirement par l'unité mobile) chiffrés avec la clé publique de l'autorité d'affiliation,
- et l'identité de l'autorité d'affiliation.

- A ce niveau, l'autorité visitée transmet le message chiffré à l'autorité d'affiliation. Cette dernière pourra ainsi déchiffrer ce message et vérifier si cet abonné est bien enregistré à son niveau. Notons que le ticket présenté est camouflé selon le procédé décrit précédemment ; donc l'autorité d'affiliation ne pourra pas connaître le contenu. Néanmoins, elle le signera en aveugle et le retransmettra à l'abonné via l'autorité visitée.

- Ce dernier (l'abonné), ôtera le facteur de camouflage du ticket et retrouvera le ticket initial signé avec la clé publique de l'autorité d'affiliation. En fait, ce ticket servira à authentifier cet utilisateur sans révéler son identité.

- Après obtention de ce ticket, le mobile pourra s'authentifier grâce à lui. En effet, durant le protocole d'authentification, l'unité mobile ne présentera que ce ticket à l'autorité visitée. Celle-ci le transmet à l'autorité d'affiliation, qui attestera que le détenteur de ce ticket est bien un de ses abonnés car le ticket est signé avec sa clé. Mais, elle ne pourra jamais révéler à qui elle a signé ce ticket car celui-ci est différent du ticket qu'elle a signé en aveugle (facteur de camouflage).

Notons que le ticket (tel que dans kerberos) a une durée de vie limitée qui peut être choisie par l'utilisateur lui même ou imposée par l'autorité d'affiliation. Lorsque cette durée est expirée, l'unité mobile doit acquérir un autre ticket.

A l'issue de cette description générale, nous pouvons diviser le protocole d'authentification en trois phases que nous décrivons dans les sections suivantes :

- Phase 1 : Obtention du Ticket d'Authentification
- Phase 2 : Authentification
- Phase 3 : Expiration du Ticket d'Authentification.

Pour illustrer les messages échangés entre les différentes entités, adoptons le schéma de notation ci-dessous :

Notation

IM: identification de l'utilisateur mobile UM.
ASV, ASF: identification du serveur d'authentification respectivement dans le domaine visité et dans le domaine d'affiliation.
$X \rightarrow Y : Z$ signifie que X envoie le message Z à Y
(M)k : Le message M est chiffré avec la clé k.
Kpf : clé publique du domaine d'affiliation.
Ksf : clé privée du domaine d'affiliation.
Tick : Ticket d'authentification.
Tick' : Ticket d'authentification camouflé.
Kpf': clé publique utilisée pour la signature aveugle
Ksf' : clé privée utilisée pour la signature aveugle
Kvf : clé secrète partagée entre ASF et ASV.
Nu : nombre aléatoire généré par U
Tu : estampille temporelle générée par U
Nv : nombre aléatoire généré par Asv

Au moment de l'abonnement, l'unité mobile garde à son niveau : IM, Kpf, kpf'

Kpf,Ksf : paire de clés publique/privée utilisée par ASF pour le chiffrement et le déchiffrement des messages durant le protocole.

Kpv,Ksv : paire de clé publique/privée utilisée par ASV pour le chiffrement et le déchiffrement des messages durant le protocole.

5.8 Obtention du ticket d'authentification

Avant que l'unité mobile ne puisse émettre un message à travers le réseau sans fil, l'utilisateur doit obtenir un ticket de son domaine d'affiliation ASF. Ce ticket va être utilisé comme ticket d'authentification lors de la phase d'authentification. Ce ticket est un laisser-passer qui permettra d'authentifier l'unité mobile. Le ticket a une durée de vie limitée et une fois expirée, une requête d'obtention d'un autre ticket est nécessaire.
Dans ce qui suit, nous allons décrire les différents messages échangés pour l'obtention de ce ticket.

Etape 1.
L'unité mobile transmet au serveur du domaine visité :

- l'identité de son domaine de résidence,
- un nombre aléatoire Nu,

son identité réelle et le ticket d'authentification chiffrés avec la clé publique de l'autorité d'affiliation.

Rappelons que la paire RSA, pour la signature aveugle est :

Ksf' = (d ,n) clé secrète
Kpf'= (e,n) clé publique

Donc : pour calculer *Tick*', l'unité mobile utilise un facteur de camouflage r,

$$Tick' = Tick\ r^{e} \ (mod\ n)$$

Etape 1 : UM ⟶ ASV : ASF, Nu, (IM, TICK')kpf	*msg1*

Etape 2.

A ce niveau, connaissant le domaine de résidence de l'unité mobile, l'autorité visitée transmet le message chiffré (IM, TICk)kpf à cette dernière. L'autorité visitée ne pourra pas connaître l'identité réelle du mobile vu que le message est chiffré avec la clé publique de l'autorité d'affiliation et par conséquent, seule ASF pourra déchiffrer ce message.

Etape 2 : ASV ⟶ ASF : (IM, TICK')kpf, Nv	*msg2*

Etape 3.

- A la réception de ce message, ASF pourra déchiffrer le message grâce à sa clé privée ksf et pourra donc avoir en clair IM autrement dit l'identité réelle de l'unité mobile. Elle pourra ainsi vérifier si cet abonné est bien enregistré à son niveau. Notons que le ticket présenté est camouflé selon le procédé décrit précédemment de sorte que l'autorité d'affiliation ne puisse pas en connaître le contenu. Néanmoins, elle le signera en aveugle et le retransmettra à l'abonné via l'autorité visitée.
- Pour la signature du ticket, l'autorité d'affiliation utilisera la transformation en blanc de RSA, décrite précédemment, nous avons donc :

$$Tick\text{“} : Tick' \text{ signé}$$
$$Tick\text{“} = Tick'^{d} \ (mod\ n)$$

- ASF transmettra donc à ASV :
  - le ticket signé en aveugle,
  - le nombre aléatoire Nv

  chiffrés avec la clé secrète partagée entre ASV et ASF.

Etape 3 : ASF ⟶ ASV : (TICK", Nv)kvf	*msg3*

Etape 4.

ASV pourra déchiffrer ce message grâce à kvf et vérifiera si Nv est bien dans le message. En récupérant le ticket signé, il pourra l'envoyer à l'unité mobile avec le nombre aléatoire Nu.

Etape 4 : ASV ⟶ UM : TICK", Nu	*msg4*

Etape 5.

A ce niveau, l'unité mobile vérifie Nu et récupère le ticket signé par son autorité d'affiliation. Elle doit à ce niveau ôter le facteur de camouflage. En effet, le but est que l'unité mobile récupère son ticket d'origine (non camouflé) signé. Soit STICK: ce ticket signé.
On a donc :

$$STICK = Tick" \, r^{-1} \pmod n = Tick'^{d} \, r^{-1} \pmod n$$
$$= (Tick \, r^{e})^{d} \, r^{-1} \pmod n = Tick^{d} \, r^{ed} \, r^{-1} \pmod n = Tick^{d} \, r \, r^{-1} \pmod n = Tick^{d} \pmod n$$

C'est donc exactement la signature de Tick par l'autorité d'affiliation ASF.
C'est ce ticket, qui va être utilisé pour l'authentification de l'unité mobile.
La figure 5.4 récapitule les différents messages échangés pour l'obtention du ticket d'authentification.
L'utilisation des nombres aléatoires Nu et Nv sont des challenges qui permettent de prouver que le message *msg4* est la réponse au message *msg1* et que *msg3* est la réponse au message *msg2*.

5.8.1 Amélioration du Protocole pour résister aux attaques par rejeu

Dans ce protocole, nous remarquons qu'un intrus pourrait intercepter la communication et récupérer le message *msg1*. De ce fait, il peut tromper ASv en rejouant le message (IM, TICK')kpf et réaliser ainsi une attaque par rejeu (voir chapitre 2).
En effet, même si l'attaquant ne peut pas générer de faux messages. Il peut néanmoins faire des copies des requêtes valides afin de les répéter ultérieurement. Ceci aura pour effet soit de rediriger le trafic du mobile vers l'attaquant soit de permettre à ce dernier d'effectuer une attaque par mascarade.
Pour empêcher les attaques par rejeu, nous renforçons le protocole en incluant des garanties de *fraîcheur* dans les messages, autrement dit des données additionnelles qui permettent aux principaux de vérifier que les messages reçus sont *récents*, éliminant ainsi le risque de rejouer d'anciens messages.

