République Algérienne Démocratique et Populaire
Université El Hadj LAKHDER - BATNA
Faculté Des Sciences
Département D'informatique

Mémoire

en vue de l'obtention du diplôme de :

Magistère en Informatique

Option : Système informatique de communication

Présenté par :

BENSARI Mouchira

Titre :

Sécurité des échanges dans un réseau de nœuds mobiles

Soutenu publiquement le : 09|12|2012 devant le jury formé de :

Dr. ZIDANI Abdelmajid	MC	**Président**	Université de Batna
Dr. BELATTAR Brahim	MC	**Examinateur**	Université de Batna
Dr. MAAMRI Remdane	MC	**Examinateur**	Université de Constantine
Pr. BILAMI Azeddine	Professeur	**Rapporteur**	Université de Batna

Dédicace

A mes chers parents qui m'ont soutenu durant mon existence et ma scolarité.

A mes chères sœurs et mon cher frère.

A mes oncles, mes tantes et cousins.

A tous mes amis.

Je leur dédie affectueusement ce mémoire.

Remerciement

Au terme de ce travail :

Je remercie, Tout d'abord, ALLAH pour la volonté, la force, la santé et la patience qu'il m'a donné afin de réaliser ce travail.

Je tiens à adresser mes plus chaleureux remerciements au Professeur. Azeddine Bilami *, et lui exprimer toute ma reconnaissance pour son encadrement, ses précieux conseils, son soutien constant, sa confiance et sa patience, ainsi que pour ses remarques pertinentes et ses contributions considérables tout au long de la réalisation de ce travail. J'ai eu l'honneur et le plaisir de travailler sous sa direction pendant mon projet de Magister et j'espère pouvoir continuer à travailler avec lui dans le futur.*

Je tiens également à remercier tous les membres de jury qui m'ont fait un grand honneur en acceptant l'évaluation de ce modeste travail.

J'aimerais également remercier mes enseignants de la première année de Magister et les responsables de département d'informatique de l'université de Batna.

J'adresse mes remerciements aussi à mes collègues de la promotion du magistère.

Je remercie toutes les personnes qui m'ont aidé durant mes études universitaires.

Résumé

Les réseaux de mobiles prennent une place de plus en plus prépondérante dans le domaine des communications sans fil. Ces réseaux présentent des caractéristiques intéressantes (confort offert par la mobilité, accès ubiquitaire à l'information,…), mais malheureusement, ils sont limités en ressources (énergétique, traitement…).

Le fait que les réseaux de mobiles offrent des services, souvent, très sensibles, rend la notion de sécurité primordiale et indispensable. Cependant, à cause de la limitation des ressources, le développement des mécanismes de sécurité est un challenge à relever.

Dans le cadre de ce mémoire de magistère, nous projetons de proposer un protocole d'authentification dédie aux réseaux de mobiles, basé sur l'échange des clés, tout en tenant compte des contraintes liées à ces réseaux (mobilité, usage économique de l'énergie,…). L'objectif est d'authentifier les nœuds du réseau et de distinguer les nœuds intrus en utilisant comme mécanisme la cryptographie elliptique.

Mots clés : Authentification, Algorithmes asymétriques, ECC, Economie d'énergie, Mobilité, Réseau de mobiles, RSA, Sécurité…..

Abstract

Mobile networks take more and more preponderant place in the field of wireless communications. These networks have particular characteristics (comfort offered by mobility, ubiquity access to information…), unfortunately, they are limited in resources (energetic, treatment…).

The fact that the mobile networks offer sensible services makes the concept of security primordial and indispensable. However, because of the limitation of the resources, the development of security mechanisms is being a challenge.

Within the work presented in this document, we propose an authentication protocol, dedicated to the mobile networks, based on the exchange of keys, taking into account the constraints related to these networks (mobility, economic use of energy…). The objective is to authenticate the nodes of the network and distinguish the intruding ones, by using mechanism like the elliptic curve cryptography.

Key words: Authentication, Asymmetric algorithms, ECC, Energy saving, Mobility, Mobile networks, RSA, Security …

ملخص

ان شبكات المحمول تلعب دورا متزايدا يوما بعد يوم في مجال الاتصالات اللاسلكية. هذه الشبكات تقدم ميزات مثيرة للاهتمام (الراحة التي توفرها خاصية التنقل، الحصول على المعلومات في أي مكان، الخ...) ولكنها للأسف محدودة الإمكانيات (الطاقة، المعالجة، الخ ...).

نظرا لكون شبكات المحمول في أغلب الأحيان تقدم خدمات حساسة للغاية، هذا ما يكسب الامن مكانة أساسية و أهمية قصوى . لكن، محدودية الإمكانيات يشكل تحديا يجب التغلب عليه لأجل تطوير آليات الأمن الموجهة لهذه الشبكات .

في إطار هذه المذكرة، ، سنعمل على اقتراح بروتوكول مخصص للمصادقة، موجه لشبكات المحمول، مبني على أساس تبادل المفاتيح، مع الاخذ بعين الاعتبار القيود الموجودة في هذه الشبكات (التنقل، الاستخدام الاقتصادي للطاقة ،...) . الهدف هو مصادقة عقد الشبكة وتمييز العقد المتسللة باستخدام آلية التشفير بالمنحنيات البيضاوية الشكل.

كلمات البحث الرئيسية: التوثيق، خوارزميات غير متناظرة، التشفير بالمنحنيات البيضاوية الشكل، توفير الطاقة، التنقل، الشبكات المحمولة، الأمن.

Sommaire

Chapitre 2 : La Sécurité Dans Les Réseaux De Mobiles

Chapitre 3 : L'authentification Dans Les Réseaux De Mobiles

Chapitre 4 : La Cryptographie A Courbe Elliptique

Chapitre 5 : Le Protocole Proposé

Chapitre 6 : Implémentation et Analyse Des Performances

Liste des Figures

Liste des tableaux

Légendes

AC	Autorité de Certification.
AES	Advanced Encryption Standard.
AKA	Authentication and Key Agreement.
AMPS	Advanced Mobile Phone System.
AuC	Authentication Center.
BSS	Basic Service Set.
CDMA	Code Division Multiple Access.
DES	Data Encryption Standard.
DoS	Denial of service.
ESS	Extended Service Set.
ECC	Elliptic Curve Cryptography.
ESN	Electronic Serial Number.
FDMA	Frequency Division Multiple Access.
GPRS	General Packet Radio Service.
GSM	Global System for mobile telecommunication.
HLR	Home Location Register.
IBSS	Independant Basic Service Set.
IDS	Intrusion Detection System.
IMSI	International Mobile Subscriber Identity.
J2ME	Java 2 Micro Edition.
LAI	Location Area Identifier.
MAC	Message Authentication Code.
NMT	Nordic Mobile Telephone.
NNI	Network Node Interface.
PKI	Public Key Infrastructure.
PN	Pseudo-random Noise.
SHA	Secure Hash Algorithm.
SIM	Subscriber Identity Module.
TACS	Total Access Communication System.
TDMA	Time Division Multiple Access.
UMTS	Universal Mobile Telecommunications System.
VLR	Visitor Location Register.

Introduction générale

La prolifération des appareils mobiles a conduit à l'augmentation et à la popularité croissante des réseaux de mobiles.

Les réseaux de mobiles sont des réseaux sans fils avec infrastructure, composés d'un ensemble d'entités mobiles de formes variées : téléphones mobiles, PDA, capteurs, tablette PC, etc. ces dispositifs mobiles ont des contraints en termes de communication, de puissance de calcul, de stockage et d'énergie.
Avec l'avènement de l'internet, les réseaux de mobiles ne se limitent pas à offrir des services vocaux, ils sont devenus, actuellement, des acteurs aux nouveaux services très importants dans notre vie quotidienne comme le M-commerce, M-Banking, M-Payment, M-Learning, etc. La sécurité est un sujet fatal pour tels services.

La sécurisation de communication dans les réseaux de mobiles passe principalement par la mise en place des conditions de base de la sécurité telles que la confidentialité, l'authentification, l'intégrité, la disponibilité et la non-répudiation. Ces conditions ont différent degrés d'importances selon le contexte d'utilisation du réseau, mais l'authentification est la base de la sécurité quelque soit le domaine d'application de réseaux de mobiles.

La conception d'un protocole d'authentification pour les réseaux de mobiles n'est pas une tâche simple, elle est un challenge à cause des contraintes dans les dispositifs mobile et la mobilité des utilisateurs.
Plusieurs recherches sont effectuées dans ce domaine et plusieurs protocoles d'authentification ont été conçus. Les protocoles existants sont basés soit sur la cryptographie symétrique, soit sur la cryptographie asymétrique ou bien les deux.
Les protocoles symétriques ont plusieurs faiblesses de sécurité malgré qu'ils soient compatibles avec les contraintes dans les dispositifs mobiles, les protocoles asymétriques sont plus sécurisés que les symétriques, mais ils sont très gourmands en matière de ressources où les protocoles hybrides consistent à fournir un compromis entre la sécurité et le coût.

Actuellement, les protocoles d'authentification sont orientés vers la cryptographie elliptique. La cryptographie elliptique est émergée comme alternative aux systèmes cryptographiques asymétriques traditionnels. Plusieurs recherches ont montré que cette technique de cryptographie est mieux adaptée aux dispositifs mobiles sans fils contraints en ressources.

L'objectif de notre travail, dans ce cas, est de proposer un protocole d'authentification destiné aux réseaux de mobiles qui présent une sécurité élevé et un faible cout.

Pour parvenir à notre fin, le présent mémoire est scindé en deux parties : la première concerne tout ce qu'on a pu lire, analyser, et comprendre, renferme quatre chapitres : le premier chapitre survole le domaine des réseaux sans fil en focalisant sur les réseaux de mobile, le deuxième chapitre analyse la sécurité dans ces réseaux, Le troisième chapitre explique en détail le concept d'authentification, et le dernier chapitre de cette partie introduit la technique de la cryptographie à courbe elliptique. La deuxième partie s'occupe de la solution proposée, de la conception et mise en œuvre de cette solution, et des tests qui ont permis d'évaluer le degré d'efficacité de cette dernière. Une conclusion vient en dernier lieu pour clôturer le travail ainsi accompli en proposant quelques perspectives pour une éventuelle continuité de ce travail dans le futur.

Chapitre 1 : Introduction aux réseaux de mobiles

Introduction

Avec l'évolution de la société actuelle, les personnes se déplacent de plus en plus, tout en ayant besoin de communiquer pendant leurs déplacements. Ce phénomène a provoqué une demande accrue de la technologie mobile et a orienté les études vers le développement de technologies très sophistiquées afin de répondre aux nouveaux besoins des utilisateurs.
La technologie sans fil, a fait de ces besoins une réalité, et elle offre aujourd'hui de nouvelles perspectives dans le domaine des télécommunications.

L'évolution récente des moyens de la communication sans fil a permis la manipulation de l'information à travers des unités de calculs portables qui ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome..) et accèdent au réseau à travers une interface de communication sans fil. Comparé avec l'ancien environnement (l'environnement statique), le nouvel environnement résultant appelé « environnement mobile », permet aux unités de calcul, une libre mobilité et il ne pose aucune restriction sur la localisation des usagers.

Les environnements mobiles offrent une grande flexibilité d'emploi, et même les services ont été effectivement améliorés; si la voix était à l'origine le seul besoin, les demandes en transmissions sans fil fournissant des communications fiables et un son à haute définition, d'images, voire de vidéos de haute qualité est devenu de plus en plus demandé par un nombre croissant d'utilisateurs. Ces derniers, exploitent une mobilité complètement transparente et bénéficient des performances comparables à celles des réseaux filaires, malgré les contraintes des unités mobiles et la gourmandise en bande passante de ces nouveaux services.
L'environnement mobile est l'une des nouvelles technologies qui bouleverseront le monde et notre manière de vivre et de travailler.

1. Réseau informatique

Un réseau est l'ensemble d'acteurs, d'agents économiques, de nœuds, ou lieux de communication grâce auxquels les messages circulent. L'information se concentre et se redistribue ainsi**.**

Un réseau informatique est un ensemble d'équipements interconnecté par une seule technologie, capable de s'échanger de l'information **[1].**
Selon *Guy Pujolle,* un réseau informatique: « désigne tout ensemble d'éléments capables de véhiculer de l'information d'une source vers une destination. Le téléphone en est la meilleure illustration » **[2].**

On appelle nœud (node) l'extrémité d'une connexion, qui peut être une interconnexion de plusieurs connexion (un ordinateur, un routeur, un concentrateur, un commutateur, un téléphone mobile,…..).

Les supports de communication entre les équipements peuvent être des câbles dans lesquels circulent des signaux électriques, l'atmosphère (ou le vide spatial) où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses.

Les équipements sont connectés directement ou non entre eux, conformément à quelques organisations types connues sous le nom de topologie de réseau.

Les informations échangées sont standardisées grâce à l'utilisation des protocoles de communication unifiés entre les équipements du réseau. Ces protocoles sont des procédures qui contrôlent le flux d'information entre des équipements.

Les réseaux informatiques sont classés suivant leur portée :

- Réseaux personnel (PAN) : relie des appareils personnels, il couvre une zone de quelque mètres ;
- Réseau local (LAN) : relie les ordinateurs ou postes téléphoniques situés dans la même pièce ou dans le même bâtiment, il couvre de quelques dizaines de mètres, à centaines de mètres ;
- Réseau métropolitain (MAN): est un réseau à échelle d'une ville ;
- Réseau étendu (WAN) : réseau à grand échelle qui relie plusieurs sites ou des nœuds du monde entier.

Les réseaux informatiques peuvent être classé selon le type de lien en : réseaux filaires et réseaux sans fil **[1].**

2. Réseau sans fil

Un réseau sans fil est un réseau informatique ; composé d'un ensemble d'appareils connectés entre eux et qui peuvent s'envoyer et recevoir des données sans qu'aucune connexion «filaire» physique reliant ces différents composants entre eux ne soit nécessaire. C'est les ondes radio qui reliées les différents nœuds entre eux.

Le rayonnement géographique des ondes est relativement limité et de faible puissance d'émission. Pour cette raison, les réseaux sans fil se sont avant tout développés comme réseaux internes, propre à un bâtiment, soit comme réseau d'entreprise, soit comme réseau domestique. Néanmoins, des projets de réalisation de réseaux à grande échelle ont vu le jour, notamment le WiMAX.

La norme la plus utilisé actuellement pour les réseaux sans fil est la norme IEEE802.11, mieux connue sous le nom de Wi-Fi. **[1]**

2.1. Les modes de mise en réseau d'un réseau sans fil

Les réseaux sans fil peuvent fonctionner de deux façons différentes : en mode infrastructure ou en mode Ad hoc.

2.1.1. Le mode infrastructure

En mode infrastructure chaque station (notée **STA**) se connecte à un **point d'accès** via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé *ensemble de services de base* (en anglais *basic service set*, noté **BSS**) et constitue une cellule. Chaque *BSS* est identifié par un *BSSID*, un identifiant de 6 octets (48 bits). Dans le mode *infrastructure*, le *BSSID* correspond à l'adresse MAC du point d'accès**[3]**.

Les terminaux peuvent se déplacer au sein de la cellule et garder une liaison directe avec le point d'accès, ou changer de cellule, ce qui s'appelle le roaming**[4].**

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS)**[3]**.

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long au format ASCII servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès.

Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles.

2.1.2. *Le mode ad hoc*

En mode ad hoc les machines sans fil se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer* en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé *ensemble de services de base indépendants*(en anglais **independant basic service set**, abrégé en *IBSS*).

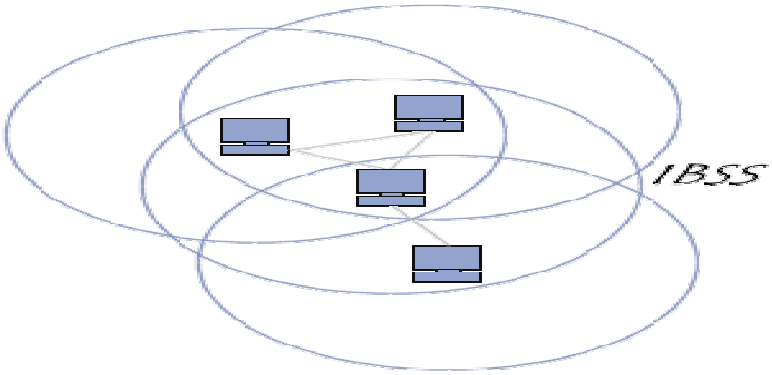

Fig1.1. : le mode ad hoc **[3]**

Un *IBSS* est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'*IBSS* constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un *SSID,* comme l'est un *ESS* en mode infrastructure **[3].**

Un réseau ad hoc est différent d'un réseau en mode ad hoc, ce dernier ne propose pas de protocole de routage permettant à une station de faire transiter les données qui ne lui sont pas destinées.

3. Réseaux de mobiles

3.1. Présentation

Le réseau de mobile est un réseau qui offre à des utilisateurs munis d'une unité mobile (téléphone mobile, PDA,…), la possibilité d'accéder à des services et à des applications évoluées, à travers une infrastructure sans fil, indépendamment de la localisation physique ou du mouvement de ces utilisateurs **[5].**

Le réseau de mobiles est basé sur la technologie du réseau cellulaire (mode infrastructure) dont le principe est fondé sur la division d'une région sur le terrain en plusieurs cellules **[6].**

Les réseaux cellulaires sont des systèmes de communication sans fil qui reposent sur une infrastructure fixe. Les terminaux qui évoluent au sein de ces réseaux doivent obligatoirement s'adresser à cette infrastructure (point d'accès) pour pouvoir accéder aux services qu'ils demandent.

3.2. Les unités mobiles

Les appareils mobiles, ou « mobiles », sont de petits engins électroniques portables qui apparurent pour la première fois vers la fin des années soixante. Les appareils mobiles de l'époque n'avaient bien entendu rien en commun avec les appareils actuels, mis à part le fait de pouvoir effectuer des appels téléphoniques. On peut dire qu'en général les premiers appareils

mobiles furent conçus pour une tâche ou pour une application spécifique, grâce à l'association d'un logiciel propriétaire et d'un matériel dédicacé, alors que les appareils mobiles actuels sont conçus pour être polyvalents.

Pour atteindre cette flexibilité, beaucoup d'appareils mobiles ont un système d'exploitation permettant l'installation d'applications additionnelles.

Les autres points clés sont l'intégration d'une connectivité réseau, l'augmentation de la puissance de calcul et des possibilités de stockage. De plus, beaucoup de PDA sont équipés de slots d'extension permettant l'ajout de matériel accessoire supplémentaire. **[9]**

Le marché expose aujourd'hui beaucoup d'appareils mobiles, et il proposera plus à l'avenir. Il n'y a aucune classification précise de tels appareils, ils sont classifiés par taille, forme, poids, ou puissance de calcul. La liste suivante donne quelques exemples des unités mobiles :

- ***Téléphone mobile***

Les téléphones mobiles présentent aujourd'hui une typologie très variée et fournissent différents niveaux de fonctionnalités. Un simple téléphone mobile offre les fonctionnalités de base, tel que la possibilité d'effectuer un appel téléphonique et l'envoi d'un court message de texte. Cependant de nos jours, même le téléphone mobile le plus basique propose des fonctions supplémentaires comme une alarme ou un calendrier **[9]** . Des téléphones mobiles plus évolués peuvent offrir des fonctions additionnelles comme la synchronisation du contenu du calendrier ou du répertoire téléphonique avec un ordinateur de bureau, ils sont enrichis par l'affichage graphique, l'écran tactile, et le navigateur d'Internet**[7]**. La plupart des téléphones mobiles font tourner un système d'exploitation spécialisé et compact.

- ***PDA***

Les PDA sont des appareils de la taille d'un téléphone mobile, mais possédant généralement un large écran tactile dont le dispositif d'entrée typique est un stylo **[7]** à la place d'un écran plus petit muni d'un clavier. Les PDA actuels disposent de processeurs relativement rapides, mais d'une capacité mémoire et de stockage plutôt limitée. Le cœur de chaque PDA est un ensemble de logiciels pour la gestion des informations personnelles. Cet ensemble est au moins composé d'un carnet d'adresses, d'un calendrier et d'un petit traitement de texte. Une des caractéristiques les plus importantes des PDA actuels est qu'ils font tourner un système d'exploitation supportant l'installation de logiciels supplémentaires. Beaucoup de PDA récents sont aussi équipés d'un affichage haute résolution et fournissent généralement une certaine connectivité sans fil **[9]**.

- ***Smartphones***

Un smartphone est une combinaison d'un téléphone mobile et d'un PDA.

Fondamentalement il existe deux variantes différentes : une version élaborée ressemblant à un PDA et une version plus simple ressemblant à un téléphone mobile. Un smartphone possède beaucoup d'applications communes à un PDA, il supporte aussi l'installation d'applications supplémentaires. Les dernières générations de smartphones offrent généralement des possibilités de gestion de réseau sans fil **[9]**.

- ***Tablette PC***

Les tablettes PC sont pour la plupart des écrans tactiles mobiles sans clavier, supportant une connectivité sans fil pour la visualisation de contenu multimédia et de documents en ligne. La majorité des tablettes sont construites en utilisant des composants standards d'ordinateurs personnels, et donc font tourner un système d'exploitation commun aux ordinateurs personnels qui peut être enrichi de quelques services d'interface spécifiques **[9]**.

- ***Notebook***

Les notebooks sont de petits ordinateurs portables. Souvent ils ne disposent pas d'un clavier complet, mais ils peuvent avoir des fonctionnalités supplémentaires, comme un écran tactile ou une souris « Touchpad ». Beaucoup de notebooks font tourner les systèmes d'exploitation standards des ordinateurs personnels, tandis que d'autres utilisent un système d'exploitation spécialisé, plus léger. Ce type d'appareil se situe normalement entre un ordinateur portable et un PDA, en termes de taille et de fonctionnalités. Néanmoins à l'heure actuelle, on ne distingue plus bien un notebook d'un ordinateur portable, et le terme notebook est maintenant communément employé pour désigner un ordinateur portable **[9]**.