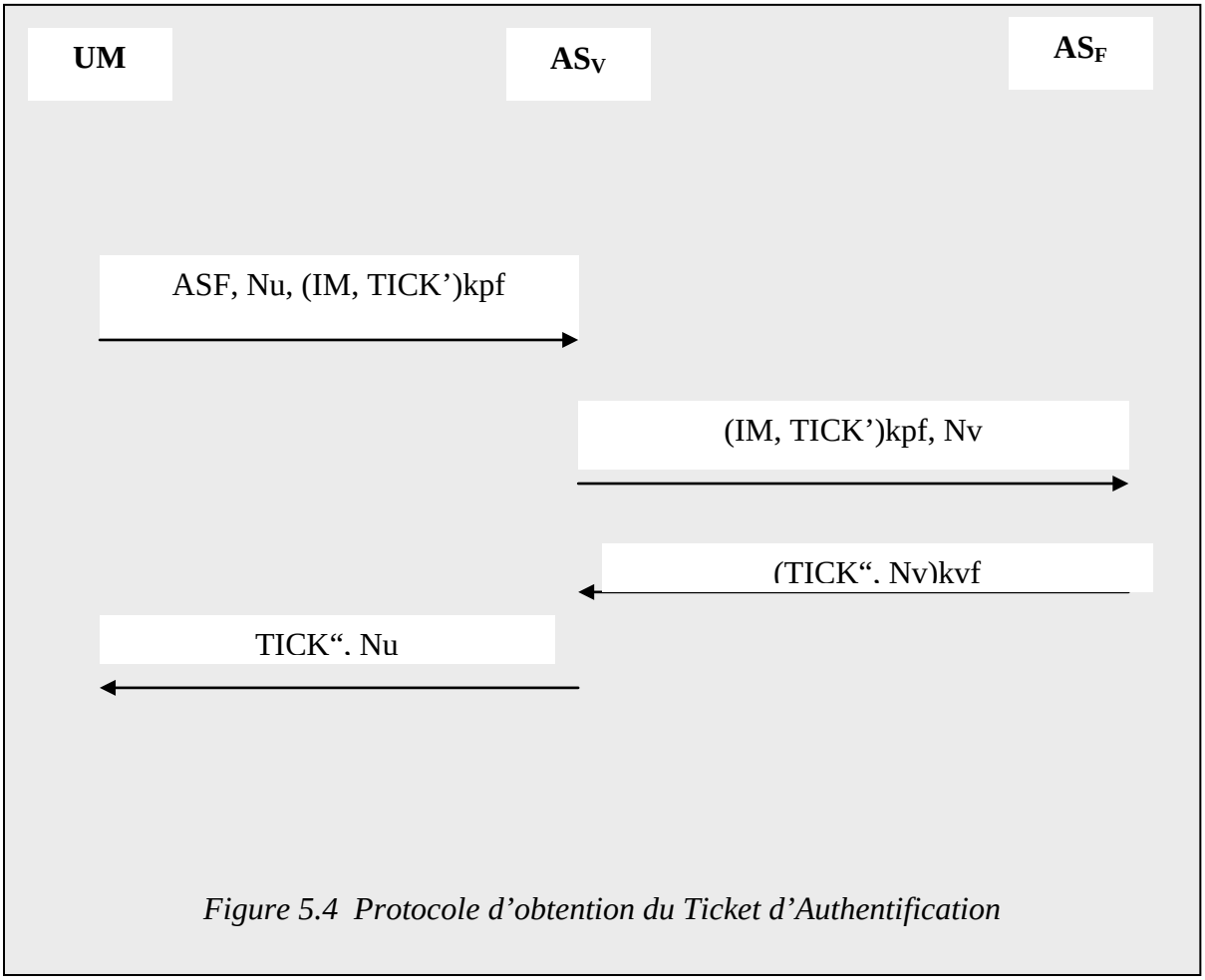

Figure 5.4 Protocole d'obtention du Ticket d'Authentification

L'utilisation des estampilles temporelles et des nombres aléatoires permettent à ASF de faire la distinction entre une nouvelle requête et la répétition d'une ancienne. En outre, cela permet de savoir si le message cryptographique reçu est réellement nouveau.

Rappelons que les solutions existantes consistent en l'utilisation de :

- Nombres aléatoires
- Estampilles temporelles

Nous avons choisi d'utiliser des estampilles temporelles pour éviter le rejeu car l'utilisation des nombres aléatoires imposerait à ASF de garder un historique de tous les anciens nombres déjà utilisés pour choisir un bon nombre. Cette solution nécessite donc trop de ressources.
La base de temps utilisée n'est pas obligatoirement le temps réel humain et l'horodatage peut être basé sur le temps local du système. Dans ce cas, la validation d'un message est effectuée en vérifiant l'estampille temporelle reçue. Le serveur de l'autorité d'affiliation ASF compare l'estampille temporelle reçue avec le temps courant de son horloge tout en admettant une marge de tolérance appropriée.
L'introduction d'estampilles temporelles modifie les messages (figure 5.5), on a donc :

Msg1' : *ASF, Nu, (IM, TICK', **T**)kpf* T: estampille temporelle

Msg2' : *(IM, TICK', **T**)kpf, Nv*

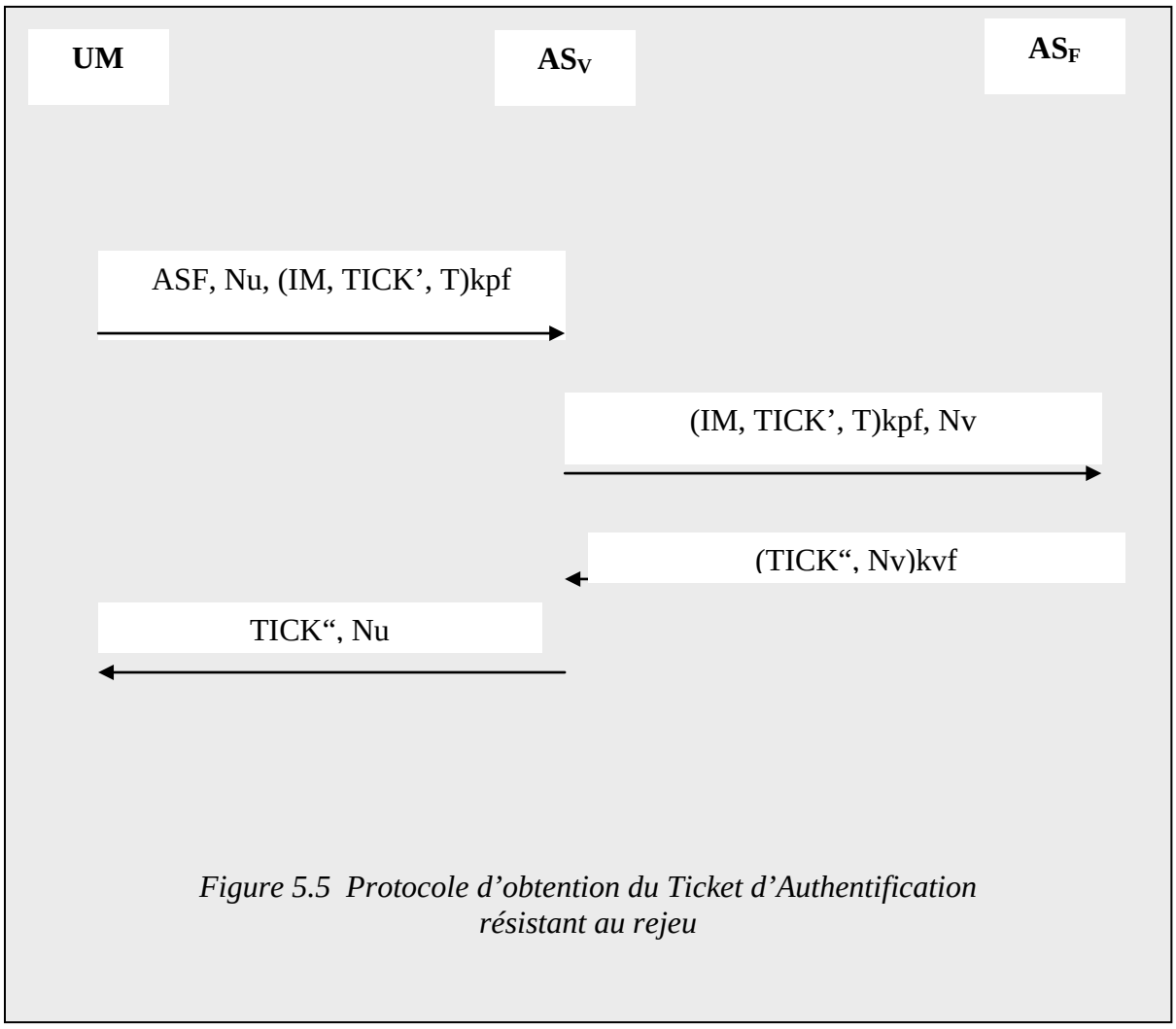

Figure 5.5 Protocole d'obtention du Ticket d'Authentification résistant au rejeu

5.8.2 Confidentialité des messages échangés durant le protocole d'obtention du ticket

Le lecteur remarquera que pour assurer la confidentialité des messages échangés, nous avons opté pour :

a. un cryptosystème à clé publique entre l'unité mobile et l'autorité d'affiliation.
b. un cryptosystème symétrique entre les différentes autorités.

a. L'utilisation d'un cryptosystème à clé publique entre l'unité mobile et l'autorité d'affiliation permet d'assurer une authentification mutuelle entre ces deux entités. Vu que les performances des unités mobiles sont limitées en terme de puissance de traitement, le choix d'un cryptosystème à clé publique est délicat. Néanmoins, nous avons choisi d'adopter

l'algorithme de la racine carrée modulaire (RCM) [Shneier 96]. Le choix de cet algorithme a été motivé par son adéquation au mobile.

Comme la plupart des algorithmes cryptographiques, l'approche est basée sur l'arithmétique modulaire et dépend de la difficulté de factoriser les nombres premiers (décrit en annexe).

En bref, RCM opère comme suit :

- La clé publique est un modulo N qui est le produit de deux grands nombres premiers, p et q. La combinaison de p et q constitue un élément de clé privée de l'algorithme.

- Si un principal A envoie un message M à B, il chiffre ce message comme suit :

$$C = M^2 \bmod N$$

- Pour retrouver M, B déchiffre le message et a :

$$M = Racine\ (C) \bmod N$$

L'application de RCM dans les environnements sans fil présente les avantages suivants :

Calculer le carré modulaire nécessaire pour le chiffrement nécessite moins de temps (le temps d'une multiplication modulaire) que le calcul de l'extraction d'une racine carrée modulaire (une exponentiation). Il est donc intéressant de placer la fonction de chiffrement dans la station mobile et la fonction de déchiffrement dans la station de base. RCM répond donc aux contraintes imposées par le mobile qui ont des processeurs lents et des réserves de batteries limitées.
Ainsi, les clés kpf et ksf utilisées dans le protocole d'obtention de tickets correspondent respectivement à la clé publique et privée de l'algorithme RCM. Dans notre cas, l'unité mobile utilise cet algorithme uniquement pour le chiffrement ce qui équivaut au temps d'une multiplication modulaire.
En reprenant le protocole d'obtention de ticket, nous remarquons que l'unité mobile chiffre m1 = (IM, Tick', T) en utilisant kpf.
Par conséquent, on obtient $c1 = m1^2 \bmod N$
A la réception, ASF utilise kvf pour déchiffrer ce message et récupère m1= racine(c1) mod N

b. Pour les messages transmis entre les stations de base, un cryptosystème à clé secrète peut être envisageable. En effet, dans ce cas, nous pouvons supposer l'existence d'un canal sécurisé par lequel ces deux entités peuvent s'échanger une clé secrète. Il ne faut pas oublier que ces deux entités n'utilisent pas l'interface air pour leurs communications.
Nous suggérons dans ce cas d'utiliser un algorithme symétrique tel que DES pour chiffrer les messages entre les stations de base. L'obtention d'une clé secrète partagée peut être faite, au préalable, sur la base d'un cryptosystème à clé publique pour négocier cette clé. Dans ce cas de figure, les deux entités peuvent utiliser l'algorithme Diffie-hellman (décrit en annexe) pour établir la clés symétrique. Dans le cadre de cette thèse, nous considérons que les deux entités partagent une clé secrète kvf partagée entre ASF et ASV qu'elles peuvent utiliser pour chiffrer leurs messages.

5.9 Protocole d'authentification

Une fois que l'unité mobile est en possession du ticket d'authentification signé par son autorité de résidence, elle peut donc le présenter à chaque authentification. Les messages échangés entre l'unité mobile, l'autorité du domaine visité et l'autorité du domaine d'affiliation se résument en :

Etape 1.

L'unité mobile envoie à ASV :

- l'identité de l'autorité de résidence ASF,
- un nombre aléatoire Nu,

le ticket Stick signé et l'estampille T' chiffrés avec la clé publique de l'autorité d'affiliation.

Etape 1 : UM ⟶ ASV : ASF, Nu, (Stick, T')kpf *msgA1*

Etape 2.

A la réception de ce message, ASV connaîtra l'identité de l'autorité d'affiliation et donc lui fera suivre le message c'est à dire : (Stick, T')kpf et un nombre aléatoire Nv.

Etape 2 : ASV ⟶ ASF : (STICK, T')kpf, Nv *msgA2*

Etape 3.

A ce niveau, ASF déchiffrera le message (Stick, T')kpf grâce à sa clé privée ksf et retrouvera le ticket Stick. Après vérification que le message n'est pas rejoué grâce à T' :

- Elle pourra vérifier que ce ticket a bel et bien été signé par elle et donc qu'il appartient à l'un de ses abonnés.
- Elle procède également, à la vérification de la durée de vie du ticket. Si celle-ci n'a pas expiré, elle répond favorablement à la requête d'authentification. Si le ticket a été présenté pour la première fois, elle crée dans sa table de tickets une nouvelle entrée en lui associant un nom de compte ayant pour identificateur Ci. Si le ticket a déjà été présenté alors cette entrée existe dans la base et il suffit donc de récupérer le nom du compte Ci. Néanmoins, pour que ce message là soit transmis chiffré à UM après par ASV, il faudrait que ASF lui envoie une clé. Pour cela, il suffit d'utiliser Stick, qui est connu par UM. On a donc ki= STick. Pour plus de sécurité, ASF peut calculer une fonction de hachage connue par UM de Stick.

Etape 3 : ASF ⟶ ASV : (Ci, ki, Nv)kvf	*msgA3*

Etape 4.

A la réception de ce message, ASF le déchiffre, vérifie Nv et récupère donc un nom de compte qu'elle transmettra à UM. A ce niveau, il ne faut pas que ASV envoie ce message en clair à UM. Pour le chiffrer, elle utilise la clé ki.

Etape 4 : ASV ⟶ UM : (Ci, Nu)ki	*msgA4*

Etape 5.

A la réception de ce message, UM pourra déchiffrer ce message grâce à ki, vérifiera la validité du challenge Nu et récupèrera donc le nom de compte pseudonyme avec lequel elle pourra envoyer des messages anonymes.

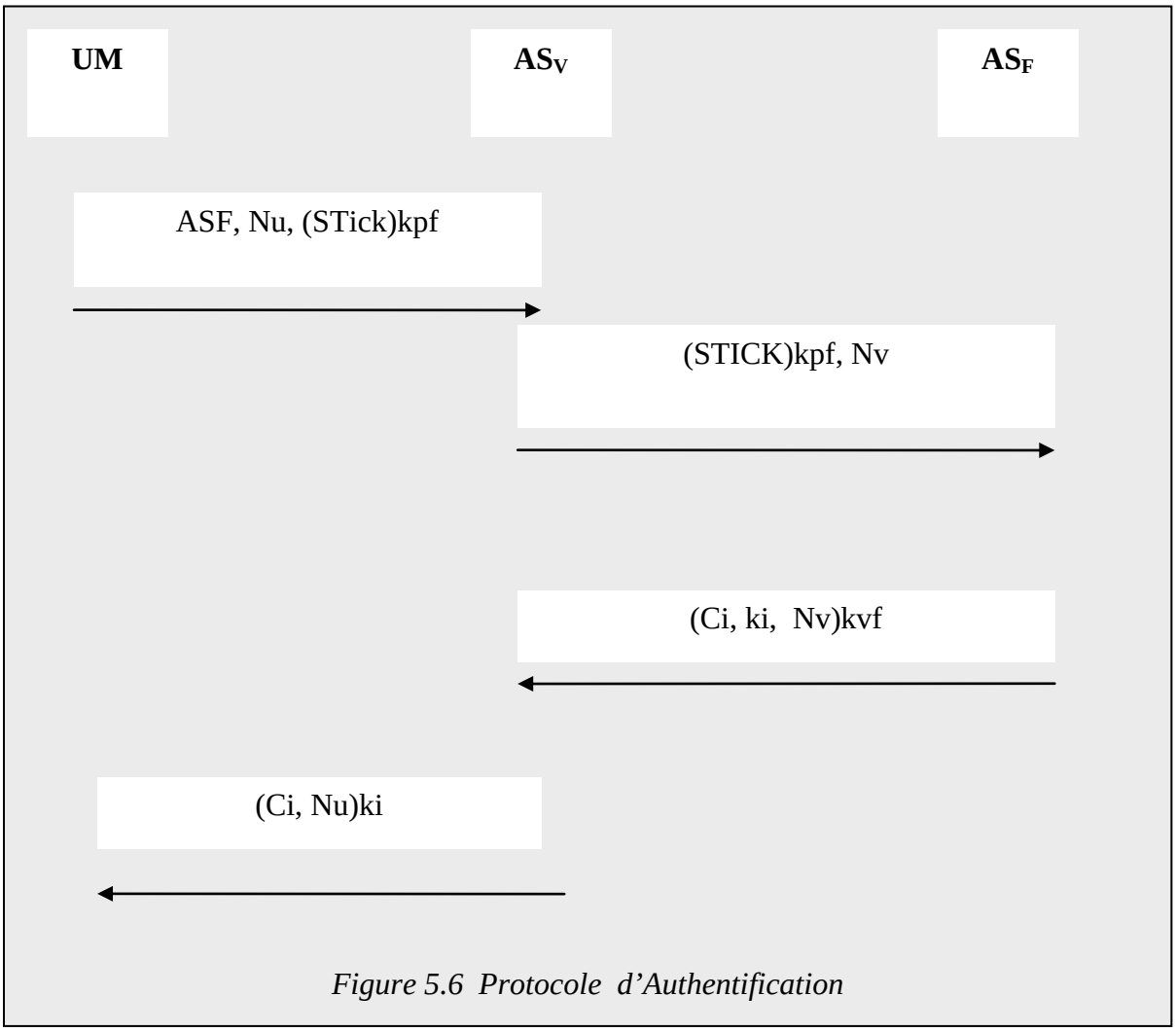

Figure 5.6 Protocole d'Authentification

A l'issue de ce protocole d'authentification, l'utilisateur mobile pourra donc engager une communication anonyme, où aucune information sur sa propre identité n'est révélée et dans la suite des messages échangés c'est Ci qui va être utilisé.
Le protocole ainsi présenté assure donc **l'authentification de l'utilisateur garantissant** l'anonymat **mais la question posée est comment garantir la solvabilité du compte de l'utilisateur**, question que nous aborderons dans la prochaine section en présentant une solution à ce problème.