- ***Lecteur multimédia mobile***

Les lecteurs multimédia sont des appareils spécialement conçus pour accéder à du contenu multimédia. Dans les versions les plus basiques, ils sont aussi appelés lecteurs de musique ou baladeurs. Les modèles haut de gamme peuvent inclure un lecteur et enregistreur vidéo portable. Les modèles récents incorporent une connectivité sans fil pour accéder à du contenu à travers un réseau. La plupart des lecteurs utilisent un système d'exploitation personnalisé et ne supporte pas l'installation de logiciels supplémentaires **[9]**.

- ***Console de jeu mobile***

Les consoles de jeu mobiles sont conçues pour jouer à des jeux vidéo.

La plupart de ces appareils sont aussi capables de fournir du contenu multimédia.

Ceci entrave donc parfois la distinction entre une console de jeu portable et un lecteur multimédia mobile. Les consoles récentes utilisent une connectivité sans fil pour supporter les jeux multi-joueurs. Comme les lecteurs multimédias, la plupart des consoles de jeux portables font tourner un système d'exploitation personnalisé et ne supportent pas l'installation de logiciels

supplémentaires autre que des jeux, bien qu'il existe des outils permettant de les utiliser comme un ordinateur portable **[9]**.

- ***Capteur (Sensor)***

Les ***Capteurs*** sont des engins destinés à une application commerciale, médicale ou militaire spécifique. Ces appareils ne possèdent pas une grande base d'utilisateurs et sont habituellement équipés de logiciels simples et personnalisés **[9]**.

3.3. Architecture de réseau de mobile

Puisque le réseau de mobile est basé sur la technologie de réseau cellulaire, dans un réseau de mobile, le territoire couvert, ou la zone de couverture, est généralement découpé en petites surfaces géographiquement limitées et communément appelées cellules. Elles sont représentées par des hexagones dont le rayon varie de quelques centaines de mètre à quelques kilomètres. Les cellules se chevauchent partiellement entre elles de manière à assurer une couverture plus complète du territoire **[9]**.

Une infrastructure de réseau de mobile typique consiste en un certain nombre de composants : les cartes à puces, les unités mobiles, les stations de bases, les centres de commutation des services mobiles (Mobile Switching Centre), satellite, les enregistreurs de localisation nominal et les enregistreurs de localisation des visiteurs **[5].**

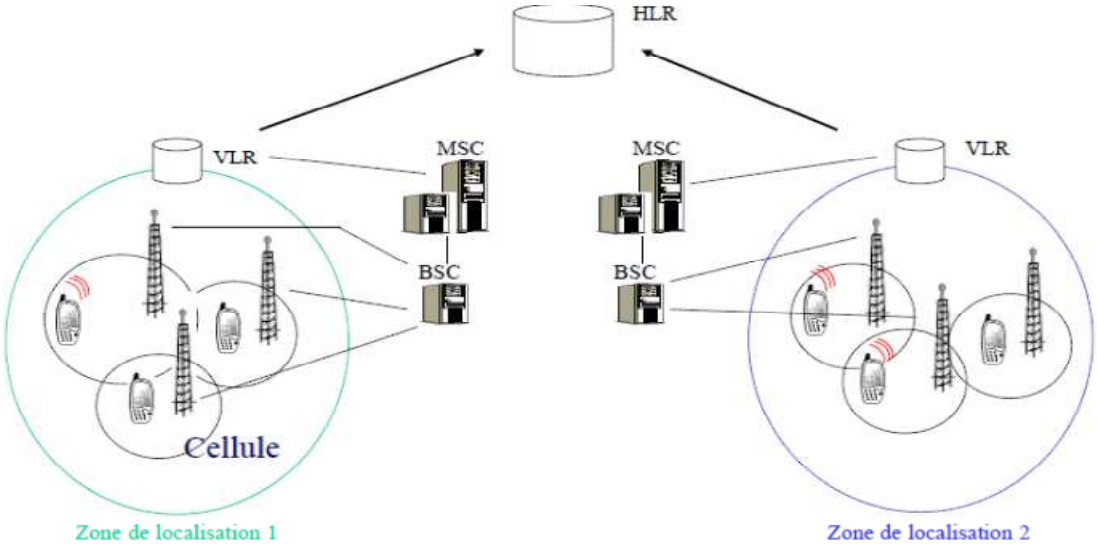

Fig.1. 2. : Architecture de réseau de mobile **[5]**

La carte à puce ou la carte SIM (Subscriber Identity Module) permet de se connecter au réseau pour bénéficier des services auxquels l'utilisateur est abonné, et ce, quelque soit sa localisation. L'établissement d'une communication commence toujours par une phase d'authentification durant laquelle le réseau dialogue avec la carte SIM pour vérifier la validité de l'abonnement. Elle contient des informations comme le numéro d'identification temporaire attribué par le réseau qui

permet la localisation de l'utilisateur, la liste des fréquences à écouter pour identifier la meilleure Station de Base et les algorithmes de chiffrement. D'autres informations sont stockées sur cette carte, tel que le code permettant de la débloquer automatiquement après un certain nombre d'erreurs sur le code entré par l'utilisateur **[10].**

La station de base (BTS) dessert une centaine d'utilisateurs mobiles dans une région donnée (cellule) en allouant les ressources permettant de lancer de nouveaux appels et de compléter des appels en cours lors de déplacements à l'intérieur des cellules**[8]**. BTS intègre une antenne assurant la transmission radio et la signalisation à l'intérieur de la cellule. En effet, intégrés à la station de base, des canaux de signalisation permettent aux unités mobiles de communiquer BTS et vice versa.

Le contrôleur de station de base (BSC) fournit un support de commutation à plusieurs stations de base voisines, desservant des milliers d'utilisateurs (les BSC et les BTS sont d'habitude reliés par un fibre optique, mais ils peuvent aussi être reliés par des liaisons micro-ondes sans fil) **[8]**;

Le commutateur (MSC) est capable de desservir des centaines, voire des milliers d'utilisateurs (les liaisons radio sont aussi de plus en plus utilisées pour relier un MSC et un BSC) **[8]**.

Dans le réseau de mobile, il existe deux éléments qui sont utilisés pour identifier la position du terminal mobile. Ce sont l'enregistreur de localisation nominal HLR (Home Location Register) et l'enregistreur de localisation de visiteurs VLR (Visitor Location Register). Ils sont connectés au MSC.

Le HLR est une base de données qui permet au MSC de gérer les informations des abonnés (utilisateurs permanents du réseau). La base de données nominale est unique dans le réseau. Même si plusieurs équipements physiques servent à stocker les données de la base de données nominale, le réseau ne reconnait qu'une seule entité logique. Cette basse de données contient les renseignements sur tous les abonnés du réseau : non, numéro, services, localisation courante. La recherche d'une donné mobile dans un réseau commencera toujours par l'interrogation de la base de données nominale **[8]**.

Le VLR est une base de données qui permet au MSC de gérer les informations des visiteurs (abonnés en transit dans la région). Il est pris en charge par le MSC local. Un réseau de mobile peut intégrer plusieurs bases de données de visiteurs. Une VLR stocke les données sur tous les abonnés enregistrés dans les zones de localisation qui dépendent d'elle. Ces données consistent en une recopie partielle des éléments contenus dans la base de données nominale des abonnés et elles sont importées soit directement à partir de la base de données nominale, soit à partir de l'ancienne base de données de visiteurs de l'unité mobile. Dans la plupart des réseaux actuels, la base de données de visiteurs dessert une seule zone de localisation **[8]**.

3.4. Les interfaces entre les équipements

Les schémas d'architecture suivants présentent les principales interfaces qui disposent le réseau théorique le plus complet. Dans la plupart des cas, l'architecture d'un réseau de mobiles ne comporte pas toutes ces interfaces.

L'interface UIM-MT :

L'interface, UIM-MT, ou SIM-MT se situe entre la carte à puces, qui détermine l'identité de l'utilisateur, et le terminal mobile.

Le rôle principal de cette interface est de ***sécuriser*** la communication (les vérifications et les contrôles d'accès) qui s'établit à partir du mobile. Cette interface permet spécialement l'authentification de l'utilisateur et permet donc de facturer correctement le client qui effectue une communication **[5].**

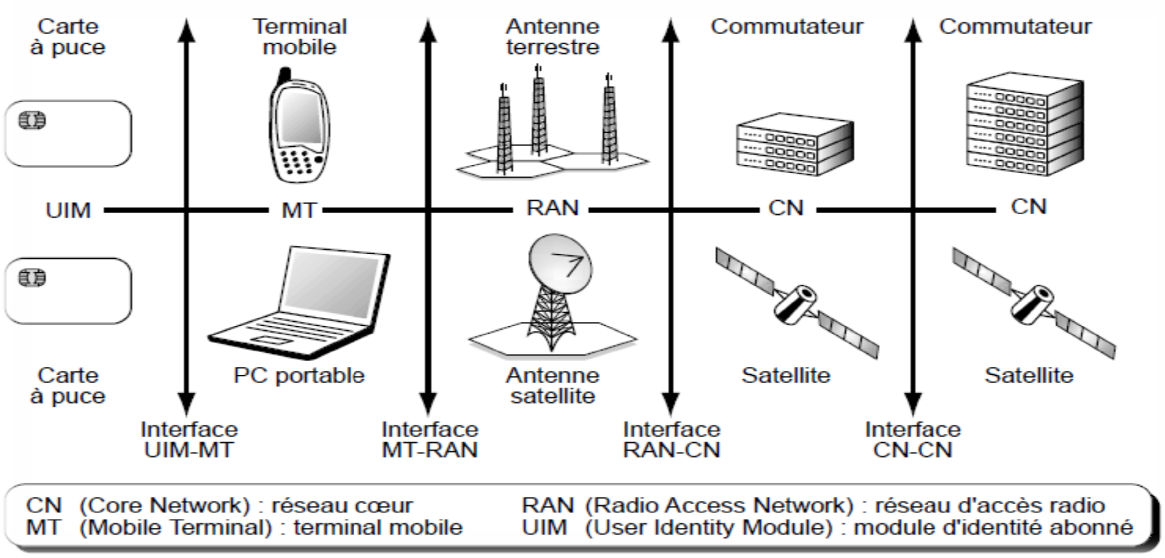

Fig.1. 3. : Interfaces entre les équipements d'un réseau de mobiles **[5]**.

L'interface MT-RAN (interface radio) :

L'interface MT-RAN (Radio Access Network), réalise le joint entre le terminal mobile et l'antenne, interface que l'on appelle encore interface radio ou interface air. Lorsqu'on parle de réseaux de mobiles, on pense immédiatement à cette interface, car c'est là que se trouve la spécificité de ces réseaux**.**

L'interface radio représente souvent le point le plus sensible du réseau car les ressources y sont faibles et doivent être optimisées **[5]**.

L'interface RAN-CN :

L'interface RAN-CN concerne la transmission de l'antenne au premier commutateur du réseau cœur. Une fois l'antenne atteinte, les signaux doivent être transportés vers l'utilisateur distant par l'intermédiaire d'un réseau terrestre, que l'on appelle le réseau cœur.

Comme indiqué précédemment, cette interface regroupe plusieurs antennes, de sorte à pouvoir gérer ces dernières collectivement. Dans le cas de l'antenne satellite, l'interface est interne au satellite puisque l'antenne et le commutateur sont tous deux situés dans le satellite.

Cette interface assure la gestion des appels en acheminant correctement chaque appel arrivant sur le commutateur du réseau fixe de liaison vers l'antenne adéquate, qui diffuse l'information de façon qu'elle soit captée par le client destinataire. Cette interface doit également ***gérer la mobilité*** puisque le client se déplace et peut se trouver connecté à une autre antenne, soit à l'intérieur du même sous-système, soit au sein d'un sous-système indépendant **[5]**.

L'interface CN-CN :

C'est ce que l'on rencontre déjà sous le nom d'interface NNI (Network Node Interface).

L'interface CN-CN relie entre deux nœuds de la partie fixe d'un réseau de mobiles. Les nœuds du réseau sont constitués par les commutateurs du réseau fixe.

Cette interface définit, entre autres choses, la technologie réseau utilisée pour acheminer les informations (commutation de circuits, commutation de paquets) **[5]**.

3.5. Gestion de la localisation dans les réseaux de mobiles

Les réseaux de mobiles sont décomposés en zones de localisations. Les zones de localisation regroupant un certain nombre de cellules (de quelques cellules à quelques dizaines de cellules) sont définies.

Le système connaît la zone de localisation précise de l'abonné, c'est-à-dire la dernière dans laquelle le mobile s'est signalé mais ignore la cellule précise où se trouve le mobile à l'intérieur de la zone de localisation **[11]**.

Dés qu'une unité mobile entre dans une nouvelle zone de localisation, elle doit s'inscrire auprès de la base de données de visiteurs (VLR) de cette zone et rapporte au réseau son nouveau serveur de localisation, selon une procédure dite de mise à jour de localisation.

Cette procédure exige l'accès à la base HLR pour la mise à jour des données de localisation de l'unité mobile.

Pour communiquer avec une unité mobile, la première chose à faire est de déterminer sa localisation. Il faut donc accéder à la base HLR selon une procédure dite de recherche de localisation. Dans cette phase, le réseau doit déterminer la zone de localisation actuelle de l'unité mobile afin d'établir une communication entre cette unité et l'unité appelante.

Les technique de gestion de localisation consistent à attribuer à chaque zone de localisation une adresse unique ou, en d'autres termes, un numéro d'identification unique LAI (Location Area Identifier). Les stations de base des cellules qui forment la zone diffusent cette adresse périodiquement aux unités mobiles qui se trouvent dans l'espace de couverture de la zone. L'unité mobile garde normalement l'adresse de sa zone actuelle, si les deux numéros sont différents, c'est qu'elle a franchi la frontière de sa zone de localisation et se trouve dans une nouvelle zone.

A ce moment, l'unité mobile doit faire connaitre sa nouvelle zone de localisation est donc un processus à deux phases : la mise à jour de localisation (enregistrement de la localisation) et la recherche de localisation (livraison de service) **[8].**

4. Méthode d'accès au réseau de mobiles

Dans les réseaux de mobiles, la transmission radio passe par l'interface radio, que se partagent les utilisateurs d'une même cellule. Plusieurs méthodes permettent aux mobiles d'accéder à la ressource radio. Ces méthodes ont toutes pour principe de diviser la bande de fréquences, généralement très limitée, en plusieurs canaux physiques assurant la communication tout en respectant les contraintes permettant d'éviter les interférences. Les trois principales méthodes d'accès utilisées par les réseaux de mobiles sont FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) et CDMA (Code Division Multiple Access) **[5]**.

4.1. FDMA (Frequency Division Multiple Access):

La méthode d'accès FDMA, ou accès multiple par division de fréquences, repose sur un *multiplexage en fréquences.* Le multiplexage fréquentiel divise la bande de fréquences en plusieurs sous-bandes. Chacune est placée sur une fréquence dite *porteuse,* ou *carrier,* qui est la fréquence spécifique du canal. Chaque porteuse ne peut transporter que le signal d'un seul utilisateur. Cette méthode nécessite une séparation entre les porteuses par des ***bandes de gardes*****[8]** pour éviter les interférences.

La méthode FDMA est essentiellement utilisée dans les générations à codage analogiques **[5]**.

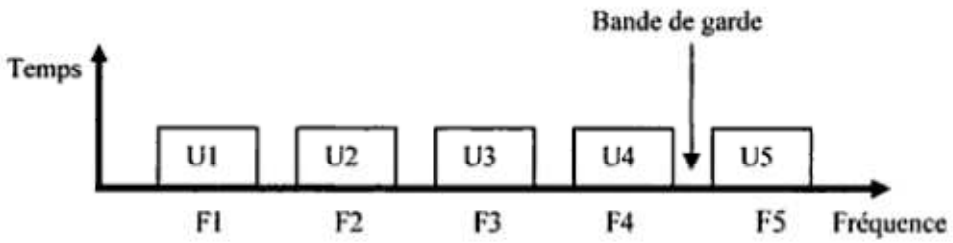

Fig.1. 4. : La téchnique FDMA **[5].**

4.2. TDMA (Time Division Multiple Access)

La méthode TDMA, ou accès multiple par division temporelle, offre la totalité de la bande de fréquences à chaque utilisateur pendant une fraction de temps donnée, dénommée *slot*.

L'émetteur de la station mobile stocke les informations avant de les transmettre sur le slot, autrement dit dans la fenêtre temporelle qui lui a été consacrée. Les différents slots sont regroupés en une *trame*, le système offrant ainsi plusieurs voies de communication aux différents utilisateurs. La succession des slots dans les trames forme le canal physique de l'utilisateur. Le récepteur enregistre les informations à l'arrivée de chaque slot et reconstitue le signal à la vitesse du support de transmission.

Le TDMA s'applique principalement à la transmission de signaux numériques, contrairement au FDMA. Toutefois, la combinaison des deux techniques est envisageable, dont la bande de fréquences disponible est divisée en sous-bandes ou canaux de fréquence (comme dans le FDMA). Ces canaux à leur tour répartis en un certain nombre de tranches de temps **[8].**

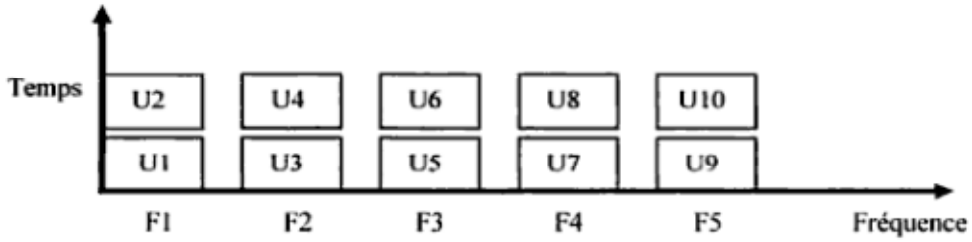

Fig.1. 5. : La téchnique TDM **[8]**.

4.3. CDMA (Code Division Multiple Access)

Troisième méthode, le CDMA, ou accès multiple par division de codes, autorise l'allocation de la totalité de la bande de fréquences, de manière simultanée, à tous les utilisateurs d'une même cellule. Pour ce faire, un code binaire spécifique PN (Pseudo-random Noise) est octroyé à chaque utilisateur. L'utilisateur se sert de son code pour transmettre l'information qu'il désire communiquer en format binaire d'une manière orthogonale, c'est-à-dire sans interférence entre les signaux, aux autres communications.

En CDMA, chaque utilisateur dispose de toute la largeur de la bande passante. L'attribution de différents codes permet une réutilisation de la même fréquence dans les cellules adjacentes.

Cela offre un avantage considérable à cette méthode par rapport aux deux autres, le TDMA et le FDMA. Toutefois, les codes étant seulement quasi orthogonaux à la réception, un problème d'auto-interférence entre en jeu, qui s'intensifie au fur et à mesure que le nombre de communications simultanées augmente. Excédant le nombre maximal de codes attribués, la surcharge de la cellule affecte en outre tous les autres utilisateurs par l'interférence provoquée sur leurs canaux, alors que, en comparaison, un seul utilisateur est brouillé en TDMA **[12].**

La difficulté demeure de pouvoir fournir des codes assez différentes à chaque utilisateur connecté pour éviter les interférences, d'une part, et pour que l'antenne puisse récupérer les émissions s'effectuant en parallèle, d'autre part **[8].**

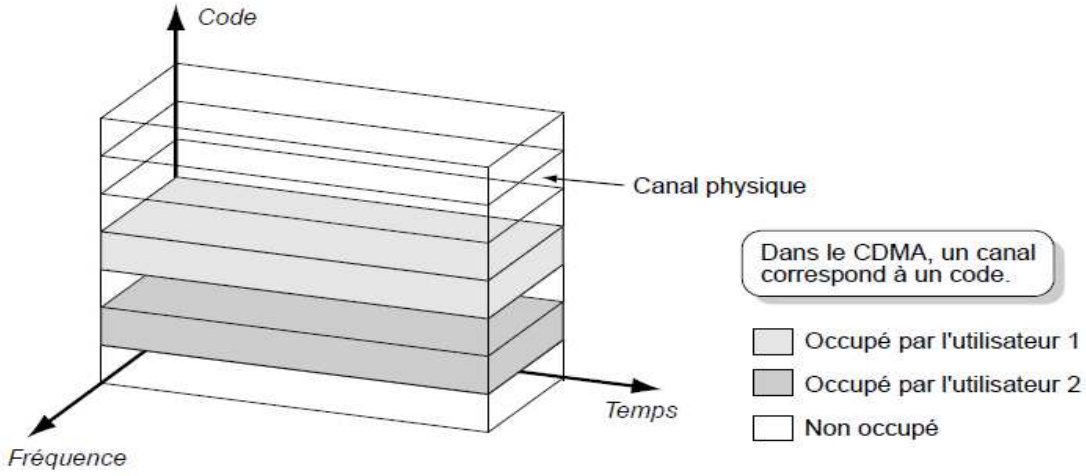

*Fig1. 6. : La technique CDMA***[8]**.

5. Générations des réseaux de mobiles

Le terme génération sert à désigner les améliorations incrémentales survenues au cours de l'évolution des réseaux de mobiles.

5.1. Première génération (1G)

Les réseaux de première génération ont été les premiers à permettre à un utilisateur mobile d'utiliser un téléphone de façon continue, n'importe où dans la zone de service d'un opérateur**[2].**

Ils apparaissaient au début des années 1970 pour remplacer les téléphones filaires, comprenait des systèmes et des plates-formes de communications analogiques essentiellement dédies à la transmission de la voix.

Les concepts clés de cette génération sont la réutilisation de fréquence, la mobilité des abonnées et le relève.

Des nombreux systèmes 1G ont été développés, AMPS (*Advanced Mobile Phone System*) aux États-Unis, le TACS (*Total Access Communication System*), version modifiée du système AMPS pour le Royaume-Uni, le NMT (*Nordic Mobile Téléphone*), utilisé dans les pays d'Europe du Nord, et Radiocom 2000, le standard français **[12].**

Les réseaux de première génération utilisent généralement la technique FDMA. Cependant, la largeur de bande du canal utilisé diffère largement d'un système à l'autre.