5.9.1 Comptabilité et Tarification

La comptabilité ou la tarification est souvent une issue négligée dans la recherche académique. La comptabilité implique qu'une entité enregistre les actions effectuées par l'utilisateur sur le système (par exemple, les appels téléphoniques sortants) afin de facturer l'usager. Un conflit fondamental apparaît entre l'anonymat de type C5 et la tarification pour une raison principale :

> *L'autorité du domaine visité ne connait pas l'identification du domaine d'affiliation et ne sera pas donc capable de facturer l'utilisateur mobile ultérieurement.*

L'anonymat semble être indésirable lorsque la tarification et le paiement des services sont en jeu. En effet, la solution proposée pour un anonymat complet semble être contradictoire avec le paiement. Néanmoins, nous allons montrer que nous pouvons intégrer dans le protocole proposé une méthode de paiement.

En effet, la méthode est intégrée lors de l'obtention du ticket d'authentification. En fait, à ce niveau lors du premier message l'unité mobile transmet son identité réelle.

msg1: ASF, Nu, (**IM**, TICK')kpf

A la réception de (IM, TICK'), l'autorité d'affiliation connaîtra l'identité de l'un de ses abonnés. A ce stade, nous proposons que l'autorité d'affiliation débite le compte de IM d'une certaine somme S qui représente la valeur du ticket. Donc le ticket est utilisé tant que la somme S n'a pas été consommée. Ce principe est analogue au principe de la monnaie électronique définie par Chaum [Chaum 83]. En effet, le ticket signé en aveugle ne garde aucune trace de quel compte est débitée la somme d'argent.
Ainsi, à chaque présentation du compte pseudonyme Ci correspondant au ticket présenté au moment de l'authentification, nous rajoutons l'information *coût* qui, initialement vaut la valeur S. Mais à chaque communication, c'est cette valeur qui va être diminuée selon le coût de la communication. Lorsque *coût* est à zéro, l'unité mobile devra obtenir un autre ticket d'authentification.
De cette manière les communications anonymes peuvent être tarifiées sur le compte de l'utilisateur.

5.10 Expiration du ticket d'authentification

A l'expiration d'un ticket, l'utilisateur mobile doit redemander un autre ticket. Dans cette situation, deux cas peuvent se produire :

- L'utilisateur anonyme a consommé la somme fixée débitée au départ.

Ou bien
- L'utilisateur anonyme n'a pas consommé la somme fixée débitée au départ.

Dans le premier cas, l'unité mobile doit obtenir un autre ticket d'authentification en suivant le protocole d'obtention de tickets décrit précédemment. Par conséquent, il retransmet son identité réelle chiffrée et obtient un nouveau ticket. Lors du protocole d'authentification, une fois ce ticket présenté à l'autorité d'affiliation, cette dernière devra créer une nouvelle entrée dans la base des tickets avec un nouveau compte anonyme.

Dans le second cas, le compte anonyme a toujours de l'argent non consommé. Donc, la demande d'un nouveau ticket est particulière dans ce cas. En effet, l'unité mobile devra transmettre l'ancien ticket et la génération d'un nouveau ticket avec la même entrée dans la table des tickets. Ainsi l'utilisateur pourra consommer la somme restante.

Nous avons décrit la solution proposée, autrement dit le protocole d'authentification basé sur la signature aveugle pour garantir l'anonymat complet. Dans ce qui suit nous allons procéder à son évaluation.

5.11 Evaluation du protocole

Rappelons que parmi les objectifs fixés pour la conception de notre protocole, l'exigence première est le respect de la propriété d'anonymat complet, à savoir **l'intraçabilité.**

Nous allons **démontrer** comment le schéma proposé garantit cette propriété.

- Le protocole proposé permet de cacher l'identité de l'utilisateur vis à vis d'un tiers non autorisé : Ceci est vrai car même lors de l'obtention du premier ticket, l'identité de l'utilisateur n'est pas transmise en clair mais est chiffrée avec la clé publique de l'autorité de résidence. Seule cette dernière pourra déchiffrer ce message.

- Dans le protocole proposé, l'identité de l'utilisateur n'est jamais révélée à l'autorité visitée.

- Même si l'identité de l'autorité d'affiliation est révélée à l'autorité visitée. Cette dernière ne pourra jamais établir de relation avec l'identité de l'utilisateur.

- Puisque le domaine d'affiliation ne connaîtra jamais l'utilisateur mobile qui a présenté le ticket, il lui est donc impossible de tracer le comportement de l'utilisateur.

L'utilisation de la signature aveugle en supposant que le schéma de l'algorithme de signature aveugle est sécurisé [Pointcheval 96] montre qu'il est impossible de faire coïncider le ticket initial avec celui signé en aveugle. L'autorité d'affiliation ne pourra jamais déduire à qui appartient ce ticket.
En fait, la question posée est : est ce que l'autorité d'affiliation peut faire une corrélation entre les messages msg1 (message transmis lors du protocole d'obtention de ticket) et msgA1 (message transmis lors du protocole d'authentification) ?

msg1 : ASF, Nu, (IM, TICK', T)kpf

msgA1: ASF, Nu, (Stick, T')kpf

Dans msg1, l'autorité d'affiliation récupère les informations IM et TICK'.
Dans msgA1, l'autorité d'affiliation récupère STICK

Or il est impossible de déduire TICK' à partir de STICK si on suppose que la signature en aveugle est sûre (hypothèse initiale). Notons, néanmoins, que beaucoup de travaux de recherche confirment cette hypothèse en démontrant que la signature aveugle est aussi complexe que la factorisation [Pointcheval 96].

Nous pouvons donc conclure que le protocole proposé garantit un anonymat de classe C5. De plus, il ne suppose pas qu'une certaine autorité est digne de confiance ou éprouvée du moment qu'il dissimule son identité même à l'autorité d'affiliation après obtention du ticket d'authentification.
En plus de l'anonymat et de l'intraçabilité, le protocole d'authentification ainsi décrit protége la confidentialité des messages en utilisant l'algorithme de la racine carrée modulaire pour chiffrer les messages. De plus, les tentatives de rejeu sont évitées grâce aux facteurs de fraîcheur : les challenges et les estampilles temporelles.
Il est important de signaler que l'utilisation d'un cryptosysème à clé publique nécessite l'existence d'une autorité de certification qui permet de garantir la validité de la clé publique de l'autorité d'affiliation dans notre cas.

Dans cette section, nous avons procédé à l'évaluation du protocole proposé. Néanmoins, La conception et la mise en place des protocoles cryptographiques est une tâche complexe et difficile. En effet, [Pointcheval 00] énumère deux aspects à considérer et à étudier afin de pouvoir proposer un protocole correct :

1. Choix algorithmique : la première difficulté consiste à décider de l'algorithme de chiffrement à utiliser. Il faut bien évidemment décider tout d'abord, de choisir entre systèmes symétriques et systèmes asymétriques. Ensuite, il faudra choisir l'algorithme de chiffrement et décider de ses paramètres.

2. Analyse globale du fonctionnement du protocole : une fois les différents paramètres et algorithmes de chiffrement choisis, il faudra considérer l'aspect du fonctionnement global et vérifier la cohérence du protocole. En particulier, il faudra s'assurer que le protocole est capable d'offrir les services de sécurité prévus sans être induit en erreur par un intrus.

Le seul moyen de résoudre ce problème est de développer des méthodes rigoureuses et formelles pour prouver la conformité des protocoles aux exigences de sécurité. Ainsi naquit toute une discipline : La vérification formelle des protocoles cryptographiques.
De nombreux travaux de recherche ont été effectués dans ce domaine. Les approches et techniques, proposées à ce jour, tombent toutes dans quatre classes :

- model-checking : vérification de propriétés en explorant les états possibles du système,

- theorem-proving : preuve garantissant qu'une propriété donnée est vraie pour toutes les configurations du système,
- techniques orientées Logique : établissement de propriétés au moyen de déductions logiques,
- et les techniques cryptographiques ou plus communément Provable security (preuve purement mathématique sur l'infaisabilité d'attaques).

Actuellement, l'approche la plus utilisée dans la preuve formelle des protocoles cryptographiques est la logique BAN [Burrows 90]. Cependant, cette preuve nous permettra seulement de prouver l'authentification mais pas l'anonymat car la logique BAN ne permet pas de modéliser le secret, et encore moins l'anonymat : objet de notre problématique.