Les systèmes 1G présentent beaucoup de point faibles, leur plus grande faiblesse demeure leur capacité limitée, qui a rendu opportune l'introduction d'une technologie de deuxième génération. On observe aussi des limitations de mobilité, particulièrement entre réseaux de fournisseurs différents, l'absence de mécanismes de sécurité contre la fraude et la perte potentielle d'utilisateurs mobiles que le réseau n'est pas capable de retracer **[8]**.

5.2. Deuxième génération (2G)

Profitant du développement des techniques de codage numérique de la parole, la deuxième génération est caractérisée par l'usage de la technologie numérique qui permet de résoudre les problèmes de capacité et de sécurité inhérents aux 1G, tout en augmentant le nombre des services avancés disponibles.

Les réseaux de cette génération autorisent l'utilisation de TDMA et CDMA comme une alternative à FDMA. Ainsi, le spectre radio est mieux rentabilisé et le nombre d'usagers possibles augmente considérablement **[6].**

Divers types de réseaux 2G ont vu le jour à travers le monde (IS-136 TDMA, IS-95 CDMA, GSM,…).

5.3. Troisième génération (3G)

Dans les réseaux de troisième génération, les efforts sont déployés aussi bien au niveau international qu'au niveau régional /national. En fait, il faut se douter des normes internationales non seulement pour assurer la mobilité globale sans coupure et la garantie des services, mais aussi pour garantir l'intégration du réseau câblé et du réseau sans fil afin de fournir des services de communication d'une manière transparente aux utilisateurs. Ces normes internationales sont assez souples pour répondre aux besoins locaux et permettre aux systèmes régionaux/nationaux d'autre génération d'évoluer de façon graduelle vers les systèmes de la troisième génération **[8].**

Les mobiles de la troisième génération sont des terminaux aux débits supérieurs aux anciennes mobiles. Ils sont capables, ainsi, d'offrir une importante gamme de services multimédias **[6].**

Divers types de réseaux 3G ont vu le jour, le fameuse est l'UMTS (Universal Mobile Telecommunications System).

5.4. Quatrième génération

La quatrième génération est pour ambition non seulement d'améliorer le débit mais de mettre en commun la grande variété de solutions mobiles, souvent complémentaires entre elles, et de les proposer sous forme unifiée, dans un équipement terminal unique. Les **générations futures** souhaitent d'aller encore plus loin dans la même direction par une unification des interfaces radio, des techniques d'accès et des services **[12]**.

6. Caractéristiques des réseaux de mobiles

Les réseaux de mobiles sont caractérisés par ce qui suit :

- *Topologie dynamique* :

Les unités mobiles peuvent se déplacer de façon libre et aléatoire. Par conséquent la topologie du réseau peut changer à tout instant de manière rapide et aléatoire.

- *Une bande passante limitée :*

A cause de l'utilisation d'un médium de communication partagé ; ce partage fait que la bande passante réservée à un mobile est modeste.

- *Des contraintes d'énergie* :

Les mobiles sont alimentés par des sources d'énergie autonomes et limitées comme les batteries ou les autres sources consommables. Ce paramètre d'énergie doit être pris en compte dans tout contrôle fait par le système.

- *Une capacité de mémoire et de puissance de calcul limitées :*

Certains équipements utilisés dans les réseaux de mobiles ont des capacités de stockage faibles et des puissances de calcul limitées. Leur sécurité physique est également faible.

- *Mode infrastructure :*

Les réseaux de mobiles se distinguent des autres réseaux mobiles par l'existence d'une infrastructure qui représente l'administration centralisée. Les hôtes mobiles ne sont pas responsables d'établir et de maintenir la connectivité du réseau de manière continue.

- *Une sécurité physique limitée :*

Les réseaux de mobiles comme les autres réseaux sans fil sont plus touché par le paramètre de sécurité que les réseaux filaires classique. Cela est justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

- *Changement d'échelle :*

L'augmentation du nombre de nœuds ou la taille du réseau peut entrainer des diminutions de performance. Il faut que le réseau dispose des mécanismes pour confronter cette situation.

7. Exemples de réseau de mobiles

7.1. GSM (Global System for mobile telecommunications)

Les premières bases de la norme GSM ont été posées dès la fin des années 1970 sous l'égide de l'Union internationale des télécommunications (UIT).

En 1982 fut mis en place un groupe de travail réunissant 13 États au sein de la Conférence européenne des postes et télécommunications (CEPT). Ce groupe prit le nom de Groupe spécial

mobile dont est issu l'acronyme GSM, qui verra ultérieurement son développement modifié pour signifier *Global System for Mobile télécommunications,* Il est qualifié de 2G.

Les réseaux de type GSM sont interconnectables aux RTCP (Réseaux Terrestres Commutés Publics) et utilisent le format numérique pour la transmission des informations, qu'elles soient de type voix, données ou signalisation(les informations nécessaires aussi bien au dialogue entre les éléments du réseau qu'à l'établissement et au maintien des communications entre les stations de base et les terminaux mobiles (passage d'une antenne à l'autre en cours de déplacement, par exemple)) **[12]**.

Le GSM se caractérise non seulement par sa technologie radio, mais aussi par la répartition des fréquences, la largeur des canaux, l'architecture du réseau, les interfaces, les protocoles et autres spécifications techniques très précisément décrites et normalisées dès le départ.

La répartition des ressources disponibles entre les utilisateurs connectés à une même station de base, munissent par des terminaux mobiles (téléphones de voiture, téléphones portable, terminaux de poches), est basée sur une technologie d'accès multiple à répartition fréquentielle (FDMA) et temporelle (TDMA) éventuellement couplée à un changement de fréquence en cours de communication *(fréquencies hopping).* La norme GSM permet un débit maximal de 9,6 kbit/s.

7.2. GPRS (*General Packet Radio Service)*

Le GPRS (*General Packet Radio Service*) est la première évolution du GSM, adaptée au transfert de données. Le GPRS ne constitue pas à lui tout seul un réseau mobile à part entière, mais une couche supplémentaire rajoutée à un réseau GSM existant. Il est qualifié de 2,5G. Il a été lancé au début de l'année 2002 en France et a connu des résultats commerciaux mitigés, dus à un débit souvent inférieur à 50 Kbit/s qui n'offre pas une qualité de service suffisante alors que théoriquement, le débit devait pouvoir atteindre 115 Kbit/s.

Le GPRS utilise les bandes de fréquences attribuées au GSM, il repose sur la transmission en mode paquet.

Le développement des usages grand public reposant surtout sur l'image ou la vidéo, qui nécessitent un accès haut débit, le GPRS ne devrait plus porter, à moyen terme, les offres de services destinées à ce segment de marché.

Les réseaux de la génération 2,5 se caractérisent souvent, comme c'est le cas dans le GPRS, par un double réseau coeur : un réseau cœur pour le transport du téléphone et un réseau cœur pour le transport des données sous forme de paquets. À ce double réseau cœur, s'ajoutent des terminaux d'une nouvelle nature, capables de gérer à la fois les voies téléphoniques, comme dans le GSM, et les voies de données, d'un caractère beaucoup plus sporadique.

Le GPRS offre des fonctionnalités intéressantes, les plus importantes sont que plusieurs canaux peuvent être alloués à un utilisateur et ces mêmes utilisateurs peuvent partager un même canal.
En plus du transfert de données et de sécurité, le GPRS permet d'élargir l'offre de services Internet, il permet un meilleur accès aux e-mails comportant des fichiers joints. Le mobile, dans ce cas, est considéré comme un modem, et doit être associé à un ordinateur portable ou un assistant personnel.
Trois types de terminaux ont été définis pour répondre aux besoins du GPRS : le modèle de base (classe B) est prévu pour la voix et les données en mode non simultané. Le modèle professionnel ou industriel (classe C) est data exclusivement dont le quel le terminal est utilisé comme un modem. Enfin le haut de gamme (classe A) est compatible voix/data simultanément **[12]**.

7.3. *UMTS (Universal Mobile Télécommunications System)*

Abréviation d'Universal *Mobile Télécommunications System,* L'UMTS est la version européenne définie par l'ETSI (Institut Européen de Normalisation des Télécommunications) de la troisième génération des services mobiles (3G).
Les puristes préfèrent utiliser le terme W-CDMA *(Wideband Code Division Multiple Access)* qui reprend le nom de la technologie déployée en Europe et par certains opérateurs asiatiques.
Celui-ci a pour but de normaliser les systèmes de télécommunications mobiles de troisième génération qui assureront l'accès radioélectrique à l'infrastructure mondiale des télécoms, dans un contexte mondial d'itinérance, Il intervient aussi bien les systèmes satellitaires.
Son principe consiste à exploiter une bande de fréquences plus large, il exploite la nouvelle technologie de communication W-CDMA et de nouvelles bandes de fréquences situées entre 1900 et 2200 MHz. À la différence du GSM qui utilise le TDMA, le W-CDMA permet d'envoyer simultanément toutes les données, par paquets et dans le désordre (sur n'importe quelle fréquence), reste au téléphone à réceptionner les paquets de données et les rassembler.
Cette technologie permet de faire transiter davantage de données simultanément et offre un débit bien supérieur à ceux permis par les GSM et GPRS. En théorie, il peut atteindre 2 Mbit/s **[12]**.
L'UMTS présente des avantages qui s'appliquent autant aux communications vocales qu'aux transferts de données. Comme la technologie exploite une bande de fréquences plus large, elle permet de passer trois fois plus d'appels. L'UMTS peut remédier à la saturation des réseaux existants et proposer des services de meilleure qualité. Le débit cinq à dix fois plus rapide à permis le développement de nouvelles applications, notamment dans le domaine du multimédia (visiophonie, diffusion de contenu vidéo et audio, MMS vidéo ou audio, etc.). Le haut débit mobile facilite aussi l'accès aux données, web et e-mails, en situation de mobilité**[5]**.

8. Application des réseaux de mobiles

Les réseaux de mobiles ne se limitent plus à offrir des services vocaux, ils sont devenus aussi à l'aide de l'internet des acteurs de nouvelles formes de services tel que :

8.1.M-Learning

L'apprentissage mobile ou m-Learning peut être définit comme l'utilisation des supports mobiles à des buts pédagogiques. Les outils mobiles voyagent souvent avec les personnes. Leur exploitation pour des buts pédagogique conduit à l'émergence d'apprentissage mobile.

L'apprentissage mobile ou m-Learning est effectivement une sous-catégorie du plus grand concept e-Learning, il est l'intersection du calcul mobile (mobile computing) et de e-Learning, C'est une prolongation d'e-Learning.

Il a le potentiel d'augmenter plus loin où, comment, et quand on apprend et accomplit dans tous les aspects de la vie.

Un avantage principal de la m-Learning est son potentiel pour augmenter la productivité en rendant l'étude disponible n'importe où et n'importe quand, permettant à des étudiants de participer aux activités éducatives sans restriction de temps et d'endroit. Les technologies mobiles ont la puissance de rendre l'apprentissage plus disponible et accessible que les environnements e-Learning existants.

Le M-Learning permet aux étudiants et aux enseignants d'accéder réellement à plusieurs supports éducatifs : recherche de l'information, la livraison de contenu, questions et réponse ad hoc, notes, des commentaires entre apprendre et la communauté, ou les tâches se sont rapportés à apprendre l'administration.

Les dispositifs mobiles les plus utilisés dans le m-Learning sont : PDAs, smart phones, portables, *Tablet PC et les n*otebook **[14].**

8.2.M-Commerce et M-business (Courses en ligne)

Le commerce mobile ou m-commerce est l'équivalent du commerce électronique appliqué aux réseaux de mobile au lieu de réseaux internet, il implique que l'ensemble du processus d'achat soit effectué depuis les mobiles.

Le m-Commerce est né au Japon à la fin des années 90, il est démarré tout juste en Europe et aux USA. Au Japon, il représente déjà 20% du e-Commerce et 50% des utilisateurs de mobile achètent régulièrement depuis leur appareil. En Europe et aux USA le m-Commerce se développe depuis 2007 avec l'explosion du marché des smart phones puissants, iPhone d'abord, puis Android plus récemment. Au niveau mondial, la progression du m-Commerce entre 2009 et 2010 est de 50% et que ce rythme de progression se maintiendra au moins jusqu'en 2014.

Le m-Commerce n'a pas vocation à remplacer les canaux traditionnels, y compris l'Internet sur ordinateur. Il convient particulièrement à certains types d'achat basés sur la simplicité des produits et l'urgence de la demande. Initialement limité à des achats de biens dématérialisés (fonds d'écran, sonneries, musique MP3), le m-Commerce couvre aujourd'hui une gamme bien plus large : jeux en ligne, système de coupons et offres d'achats, cartes de fidélité, réservations de tickets en ligne, industrie du tourisme (transports, hôtels, locations), m-Banking, m-Shopping (VPC, grande distribution), sites d'enchères, accès à l'information et aux services payants… les possibilités sont quasiment illimitées. Les nouvelles offres utilisent les fonctionnalités avancées des nouveaux appareils comme la géo-localisation ou la vidéo, pour offrir aux consommateurs des produits et services ciblés, qui correspondent bien au type d'achat impulsif **[15]**.

Par contre le m-commerce qui est basé, uniquement sur des transactions financières, le m-business couvre d'autre forme de transactions en plus les financières, c'est pour ça le m-business est considéré un terme générale de m-commerce **[16].**

8.3.M-Banque et M-Payment (Paiement sur mobile)

Le M-Banking est définis comme étant la réalisation d'opérations de gestion d'un compte bancaire via les réseaux de mobile avec des outils mobiles. Il s'inscrit dans la continuité du développement des canaux de distribution électroniques à distance et la banque multi-canal**[17]**.

Le procédé de paiement dans un environnement mobile est très semblable à celui de carte de paiement. La seule différence est que le m-paiement implique des fournisseurs de services sans fil pour transporter les détails de paiement comme Bluetooth, l'infrarouge et WAP/HTML.

Pour qu'un client peut utiliser le m-paiement il faut premièrement s'enregistrer par l'ouverture d'un compte avec le fournisseur de services de paiement (M-Banque par exemple) par une méthode particulière de paiement.

Quand le client indique le désir d'acheter un contenu utilisant un bouton de dispositif mobile ou en envoyant un SMS. Le fournisseur de contenu envoi une demande au fournisseur de services de paiement pour qu'il vérifie l'autorisation et l'authentification du client.

Le règlement de paiement peut être en temps réel, prépaiement ou post paiement **[18]**.

8.4.M-Media (publicité sur mobile)

Le service M-Media, améliore la visibilité des entreprises, des services, des points de ventes. Avec M-media, les entreprises peuvent contacter leurs clients qu'ils soient sur, à proximité, et même hors des point de vente.

Par l'envoi des SMS, des MMS, des musiques, des vidéos ou même la création des sites Wap, les clients ont toujours les nouvelles des entreprises.

La publicité sur mobile devrait ainsi passer de 320 M$ en 2008 à 593 M$ en 2010 et davantage encore les années suivantes. Elle ne se développe pas plus vite pour le moment, seulement 1% des investissements publicitaires y est consacré, à cause d'un manque de standards technologiques, d'un coût pour mille élevé, d'un cadre règlementaire contraignant et du peu d'outils de mesure d'efficacité **[19]**.

8.5.M-Tickets (Tickets et accès)

M-Tickets permet aux clients de réserver leurs billets de spectacle, concert, match de football… sur leur téléphone portable. En se présentant le jour de la manifestation, ils passent leur mobile devant une borne pour pouvoir entrer.

M-Access autorise aussi le contrôle d'accès au sens large (droit d'entrée dans tel immeuble d'un médecin, d'une femme de ménage…) avec un droit d'accès qui peut être permanent ou restreint, selon le besoin et le public **[19]**.

Fig.1. 7. : Application des réseaux de mobiles

9. Système d'exploitation pour les réseaux de mobiles

Les systèmes d'exploitation pour mobiles sont différents de ceux développés pour les ordinateurs personnels. Les raisons de ces différences sont les contraintes d'énergie et d'espace mémoire associés à ces matériels spécifiques, et des contraintes comme le support d'un usage interactif et sporadique. Par exemple, le système d'exploitation d'un PDA peut nécessiter une fonction matérielle de réveil pour implanter des fonctions comme des rappels (pour se souvenir d'un rendez-vous par exemple), qui peut se produire quand l'appareil est en veille pour économiser son énergie.

D'autres différences sont induites par la partie logicielle du système plutôt que par le noyau du système d'exploitation. Les différences du système logiciel tirent leur origine des contraintes très

différentes de l'interface utilisateur de ces appareils, comme l'absence d'un clavier complet et l'affichage relativement de petite taille.

Il y a beaucoup de systèmes d'exploitation pour mobiles. Les systèmes d'exploitation les plus utilisés dans les appareils mobiles sont : Symbian OS, PalmOS, Linux et Windows CE**[9]**.

9.1. Symbian OS

Symbian OS est le système d'exploitation le plus populaire, utilisé par de nombreux fabricants de téléphones, comme Nokia, Panasonic, Samsung, Siemens ou SonyEricsson. SymbianOS est issu de la famille des systèmes d'exploitation EPOC qui fut développée par Psion dans les années 90 pour leurs PDA. Symbian OS existe depuis environ 2001 et tourne exclusivement sur les processeurs ARM.

Symbian OS est basé sur un design de micro kernel (le noyau ne comporte que le minimum nécessaire) et implante la plupart des fonctions que l'on trouve actuellement sur un système d'exploitation comme : un système préemptif multi-tâches et multi-threads, un gestionnaire du système de fichier et une protection de la mémoire. Le système d'exploitation ne requiert donc qu'une petite puissance CPU et peu d'espace de stockage et est fondamentalement développé pour économiser l'énergie. Symbian OS est mono-utilisateur et distingue seulement le mode utilisateur du mode kernel **[9]**.

9.2. PalmOS

Palm OS est développé par la société Palm comme le système d'exploitation pour les PDA de la série des PalmPilot. PalmOS existe depuis 1996 et fut à l'origine uniquement utilisé par Palm lui-même. Plus tard, Palm commença à accorder des licences d'usage de son OS à d'autres fabricants d'appareils **[9].**

Palm OS est facile d'utiliser et simple d'apprendre. Il optimise les étapes pour naviguer entre les écrans et choisir les applications. Par exemple, pour lancer un programme, appuyez sur son icône. Quand on passe à une autre application, cette application se termine. Palm OS offre un système de messagerie électronique, Il a aussi de plus 20.000 applications tierces pour élargir la fonctionnalité des appareils comme regarder la vidéo, la TV, ou travailler avec Office **[20]**. La première version de Palm fut développée pour tourner sur un matériel très limité, et donc ne fournissait pas de fonctions comme le support multitâches, hormis certaines tâches spécifiques du système d'exploitation **[9]**, mais Palm OS est devenus multitâche à partir de la version 6.0. De plus, la nouvelle version offre plusieurs améliorations comme la communication, la multimédia, la synchronisation, etc, tandis qu'il retient encoure les bons caractéristiques des versions précédentes **[20].**

Une autre différence avec les systèmes d'exploitation traditionnels est le manque de protection mémoire. Avec la version 5, Palm passa des processeurs Motorola 68k aux processeurs ARM pour ses appareils, mais garda une émulation du 68k pour assurer une compatibilité ascendante. De plus, avec PalmOS 5, Palm introduisit des mécanismes de sécurité, et fournit à présent le premier système d'exploitation pour appareil mobile avec un chiffrement du système de fichier en natif **[9]**.

Palm OS est un bon choix pour les consommateurs mais non pas pour les sociétés.

9.3. Linux

C'est un système d'exploitation complet, incluant toutes les fonctionnalités nécessaires, comme le support multitâches, la protection mémoire et le support multiutilisateurs.

Linux pour les appareils mobiles a divers désavantages, le principal est le manque de mécanisme avancé pour la sauvegarde de l'énergie, et le besoin assez conséquent de mémoire, que ce soit pour l'exécution ou le stockage. Linux est utilisé de façon très diverse comme système d'exploitation, et seuls le noyau et les bibliothèques restent inchangés d'un appareil à un autre. Linux ne fournit pas non plus d'interface graphique standard. A la place, chaque fabricant choisit un des nombreux systèmes disponibles ou développe sa propre plateforme.

MontaVista, Green Hills Software, Wind River Systems ou LynuxWorks sont des exemples de sociétés spécialisées dans la conception de systèmes d'exploitation basé sur le noyau de Linux et destinés à être utilisés dans des systèmes embarqués ou des appareils mobiles.

MontaVista ajoute un support avancé de la gestion d'énergie, un boot rapide (permettant de démarrer le mobile en moins de 10 secondes), le support temps réel avec un ordonnanceur temps réel, et une gestion plus fine de la mémoire.

Il faut néanmoins se rendre compte que les implantations de Linux dans les appareils mobiles peuvent parfois varier énormément d'un appareil à un autre **[9].**

9.4. Windows CE

Windows CE est le système d'exploitation pour appareils mobiles de Microsoft, c'est un système d'exploitation modulaire qui sert de fondation pour de nombreux types d'appareils.

Windows CE existe en différentes versions et peut être personnalisé par les fabricants pour s'adapter à leurs besoins. Souvent, on confond Windows CE, Windows Mobile et Pocket PC sont employés l'un pour l'autre.

En pratique ce n'est pas tout à fait exact, Chacune de ces plateformes utilise différents composants de Windows CE, et rajoute des fonctionnalités supplémentaires dépendant de leurs appareils respectifs.

Windows CE est un système multitâche, mais comme il fut optimisé pour un environnement mobile, certaines fonctionnalités sont absentes, comme le support multiutilisateurs. Windows CE essaie de réutiliser un certain nombre de concepts de la version bureautique de Windows dans le but d'inciter les utilisateurs et les développeurs à utiliser et développer des applications dans leur environnement familier. Similairement à Linux, Windows

CE supporte une grande variété d'architectures matérielles (il supporte les architecture Intel x86, MIPS, ARM, PPC et Hitachi SuperH) et est donc utilisé par de nombreux fabricants.

L'architecture de Windows CE est relativement proche de celle de windows 95. Elle est composée de différentes couches d'abstraction matérielle permettant de rendre indépendant le matériel du logiciel. Cette couche d'abstraction matérielle est très importante pour les constructeurs de matériels, car elle permet de réduire considérablement les coûts de développement et surtout d'évolution du matériel : lorsque le matériel évolue, il suffit d'écrire un nouveau pilote pour ce matériel sans changer tout ce qui existe au dessus et au dessous**[9].**

10. La sécurité des réseaux de mobiles

Dans un réseau de mobiles, tous les utilisateurs partagent un même support de transmission. Pour éviter que les conversations soient écoutées ou que les données informatiques et multimédias soient espionnées, il est nécessaire d'incorporer un mécanisme sécurisant l'envoi de l'information. Un ou plusieurs algorithmes de cryptage sont donc introduits dans les systèmes de mobiles, à seule fin de protéger le contenu des flux voyageant sur l'interface radio.

Dans les réseaux de mobiles, les informations qui gèrent la localisation d'un utilisateur sont également exposées à ce problème. Le système doit donc s'accommoder d'une protection voilant la libre circulation de l'individu. Concernant, l'***authentification*** de l'utilisateur, le système de communication attribue des codes individuels aux abonnés, qui doivent les tenir secrets de façon à éviter toute utilisation abusive. Les systèmes de première génération étaient très vulnérables à ce genre d'attaque.

La sécurité des réseaux de mobiles, comme les autres réseaux, utilisant l'interface radio nécessite l'authentification de l'utilisateur, ainsi que le cryptage des données et la protection des données de contrôle **[5]**.

Malgré toutes les solutions proposées, il n'existe pas d'une solution efficace pour sécuriser totalement un réseau de mobiles qui reste encours vulnérable par plusieurs attaques.

Conclusion

La prolifération d'appareils mobiles conduit à l'augmentation et la popularité croissante des réseaux de mobiles. Ces derniers sont utilisés pour offrir certains services importants dans nos jours comme: Services Web, jeux, messageries, commerce mobile, ...

Les réseaux de mobiles possèdent des caractéristiques particulières qui les différencient des autres types de réseaux sans fil. Ces spécificités telles que la limitation de l'énergie, faible puissance de traitement, mémoire limitée … Alors ; toutes applications orientées vers ces réseaux doit respecter ces contraintes et limitations.

L'utilisation des ondes radios comme support de communication rend les réseaux de mobiles comme les autres réseaux sans fil souffrent de problème de sécurité qui sera le sujet de notre prochain chapitre.

Chapitre 2 : La sécurité dans les réseaux de mobiles

Introduction

Le développement rapide des réseaux de mobiles incite des personnes à compter fortement dessus services mobiles dans leur vie quotidienne pour des tâches importantes et sensibles.

Au départ, les réseaux de mobiles sont utilisés pour les communications téléphoniques, maintenant nous somme capable d'accéder à Internet, conduire les transactions monétaires, envoyer des messages textuels… etc par l'utilisation des petits terminaux mobiles, et des nouveaux services continuent à être ajoutés.

Tout en fournissant une grande convenance, ces nouveaux services éclatants ont apporté des problèmes de sécurité sérieux. Le manque de sécurité a devenu l'un des obstacles principaux empêchant des communications sans fil de fournir des services telles que des M-bancing ou des M-Shopping. Alors, il est important de fournir aux utilisateurs des systèmes de communication sécurisés. Cependant, l'environnement sans fil a certaines limitations comparativement à l'environnement câblé tel que l'accès ouvert, la limite de la largeur de la bande et la complexité des systèmes. Ces limitations et d'autres liés aux caractéristiques spéciales des unités mobiles rendent difficile bien que possible la mis en place des dispositifs de sécurité tels que l'authentification, l'intégrité et la confidentialité.

Bien qu'il y ait beaucoup de mécanismes de sécurité dans les réseaux de mobiles **[21],** le nombre d'incidents de sécurité continue à augmenter.

Comment concevoir un réseau de mobile fortement sécurisé est toujours une issue très provocante en raison de l'environnement ouvert de transmission par radio et de la vulnérabilité physique du dispositifs mobile.

1. Sécurité informatique

En premier lieu, il est important d'éclaircir la notion de la sécurité.

On trouve dans la littérature plusieurs définitions de la sécurité. Le dictionnaire de l'académie française **[22]** définit la sécurité comme suit « Sécurité. n.f. Confiance, tranquillité d'esprit qui résulte de l'opinion, bien ou mal fondée, qu'on n'a pas à craindre de danger. ».

Plusieurs aspects discutés ci-dessous sont visibles dans cette définition où la sécurité est vue comme une situation caractérisée par l'absence de tout risque pour les personnes concernées. Bien que cette définition soit d'un niveau suffisamment haut et notamment elle n'est pas applicable sur tous les cas.

D'autre définit la ***sécurité*** comme est un ensemble de conditions et de façon d'agir qui assure d'accomplir des taches sans interférences. **[23]**

On note une aspect important inhérent à toute définition de la sécurité : la notion de la ***confiance***, il est évident que la confiance absolue dans tout acteur de l'environnement étudié enlève le besoin pour la sécurité de la même façon que la méfiance totale interdit toute exposition d'un actif à son environnement et met en question la notion de la propriété privée. En effet, si tout acte possible sur l'actif est perçu comme un risque, le système converge inévitablement vers la clôture totale. Ceci souligne l'interdépendance entre la confiance et la sécurité. Pourtant dans le cas général, on ne connaît pas de transformation directe entre la confiance et la sécurité. Malgré leur influence mutuelle, il faut faire une distinction nette entre la sécurité et la confiance. **[22]**

La ***sécurité informatique***, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu**. [3]**
C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs des systèmes en regard de la sécurité. **[25]**

2. La sécurité des réseaux

2.1.Définition

La sécurité d'un réseau est une prolongation de la sécurité d'ordinateur. Cela signifie que toutes les mécanismes dans la sécurité d'ordinateur sont toujours nécessaires, mais en plus d'autres choses sont également exigées, afin de protéger la communication entre les ordinateurs ou d'autres dispositifs. Cette phrase montre également un nouvel aspect comparé à la sécurité d'ordinateur, les dispositifs ne sont pas tous des ordinateurs, on peut trouver d'autres qu'ils ne sont pas capable d'implémenter les services de sécurité existants dans les systèmes d'exploitations des ordinateurs.
La sécurité de réseau peut être définie comme faisant sure que les nœuds respectent la sécurité d'ordinateur approprié et sécuriser ensuit la communication entre eux. **[26]**
On peut classifier la sécurité du réseau en trois niveaux :

- ✓ *Niveau physique :* pour protéger les matériels et logiciels contre les agressions.
- ✓ *Niveau données* : pour fournir la confidentialité, l'intégrité, la disponibilité, et la non-répudiation dans le but de protéger les données contre tout accès non autorisé.
- ✓ *Niveau transfert de données* : pour protéger les données contre toute sorte d'attaque ou contre tous problèmes de connexion. **[23]**

2.2.Risques sur la sécurité des réseaux

2.2.1. *Vulnérabilité*

Il s'agit d'une faiblesse de sécurité qui peut être de nature logique (faiblesse d'implémentation), physique (faiblesse de configuration), etc. Une vulnérabilité peut découler, par exemple, d'une erreur d'implémentation dans le développement d'une application, erreur susceptible d'être exploitée pour nuire à l'application (pénétration, refus de service, etc.). Elle peut également provenir d'une mauvaise configuration. Elle peut enfin avoir pour origine une insuffisance de moyens de protection des biens critiques, comme l'utilisation de flux non chiffrés, l'absence de protection par filtrage de paquets, etc. **[27]**

Il est cependant important de dresser une typologie des faiblesses de sécurité afin de mieux appréhender les attaques, qui ont pour point commun d'exploiter les faiblesses de sécurité.

2.2.2. Menace

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Elle désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces dernières sont difficiles à réaliser. Cette menace peut-être accidentelle, intentionnelle (attaque), active ou passive. **[27]**

Les différentes catégories de menaces qui pèsent sur un réseau peuvent être classées comme illustré à la figure suivante :

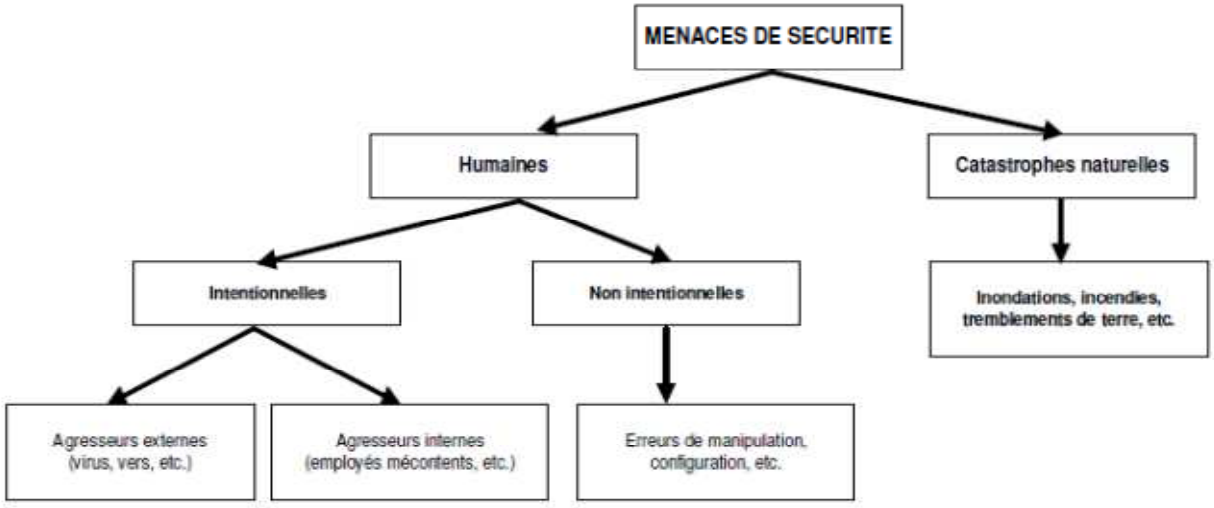

Fig.2. 1 : classification des menaces **[27]**.

Les menaces non intentionnelles ou imprévisibles, comme les catastrophes naturelles, ne mettent pas en œuvre d'outils ou de techniques particulières et n'ont évidemment pas d'objectif

déterminé. À l'inverse, les menaces intentionnelles mettent généralement en œuvre des outils et des techniques d'attaques très variés. **[28]**

2.2.3. *Attaque*

Une attaque est la mise en œuvre d'un plan pour exécuter une menace.

C'est l'attaquant qui crée des menaces en exploitant les vulnérabilités dans ou autour du bien. Le propriétaire veut minimiser ses risques et impose des contre-mesures qu'il considère comme nécessaires pour protéger le bien. **[22]**

L'attaquant peut êtres un nœud interne ou externe du réseau.

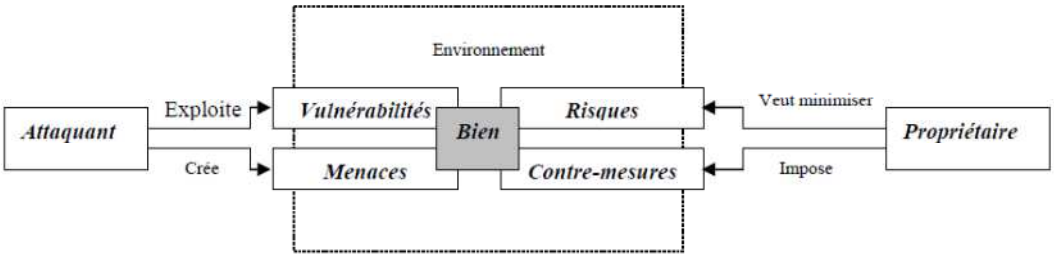

Fig.2. 2 : relation entre attaque, vulnérabilité et menaces **[22]**.

2.2.4. Virus

Avec l'avènement d'Internet et des moyens de communication modernes, une nouvelle forme d'insécurité est apparue, qui s'appuie sur l'utilisation de code informatique pour perturber ou pénétrer les systèmes informatiques, c'est le virus. **[28]**

Un **virus :** est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé. On distingue différents types de virus :

- ***Les vers*** : sont des virus capables de se propager à travers un réseau.
- ***Les Troyes :*** (chevaux de Troie) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle)
- ***Les bombes logiques :*** sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...) **[3]**

2.2.5. *Pirate*

Le pirate est généralement décrit un individu qui consiste à espionner les réseaux informatiques de notre planète, à l'affût de quelques failles qui lui ouvriraient l'accès aux données secrètes ou aux serveurs protégés. Pour être pirate aujourd'hui, à cause de la démocratisation d'Internet, il n'est plus nécessaire d'être spécialisé dans les problèmes

informatiques, ni de disposer de connaissances approfondies, encore moins d'avoir une longue expérience en informatique. Il suffit de connaître les bonnes adresses web ou de savoir manipuler habilement un moteur de recherche pour repérer les informations et les programmes voulus en quelques secondes**. [22]**

2.2.6. *Hacker*

Le terme "hack" a été utilisé pour désigner un procédé de programmation élégant ou très astucieux, obligeant la station à accomplir des taches pour lesquelles il n'était nullement prévu. Celui qui en a les aptitudes est appelé "hacker", c'est un maître en informatique. Aujourd'hui la notion de hacker est étendue au domaine de la violation des données, dans ce contexte on parle de crackers. Il détruit les données d'autrui ou provoque volontairement des désastres. Un hacker est une personne plutôt constructive ayant hérité de l'âme de ses inventeurs, s'il découvre une faille, il met en garde le concerné sans causer de dégâts, c'est le cas de celui qui a trouvé des failles dans un système informatique d'une banque mais qui n'a retiré qu'un centime symbolique comme preuve de faits. **[22]**

3. Les attaques réseau et leur classification

Les attaques touchent généralement les trois composantes suivantes d'un réseau, la couche réseau, en charge de connecter le réseau, le système d'exploitation, en charge d'offrir un noyau de fonctions au système, et la couche application, en charge d'offrir des services spécifiques. Toutes ces composantes d'un réseau constituent autant de moyens de pénétration pour des attaques de toute nature.

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. **[28]** Ils peuvent se produire de différentes manières. La classification de ces attaques dépend de plusieurs paramètres:

3.1. *Les attaques internes*

Se posent dans le cas d'un nœud compromis. Dans ce cas, il est relativement difficile de détecter une telle attaque puisque l'intrus a l'accès simple au réseau en utilisant le nœud compromis qu'il possède. Ce type d'attaque pose le problème de confiance entre les nœuds d'un réseau, une station ne peut pas par suite avoir toujours confiance en ses voisines. Par contre, dans le cas :

3.2. *Des attaques externes*

L'intrus ne possède pas un terminal du réseau mais peut se connecter au réseau de l'extérieur c'est-à-dire à partir d'un autre réseau comme l'Internet par exemple. Dans ce type d'attaque, il

est difficile de déterminer la source d'une attaque puisque l'attaquant peut rejoindre le réseau à partir de différents points d'accès. **[29]**

3.3. *Les attaques actives*

Permettent de récupérer des informations à partir les nœuds ou les paquets transmis entre les différents terminaux. Ces attaques peuvent être très graves si les informations récupérées sont sensibles.

3.4. *Les attaques passives*

Ne permettent pas de récupérer des données mais elles peuvent par exemple empêcher le réseau de bien fonctionner et ceci en exploitant les failles des programmes ou des protocoles utilisés. Ces attaques ont un aspect désastreux et sont aussi très dangereuses.

3.5. *Les attaques sur protocoles*

Sont des attaques qui visent les processus qui nécessitent un travail collectif entre les différents nœuds.

Dans ce cas, l'intérêt de l'attaquant consiste essentiellement à nuire au bon déroulement des processus de réseau. Exemples des ses protocoles : protocole de routage et protocole d'accès au médium.

3.6. *Les attaques individuelles*

Sont simples et elles sont issues d'une seule source et par un chemin simple sans utiliser des stations intermédiaires. Par contre :

3.7. *Les attaques distribuées*

Sont des attaques évoluées invoquant plusieurs stations ou provenant de plusieurs sources. Les attaques distribuées sont plus dangereuses et difficiles à détecter puisqu'elles utilisent plusieurs stations intermédiaires, ce qui a pour effet la difficulté de déterminer la source d'une telle attaque. Les attaques par déni de service ont souvent l'aspect d'attaques distribuées. Ces attaques peuvent viser le fonctionnement de l'un des protocoles du réseau comme ils peuvent viser une partie ou un nœud de ce réseau. **[29]**

4. Conditions de la sécurité

Classiquement le processus de sécurité est décomposé en trois aspects se référant à l'objet de sécurisation en spécifiant notamment ce qui doit être protégé. Cette vue de la sécurité est connue sous la trinité ***CIA*** (Confidentialité, intégrité et disponibilité). Cette décomposition est aujourd'hui normalement insuffisante, car elle ne couvre pas bien certaines nouvelles menaces comme les virus informatiques, les messages non sollicités, ou l'utilisation abusive. **[22]**

4.1. La confidentialité

La confidentialité des données est la question la plus importante dans la sécurité de réseau. Elle consistant à assurer que seules les personnes autorisées aient accès aux ressources, alors empêcher les utilisateurs non autorisés d'accéder à une information. C'est une protection des communications ou des données stockées contre l'interception par des personnes non autorisées.
La confidentialité est particulièrement nécessaire pour la transmission des données sensibles et constitue une des exigences pour aborder les problèmes de protection de la vie privée des utilisateurs des réseaux de communication. **[30]**
L'approche standard pour sécuriser le transfert de données et assurer la confidentialité est le ***cryptage*** de données avec une clé connue par l'émetteur et le récepteur. Même si elles sont interceptées, les données correctement chiffrées sont incompréhensibles pour tout le monde, sauf le destinataire autorisé.

4.2. L'intégrité

Les données transférées peuvent être exposés à une transaction (par un nœud malveillant) qui peut conduit à une altération des informations transportées. La perte ou le dommage de données peut même se produire sans l'entremise d'un nœud malveillant dû aux obstacles durs opposés à l'environnement comme celui qui confronte un environnement sans fil.
L'intégrité consiste à assure que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé. C'est une confirmation que les données qui ont été envoyées et reçues sont complètes et n'ont pas été modifiées ni intentionnellement ou accidentellement. Ceci est particulièrement important quand l'exactitude des données est nécessaires (données médicales, design industriel, etc.). **[30]**
Plusieurs mécanismes sont utilisés pour vérifier l'intégrité des informations comme la signature numérique, l'algorithme CRC 32, le checksum et d'autres. **[27]**

4.3. La disponibilité

La disponibilité permettant de maintenir le bon fonctionnement du système informatique. C'est un ensemble des mécanismes garantissant que les ressources (les données et les services opérationnels) sont accessibles, même en cas d'événements perturbants tels que des pannes de courant, des catastrophes naturelles, des accidents ou des attaques. Ces ressources concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc. **[27]**
Cette caractéristique est particulièrement importante lorsqu'une une défaillance du réseau de communication peut provoquer des pannes dans d'autres réseaux critiques tels que les transports aériens. **[24] [30]**

La disponibilité est la condition la plus dure d'accomplir, parce que à ce moment, il n'y a aucune méthode efficace pour empêcher les attaques de type déni de service qui sont considérés comme le premier ennemi pour cette condition.

Une stratégie qui résout partialement ce problème est la redondance, pour faire assurer que plusieurs nœuds pourvoient les mêmes services. D'autre stratégie est la forte protection physique, pour empêcher un attaquant de découper physiquement un nœud et le rend d' dehors le réseau. **[25]**

4.4. Non répudiation

La non répudiation permet d'assurer qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié. Donc il permet de garantir qu'une transaction ne peut être niée**. [3]**

Elle permet d'assurer qu'un émetteur ou un récepteur ne peut pas plus tard nier faussement qu'il a envoyé ou reçu un message. Une certaine preuve de chaque transaction doit être stockée. Ceci est habituellement résolu en employant les signatures numériques ou un tiers de confiance qui délivre des certificats énonçant à qui appartiennent certaine signature. La preuve alors doit être correctement stockée et protégée, comme un mot de passe d'un fichier. En général la non-répudiation n'est pas mise par une application spécifique mais par l'utilisation de la cryptographie. **[25]**

4.5. L'authentification

L'une des mesures les plus importantes de la sécurité, elle consiste à assurer l'identité d'un utilisateur. L'authentification correspond à la vérification de l'identité d'une entité, elle permet donc de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué et y a pas d'usurpation d'identité. **[24][31]**

5. Mécanismes de sécurité

5.1. Classification

On peut classifier toutes les mécanismes utilisés pour sécuriser les réseaux dans deux catégories qui sont les mécanismes proactives et les mécanismes réactives.

5.1.1. Mécanisme proactive

Regroupe l'ensemble des mesures pour protéger l'information, alors elle dépend principalement de protocoles cryptographiques, l'authentification, l'autorisation.

5.1.2. Mécanisme réactive

Consiste à détecter les comportements malveillants, il s'agit principalement de *détection d'intrusion* et d'*antivirus*.

5.2. Mécanismes de bases

5.2.1. La cryptographie

La cryptologie (appelée aussi **chiffrement** ou **cryptographie**) est l'art de rendre des données secrètes. Elle est essentiellement basée sur l'arithmétique: Il s'agit de transformer les lettres qui composent le message à l'aide d'une *clé de chiffrement* en une succession de chiffres qui s'appel cryptogramme.

La méthode inverse, consistant à retrouver le message original, est appelé ***décryptage***. [3]

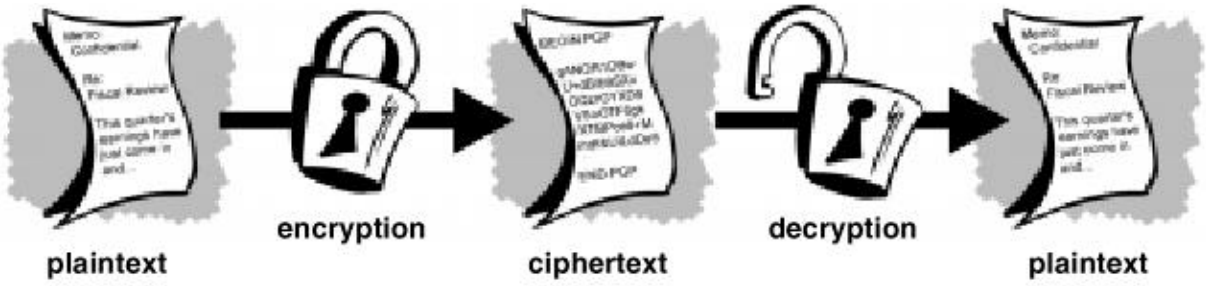

Fig.2. 3 : Le processus de cryptographie **[3]**.