5.11.1 Complexité de calcul

En termes de complexité de calcul, nous avons essayé d'adapter la solution à un environnement mobile. Ainsi :

- Pour le chiffrement des messages, l'utilisation de l'algorithme de racine carré modulaire est efficace vu que l'opération que doit accomplir l'unité mobile est une multiplication modulaire (et non pas une racine carrée qui est une opération exponentielle et donc coûteuse). Durant, le processus d'authentification, le mobile devra effectuer deux multiplications modulaires.

- Pour la signature aveugle, l'unité mobile calcule l'expression : $Tick' = Tick\ r^e \pmod n$. L'opération $r^e \pmod n$ est une exponentiation et par conséquent coûteuse pour des équipements mobiles (ne disposant pas de cryptoprocesseur). Cependant, ce calcul n'a cependant pas besoin d'être réalisé pendant l'authentification; il peut au contraire être réalisé à l'avance et stocké dans la mémoire de la carte à puce. De cette manière, en précalculant cette expression, l'authentification de l'unité mobile se fera plus rapidement.

La solution proposée définit un schéma d'authentification générique pouvant être intégré dans les réseaux cellulaires. Elle permet d'assurer un anonymat complet. Néanmoins, un tel objectif n'est pas sans conséquences.

5.12 Conséquences d'un anonymat Complet

Dans le protocole décrit, nous ne considérons pas l'anonymat dans le cas des appels entrants.
La politique d'anonymat d'un réseau mobile dépend étroitement de la nature des appels (entrants ou sortants) reçus ou effectués par un utilisateur mobile.
En effet, un anonymat de classe supérieure à C3 devient complexe à mettre en œuvre si l'on désire accepter des appels entrants. Dans la plupart des architectures de réseaux mobiles existants, les appels entrants sont routés par un agent localisé dans le domaine d'affiliation.
Afin que cet agent puisse atteindre l'usager à tout moment, il doit pouvoir connaître à tout moment la localisation exacte de l'utilisateur. Cette caractéristique, inhérente aux fonctionnalités du réseau, est en contradiction avec les politiques d'anonymat de la classe C5. En effet, l'agent de routage dans le domaine visité doit communiquer les données concernant

la localisation courante de l'utilisateur à l'agent de routage du domaine d'affiliation lors de chaque déplacement de l'utilisateur mobile. Cette contradiction introduit un nouveau besoin, celui du routage anonyme qui éliminerait la nécessité pour le domaine d'affiliation de pister l'utilisateur mobile.
La solution présentée tend à fournir un anonymat complet aux utilisateurs et aux organisations. Il est incontestable que tant que cette notion d'anonymat complet ne soit pas intégrée et que l'utilisateur n'a pas la garantie que son intimité numérique est préservée, des applications telle que le commerce électronique ne connaîtra pas l'essor attendu. Néanmoins, cette intimité numérique peut être inacceptable sous certaines politiques de sécurité car un anonymat complet peut permettre à un usager de perpétrer « le crime parfait ». Par exemple, il serait impossible dans un contexte de détection d'intrusion de repérer un attaquant, s'il n'y a pas une autorité centrale qui puisse enregistrer les actions des utilisateurs.
En effet, la détection d'intrusions est un service important dans les systèmes distribués. Dans le cas des réseaux mobiles, ce service peut être un besoin conflictuel avec celui de l'anonymat des utilisateurs. Le but d'un système de détection d'intrusions est d'enregistrer tout ou une partie des actions effectuées sur le réseau mobile surveillé [Samfat 95]. Toutefois, dans la solution proposée, il serait impossible pour le domaine d'affiliation de collecter les données relatives à l'activité d'un utilisateur, ce dernier étant totalement intraçable.

5.13 Conclusion

Dans ce chapitre, nous avons présenté une solution pour un anonymat complet en environnement mobile. Rappelons les critères de comparaison, adoptés au chapitre 4, entre les différentes solutions :

- Politique d'Anonymat.
- Intraçabilité des mouvements de l'utilisateur mobile.
- Tierce Digne de Confiance

Basée sur le principe de signature aveugle, la solution que nous proposons garantit un niveau d'anonymat de classe C5. Les mouvements de l'utilisateur mobile ne peuvent pas être liés à son identité réelle même par son autorité d'affiliation. En fait, dans notre solution même cette dernière n'est pas considérée digne de confiance.

	GSM	**UMTS**	**Herzberg et al.**	**Protocole amélioré de Molva**	**Notre Protocole**
Politique d'anonymat	*Partiellement C1*	*C1et C2*	*C1 et C2*	*C4*	*C5*

Intraçabilité	Outsider	Domaine visité	Domaine d'Affiliation
GSM	~oui	non	non
UMTS	oui	non	non
Herzberg	oui	non	non
Samfat	oui	oui	non
Notre protocole	oui	oui	oui

	Autorité éprouvée
GSM	oui
UMTS	oui
Herzberg	oui
Samfat	oui
Notre protocole	non

Conclusion Générale

La mobilité a introduit de nouveaux besoins en sécurité en comparaison aux traditionnels réseaux fixes. Ces réseaux, de part leur structure, sont plus vulnérables à l'usurpation d'identité, le refus de service, l'écoute et la surveillance des utilisateurs mobiles.
Dans un article intitulé : « The Challenges of Mobile Computing » [Forman 94] qui récapitule les différences entre les environnements filaires et sans fil et les problèmes que les réseaux sans fil posent aux développeurs de logiciels. Forman et Zahorjan ont distingué trois besoins essentiels : l'utilisation des réseaux sans fil, la possibilité de changer de location et le besoin d'une portabilité non encombrante. Les remarques et conclusions des auteurs quoique énoncées en 1994, demeurent valables de nos jours [Curtis 01]. Les auteurs insistent sur le fait que le plus grand défi pour les concepteurs est d'adapter les conceptions qui ont si bien fonctionné dans les environnements fixes aux environnements mobiles. Néanmoins, nous noterons que dans le domaine de la sécurité, c'est donc rajouter une incertitude à l'équation [Curtis 01].
Les concepteurs d'architectures de sécurité pour les réseaux sans fil doivent donc faire face aux challenges posés par ces derniers, et offrir des mécanismes de sécurité adaptés aux environnements mobiles.
Parmi les mécanismes de sécurité mis en œuvre, nous retrouvons les mécanismes d'authentification.
Toutefois, l'authentification de l'utilisateur mobile introduit un nouveau besoin : l'anonymat.
L'anonymat peut être vu comme un besoin conflictuel avec l'authentification, puisque l'anonymat a pour but de dissimuler l'identité de l'utilisateur alors que l'authentification nécessite la révélation de l'identité dans le but d'être prouvée. Les solutions étudiées ont montré la possibilité de concilier entre l'authentification et l'anonymat.
En nous intéressant au problème de l'anonymat, nous nous sommes confrontés à un domaine très sensible. En effet, d'un point de vue social, les communications anonymes semblent être désirées seulement par une minorité de gens concernées par le problème de préserver confidentielles les informations privées et souvent non acceptées par les gouvernements ou organisations. C'est pourquoi, les solutions pour les communications anonymes ne sont pas intégrées dans des produits existants ou infrastructures. Notons que l'anonymat assuré par GSM n'est que partiel et qu'à ce jour, les travaux de UMTS n'envisagent pas un anonymat complet. Même les travaux de recherche dans ce domaine (du moins ceux qui sont rendus publics)[1] proposent des protocoles d'authentification conciliant l'anonymat certes, mais ces solutions basées, sur la notion d'alias, offrent seulement un anonymat partiel de l'utilisateur**.**

Il est cependant incontestable, que tant que l'utilisateur n'a pas le sentiment que son intimité numérique n'a pas été préservée, des applications telles que le commerce électronique, le vote électronique ne connaîtront pas l'essor attendu dans le contexte mobile.

L'étude des différentes techniques d'anonymat nous a permis de conclure que la seule méthode pouvant offrir un anonymat complet est la signature aveugle utilisée dans le paiement électronique.
Basée sur un cryptosystème à clé publique, la signature aveugle semble à première vue inadéquate aux environnements mobiles. Néanmoins, les avancées technologiques en termes

[1] Vu la sensibilité du domaine

de performances des mobiles et les progrès réalisés dans le domaine de la cryptographie, nous a encouragé à proposer une solution basée sur la signature en aveugle.

Dans cette thèse, nous proposons donc un protocole d'authentification dans un environnement mobile qui concilie l'anonymat. Le protocole est basé sur la technique de signature aveugle pour assurer l'intraçabilité de l'utilisateur mobile même par son domaine d'affiliation. Ce dernier ne pourra pas connaître les différents déplacements de son abonné. En fait, l'utilisateur mobile obtient un premier ticket d'authentification signé de la part de son autorité d'affiliation. C'est ce ticket qui permettra à l'utilisateur de s'authentifier auprès des différents domaines visités. De plus, le protocole proposé assure:

- La confidentialité des messages échangés grâce au chiffrement. L'algorithme de chiffrement choisi répond bien aux challenges posés par les mobiles.
- Le protocole est résistant contre les attaques de rejeu, en introduisant les estampilles temporelles.