Il existe des techniques de cryptographie :

- **La cryptographie à clé symétrique**

Il fondée sur l'utilisation d'une clé unique, qui permet à la fois de chiffrer et de déchiffrer les données.

Cette clé est appelée la clé symétrique (par fois secrète). Dans le cadre d'échanges sur un réseau, une entité émettrice chiffre les données avec une clé et l'entité destinatrice déchiffre les données avec la même clé. Si les algorithmes symétriques sont performants et permettent d'atteindre des débits importants dans le chiffrement et déchiffrement, ils posent cependant le problème de la mise en place d'une même clé entre émetteur et récepteur. Partager une clé avec chaque entité communicante potentielle, même dans un groupe fermé d'entités est extrêmement contraignant et conduit rapidement à un très grand nombre de clés à gérer. Il est donc préférable d'automatiser la mise en place de ces clés.

Les algorithmes symétriques les plus connus sont dans l'ordre chronologique de définition, le DES (*Data Encryption Standard*), le 3DES (prononcé « Triple DES »), et l'AES *(Advanced Encryption Standard*). **[22] [31]**

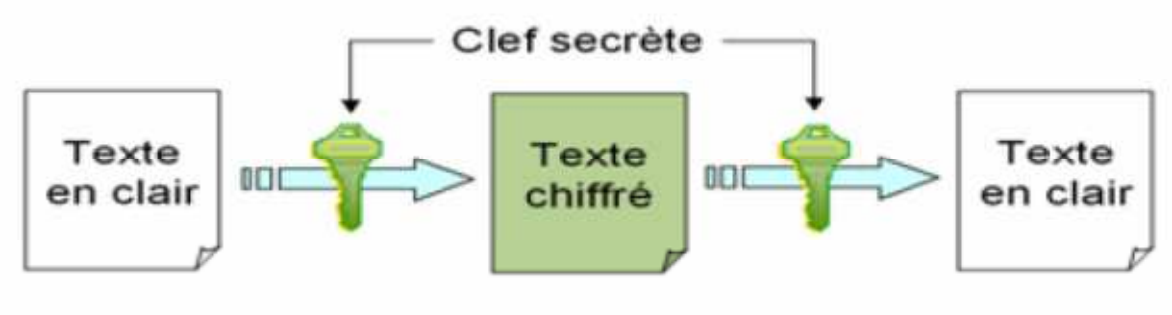

Fig.2. 4 : cryptographie à clé symétrique **[3]**.

- **La cryptographie asymétrique (à clé publique)** :

La technique de cryptographie à clé publique résout le principal problème des clés symétriques, qui réside dans la transmission de la clé. **[31]**

La cryptographie asymétrique ou à clé publique considère deux clés de chiffrement, dites “clés asymétriques”. Ces deux clés sont générées simultanément et sont complémentaires car le chiffrement avec l'une de ces clés nécessite le déchiffrement avec l'autre clé. Chaque clé a un rôle bien défini. La clé privée est une clé qui ne doit être connue que d'une seule entité, c'est elle qui permettra à cette entité de s'authentifier par exemple. La clé publique peut être largement diffusée **[22] .** Bien entendu, la connaissance de la clé publique ne doit pas permettre de déduire la clé privée complémentaire car ces deux clé sont liées mathématiquement de sorte qu’il soit très difficile de trouver la valeur d’une des deux clés par l’intermédiaire de l’autre. **[31]**

Pour garantir la confidentialité d'un message, il est nécessaire de chiffrer le message émis avec la clé publique du destinataire. Cette clé publique est connue de tout le monde et peut donc servir à n'importe quelle entité pour chiffrer un message. Par contre, la clé privée complémentaire n'est connue que du destinataire du message; le destinataire sera donc le seul à pouvoir déchiffrer le message. La propriété de confidentialité est ainsi obtenue. **[22]**

Différents algorithme sont utilisé dans la cryptographie à clé publique notamment RSA et Diffie-Hellman. **[31]**

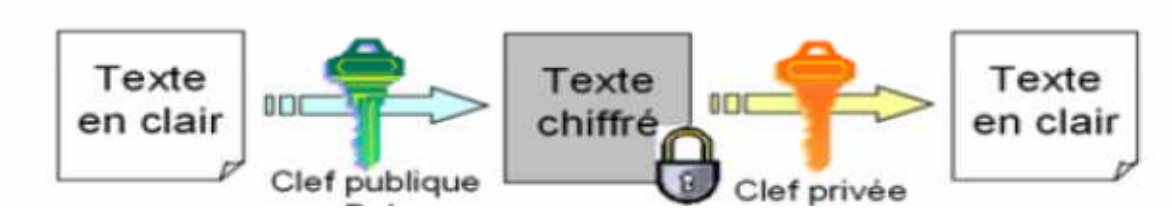

Fig.2. 5 : cryptographie asymétrique **[3]**.

- **La cryptographie à clé mixte** :

La cryptographie à clé mixte fait appel aux deux techniques précédentes, elle combine les avantages des deux tout en évitent les inconvénients. Ces derniers sont bien connu, la cryptographie à clé symétrique ne permettant pas de transmission de la clé sécurisée et les algorithmes à clé publique sont trop lents pour le cryptage de données.

Lors d'un envoi des données, l'émetteur chiffre le message avec une clé secrète grâce à un algorithme à clé symétrique. Dans le même temps, il chiffre cette clé secrète avec la clé publique générée par le destinateur.

La transmission de la clé secrète peut se faire de manière fiable et sécurisée.

Le tout est ensuite transmis au destinateur. Ce dernier déchiffre la clé secrète de l'émetteur grâce à sa clé privée. Le destinataire possède maintenant la clé privée en claire et peut l'utiliser pour déchiffrer le message.

Un autre avantage de cette technique est qu'il n'est plus nécessaire de chiffrer plusieurs fois un message lorsqu'il est destiné à plusieurs destinataires. Le message chiffré étant transmis avec sa clé secrète, il suffit de chiffrer cette clé avec les différentes clés publiques des destinataires. **[31]**

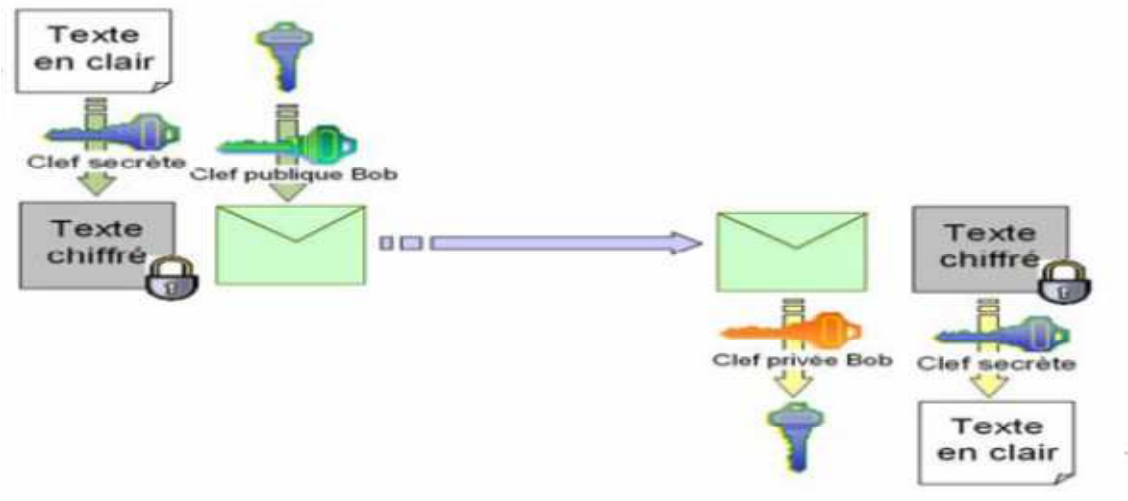

Fig.2. 6 : cryptographie mixte **[3]**.

5.2.2. Les fonctions de hachage

Le hachage consiste à déterminer une information de taille fixe et réduite à partir d'une donnée de taille indifférente**. [32]** C'est en particulier cette propriété que l'on utilise pour valider l'intégrité d'un transfert des données.

Les fonctions de hachage ont pour objectif de fournir un résultat représentatif du contenu d'un message, et ce, sur un nombre d'octets restreints.

Les propriétés attendues de ces fonctions de hachage sont les suivantes :

- ✓ Un résultat sur un nombre limité d'octets.

- ✓ L'impossibilité de retrouver le message original à partir du résultat de la fonction.
- ✓ Deux messages différant de 1 bit seulement produisent deux résultats qui diffèrent d'au moins la moitié des bits.

Plusieurs termes désignent les fonctions de hachage, à savoir : fonctions irréversibles, ou fonctions à sens unique. De même, plusieurs termes désignent le résultat de cette fonction appliquée à un message : hash, haché, empreinte, condensat ou encore condensé. **[22]**

Différentes technique sont utilisées, notamment les suivantes :

MD2, MD4, MD5 : message digest 2,4 et 5 ont été développée par Ron Rivest pour le RSA Security. Ce sont des fonctions de hachage qui produisent toutes des empreintes d'une taille de 128 bits. Le MD2est le plus fiable mais n'est optimisé que pour des machines 8 bits alors que les deux autres le sont pour des machines 32 bits.

MD4 a été abandonné car trop sensible à certaine attaques. MD5 est une évolution de MD4, il est considéré comme fiable, même s'il est vulnérable à certaine attaques, et est utilisé dans de nombreuses applications.

SHA et SHA1 : le SHA (Secure Hash Algorithm) et son évolution ont été développés par la NSA. Ces deux algorithmes produisent des empreintes de 160 bits pour un message peut atteindre un taille de deux millions de téraoctets. La taille de son empreinte le rend très à percer, mais il est plus lent que MD5. **[31]**

5.2.3. Signatures électroniques et MAC

L'objectif d'une signature électronique ou d'un MAC *(Message Authentication Code)* apposé à un message a pour double objectif de permettre au destinataire d'authentifier l'origine de ce message et de lui prouver son intégrité. Leur implémentation fait appel aux fonctions de hachage et aux clés symétriques ou asymétriques. Dans le cas de l'usage de la cryptographie symétrique, on emploie exclusivement le terme de *MAC*, tandis que dans l'usage de la cryptographie asymétrique, on peut parler de MAC, mais on préférera le terme de *signature électronique*. **[22]**

5.2.4. Le certificat numérique

C'est une structure de données dont le format le plus courant est fourni par le standard X.509v3 **[22]** permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'**autorité de certification** (AC). **[13]**

Le certificat numérique comprend: un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification (AC) émettrice du certificat, la signature du certificat à

l'aide de la clé privée de l'autorité de certification. C'est la signature apposée par l'AC qui garantit l'authenticité du certificat. **[22]**

5.2.5. Infrastructure à clés publiques PKI (Public Key Infrastructure)

Une infrastructure à clés publiques est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériels), de procédures humaines (vérifications, validation) et de logiciels (système et application) qui permettent de gérer le cycle de vie des certificats numériques.

Une infrastructure à clés publiques fournis un ensemble de services pour le compte de ses utilisateurs comprenant leur enregistrement, la génération de clés publiques/privées et leur distribution à leurs propriétaires à l'initialisation d'une nouvelle entité dans la PKI, ainsi que la publication, révocation et validation de clés publiques, la génération et le renouvellement de certificats et la publication de la liste de révocation de certificats LRC1. Ce dernier service est vital pour la sécurité d'un réseau de mobile, dans lequel les clés peuvent être compromises à n'importe quel moment. **[22] [13]**

5.2.6. L'antivirus

Les antivirus visent à détecter des fichiers contenant un code malicieux. De tels fichiers utilisent généralement une faille du système pour exécuter le code malicieux et se propager. Les antivirus reposent principalement sur une base de signatures et vérifient que les fichiers ne présentent pas ces signatures.

Des mécanismes d'analyse heuristique sont également présents, visant à détecter des *comportements suspects*. **[33]**

Néanmoins, étant donnée la grande variété de virus, ces heuristiques sont peu efficaces.

5.2.7. Firewall

Un **pare-feu** (appelé aussi *coupe-feu* ou **firewall** en anglais), est un système permettant de protéger un terminal des intrusions provenant du réseau (ou bien protégeant un réseau local des attaques provenant d'Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante.

Un système pare-feu fonctionne sur le principe du filtrage de paquets. Il analyse les en-têtes de chaque paquet (*datagramme*) échangé entre une machine du réseau local et une machine extérieure.

La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue). **[3]**

5.2.8. Les systèmes de détection d'intrusions IDS

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS :

• Les H-IDS (Host Based Intrusion Detection System) qui assurent la sécurité au niveau des hôtes. Le H-IDS réside sur chaque hôte et la gamme de logiciels couvre une grande partie des systèmes d'exploitation. Il se comporte comme un démon ou un service standard sur un serveur. H-IDS peut capturer les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de Troie, tentatives d'accès non autorisés, exécution de codes malicieux, attaques par débordement de buffers…).

• Les N-IDS (Network Based Intrusion Detection System) et les N-IPS (Network Based Intrusion Prevention System) qui assurent la sécurité au niveau du réseau.

- ✓ Les N-IDS sont des IDS passifs puisque ce type de systèmes se contente d'informer l'administrateur qu'une attaque a ou a eu lieu, et c'est à ce dernier de prendre les mesures adéquates pour assurer la sécurité du système.
- ✓ Les N-IPS sont des IDS actifs capables de rendre compte après coup d'une intrusion et de réagir en temps réel car le constat des dégâts ne suffisait, il fallait réagir et pouvoir bloquer les trafics douteux détectés. **[34]**

Les système de détection d'intrusion les plus efficaces sont fondés sur un Système Multi-Agents (SMA). Les agents intelligents, répartis en couches, coopèrent et communiquent pour détecter efficacement des attaques suivant des schémas d'attaques définis dans leur base de connaissances. Chaque agent allie des principales fonctionnalités et l'interaction avec les autres agents pour une détection plus approfondie relative aux scénarios d'attaque complexes. **[21]**

6. Attaques sur les réseaux de mobiles

Les attaques sur les réseaux de mobiles sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes.

Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité.

On peut classer les attaques sur les réseaux de mobiles dans les catégories suivantes:

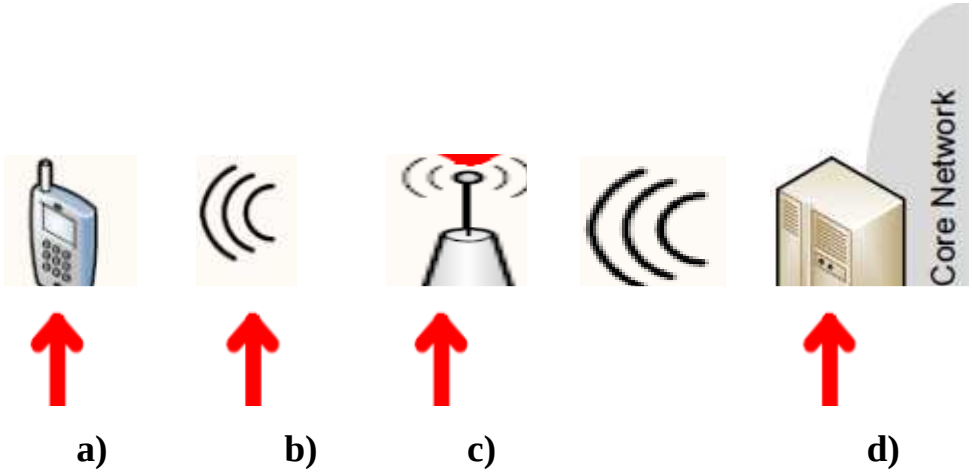

Fig.2. 7 : Les attaques sur les réseaux de mobiles **[9]**

a) **Les attaques sur les unités mobiles**

Les unités mobiles sont exposées à des attaques que les ordinateurs. La sécurité des unités mobiles est plus complexe que la sécurité des ordinateurs à cause de leurs propres caractéristiques. L'unité mobile peut exposer à plusieurs risques comme :

- ***Perte***

Si un appareil est perdu ou volé, sa confidentialité est cassée et son intégrité peut être endommagée. Cependant, les unités mobiles sont plus susceptibles de disparaître car ils sont petits et constamment transportés par leurs utilisateurs. **[9]**

- ***Attaques par déni de service***

Ils ont pour but de rendre un service ou un appareil inutilisable pour son utilisateur, en le rendant indisponible. Les problèmes des attaques DoS contre les appareils mobiles sont imputables principalement à leur forte connectivité et fonctionnalités réduites. Par exemple, une attaque DoS courante consiste à envoyer une grande quantité de trafic à une unité connectée au réseau. Alors qu'un attaquant a besoin de beaucoup de ressources pour attaquer un ordinateur normal ou un serveur, un appareil mobile, par le fait de sa capacité de traitement limitée, peut être plus facilement rendu inutilisable par l'envoi massif de trafic depuis l'attaquant. D'autres attaques DoS plus spécifiques contre des appareils mobiles peuvent utiliser le fait que ces appareils tournent sous batteries. Dans ce cas, le but de l'attaque est de décharger le plus vite possible les batteries de la cible. **[9]**

- ***Virus***

Les virus, vers et chevaux de Troie, sont des menaces pour les appareils mobiles, de la même manière qu'ils le sont pour les ordinateurs. Les vers peuvent avoir un coût s'ils se répandent en utilisant un service pour lequel l'utilisateur est facturé, comme le MMS par exemple. Dans ce cas, un vers s'envoyant lui-même à des centaines d'unités mobiles peut causer un dommage substantiel au propriétaire de l'appareil infecté. D'autre type de virus peut facilement outrepasser les mécanismes de sécurité configurés seulement pour détecter des attaques externes. Les virus peuvent aussi placer un cheval de Troie sur l'appareil, permettant le vol des données ou l'enregistrement des activités d'un utilisateur, en envoyant périodiquement des rapports. **[9]**

- ***L'usurpation de l'identité***

L'usurpation de l'identité (en anglais, *Spoofing* ou *Impersonation*), dans ce type d'attaques, l'attaquant essaie de prendre l'identité d'un autre nœud mobile afin de pouvoir recevoir ses messages ou d'avoir des privilèges qui ne lui sont pas accordés. **[32]**

b) Attaques sur l'interface radio

L'interface radio par leur nature plus vulnérable aux attaques que l'interface filaire.

Le support de transmission étant partagé. Quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise. De plus, si une personne malveillante est assez bien équipée, cette dernière n'a pas besoin d'être située dans la zone de couverture. Il lui suffit d'utiliser une antenne avec ou même sans l'aide d'un amplificateur pour accéder au réseau. **[31]**

Il existe un grand nombre d'attaques différentes qui influencent la connectivité d'une cible.

- **Attaque par interposition** (Man In The Middle Attack)

Un attaquant peut se reposer entre une unité mobile et un point d'accès et intercepter les messages entre eux **[35]**.

C'est une attaque dangereuse qui touche la confidentialité et l'intégrité des informations, elle est désigné aussi écoute clandestine des transmissions sans fil pour objectif d'extraire des informations confidentielles.

Les attaques sur l'interface radio par interposition peuvent être :

- ✓ ***Passive*** : l'attaquant écoute seulement les communications entre le dispositif mobile et la station de base pour extraire des informations confidentielles comme les noms d'utilisateurs et mots de passe présente dans toutes les communications sans fil. **[36]**
- ✓ ***Active*** : en plus de l'écoute, l'attaquant injecte ou modifie les données transmisses.

- ***Dénie de service***

Un nœud peut très bien saturer le médium en émettant des trames de contrôle ou de données et empêcher ainsi les autres nœuds de communiquer.

c) Attaque sur les points d'accès

- ***Dénie de service***

Un attaquant peut acheter un équipement de station de base BTS et l'installe. Le terminal mobile se reliera au BTS attaquants, s'il a les caractéristiques de l'opérateur et un meilleur signal que la vraie station de base.

La fausse station de base se pose entre les unités mobiles et la station de base d'origine et intercepte les communications sans être découvert.

L'attaquant pourrait envoyer un signal "occupé" à l'unité mobile chaque fois qu'il demande un service. Aussi, il est possible que le BTS réponde à une demande de service par un message interdisant la station mobile d'accéder au canal dans un temps spécifique. Cette attaque peut être considérée comme déni de service puisqu'elle dénie les utilisateurs légitimes d'employer le réseau. **[37]**

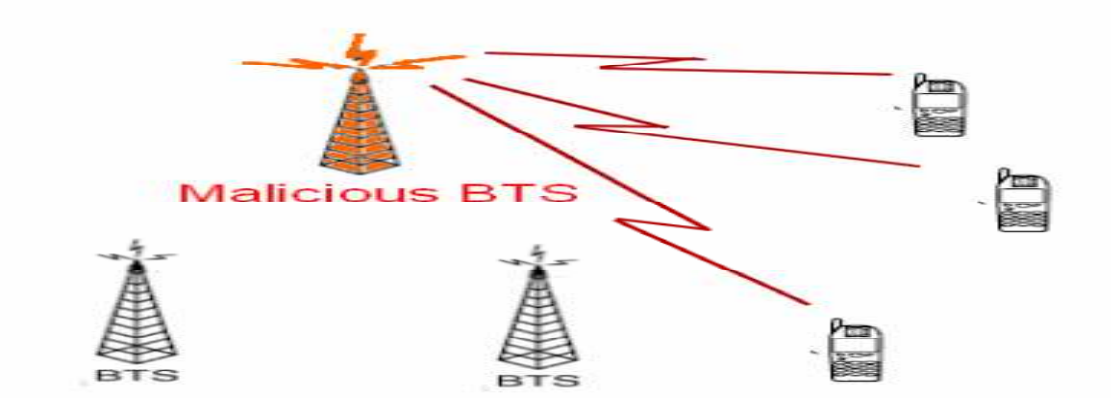

Fig.2. 8 : attaque sur les BTS **[37]**

- ***Détournement d'une session***

Un utilisateur malveillant peut détourner une session déjà établie, et peut agir en tant que station de base légitime.

d) Attaques sur le réseau cœur

Le réseau cœur est considéré la base des réseaux de mobiles. Il représente la base des fonctionnalités des unités mobiles, comme la fonctionnalité téléphonique ou de suivi d'emails. Donc, une attaque réussie sur le cœur réseau peut bloquer totalement le réseau de mobile.

- ***Dénie de service distribué***

Le but principal d'une attaque de type dénie de service distribué DDoS est de rendre un serveur public incapable de fournir des services aux utilisateurs légitimes. Une station de base peut être une cible typique d'une telle attaque de DDoS. Come les virus informatique ne concernent pas seulement les ordinateurs, ils touchent même les réseaux informatiques comme les réseaux de mobiles, donc lis sont considérés le moyen principale pour réaliser ce type d'attaque.
Un attaquant équipé par des virus peut envoie des paquets de commande à tout les nœuds de réseau pour demander des services de réseau cœur. Avec la limitation des capacités de traitement des requêtes des demandes ; la cible sera immédiatement bloqué et par conséquence le réseau sera bloqué. **[37]**

Quand le réseau cœur stocke des informations vitales pour la sécurité comme les mots de passe des utilisateurs, les clés,….. , on distingue d'autre forme d'attaque comme :

- ***l'attaque par force brute***

Généralement les mots de passe de la plupart des logiciels sont stockés cryptés dans un fichier. Pour obtenir un mot de passe, il suffit de récupérer ce fichier et de lancer un logiciel de brute force craking. Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumériques + symboles), de manière à trouver au mois un mot de passe valide. Cette attaque se base sur le fait que n'importe quel mot de passe est crackable. Ce n'est qu'une histoire de temps. Mais la puissance des machines double tous les deux ans. On parle de plus en plus de processeurs 1,2 GHz… de plus, les crackers n'hésitent pas à fabriquer des cartes électroniques de creacking, ce qui améliore en conséquence la rapidité de la machine, donc les chances de trouver un mot de passe valide. En générale, cette méthode est empruntée lorsque la méthode du dictionary cracking a échoué. **[38]**

7. Mécanismes de sécurité dans les réseaux de mobiles

Les mécanismes de sécurité dans les réseaux de mobile se diffèrent d'une génération à l'autre :

7.1. 1er génération

Les réseaux de 1ère génération sont conçus avec peut de sécurité. Puisque les réseaux de 1ère génération s'appuient sur la transmission analogique et puisque aucune technique de cryptage est employée, il est relativement simple pour un attaquer d'intercepter toutes les conversations. Concernant l'authentification, la station mobile envoi un Electronic Serial Number (ESN) qu'il stock le réseau. Le réseau vérifie si le ESN valide et permet ensuite au abonné d'accéder aux

services de réseau. Le problème avec ce processus d'authentification est que le ESN est envoyé en claire sur l'interface radio. Ceci signifie qu'un attaquer ne peut seulement écouter la conversation mais il peut également capturer le ESN valide et l'emploie pour accéder aux services qu'il fournit le réseau. Ces problèmes qui ont conduit aux réseaux de 2èmme génération**.[39]**

7.2. 2ème génération

L'utilisation de la transmission numérique a mené à des améliorations significatives dans la sécurité du réseau.

7.2.1. Confidentialité de l'identité de l'abonnée

Lors de la souscription au service, l'operateur fournit a l'abonné une Carte SIM. Cette carte contient l'identité de l'abonné sous la forme d'un IMSI (International Mobile Subscriber Identity). Pour que l'identité de l'abonné soit confidentielle, l'IMSI ne doit pas être intercepté par des entités non autorisés, donc la solution consiste à limiter le plus possible l'envoie de cette identité sur le lien radio et d'utiliser une identité temporaire, le TMSI (Temporary Mobile Subscriber Identity) pour identifier le mobile lors des interactions Station Mobile / Réseau. **[40]**

7.2.2. Clés et algorithmes utilisé

Une clé Ki est attribuée à l'usager, lors de l'abonnement, avec l'IMSI. Elle est stockée dans la carte SIM de l'abonné et dans l'AuC (Authentication Center qui fait généralement partie du HLR) au niveau du réseau. Afin d'éviter toute possibilité de lecture de la clé Ki, celle-ci n'est jamais transmise sur le réseau.

Le centre d'authentification AuC dispose de l'algorithme d'authentification A3, de l'algorithme de génération de la clé de chiffrement A8 et des clés Ki des clients du réseau.

Le BTS dispose de l'algorithme de chiffrement A5 pour le chiffrement des données usager et des données de signalisation. L'algorithme de chiffrement A5 est contenu aussi dans l'équipement mobile.

La carte SIM dispose de l'algorithme d'authentification A3, de l'algorithme de génération des clés de chiffrements A8, de la clé d'authentification individuelle de l'utilisateur Ki.

L'AuC et la carte SIM contiennent la même clé Ki et l'algorithme A3. Les algorithmes A3 et A8 sont quant à eux les mêmes pour tous les clients d'un même réseau**. [39][41]**

7.2.3. La confidentialité et l'authentification

Après que l'usager se soit identifié au réseau à l'aide de son TMSI, il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification A3

sont utilisés. Pour initier le processus d'authentification, l'AuC génère un nombre aléatoire, RAND, d'une longueur de 128 bits. Ce nombre RAND ainsi que la clé Ki de l'usager mobile servent de paramètres d'entrée à l'algorithme d'authentification A3. Le résultat est appelé SRES, il s'agit du résultat d'authentification attendu. Les mêmes paramètres RAND et Ki sont passés en paramètres de l'algorithme A8 qui produit un résultat Kc. Cette clé Kc sert de clé de chiffrement pour le trafic de l'usager et le trafic de signalisation entre le mobile et le BTS.

Le HLR retourne au MSC/VLR plusieurs triplets (RAND, SRES, Kc). Le MSC/VLR utilise le premier triplet et demande au mobile de s'authentifier à partir de la valeur RAND.

Le mobile réalise la même procédure que l'AuC et produit un résultat d'authentification SRES et une clé de chiffrement Kc à partir de la valeur RAND reçue du réseau, de la clé Ki présente sur la SIM et des algorithmes A3 et A8 aussi présents sur la SIM.

Le mobile soumet le résultat SRES au réseau (i.e., MSC/VLR) qui le compare au SRES soumis pas le HLR. S'ils sont égaux, l'authentification du mobile a réussi.

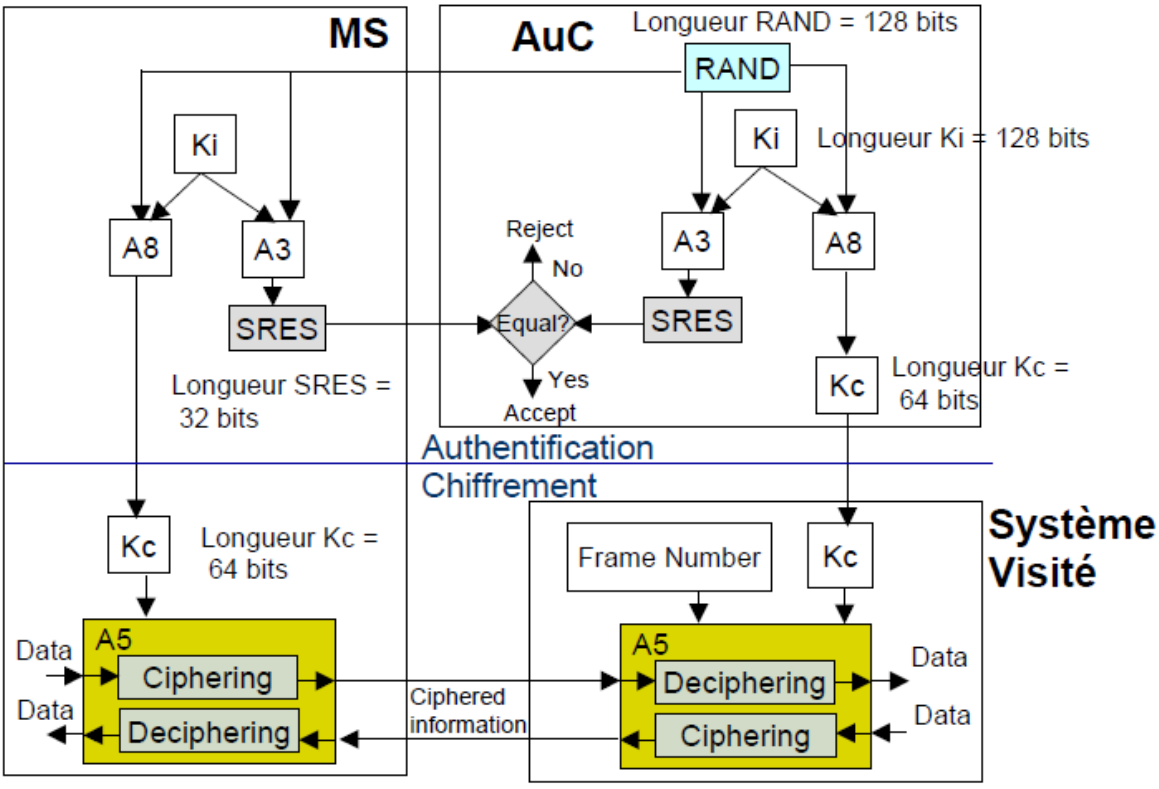

Fig.2. 9 : L'authentification et le chiffrement dans les réseaux de 2émme génération **[39]**

Un algorithme de chiffrement A5 présent sur la station mobile et la BTS est alors utilisé pour chiffrer / déchiffrer les données de signalisation et de trafic en utilisant Kc. **[41]**

Le processus d'authentification décrit ci-dessus a plusieurs failles de sécurité, les plus remarquables sont :

- *L'authentification n'est pas mutuelle*: Le station mobile MS s'authentifie au réseau en prouvant sa connaissance de la clé secret, Ki, mais le réseau ne s'authentifie pas à la MS. Un adversaire peut installer une fausse station de base, quand le réseau initie protocole l'authentification, l'adversaire commence le procédé d'authentification par l'envoie de challenge r et puis l'ignore. L'adversaire peut ne pas commencer le protocole d'authentification du tout. La MS ferait inconsciemment des communications avec l'adversaire.
- *Les failles dans l'implémentation de A3*: les travaux ont montré que les implémentations courantes d'algorithmes A3 basé sur les fonctions de hachages utilisant la clé secret stockée dans la carte SIM ont des failles de sécurité graves. Par exemple la clé secrète k_i pouvait être déduite par l'analyse des réponses (SR signé sur 32 bits). L'attaque nécessite l'interrogation de la carte SIM environ 150.000 fois. La carte à puce délivre 6,25 requêtes par seconde, donc l'attaque pouvait être accomplie avec succès en 8 heures. **[43]**

7.3. 3ème génération

La sécurité des réseaux 3G a été conçue utilisant la sécurité des réseaux 2G comme un point de départ. La raison est d'utiliser les points forts de sécurité dans les réseaux 2G et d'éviter leurs faiblesses. L'autre raison est d'assurer interopérabilité entre les réseaux 2G et 3G. **[39]**

7.3.1. L'authentification

L'authentification dans 3G (AKA, Authentication and Key Agreement) est une authentification mutuelle **[39]** basée sur une clé partagée qui est uniquement présente dans le HLR et la carte USIM. Comme le HLR ne communique jamais directement avec l'unité mobile, le MSC Server réalise la procédure d'authentification.

Le centre d'authentification génère un vecteur d'authentification à partir de la clé Ki qu'il partage avec la carte USIM du terminal ainsi que deux autres paramètres qui sont : un numéro de séquence et un nombre pseudo aléatoire.

1 à 5 vecteurs d'authentification (AV, Authentication Vector) sont téléchargés par le MSC Server à partir du HLR lorsque le MSC Server reçoit la demande de l'unité mobile.

Les paramètres présents dans l'AV sont :

- RAND : le challenge qui sert en tant qu'un des paramètres d'entrée pour générer les 4 autres paramètres de l'AV (128 bits).
- XRES : Le résultat attendu, utilisé par le réseau pour l'authentification de l 'USIM de l'unité mobile (32-128 bits).

- AUTN : Le jeton d'authentification utilisé par l 'USIM pour l'authentification de réseau (128 bits).
- CK : La clé de chiffrement (128 bits). Cette clé permet le chiffrement du trafic de l'usager et du trafic de signalisation entre l'unité mobile et le réseau.
- IK : La clé d'intégrité (128 bits). Cette clé permet la protection de l'intégrité de la signalisation entre l'unité mobile et le réseau.

Le VLR/SGSN à la réception du quintuplé (RAND, AUTN, XRES, CK, IK), transmet le challenge RAND et le nombre AUTN qu'il a reçu du HLR au terminal et attend une réponse RES de ce dernier.

Le mobile est authentifié si le résultat RES transmis est identique à XRES reçu du centre d'authentification. Le nombre AUTN permet au module USIM de vérifier si le centre

D'authentification est authentique et qu'il ne s'agit pas d'une attaque de type man in the middle par le réseau d'accès. **[39][41]**

7.3.2. Chiffrement des données (confidentialité)

L'algorithme de chiffrage dans 3G est connu comme KASUMI et emploie une clé de 128 bits CK. L'algorithme de KASUMI est plus sécurisé qu'A5 de 2G, le raisons est l'utilisation d'une longue clé.

Le processus de chiffrement commence par la génération de la clé CK dans l'étape d'authentification et utilisée par le USIM et VLR/MSC. En second lieu, il y a le COUNT-C de 32 bits qui est un numéro de séquence de chiffrage mis à jour séquentiellement pour chaque bloc à transmis. Troisièmement, il y a le BEARER de 5 bits qui est une marque unique pour le canal (le numéro de canal qui est employé pour porter le trafic de l'utilisateur). Quatrièmement, il y a la valeur DIRECTION d'un seul bit qui indique la direction de transmission (liaison montante ou liaison descendante) et finalement la longueur du bloc de données à chiffrer LENGTH de 16 bits.**[41]**

Toutes ces valeurs sont entrées dans l'algorithme de chiffrage f8 pour générer un résultat appelé *keystream* bloc. Ce dernier est combiner avec le texte à chiffrer l'entrée appelée *plaintext* bloc par l'opération XOR pour produire le résultat *ciphertext* bloc (le texte chiffré).

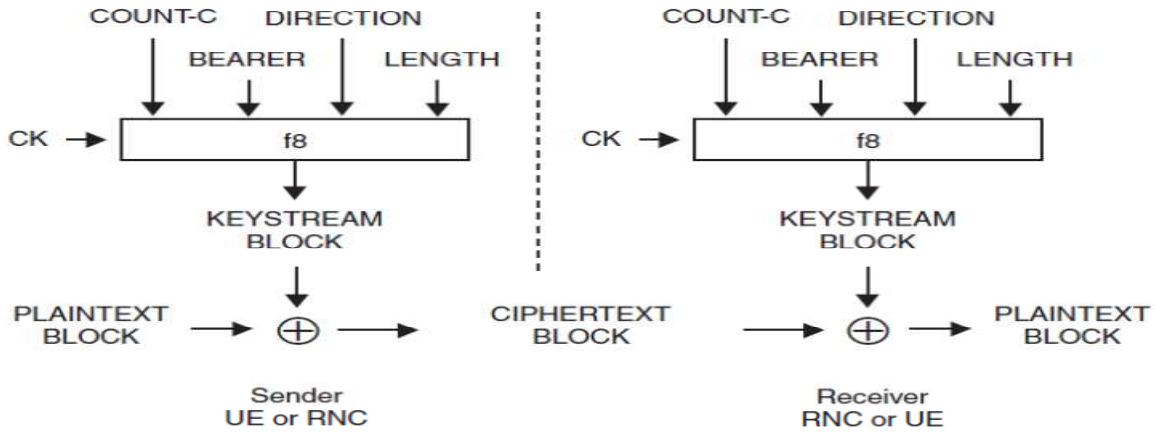

Fig.2. 10 : le chiffrement dans les réseaux 3G **[39]**

Il ya une amélioration de la confidentialité dans les réseaux 3G par rapport les réseaux 2G.

La confidentialité dans 2G a été limitée entre le terminal mobile et le BTS. Ceci a fait le lien entre le BTS et cœur réseau insécurisé. Les réseaux 3G prolongent l'interface chiffrée jusqu'au le cœur réseau.

Une dernière chose à noter est que le chiffrage dans les réseaux 3G est appliqué à tout le trafic d'abonné même pour les messages de signalisation. **[39]**

7.3.3. L'intégrité des données

Par contre les réseaux 2G qui n'offrent aucune méthode pour vérifier l'intégrité des données, les réseaux 3G utilisent la l'algorithme f9.

L'algorithme f9 génère un code d'authentification de message (MAC, Message Authentication Code) de longueur fixe à partir d'un message de longueur variable sous le contrôle de la clé secrète IK et un ensemble de valeurs d'initialisation. La clé IK a une longueur de 128 bits.

L'émetteur et le récepteur génère le code MAC sur 32 bits en utilisant la même fonction. L'émetteur envoie son résultat MAC au récepteur, qui compare la valeur du code MAC reçu avec la valeur attendue qui est celle calculée par le récepteur.

Le récepteur accepte le code MAC si la valeur calculée et celle reçue sont égales.

Les paramètres en entrée de l'algorithme d'intégrité sont la clé d'intégrité (IK), une entrée dépendant du temps (COUNT-I) de longueur 32 bits, une valeur aléatoire générée par le réseau (FRESH) aussi de 32 bits, le bit de direction '(DIRECTION) et le message de signalisation (MESSAGE).

Sur la base de ces paramètres d'entrée, l'usager utilise la fonction f9 pour calculer MAC-I (MAC-Integrity of signaling data) pour l'intégrité des données. MAC-I est ensuite ajouté au message lors de la transmission sur le canal radio. Le récepteur calcule la valeur de MAC

attendue (XMAC-I) sur le message reçu de la même façon que l'émetteur a calculé MAC-I sur le message envoyé. **[41]**

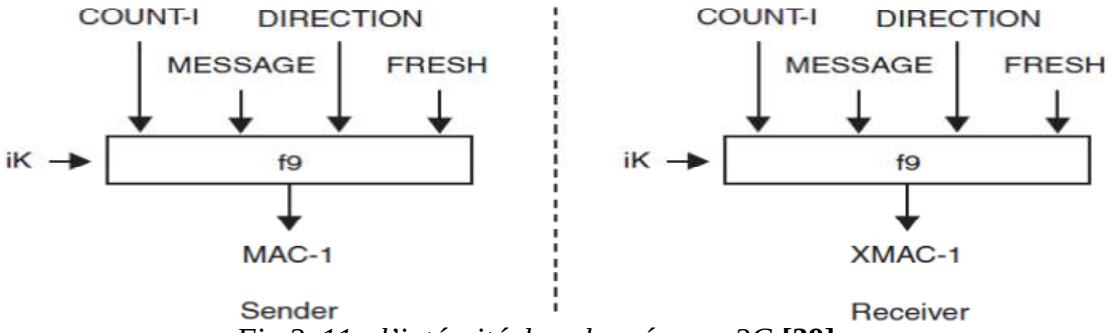

Fig.2. 11 : l'intégrité dans les réseaux 3G **[39]**

8. Système de détection d'intrusion pour les réseaux de mobiles

La majorité des travaux proposés dans les secteurs d'IDSs destinés aux réseaux sans fil utilise l'approche comportementale et exploite la régularité de comportement d'utilisateurs (par exemple, modèles de mobilité, ses activités) pour construire leur profil normale. La régularité est l'une des prétentions de base pour développer IDSs réaliste. Le modèle de la mobilité d'un utilisateur est une réflexion de ses routines quotidiennes et la plupart des utilisateurs mobiles ont les itinéraires préférés et les modèles habituels de mouvement. La plupart des utilisateurs mobiles ont des activités régulières, par exemple, en raison des rythmes fonctionnelles réguliers comme les affaires téléphonique quotidien ou hebdomadaire, la plupart des utilisateurs manifestent certain modèle d'appelle. Un attaquant ne pourrait pas imiter le profil d'utilisateur authentique et suivre leur modèle de mouvement exactement.

Relativement peu d'efforts de recherches ont été consacrés à la détection d'intrusion pour les Réseaux de mobiles. *Buschkes et al* **[21]** ont appliqué les règles de décisions pour le modèle de mobilité d'utilisateur pour augmenter la sécurité dans les réseaux de mobiles (approche comportementale).

Samfat *et al* **[21]** ont proposé IDAMN (Intrusion Detection Architecture for Mobile Networks), ce dernier a inclus deux algorithmes pour modeler le comportement des utilisateurs, en termes des deux modèles : d'activité et de migration. Y. - B Lin **[21]** a présenté une excellente étude pour détecter les utilisateurs frauduleux (dans ce qui concerne la copié d'identité) dans les réseaux de mobiles. Ils ont montré la rapidité de détection sous GSM/UMTS.

Les activités des utilisateurs sont employées pour décrire les modèles comportementaux des utilisateurs mobiles. Les réseaux de neurone et les modèles statistiques sont utilisés pour

apprendre leurs modèles d'utilisation. Basant sur ces modèles, les changements des comportements établis pour l'utilisateur privés peuvent être détectés. **[21]**

9. Rôle de la carte à puce dans la sécurité

La carte à puce (*smart card*) est un dispositif de sécurité très fiable grâce aux contre-mesures des fabricants. C'est une enceinte hermétique portable de sécurité, une entité de confiance attachée à un individu par l'intermédiaire d'un code secret. Elle évite la multiplication des mots de passe souvent peu protégés par les utilisateurs négligents. Elle obéit à des normes de sécurité et se généralise dans les applications des réseaux et des SI pour la sécurité de bout en bout entre deux protagonistes, le client, l'abonné ou l'utilisateur d'une part et le vendeur, l'opérateur ou le serveur informatique, d'autre part.

La carte à puce est un authentique micro-ordinateur doté d'un coffre fort qui renferme des secrets, assisté par un processeur spécifique étanche capable d'exécuter des primitives cryptographiques.