Le désir de réaliser un anonymat complet même vis à vis de l'autorité d'affiliation peut sembler contradictoire avec la tarification des services demandés. Pour cela, nous intégrons un moyen de paiement semblable à celui de la monnaie électronique, sans compromettre l'anonymat.
L'évaluation du protocole proposé nous permet de conclure que ce dernier permet de garantir un anonymat complet, autrement dit l'intraçabilité.
En effet, les mouvements de l'utilisateur mobile ne peuvent pas être liés à son identité réelle même par son autorité d'affiliation. En fait, dans notre solution même cette dernière n'est pas considérée digne de confiance.
Proposer une solution pour un anonymat complet n'est certes pas sans conséquences. En fait, la solution proposée ne garantit pas un anonymat dans le cas des appels entrants. De plus, étant donné qu'il est impossible pour le domaine d'affiliation de collecter les données relatives à l'activité d'un utilisateur, ce dernier étant totalement intraçable ; il serait donc impossible dans un contexte de détection d'intrusion de repérer un attaquant, s'il n'y a pas une autorité centrale qui puisse enregistrer les actions des utilisateurs.

Nous prévoyons à ce travail des extensions de divers types, dont nous citons:

1. Dans un premier temps, Il est intéressant de calculer la complexité de calcul du protocole proposé dans un environnement mobile et ainsi évaluer la signature aveugle. Il en découle donc de tester les différents algorithmes cryptographiques et évaluer leurs performances dans le contexte mobile.

2. Procéder à la preuve du protocole proposé : Actuellement, la preuve des protocoles d'authentification utilisent la logique BAN [Burrows 90]. Cependant, elle ne modélise pas la connaissance, elle peut seulement vérifier l'authentification. Elle ne peut donc pas être utilisée pour vérifier l'anonymat. L'idée est d'étendre cette logique en vue de modéliser la notion d'anonymat et de la vérifier.

3. Etudier le routage anonyme pour assurer l'anonymat dans le cas des appels entrants.

4. Appliquer le protocole proposé dans une architecture d'agents mobiles [Jansen 99].

ANNEXE
SECURITE ET COMPLEXITE

1. Difficulté des problèmes mathématiques

Un problème mathématique sera dit difficile si la puissance de calcul à mettre en oeuvre pour le résoudre en un temps raisonnable n'est pas réaliste. Cette définition, très subjective, n'est pas très satisfaisante pour l'esprit mathématique, mais correspond bien à la préoccupation cryptographique, à savoir assurer la sécurité des protocoles en pratique. Une telle définition fixe donc notre objectif, sans pour autant fixer les moyens pour y arriver : comment savoir que le protocole va résister à la puissance de calcul mise en oeuvre ?

2. Cryptographie et NP-complétude

Un premier élément de réponse peut se trouver dans la théorie de la complexité qui étudie la complexité algorithmique dans le pire des cas, et classifie ainsi les problèmes, en définissant des classes d'équivalence à partir du concept de machine de Turing.
Ainsi, la classe P correspond aux problèmes pour lesquels il existe un algorithme qui détermine une solution en temps polynomial en la taille de la donnée. Par exemple, déterminer le résultat de la multiplication de deux matrices de taille n x n peut se faire en n^3 multiplications : l'algorithme de calcul est ici polynomial en la taille de la donnée. En revanche, un problème dont le meilleur algorithme de résolution est de complexité k^n, dit exponentiel, n'appartiendra pas à la classe P. De ce fait, les algorithmes s'exécutant en temps polynomial seront considérés comme réalistes.
La classe NP est constituée quant à elle des problèmes pour lesquels il est possible de déterminer si une solution est valide en temps polynomial, sans nécessairement pouvoir déterminer une telle solution en temps polynomial.
S'il est clair que $P \subseteq NP$, i.e. que tout problème qui détermine une solution en temps polynomial peut aussi vérifier une solution en temps polynomial, une question fondamentale reste ouverte : a-t-on :
$NP \subseteq P$?
Bien qu'aucune réfutation de cette inclusion ne soit prouvée, il est raisonnable de conjecturer que :

$P \neq NP$

Les définitions 1 et 2 vont nous aider à étayer nos propos.

Définition 1 (Réduction polynomiale) Une réduction polynomiale d'un problème A à un problème B est un algorithme, qui s'exécute en temps polynomial, et qui transforme toute donnée a du problème A en une donnée b du problème B tel que a est solution de A si et seulement si b est solution de B.

si un tel algorithme existe, alors on dit que A se réduit polynomialement à B, et on note $A \leq B$. Autrement dit, si l'on détermine un algorithme qui résout le problème B en un temps polynomial, alors le problème A peut également être résolu en un temps polynomial : B est plus difficile que A.

Définition 2 (NP-complétude) Un problème décisionnel est NP-complet s'il appartient à NP et si tout problème décisionnel de NP lui est polynomialement réductible.
Entre d'autres termes, les problèmes NP-complets, sont les problèmes les plus difficiles de la classe NP, et sont tous de même difficulté. La découverte d'un algorithme qui s'exécuterait en temps polynomial et qui permettrait de résoudre un problème NP-complet permettrait alors de résoudre également tous les autres problèmes de NP. Les problèmes NP-complets sont nombreuses ; pourtant les abondantes tentatives de recherche d'un tel algorithme restent vaines ; on peut alors raisonnablement admettre la conjecture 3.1.

Définition 3 (NP-difficulté) Un problème est NP-dur si tout problème de NP lui est polynomialement réductible. En d'autres termes, un problème NP-dur est au moins aussi difficile que tous les problèmes appartenant à NP. Par conséquent, si $P \neq NP$ alors aucun problème NP-dur ne peut être résolu en temps polynomial, mais si $P = NP$ alors on ne peut rien conclure.
Faire reposer la sécurité d'un protocole cryptographique sur un problème NP-complet ou NP-dur peut ainsi sembler séduisant puisqu'aucun algorithme connu ne peut résoudre le problème en temps polynomial ; il faut toutefois relativiser cette diffculté apparente, car la théorie de la complexité ne s'intéresse qu'à la complexité dans le pire des cas : s'il n'existe pas d'algorithme permettant de résoudre le problème considéré en temps polynomial, il est tout à fait possible qu'un tel algorithme existe pour certaines instances du problème considéré.
Le problème du sac à dos, sur lequel est basé le cryptosystème de Merkle-Hellman [MH78], est l'exemple type de problème NP-dur dont presque toutes les instances intéressantes pour la cryptographie sont faciles à résoudre avec un algorithme efficace en pratique [Ngu99].
Ainsi, si la théorie de la complexité peut apporter un élément de réponse dans l'évaluation de la difficulté du problème considéré, elle ne doit en aucun cas cacher la réelle difficulté du problème.

3. Cryptographie et problèmes réputés difficiles

Au lieu de faire reposer la sécurité d'un problème sur l'étude de sa complexité dans le pire des cas, on préfèrera généralement se ramener à un problème connu et réputé difficile, sans nécessairement appartenir aux classes de complexité citées. C'est le cas du problème de la factorisation (cf. paragraphe 3.2.1) ou du logarithme discret (cf. paragraphe 3.2.4).
Nous avons alors, comme nous l'avons précisé, une sécurité assurée face à une puissance de calcul réaliste. Ces dernières années ont cependant vu apparaître la notion d'ordinateur quantique, dont la mise en oeuvre bouleverserait la cryptographie asymétrique, puisque des algorithmes permettant de résoudre le problème de la factorisation ou du logarithme discret pourraient s'exécuter en temps polynomial. Si cette révolution semble lointaine, voire

utopique, les extraordinaires conséquences qu'elle apporterait pourraient faire avancer les recherches plus rapidement que l'on peut l'imaginer aujourd'hui.

Notations
Bien que notre volonté soit de restreindre au maximum l'emploi de mathématiques, les notations suivantes seront cependant indispensables :

- [a, b] désigne l'intervalle des nombres entiers plus grands que a et plus petits que b.
- Beaucoup d'opérations sont modulaires, i.e. on réalise les opérations de multiplication, d'addition et d'exponentiation de manière classique mais on ne garde que le reste de la division entière du résultat par le module. Le calcul de x modulo y est noté x mod y.
- Soit n un entier. On note Z_n l'ensemble des entiers modulo n, i.e. l'intervalle [0 n-1]
- On note Z_n^* l'ensemble des éléments de Z_n inversible modulo n, i-e. premiers avec n.

4. Problèmes réputés difficiles

4.1 Factorisation d'entiers

Problème 1 FACT(n)

Le problème de la factorisation est le suivant : étant donné un nombre N, trouver les nombres premiers p_1, p_2,... p_r tels que le produit des p_i soit égal à N.

On ne connaît pas, pour le moment, d'algorithme polynomial en la taille du nombre N (i.e. log N, le nombre de chiffres de N) résolvant la factorisation. On connaît des algorithmes sub-exponentiels (en temps exp((log N)*log(log N)) par exemple). Les recherches sont très actives sur le sujet parce que résoudre facilement le problème de la factorisation permet de casser RSA, qui est le plus répandu des systèmes de chiffrement à clé publique.