La carte à puce offre principalement une authentification robuste, et fournit également des fonctions d'identification comme une carte d'identité électronique. Elle est en outre un moteur miniature de sécurité, une machine de chiffrement de messages courts et de calcul de signatures.

La carte à puce peut stocker des certificats pour l'identification et des caractéristiques biométriques. Elle connaît une puissance croissante de calcul, améliorant ainsi les performances de résistance aux attaques par essais et erreurs, et une ouverture plus grande grâce à l'émergence d'applications en langage Java, au sein même de la carte. Le crypto-processeur permet de calculer en toute confidentialité les opérations de sécurité : la clé privée reste secrète à l'intérieur de la carte à puce.

Avec la commercialisation massive des cartes à puces et leur rôle dans les transactions de paiement, les pirates redoublent d'imagination pour élaborer de nouvelles attaques physiques ou par canaux cachés sur le matériel afin de contourner la sécurité. **[42]**

10.Les obstacles de sécurité dans les réseaux de mobiles

Un réseau de mobile est un réseau spécial qui a plusieurs contraintes comparativement au réseau traditionnel. A cause de ces contraintes, il est très difficile d'appliquer directement les approches de sécurité existantes pour les cas des réseaux de mobiles. Donc, pour développer des mécanismes de sécurités utiles tout en empruntant les idées depuis les techniques de sécurité courantes, il est nécessaire de connaitre et comprendre ces contraintes premièrement.

10.1. Les ressources limitées

Toutes les approches de sécurité exigent une certaine quantité de ressources pour les implémenter, y compris l'espace mémoire, capacité de traitement et l'énergie pour actionner l'unité mobile. Cependant, actuellement ces ressources sont très limitées dans une unité mobile. Ces ressources limitées ont un impact important sur la sécurité du terminal.

• *Espace Mémoire et de stockage limité* : Une mobile est un dispositif minuscule avec seulement un peu de capacité mémoire et d'espace de stockage. Afin d'établir un mécanisme de sécurité efficace, il est nécessaire de limiter le nombre d'instructions de l'algorithme de sécurité. Avec une telle limitation, le logiciel établi pour le mobile doit également être tout à fait petit.

• *Limitation de puissance d'énergie* : est la plus grande contrainte aux possibilités des unités mobiles. Par conséquent, la charge de la batterie prise avec l'unité mobile doit être conservée pour prolonger la vie du nœud. En mettant en application une fonction ou un protocole cryptographique dans un nœud mobile, l'impact du code de sécurité supplémentaire sur l'énergie doit être considéré. En ajoutant la sécurité à un nœud mobile, nous sommes intéressés par l'impact que la sécurité a sur la durée de vie d'un nœud (c.-à-d., sa durée de vie de la batterie). La puissance supplémentaire consommée par des nœuds mobiles dus à la sécurité est liée au traitement exigé pour des fonctions de sécurité (par exemple, chiffrage, déchiffrage, signature de données, vérification des signatures), à l'énergie exigée pour transmettre les données ou les frais généraux liés à la sécurité (par exemple, vecteurs d'initialisation requis pour le chiffrage/déchiffrage), et à l'énergie exigée pour stocker des paramètres de sécurité d'une façon sécurisé (par exemple, le stockage principal cryptographique). **[44]**

10.2. L'utilisation de l'interface sans fil

Le médium sans fil est très vulnérable par sa nature, beaucoup plus vulnérable que le medium filaire. Le médium sans fil permet un accès libre de tout acteur : la lecture, l'injection, la suppression et la modification des données sont possibles dans la plupart des configurations. De plus toute communication est de nature purement virtuelle : en général, on ne peut ni limiter le périmètre du réseau (à cause de propriété physiques : l'affaiblissement est fort, mais la propagation multi-chemin, les réflexions/réfraction, etc., produisent souvent des résultats étonnants), ni distingues ses vis-à-vis. Autrement dit, le médium ne permet pas de limiter le cercle des acteurs impliqués dans le traitement des données envoyées. Il ne permet pas non plus de détecter si un accès au médium ou aux données a eu lieu pendant la transmission.

Pour un attaquant le medium sans fil est souvent plus attractif, car il ne nécessite pas de la présence physique de l'attaquant. Bien équipé, il est capable de monter des attaques contre les vulnérabilités naturelles du medium en restant en dehors du domaine attaqué (*parking lot attack*).

Les équipements peuvent enregistrer les trames reçues pour espionner l'infrastructure rencontrée (*wardriving*) ou même un traitement autonome a posteriori (attaque par dictionnaire, attaque par force brute), même sans exploiter les failles éventuelles dans les contre-mesures de sécurité normalement implémentée dans ce genre de réseau. **[22]**

Pour résoudre ces types de problèmes, un certain nombre de mécanismes sont implémentés pour empêcher toute écoute clandestine ainsi que toute tentative d'accès non autorisé. Malgré la diversité de ces mécanismes, ils sont toutefois vulnérables, et il existe toujours des techniques pour les contourner. **[31]**

10.3. La mobilité

Compare a un environnement statique, ce nouvel environnement mobile permet aux unités de calcul une libre mobilité et ne pose aucune restriction sur la localisation des nœuds. La mobilité représente en effet un problème connu pour la sécurité car elle introduit non seulement des nouveaux mécanismes et sous-systèmes et donc une nouvelle complexité mais surtout la présence potentielle de plusieurs domaines d'autorité. Donc la sécurité de la mobilité doit être traitée avec une prudence élevée. Le problème c'est que les mécanismes de sécurité interviennent souvent en même temps que les mécanismes typiques de mobilité comme le changement de cellule. **[22]**

Conclusion

Les réseaux sans fil et mobile et la sécurité sont vus comme un oxymoron par beaucoup d'utilisateurs. En effet il est difficile de croire à une sécurité lorsqu'on a une accessibilité aussi évidente à un support sans fil.

Les réseaux de mobiles héritent le problème de sécurité a cause de la présence de support sans fil sans oublie les caractéristiques physiques des unités mobiles comme la limité d'énergie et les ressources de traitement.

Cependant, la communauté de recherche académique et industrielle développe des mécanismes et des protocoles de sécurité pour pérenniser ce mariage entre les réseaux sans fil et mobile et la sécurité.

Malgré la diversité de ces mécanismes de sécurité, ils ne sont pas tous applicables dans les réseaux de mobiles à cause des contraintes de ces derniers.

Alors, il faut concevoir des mécanismes de sécurité spécifiques aux réseaux de mobiles, tout en respectant ces propres caractéristiques.

Chapitre 3 : L’authentification Dans Les Réseaux De Mobiles

Introduction

La sécurisation des communications dans les réseaux sans fil comme dans les réseaux filaires passent par la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs de sécurité généraux. Ces objectifs, lorsqu'ils sont suivis, peuvent concourir à établir des contre-mesures efficaces à l'immense majorité des attaques dans ces réseaux. On peut citer principalement parmi ces objectifs: *l'authentification,* confidentialité et l'intégrité.

Il est important de relever que les objectifs de sécurité généraux précédents peuvent revêtir des degrés d'importance divers selon le contexte spécifique d'utilisation du réseau. Un contexte militaire mettra en avant le fort besoin d'authentification, de confidentialité et d'intégrité alors qu'une utilisation commerciale grand public nécessitera de se focaliser sur l'authentification et la disponibilité des services. Il est donc indispensable d'adapter chaque solution à son contexte d'utilisation à travers une analyse approfondie intégrant toutes les spécificités contextuelles.
Il est remarquable que l'authentification est une brique de base de la sécurité quelque soit le domaine d'application, elle est le premier rempart aux attaques informatique. Elle implémente le contrôle d'accès en identifiant solidement les utilisateurs ou les nœuds essayant d'accéder au réseau. Si seulement les personnes de confiance peuvent accéder au réseau, une protection inhérente est établie dans le système.
Aujourd'hui l'authentification des utilisateurs mobiles est un domaine de recherche important dans beaucoup de réseaux sans fil tels que les réseaux de mobiles, les réseaux maillés sans fil et ainsi de suite.

1. Authentification

Au début de chaque communication confidentielle, les correspondants doivent identifier leur interlocuteur et vérifier qu'il s'agit bien de la personne supposée. C'est le principe de l'authentification.
L'authentification des utilisateurs est l'un des pré-requis de la sécurité informatique. En effet, il est nécessaire de reconnaître et distinguer les différents utilisateurs pour savoir à quelles informations ils ont le droit d'accès. **[45]**
Elle est utilisée comme un premier processus pour autoriser un nœud dans un réseau à communiquer par les qualifications secrètes afin de fournir des services de sécurité.
L'authentification peut être définie comme l'acte d'établir ou de confirmer quelque chose (ou quelqu'un) comme authentique. **[46]** C'est la vérification d'informations relatives à une personne ou à un processus informatique.

Elle est la vérification de l'identité d'un sujet, c.-à-d. une vérification pour cela si le sujet qui s'identifie par l'identificateur de l'opérateur est le même et non pas un pirate informatique. L'opérateur affirme son identité à l'aide *d'une information d'authentification*, qui n'est pas connue à d'autres sujets.

L'authentification permet aux entités du réseau de s'assurer de la bonne identité ou du bon droit des entités avec lesquelles elles communiquent. Ainsi par exemple, l'infrastructure fixe peut avoir l'assurance que les stations clientes sont bien celles qu'elles prétendent être et inversement ou qu'elles ont bien les droits qu'elles prétendent avoir et inversement. La réalisation de cet objectif de sécurité va donc mettre en échec toutes les attaques procédant par des usurpations d'identité ou de rôle. **[47]**

L'authentification s'interpose entre deux phases importantes, l'identification et l'attribution des droits. Elle complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. **[48]**

L'identification est la reconnaissance du sujet par son identificateur. Pour ce but le sujet répond à une demande du système en lui offrant son identificateur personnel, et celui-ci de sa part, trouve cet identificateur dans la base des données qui contient tous les identificateurs enregistrés.

Après une authentification réussie, le système donne l'accès aux données, applications, bases de données, fichiers ou sites Internet…. Dans le cas contraire, l'accès est refusé. **[48]** C'est la phase d'attribution des droits.

L'attribution des droits représente la permission à l'opérateur à utiliser les ressources du système. Il faut avoir aussi la garantie que l'opérateur ne reçoit pas de droits plus grands qu'on en a préalablement déterminé. Cette phase s'appelle encore une phase de gestion de l'accès.

C'est évident que les trois phases en interaction (identification, authentification et attribution des droits) sont très importantes dans le processus de sécurité. La deuxième phase quand même peut être définie comme la plus importante et la plus responsable, parce que une faible authentification porte plus de risques et dans la plupart des cas mènent aux percées du système et à l'utilisation non-sanctionnée des ressources.

Un but essentiel du processus d'authentification est de permettre aux entités authentifiées de s'engager dans une communication sécurisé. Ceci nécessite la génération d'une clé cryptographique forte (appelée la clé de session) pour être partager par les entités après une exécution réussie de protocole d'authentification. **[43]**

Authentification vient sous divers formes, et les protocoles d'authentification sont employés d'un certain nombre de manières selon les propriétés de sécurité précises qu'ils sont censées pour fournir. La norme internationale ISO distingue deux formes d'authentification **[49]** :

- *L'authentification des entités* : consiste à vérifier l'identité de l'autre partie communicante, quoique l'authentification des entités couvre l'authentification de dispositif et l'authentification d'utilisateur. **[50]**
- *L'authentification des données* : se focalise de fournir des garanties quant à l'origine des données. **[49]**

La vérification d'identité peut se faire par divers mécanismes plus au moins sophistiqués, plus au moins sûrs, plus au moins coûteux. La complexité et le coût d'une stratégie d'authentification sont importants et doivent être pris en compte dès la conception de cette stratégie, pour éviter d'être confronté à des problèmes du type : le système est trop lent, le système coûte très cher en maintenance. **[45]**

2. Facteurs d'authentification

L'authentification consiste à confirmer l'identité présumée de l'utilisateur. Il s'agit donc d'un challenge entre un prouveur (l'élément qui veut s'authentifier) et un vérifieur (l'élément qui authentifie). Dans les deux cas, il peut s'agir de personnes, de machines, de programmes, de modules, etc.

On classe les différentes preuves possibles en plusieurs catégories appelées facteurs d'authentification :

2.1. Ce qu'il sait : Il s'agit dans la plupart des cas d'un mot de passe, mais peut très bien être une toute autre information qu'il aurait en sa possession (son adresse, son numéro de sécurité sociale, etc.)

2.2. Ce qu'il possède : On parle ici de moyens d'authentification par hardware comme les clés USB, les cartes d'accès, etc.)

2.3. Ce qu'il est : Ceci comprend notamment les paramètres physiques de l'utilisateur comme une empreinte digitale, un scan rétinien, une reconnaissance vocale, etc.

2.4. Ce qu'il peut faire : Ceci englobe les gestes que l'utilisateur pourrait faire, les comportements qu'il pourrait avoir comme un signe de la main.

Ces différents moyens ont chacun leurs avantages et inconvénients, mais permettent d'avoir une flexibilité dans la mise en œuvre d'une politique de sécurité.

On parle *d'authentification* ***simple*** lorsqu'un seul de ces facteurs est nécessaire, et *d'authentification* ***forte*** lorsque plus de deux le sont. De nos jours, l'authentification forte est devenue un enjeu majeur, en particulier dans la protection de données sensibles ou encore dans l'accroissement des échanges électroniques. **[51]**

3. Méthodes courantes d'authentification

3.1. Mots de passe

Les mots de passe pris dans leur ensemble sont le moyen d'authentification le plus répandu à ce jour. On distingue deux catégories : les mots de passe statiques et les mots de passe dynamiques. **[52]**

3.1.1. *Les mots de passe statiques*

L'authentification par mot de passe statique est très répandue. Les mots de passe statiques sont ceux qui restent identiques pour plusieurs connexions sur un même compte. Cette technique d'authentification est la plus utilisée mais aussi la moins robuste. **[48][52]**

La procédure d'authentification débute par une procédure de login durant laquelle un "login" et un mot de passe (chaîne de caractères secrète) sont fournis. Le système récupère ces informations et regarde dans sa base des utilisateurs si la personne est bien enregistrée et si le mot de passe qui a été tapé est correct. Si le couple login/mot de passe est correct, l'authentification est réussie et l'accès au système est permis.

Pour un "hacker" expérimenté ou un utilisateur "initié", il est techniquement facile en utilisant des outils disponibles, de découvrir le mot de passe d'un utilisateur. De tels outils sont basés sur l'utilisation d'un dictionnaire répertoriant les mots de passe les plus utilisés. Plus le mot de passe est simple, plus il sera facile et rapide de le découvrir. Pour les mots de passe plus complexes, il faudra un peu plus de temps mais sa découverte reste toujours possible. **[47]**

Par ailleurs, l'authentification peut aussi reposer sur un protocole d'authentification, qui permet de sécuriser les mots de passe statiques lorsqu'ils sont transmis sur le réseau par des mécanismes cryptographiques. **[48]**

3.1.2. *Les mots de passe dynamique (à usage unique)*

Avec les mots de passe classiques ou hachés, il est possible pour un attaquant de rejouer le même mot de passe une fois qu'il l'a intercepté. Pour remédier à ce problème, on utilise des mots de passe dynamiques ou à usage unique — One Time Password (OTP) en anglais — pour limiter la validité du mot de passe, ils sont modifiés à chaque session. En effet, à chaque demande de connexion l'utilisateur fournit un mot de passe différent généré par une petite calculette affichant périodiquement un nouveau mot de passe. Ce mécanisme est souvent associé à l'utilisation d'un code PIN que seul l'utilisateur connaît.

Le principe est simple : un même algorithme tourne de manière indépendante sur le serveur et sur la calculette. Lorsque la calculette fournit un nouveau mot de passe à usage unique le serveur, de son côté, connaît le mot de passe sans pour autant qu'il y ait une communication

entre les deux entités. Il n'est pas utile de chiffrer ce mot de passe puisqu'il 'est pas « rejouable » .**[47]** Les mots de passes à usage unique utilisant des calculettes logicielles comportent des failles exploitables. Il suffit de télécharger la calculette et savoir le secret de l'utilisateur pour pouvoir générer la vraie réponse. Il est possible de faire une attaque par dictionnaire ou par force brute sur le secret.

En version logicielle, les générateurs de mots de passe dynamiques utilisent certains composants des nœuds, comme l'horloge interne (on parle alors de méthode d'authentification en mode synchrone dépendant du temps). **[47][48]**

3.2. Signature numérique

La signature numérique est l'une des moyennes importantes de l'authentification.

Elle est authentique, difficilement imitable et ne devrait pas être réutilisable. La signature électronique s'appuie, depuis l'origine, sur la technologie d'infrastructure de gestion de clé publique (PKI pour Public Key Infrastructure). Les personnes qui désirent de se vérifier les identités utilisent un document dont ils ont une copie. **[53][54]**

Il existe plusieurs méthodes pour générer une signature numérique, les plus utilisé sont :

3.2.1. *Signature par la clé publique*

Il est possible de chiffrer un message de manière sûre avec la clé publique, et seule la personne possédant la clé privée pouvait le déchiffrer.

Mais de cette manière, il est également possible de chiffrer un message avec la clé privée, ainsi le message peu être authentifié avec la clé publique, c'est le principe de l'authentification avec une signature utilisant une clé publique.

Chiffrer un document avec la clé privée engendre une signature numérique sûre du document (ou un nombre aléatoire en cas de challenge/réponse) **[53]**, car seul le propriétaire de la clé privée a été capable de le chiffrer.

Cette méthode est efficace, l'authenticité est respectée et la signature est infalsifiable car c'est la clé privée qui la générée.

La signature n'est pas réutilisable car elle fait partie intégrante du document.

3.2.2. *Signature par fonction de hachage et clé publique*

Dans les applications pratiques, les algorithmes à clé publique sont souvent trop inefficaces pour signer de longs documents. Pour gagner du temps, les protocoles de signatures numériques sont souvent réalisés avec des fonctions de hachage. Au lieu de signer le document, on signe l'empreinte du document. La vitesse de ce procédé est beaucoup plus élevée et comme les

chances d'avoir deux documents différents ayant la même empreinte est très faible, signer l'empreinte est aussi fiable que signer le document tout entier.

La personne dont on désire vérifier l'identité calcule l'empreinte d'un document à l'aide d'une fonction de hachage à sens unique, puis le chiffre avec sa clé privée.

L'empreinte de l'émetteur est déchiffré avec sa clé publique, puis comparé avec l'empreinte calculée du même document avec la même fonction de hachage, si l'empreinte est la même, c'est que l'identité de l'émetteur est correcte.

3.3. Certificats électroniques

Les certificats électroniques sont l'une des techniques d'authentification les plus usitées à ce jour, certes loin derrière les mots de passe, mais ce moyen d'authentification devient de plus en plus populaire. **[55]**

Un certificat est l'équivalent d'une carte d'identité ou d'un passeport. Il repose sur les mêmes principes. Il permet de justifier de l'identité d'un individu (ou d'une entité) sur présentation du certificat. Tout comme le passeport, il contient des informations concernant son propriétaire (nom, prénom, adresse, une signature, une date de validité).

Il doit être également possible de s'assurer que ce certificat n'est pas un faux et qu'il a été délivré par une autorité reconnue. Le passeport est certifié par la préfecture tandis que le certificat est validé par une autorité de certification (AC). **[54]**

La technologie des certificats électroniques est utilisée dans le cadre d'une infrastructure à clé publique. Cette technologie d'authentification, dite forte, peut être combinée à deux autres techniques d'authentification que sont le mot de passe ou la biométrie pour atteindre un niveau de sécurité supplémentaire (authentification à deux facteurs).

3.4. Biométrie

L'être humain comporte des caractéristiques physiologiques et physiques qui permettent de l'authentifier de manière univoque. La biométrie est la discipline qui utilise ces différences biologiques pour déterminer, vérifier et identifié un individu.

Les contrôles biométriques principaux se basent sur les empreintes digitales, reconnaissance vocal, scan faciale, scan de l'iris, géométrie de la main. Le but est de retirer de ces caractéristiques biologiques le minimum d'information affin de générer un échantillon unique, cet échantillon sera comparé avec la mesure effectuée lors de chaque contrôle d'identité. **[53]**

La biométrie, prise dans sa définition moderne, est, aujourd'hui, une technique d'identification en pleine évolution qui génère une activité étatique et industrielle très importante. Il semble dès lors naturel d'introduire la biométrie dans le champ de la sécurité informatique, notamment par son application à l'authentification.

La mise en œuvre de l'authentification biométrique se présente en cinq phases **[48] :**

● Phase 1 : présentation de la donnée biométrique par la personne à authentifier;

● Phase 2 : acquisition de cette donnée par un lecteur biométrique ;

● Phase 3 : traitement de cette donnée par un dispositif électronique qui la transforme en une information numérique, sous forme d'un fichier ; ce codage peut faire appel à des techniques cryptographiques ;

● Phase 4 : comparaison de ce fichier caractérisant la personne à authentifier avec une donnée de référence (quand la personne s'est identifiée au préalable) ou des données pré-stockées de références (représentant l'ensemble des personnes que l'on souhaite authentifier) ;

● Phase 5 : décision, à partir de la comparaison effectuée en phase 4, d'authentifier ou non la personne. La décision binaire est propagée au dispositif informatique demandant l'authentification.

4. Protocoles d'authentification pour les réseaux de mobiles

L'authentification dans les réseaux de mobiles comme les réseaux sans fil est une tâche challenge, L'absence d'un milieu câblé crée de nouvelles menaces dans la construction des protocoles d'authentification. Dans un environnement sans fil, le milieu radio peut être accédé par n'importe qui s'il a l'équipement approprié. Un adversaire mobile peut recevoir et envoyer des messages dans le réseau sans fil, et même si de tels adversaires sont détectés, il est difficile de les enlever du réseau en raison de leur nature mobile. D'ailleurs, les dispositifs mobiles ont des contraintes typiques en matière de ressources, en termes puissance de calcule, d'espace mémoire, de largeur de bande….

Le protocole d'authentification devrait être soigneusement conçu, prenant en considération la nature et les contraintes de ces appareils. **[43]**

4.1. Les phases du protocole

Un protocole d'authentification pour les réseaux de mobiles comme les autres réseaux sans fil est composé de deux phases distinctes: la *bootstrapping* phase et la phase *d'authentification*.