L'état de l'art est le suivant : un nombre de 140 chiffres décimaux (soit environ 465 bits), qui était le produit de deux nombres premiers de 70 chiffres chacun, a été factorisé en environ un mois de calcul, au début de 1999, par l'équipe de Montgomery, à l'aide d'un imposant parc de machines. Les nombres de 512 bits sont à la portée d'agences gouvernementales fortunées (même si cela n'a jamais officiellement été fait) ; un nombre de 768 bits devrait résister pendant encore une dizaine d'années au moins, sauf percée théorique.

Problème 2 : Problème équivalent à celui de la factorisation
Plusieurs problèmes sont équivalents à celui de la factorisation. Nous citerons : le calcul de racines carrées modulaires.
Racines Carrées Modulo n
Si n est le produit de deux nombres premiers, alors la possibilité de calculer des racines modulo n demande une puissance de calcul équivalente à celle nécessaire pour factoriser n.

Problème3 : calcul de Logarithme Discret dans un corps fini
A coté des problèmes liés à la factorisation, l'autre grande famille de problèmes est celle du calcul de logarithmes discrets modulaires.
L'exponentiation modulaire est une fonction à sens unique fréquemment utilisée en cryptographie. Evaluer l'expression suivante est facile :

$$y = a^x \bmod n$$

Le problème inverse de l'exponentiation modulaire est celui de la recherche du logarithme discret d'un nombre. C'est un problème difficile :
Pour y donné, trouver x tel que : $a^x \equiv b \pmod n$

Une application directe du problème des logarithmes discrets est l'algorithme Diffie-Hellman utilisé pour la distribution de clés. Deux utilisateurs i et j peuvent utiliser cet algorithme pour engendrer une clé secrète.
Au départ, les deux utilisateurs se mettent d'accord sur deux grands entiers n et g de telle manière que g soit inférieur à n mais plus grand que 1.
L'utilisateur i choisit un grand nombre entier aléatoire x et calcule : $X = g^x \bmod n$
L'utilisateur j choisit un grand nombre entier aléatoire y et calcule : $Y = g^y \bmod n$
i envoie X à j et j envoie Y à i.
i calcule $k = Y^x \bmod n$
j calcule $k' = X^y \bmod n$

5. Cryptosystème RSA

Le système de chiffrement développé au M.I.T. en 1976 par Ronald Rivest, Adi Shamir et Leonard Adleman semble être sûr et utilise le système de clefs publiques.
C'est un système de chiffrement exponentiel, dans lequel chiffrement et déchiffrement sont réalisés par des fonctions du type:

$$M \rightarrow C = a^A \pmod M$$

5.1 Mathématiques appliquées au système RSA

5.1.1 Congruence

Soient quatre entiers y, r, m et k avec $m \neq 0$.
On dit que y est congru à r relativement au modulo m et on écrit $y \cong r \pmod m$, si et seulement si on a la relation:

$$y - r = k * m.$$

5.1.2 Nombre premier

Tout entier positif y ($y > 1$) est appelé un nombre premier si ses seuls diviseurs entiers sont les diviseurs +1 ou -1 et +y ou -y, c'est à dire ses seuls diviseurs sont 1 et lui-même.

5.1.3 Nombres premiers entre eux

On dit que deux entiers sont premiers entre eux si le plus grand entier qui les divise tous les deux est un, c'est à dire leur pgcd est 1.

5.1.4 Fonction de totalisation d'Euler

On appelle fonction de totalisation d'Euler ou fonction totient d'Euler la fonction $\Phi(n)$ telle que:

$$\Phi(n) = n [(1 - (1/P_1)) * (1 - (1/P_2)) ... (1 - (1/P_n))]$$

où p_1, p_2, ..., p_n sont les facteurs premiers de n.

Cette fonction nous donne le nombre de facteurs qui sont premiers avec n.

5.1.5 Inverse multiplicatif pour le modulo

Pour tout x appartenant à l'ensemble décrit par $\Phi(n)$ on a: $x^{\Phi(n)-1} (\text{mod } n) = 1$.par généralisation d'Euler du théorème de Fermat.
On appelle donc inverse multiplicatif de x, et ont le note x* le nombre qui vérifie la relation:

$$x^* = x^{\Phi(n)-1} (\text{mod } n)$$

On remarque qu'un entier modulo n possède un inverse multiplicatif modulo n si et seulement si il est premier avec n.

5.2 Algorithme RSA

Le principe du Cryptosystème RSA repose sur l'utilisation des fonctions puissance dans le sous ensemble des entiers modulo n. Chaque utilisateur dispose:

a) d'une clef publique, servant à chiffrer les données, constituée d'un nombre n très grand, n étant le produit de deux nombres premiers p et q, et d'un nombre E choisi au hasard dans l'intervalle $[2,(p-1)*(q-1)-1]$;

b) d'une clef secrète formée du produit $\Phi(n) = (p-1) * (q-1)$ des facteurs premiers de n et d'un nombre D tel que:

$E * D = K * \Phi(n) + 1 \cong 1 (\text{mod } \Phi(n))$ où $\cong$ représente la congruence, et $\Phi(n)$ est la fonction totient d'Euler précédemment décrite. Cette clef secrète sert à chiffrer l'information.

Quand l'utilisateur B veut envoyer un message M à l'utilisateur A, il le chiffre au moyen de la clef publique de A, définie par n_A, E_A, comme suit:

$$M \rightarrow C = M^{E_A} (\text{mod } n_A)$$

L'utilisateur A déchiffre C au moyen de sa clef secrète D_A, comme suit:

$$C \rightarrow C^{D_A} = M^{E_A D_A} = M^{1+K\Phi(n_A)} (\text{mod } n_A)$$

Cette dernière équation de déchiffrement du RSA est déduite d'un théorème classique d'arithmétique, connu sous le nom de petit théorème de Fermat, affirmant en effet que, si PGCD(M,p) = 1 alors:

$M^{\Phi(p)} \cong 1 \text{ (mod } n_A)$

BIBLIOGRAPHIE

[Asokan 94] N. Asokan, "Anonymity in a Mobile Computing Environment", Proceedings of the Workshop on Mobile Computing Systems and Applications, Santa Cruz, December, 1994.

[Asokan 95] N. Asokan, R. Molva, D. Samfat, "Untraceability in Mobile Networks" in the proceedongs of the first ACM International Conference on Mobile Computing and Networking, November 1995

[Aziz 94] A. Aziz, W. Diffie, "Privacy and Authentication For Wireless Local Area Networks", IEEE Personal Communications, pp 25-31, 1994.

[Badache 98] Nadjib Badache, "La mobilité dans les systèmes répartis", Techniques et Sciences Informatiques,Vol.17 (8), pp : 969 – 997, Octobre 1998.

[Badr 95] Badr, N.G., "Cellular Digital Packet Data CDPD", Conference Proceedings of the 1995 IEEE Fourteenth Annual International Phoenix Conference on Computers and Communications, Scottsdale, AZ, USA, 28-31 March 1995.

[Baggio 95] Baggio Aline, "Environnements mobiles: Caractéristiques et Problèmes", Dans le seminaire sur les systèmes et applications réparties, Rapport de DEA, CNET-Issy les moulineaux, Fevrier 1996.

[Benmeziane 01] Souad Benmeziane, "Anonymat sur Internet", Rapport de promotion, CERIST, Mars 2001.

[Benmeziane 01a] Souad Benmeziane, "Authentification : Concepts et Techniques", Support de Cours, CERIST, 2001.

[Benmeziane 02] Souad Benmeziane, Lyes Khelladi, « i-vote : un système de vote électronique hautement sécurisé », Internet Security Communication Workshop SECI'02, Tunis, Septembre 2002

[Beller 92] M.J Beller, L.F. Chang, Y. Yacobi, "Security for personal Communication Services : Public-Key vs. Private key Approaches", Procceeding of the 2nd International Symposium on Personal, Indoor and Mobile Radio Communications, October 1992.

[Bidan 95] C. Bidan, V. Issarny, "Un Aperçu des problèmes de sécurité dans les systèmes Informatiques", Publication Interne n°959, IRISA, Octobre 1995.

[Bird 95] Ray Bird, Inder Gopal, Amir Herzberg, Phil Janson, Shay Kutten, Refik Molva, and Moti Yung, "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution", IEEE/ACM Transactions on Networking, Vol.3, No.1, February 1995

[Burrows 90] M. Burrows, M. Abadi, R. Needham, “A logic of Authentication”, ACM Transactions on Computer Systems, 18-36 February, 1990.

[Chaum 81] David Chaum, "Untraceable Elctronic Mail, Return Addresses, and Digital Pseudonyms" , Communications of the ACM, Vol. 24, n° 2, pp. 84-88, Feb. 1981.

[Chaum 83] David Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology, Proceedings of CRYPTO 82, p 199-203, Plenium Press, 1983.

[Curtis 01] H. W. Curtis, "Subscriber Authentication and Security in Digital Cellular Networks and Under the Mobile Internet Protocol", A thesis for the degree of Master of Science in Engineering, The University of Texas and Austin, May 2001

[Diffie 76] Whitfield Diffie, Martin Hellman,"New Directions in Cryptography", IEEE Transactions on Information Theory, Vol.22, No.6, November 1976, pp644-653.

[Dingledin 00] Roger R. Dingledin, “The free Haven Project : Design and Deployment of an Anonymous Secure Data Haven “, Master’s thesis, Massachusetss Institute of Technology, June 2000.

[Dix 02] Alexander Dix, “Techniques améliorant la protection des données dans les télécommunications”, rapport interne, Bradenburg, 2002.

[Duchamp 92] Duchamp D., "Issues in wireless mobile computing", In Proceeding of the Third Workshop on Workstation Operating Systems (Key Biscaryne, FL), IEEE, April 1992.

[Ford 94] Warwick Ford, “Computer Communications Security - Principles, Standard Protocols and Techniques”, PTR Prentice Hall, First Edition, 1994

[Forman 94] Forman G. H., Zahorjan J., "The challenges of mobile computing", IEEE Comp uter 27(4), pages: 38-47, April 1994.

[Go 01] Jaeseung Go, “Wireless Authentication Protocols Assuring User Anonymity and End-to-end Confidentiality”, A Thesis for the Degree of Master, School of enginneering Information and Communications University, 2001

[Goldschlag 96] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson,"Hiding Routing Information," Information Hiding, R. Anderson (editor), Springer-Verlag LLNCS 1174, 1996, pp. 137-150.

[Goldschlag 99] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, " Onion Routing for Anonymous and Private Internet Connections " Communications of the ACM, vol. 42, num. 2, February 1999.

[Gunter 99] Günther Horn, Bart Vinck, Klaus Müller, “Towards a UMTS Security Architecture“, European Wireless, Munich, Germany, October 1999

[Gunter 00] Günther Horn, Peter Howard, “Review of Third Generation Mobile System Security Architecture”, ISSE 2000, Barcelona, Spain, September 2000.

[Hellberg 98] Niklas Hellberg, "Security in Interconnected Open Environments : How to achieve privacy and trust in a mobile environment ", Master’s thesis, Stockholm University, 1998.

[Herzberg 94] Amir Herzberg, Hugo Krawczyk, and Gene Tsudik. "On traveling incognito." In Workshop on Mobile Computing Systems and Applications, December 1994.

[Horlait 01] Eric Horlait, Gwendal Le Grand, “An End to End QoS architecture for Mobile Hosts”, Proceedings of the 15th International Parallel & Distributed Processing Symposium (IPDPS-01), San Francisco, CA, April 23-27, 2001. IEEE Computer Society 2001, ISBN 0-7695-0990-8

[ISO 99] ISO IS 15408, "Information Technology-Security Techniques-Evaluation Ceriteria For IT Security Part 2 : Security Functionnal Requirements", Décembre 1999.

[ISO 89] ISO 7498-2, "Systèmes de Traitement de l’Information- Interconnexion de systèmes ouverts – Modèle de Référence de Base. Partie 2 : Architecture de Sécurité ", Février 1989.

[Jansen 99] Wayne Jansen, Tom Karygiannis, “ Nist Special Publication 800-19-Mobile Agent Security”, National Institute of standards and Technology, August 1999

[Khamitov 03] I. Khamitov, A. Monshonkin, “Blind Unanticipated RSA Signature Schemes”, Press PayCash, Mars 2003.

[Khelalfa 00] Halim M. Khelalfa, “ Introduction à la Sécurité Informatique “ , Support de Cours, CERIST, Session 2000.

[Koch 93] Koch H., Krombholz L., Theel O., “ A brief introduction into the world of mobile computing“ , Technical Report, Department of Computer Science, University of Darmstadt, May 1993.

[Legrand 98] Gwendal LE GRAND, “Mobilité et Qualité de Service”, Rapport de DEA, 1998

[Lee 99] S. Lee, S.M. Hong, H. Yoon, and Y. Cho, "Accelating Key Establishment Protocols for Mobile Communication", Lecture Notes in Computer Science, Vol. 1587, P. 51 - 63, 1999

[Mart 99] David Michael Martin JR, " Local Anonymity in the Internet " , Phd thesis, Boston University Graduate School of Arts and Sciences, 1999.

[Mart 98] David Martin, " Internet Anonymizing Techniques ", Special Security Issue, May 1998

[Menzus 96] Alfred J.Menzus, Paul C.vanoorschot, Scott Avanstone, "Handbook of Applied cryptography", August 96

[Meot 93] M. Meot, F. Pignal, M. Saint Martin, M. Seillier, " La Cryptographie ", Epitf, Telecom, 1993

[Mé 99] Ludovic Mé et Renaud Chaillat, "Le commerce électronique : Un état de l'art ", Annales des Télécommunications, 53(9-10), pp361-376, octobre 1998.

[Mé 01] Ludovic Mé et Cédric Michel, "Intrusion Detection: A Bibliography ", Supélec., Technical report SSIR-2001-01, September 2001.

[Molva 92] Refik Molva, Gene Tsudik, Els Van Herreweghen, Stefano Zatti, "KryptoKnight Authentication and Key Distribution System", In Proceedings of the European Symposium on Research in Computer Security, Toulouse, pp155-174, France, 1992.

[Molva 97] Refik Molva, Didier Samfat, "IDAMN: An Intrusion Detection Architecture for Mobile Networks", IEEE Journal on Selected Areas in Communications 15 (7): 1373-1380, 1997

[Olovsson 92] T. Olovsson, "A Structured approach to Computer Security ", Technical report n° 122, Chalmers University of Technology, Sweden, 1992.

[Pfitzmann 86] Andreas Pfitzmann, Michael Waidner, "Networks without User Observability", Eurocrypt '85, LNCS 219, Springer-Verlag, Berlin 1986, 245-253, *Revision in: Computers & Security 6/2 (1987) 158-166.* April 1986

[Pfitzmann 00] Andreas Pfitzmann, Marit Kohntopp, "Anonymity, Unobservability, and Pseudonimity- A proposal for Terminology", July 2000.

[Pitoura 93] Pitoura E., Bhargava B., "Dealing with mobility: Issues and Research Challenges", Technical Report CSD-TR-93-070, Department of Computer Science, Purdue University, November1993

[Pointcheval 96] David Pointcheval, "Les Preuves de Connaissance et leurs Preuves de Sécurité", Thèse de Doctorat, Université de CAEN, Décembre 1996.

[Pointcheval 00] David Pointcheval, Jacques Stern, "Security Arguments for Digital Signatures ans Blind Signature", Journal of Cryptology, 2000.

[Rahnemma 93] Rahnema, M. “Overview of the GSM system and protocol architecture“, IEEE Communications Magazine, vol. 31, no. 4, p. 92-100, April 1993.

[Ramzan 99] Zulfikar Amin Ramzan, “Group Blind Digital Signatures : Theory and Applications “, Master’s thesis Massachusetts Institute of Technology, May 1999.

[Reed 98] M. G. Reed, P. Syverson, D. M. Goldshlag, “Anonymous Connections and Onion Routing “, IEEE Journal on Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, Vol. 16. N° 4, May 1998

[Reed 99] Michael G. Reed and Paul F. Syverson, "Onion Routing," Proceeding of AIPA '99, March 1999

[Reiter 98] M. K. Reiter, A. D. Rubin, “ Crowds : Anonymity for Web transactions “, ACM. TISSEC , vol 1, 1998.

[Samfat 94] D. Samfat, R. Molva, “A method providing Identity Privacy During Authentication”, Proccedings of the first IEEE Workshop on Mobile Computing and its Applications”, Santa-Cruz, December 1994.

[Samfat 96] D. Samfat, R. Molva, N. Asokan, “Anonymity and Untraceability in Mobile Networks”, ACM Wireless Networks Journal, Special Issue on Security in Mobile Networks, 1996.

[Schafer 01] G. Schafer et. al., “Current Approaches to Authentication in Wireless and Mobile Communications Networks”, TKN, Technical University of Berlin, March 2001

[Schneier 96] Bruce Schneier, "Applied Cryptography - Protocols, Algorithms and Source Code in C", Second Edition, John Wiley & Sons, Inc., 1996.

[Stadler 95] Stadler M., Piveteau J.-M. and Camenisch J., “Fair Blind Signatures”, *Proc. EUROCRYPT '95*, LNCS 921, pages 209-219, Springer-Verlag, 1995

[Syverson 97] D. Goldshlag, M. Reed, P. Syverson, “Privacy on the Internet “, INET'97, Kuala Lumpur, Malaysia, June 1997.

[Tsudik 96] C. Culcu, G. Tsudik, “Mixing emails with Babel “, Proc. ISOC, Février 1996.

[Uskela 97] Sami Uskela, “Security in Wireless Local Area Networks”, Department of Electrical and Communications Engineering, Helsinki University of Technology., Seminar on Network Security, Kirkkonummi, December 3-4, 1997

[Win 01] Bart De Win, “On the Anonymity of Electronic Cash”, Report CW 216, K.U. Leuven, Juin 2001

[Zimmermann 02] Jacob Zimmermann et Ludovic Mé, “Les systèmes de détection d'intrusions : principes algorithmiques“, MISC. Numéro 3. pp24-30. juin 2002.