Dans la bootstrapping phase, les nœuds qui demandent les services du réseau sont fournis avec quelque chose qu'ils doivent savoir, comme un mot de passe ou un code PIN, qui est connu au vérificateur. Ce secret partagé est appelé "bootstrapping material". Le vérificateur oblige le demandeur d'authentification de démontrer la connaissance de la "bootstrapping material" comme une preuve d'éligibilité pour accéder aux ressources protégées ou l'utilisation des services payants. Puisque dans la bootstrapping phase, le demandeur n'est pas encore authentifié, le "bootstrapping material" doit être envoyé au demandeur via un canal sécurisé.

La deuxième phase (la phase d'authentification) commence après que la première phase (bootstrapping) a été achevée avec succès. Dans la phase d'authentification, le demandeur fournit la preuve au vérificateur qu'il a le «bootstrapping material» qui a été fourni par le vérificateur. Dans le cas de l'authentification mutuelle, les deux entités doivent s'identifier l'un au l'autre utilisant le "bootstrapping material" qui a été échangé dans la première phase.

4.2. Exigences à respecter :

La réalisation viable du protocole d'authentification pour les réseaux de mobiles exige ce qui suit:

- *Efficacité computationnelle*: Ceci dénote le nombre total d'opérations nécessaires pour exécuter le protocole d'authentification. Le cryptage et le décryptage suivant l'approche symétrique exige moins de calculs que suivant l'approche asymétrique. Cependant, l'avantage de l'utilisation de la cryptographie à clé publique est que le canal utilisé pour distribuer la "bootstrapping material" ne doit pas être confidentielles. La charge de calcul pendant l'exécution du protocole d'authentification devrait être partagé entre les nœuds des réseaux car ils ont presque les mêmes capacités, on cas de contraire, la charge est orienté vers l'entité qui est riche en matière de ressources.
- *Stockage des secrets*: Le "bootstrapping matériel" nécessaire pour initier la phase d'authentification doit être de petite taille pour répondre à l'exigence de la mémoire limité disponible sur les appareils mobiles.
- *Efficacité de Communication*: Les nœuds mobiles passent la plupart de leur énergie (Batterie) pour transmettre des messages. Le protocole d'authentification devrait être soigneusement conçu de manière à minimiser le nombre des messages échangés et le nombre total de bits transmis.
- *Implication d'un tiers de confiance*: Le «matériel bootstrapping" est souvent distribué par un tiers de confiance. Dans l'approche symétrique, un tiers de confiance distribue (et initialise les stations mobiles avec) des clés symétriques. Dans l'approche asymétrique, l'autorité de certificat (CA) agit en tant que tiers : le CA aide avec la distribution des clés publiques, des certificats et la vérification de la validité de ces certificats par l'intermédiaire des listes de révocation de certificat. La conception du protocole d'authentification doit prendre en considération la disponibilité de ce tiers de confiance.
- *garantie de sécurité*: Avant la mise en œuvre, le protocole d'authentification devrait subir au cryptanalyse approfondie afin de vérifier la sécurité qu'il garantit.

Les protocoles d'authentification pour les réseaux de mobiles à besoin plus que les arguments heuristiques pour garantir la sécurité. L'utilisation des méthodes formelles pour analyser et

valider des questions de sécurité est très importante dans la construction des protocoles d'authentification «acceptables». **[43]**

4.3. Panorama de protocoles existants :

Certains protocoles d'authentification dans les réseaux de mobiles tels que le GSM utilisent la cryptographie à clé symétrique (à clé secrète).

L'authentification par ces protocoles est unilatérale seulement (n'est pas mutuelle), et l'identité et l'endroit de l'utilisateur ne sont pas anonymes. En plus ces protocoles ont besoin d'une tierce partie, c.-à-d., un tiers de confiance tel que HLR et le VLR. Le HLR agit en tant que CA ; VLR est le responsable d'authentification des stations mobiles. Même ces protocoles ont subis par la suite à des améliorations, ils restent toujours exposés à certain attaques. **[56]**

Les protocoles d'authentification à base de *ticket* (à titre d'exemple le protocole Kerberos) sont le bon exemple de protocole d'authentification symétrique.

D'autres protocoles s'appuient sur la cryptographie asymétrique (à clé public), qui emploie différentes clés, à savoir, clé publique et clé privée pour le décryptage et le cryptage respectivement.

Ce genre de protocole d'authentification utilisant l'approche asymétrique, assume l'existence d'une infrastructure de clé public (PKI) dans l'architecture de réseau. Le centre d'authentification de réseau et les stations mobiles ont des certificats à clé public signés par un tiers de confiance qui est l'autorité de certificat CA.

Le certificat de chaque entité (station mobile et centre d'authentification) lie leur identité à sa propre clé publique. Le certificat est utilisé pour la vérification de la validité des clés publiques des parties communicantes.

L'idée fondamentale derrière ces protocoles est de minimiser le transfère entre le VLR et le HLR même avec le fort déplacement des stations mobiles entre les zone de localisation (roaming and handover). L'inconvénient de ces protocoles est que l'utilisation incorrecte des certificats peut avoir des graves conséquences sur la sécurité du réseau, par exemple, il pourrait être facile d'usurper l'identité d'un utilisateur si son certificat est cloné.

Les protocoles d'authentification à base de *certificat* sont le bon exemple de protocole d'authentification symétrique.

En trouve d'autres protocoles qui s'appuient sur l'approche hybride.

L'approche hybride emploie une combinaison de cryptographie symétrique et asymétrique pour concevoir des protocoles d'authentification. Ces protocoles hybrides sont très efficaces et le trafic

d'authentification est minimisé au maximum. Ils sont souvent les plus utilisables dans les réseaux de mobiles car ils sont conçus spécifiquement à ce type de réseau. **[56][43]**

Conclusion

L'authentification est la brique de base de la sécurité dans les réseaux informatique. C'est la phase la plus importante dans le processus de sécuriser les réseaux de mobiles et les autres réseaux sans fil quelque soit leur domaine d'application. Elle consiste à augmenter le pourcentage de confiance entres les entités qui communiquent dans le réseau.

Les protocoles d'authentifications conçus pour les réseaux de mobiles doivent respecter les caractéristiques particulières de ces réseaux comme la limite de capacité de traitements et les espaces de stockage des stations mobiles, la limité de la bande passante et surtout la nature du support sans fil.

L'authentification peut se faire par divers mécanismes. Plusieurs protocoles sont concrétisés à base ces mécanismes mais souvent les plus adaptés aux réseaux de mobiles sont les protocoles basés sur l'approche hybride. Enfin, il ne faut pas oublier que la sécurité est un tout, et que l'authentification en est la première brique, elle doit impérativement être complétée, par exemple par des technologies de gestion des droits et de déchiffrement.

Chapitre 4 : La Cryptographie A Courbe Elliptique

Introduction

La cryptographie elliptique *ECC (Elliptic curves cryptography)* a été proposée par *Victor Mill*er et *Neal Koblitz* au milieu des années 1980s. Actuellement *ECC* est un crypto système mur, il est une alternative attractive au crypto système *RSA* particulièrement pour les dispositifs contraints en ressources. Il a été récemment adopté par le gouvernement U.S. **[57]**

Les crypto systèmes à clé publique conventionnels (*RSA, DH* et *DSA*) opèrent directement sur des entiers longs, la cryptographie *ECC* opère sur des points appartenant à une courbe elliptique.

La technologie ECC émergente a remplacé les systèmes cryptographiques traditionnels de clé publique. Le souci de pousser la cryptographie à clé publique sur les dispositifs mobile a été abordé par l'utilisation de l'ECC. ECC a deux mérites considérables, l'une est qu'il est extraordinairement sûr et l'autre est qu'il exige une longueur plus courte relativement aux autres systèmes cryptographique. La rapidité des calculs et la faible consommation de la puissance en plus d'épargne de la mémoire et de la largeur de bande passante sont des caractéristiques avantageuses pour utiliser l'ECC sur les dispositifs mobiles. **[46]**

1. Présentation mathématique des courbes elliptique

Soit K un corps, on appelle équation de Weierstrass sur K une ´équation de type :

E : $y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4 x + a_6$ ……. **(1)**

avec $a_i \in$ K. Une courbe donnée par une telle équation est dite lisse (sans point singulier) si le système suivant n'admet pas de solution :

$$\begin{cases} a_1 y = 3x^2 + 2a_2x + a_4 \\ 2y + a_1x + a_3 = 0 \end{cases} \qquad \text{……. (2)}$$

Autrement dit si les dérivées partielles en x et en y de

f(x, y) = $y^2 + a_1xy + a_3 y - x^3 - a_2x^2 - a_4 x - a_6$

ne s'annulent pas en même temps.

Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass définie sur K à laquelle on a rajouté un point "à l'infini", noté O ;

E = { (x, y) ∈ K | $y^2 + a_1x y + a_3 y = x^3 + a_2x^2 + a_4 x + a_6$ } ∪ {O}.

Dans un corps de caractéristique idoine (car(K) ≠ {2, 3}), les changements de variables amène à la forme courte de Weierstrass :

$y^2 = x^3 + ax + b$

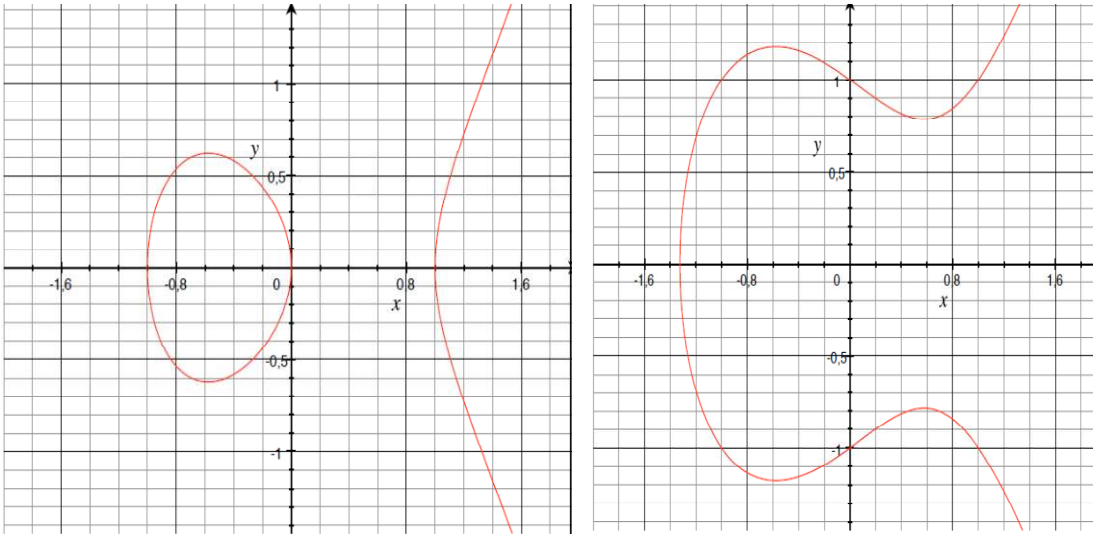

Fig.4. 1 : Exemples de courbes elliptiques **[60]**

Algébriquement, une courbe elliptique et un ensemble d'éléments avec des opérations arithmétiques personnalisées. C'est un locus des points dans la courbe elliptique dont les coordonnées se conforment à une équation particulière avec le point à l'infini O (le point auquel le locus dans le plan projectif intersecte la ligne à l'infini). **[58] [59] [60]**

2. Les fondamentaux d'ECC

Quelques fondations de la ECC sont nécessaire pour comprendre les descriptions mathématiques des courbes elliptiques utilisées dans la cryptographique sont discutées ci-dessous :

Un scalaire : N'importe quel élément se nomme scalaire si c'est un constituant de l'un ou l'autre *GF* (*p)* ou GF (2^k). Les scalaires sont dénotés utilisant des lettres minuscules.

Addition scalaire : Deux scalaires ou plus peuvent être additionnés pour avoir comme conséquence un nouveau scalaire. En cas de GF(p), l'addition est exécuté utilisant l'addition commune de nombre entier modulo p ce qui est comparable à l'addition polynômiale modulo un polynôme irréductible du degré k, produisant le champ GF(2^k). L'addition scalaire de deux scalaires r et s ayant pour résultat e est donnée par $e = r + s$.

Multiplication scalaire : deux scalaires ou plus peuvent être multipliées pour obtenir un nouveau scalaire. En cas de *GF*(*p)*, la multiplication est exécuté utilisant la multiplication commune de nombre entier modulo p qui est comparable multiplication polynômiale modulo un polynôme irréductible du degré *k*, produisant le champ GF(2^k). L'e scalaire e qui dénote la multiplication scalaire de deux scalaires r et s est donné par $e = d * r$.

Inversion scalaire : Le signe de l'inverse multiplicatif de tout élément constitutif de *GF* (*p)* ou *GF* (2k), a^{-1} a la propriété $a.a^{-1} = 1$. Le calcul d'a^{-1} est fait utilisant la méthode ou l'algorithme euclidien prolongé du Fermat.

Point : une paire ordonnée de scalaires conformément à l'équation de la courbe elliptique est connue comme *point*. Des majuscule telle que P_1, P_2 sont employés pour dénoter les points. Alternativement, un point P_1 est dénoté en tant que $P_1 = (x, y)$ où x et y appartiennent au champ. Les coordonnées x et y *du* point P_1 sont dénotées en tant que $P_1 \cdot x$ ou $P_1 \cdot y$, respectivement pour la clarté.

Addition et doublement de point : Utilisant l'addition des points d'une courbe elliptique, il est possible d'obtenir un troisième point R sur la courbe, offrant deux points P et Q à l'aide d'un ensemble de règles. Le symbole '+ ' dans $P_3 = P_1 + P_2$ représente l'addition elliptique. L'addition de point se différencie de l'addition scalaire habituelle.

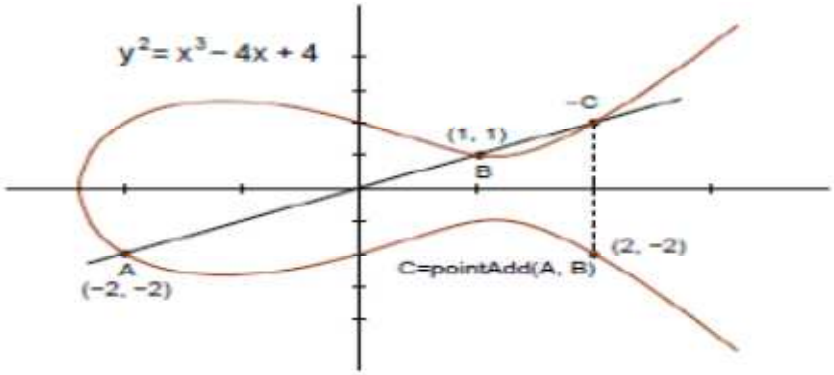

Fig.4. 2 : Addition de points **[60]**

Pour ajouter deux points, tracer une ligne entre ces deux points et refléter le 3ème point. Algébriquement, le résultat de l'addition de deux points est défini par les règles suivantes :

Soient E : $\boldsymbol{y^2 = x^3 + ax^2 + b}$ une courbe elliptique et P1 = $(\boldsymbol{x_1}, \boldsymbol{y_1})$, P2 = $(\boldsymbol{x_2}, \boldsymbol{y_2})$ des points de E, avec P1, P2 ≠ O. On a P1 + P2 = P3 = $(\boldsymbol{x_3}, \boldsymbol{y_3})$ avec :

1. Si $\boldsymbol{x_1 \neq x_2}$, alors

$\boldsymbol{x_3 = m^2 - x_1 - x_2}$, $\boldsymbol{y_3 = m(x_1 - x_3) - y_1}$, où $\boldsymbol{m = (y_2 - y_1)/(x_2 - x_1)}$

2. Si $\boldsymbol{x_1 = x_2}$ mais $\boldsymbol{y_1 \neq y_2}$, alors P3 = O.

3. Si P1 = P2 et $\boldsymbol{y_1 \neq 0}$ (la ligne de P1 à P2 sera la tangente dans P1 : cas de doublement), alors :

$\boldsymbol{x_3 = m^2 - 2x_1}$, $\boldsymbol{y_3 = m(x_1 - x_3) - y_1}$, où $\boldsymbol{m = (3x_1^2 + a)/2y_1}$

4. Si P1 = P2 et $\boldsymbol{y_1 = 0}$, alors P3 = O.

De plus, on a P + O = P pour tout P sur E.

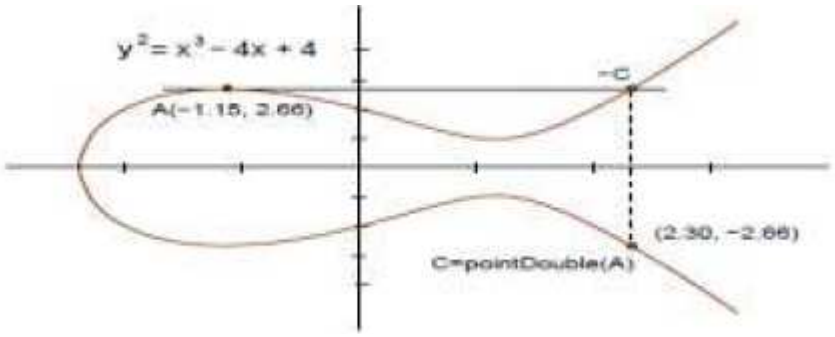

Fig.4. 3 : Doublement de point **[60]**

Soustraction de point

Considérer deux points distincts J et K tels que J = (x_j , y_j) et K = (x_k , y_k),

$J - K = J + (-K)$ Où $-$ K = (x_k , $-y_k$ mod p). **[62]**

Multiplication de point : L'opération cryptographique principale dans *ECC* est la multiplication de point scalaire qui calcule *Q=k.P*.

La multiplication d'un point d'une courbe elliptique P par un nombre entier *k* est semblable à l'addition de *P à* lui-même *k* fois qui a comme conséquence un autre point sur la courbe.

La multiplication est réalisée à travers une combinaison d'addition de points et des doublements de points, par exemple : *11P = 2((2(2P)) + P) + P*.

Chaque courbe a un point particulier *G* appelé point de base choisi tel qu'un grand nombre de points de la courbe sont des multiples de ce point.

3. Le problème du logarithme discret et le niveau de sécurité ECC

La cryptographie à clé publique repose sur un couple de clés, l'une publique, l'autre privée. Retrouver la clé privée à partir de la clé publique doit revenir à résoudre un problème considéré comme difficile (en termes de temps de calcul). Dans le cas des courbes elliptiques, le problème en question est celui du logarithme discret (PLD) et problèmes connexes dans le groupe des points d'une courbe elliptique sur un corps fini.

Commençons par définir ce qu'est le problème du logarithme discret dans un groupe G quelconque. **[60]**

Soient *G* un groupe et $g \in G$.

Le problème du logarithme discret de G par rapport à la base g est le problème suivant : étant donné $y \in G$, trouver $x \in$N tel que $g^x = y$ si un tel *x* existe.

Dans le cas des courbes elliptiques, le problème du logarithme discret de *E* par rapport à la base *P* est : étant donné $Q \in E$, de trouver $x \in$ N tel que $Q = xP$. **[63]**

La difficulté relative pour résoudre un problème mathématique difficile, détermine la force de sécurité du système correspondant.

La sécurité du crypto système *ECC* est liée à la difficulté pour résoudre le problème de logarithme discret *PLD* (retrouver l'entier x à partir de la donnée publique (E; P;Q)). Le problème est incassable pour des grandes valeurs de *x*.

La sécurité des protocoles basés sur les courbes elliptiques repose sur la résolution de ce problème. **[61]**

Une sécurité réelle n'est pas offerte pour chaque courbe elliptique, pour certaines courbes elliptiques (courbes faibles), on peut transférer le problème du logarithme discret PLD vers un problème de logarithme discret plus facile à résoudre. **[57]**

Pour confronter à ce problème et d'autre attaque sur les courbes elliptique, la théorie a publié un ensemble de courbes recommandées et présenté une classe des groupes finis qui ont été établis entièrement comme des appropriés pour l'usage cryptographique et qui offrent des propriétés réelles de sécurité.

Les courbes elliptiques utilisées dans la cryptographie sont définies sur la base de deux genres de champs finis à savoir les champs du caractéristique impaire *GF(p)* (appelé aussi *Prime Field* ou *modulo p*), là où $p > 3$ est un grand nombre premier et des champs de la caractéristique paire $GF(2^m)$ (appelé aussi *Binary Field* ou *over a finite field with* 2^m *elements)* où chaque élément est un polynôme binaire de degré *m* représenté comme une chaine de *m* bits. Ils sont dénotés par *GF(q)*, où $q = p$ ou $q = 2^m$.

L'équation de la courbe sur le champ $GF(p)$ est de la forme : $\boldsymbol{y^2 = x^3 + ax + b}$ où *a* et b ∈ $GF(p)$ et $\boldsymbol{4a^3 + 27b^2 \neq 0}$ (pour que la courbe soit lisse). En cas de champ binaire $GF(2^m)$ (appelées les courbes de *Koblitz*), l'équation de la courbe est de la forme : $\boldsymbol{y^2 + xy = x^3 + ax^2 + b}$ où *a* et b ∈ $GF(2^m)$ et $\boldsymbol{b \neq 0}$. **[46]**

Le meilleur algorithme connu pour attaquer *ECC* (*Pollardrho)* a un temps d'exécution complètement exponentiel, donc il s'exécute plus lentement que le meilleur algorithme connu pour attaquer *RSA (NSF- Number Field Sieve).* **[57]**

Idée fondamentale et que rien n'est incassable, mais le temps qu'il faudrait pour déchiffrer le message est jugé supérieur au délai de sécurité voulu. **[59]**

4. Pour quoi ECC ?

La théorie mathématique de courbes elliptiques fournit une classe des groupes finis qui ont prouvé tout à fait approprié pour l'utilisation dans la cryptographie. De plus, l'ECC est plus appropriée à l'authentification pour les réseaux de mobiles dû à quelques caractéristiques prospères qui sont donnés ci-dessous : [61]

- Des réalisations matérielles extrêmement efficaces sont disponibles pour les opérations exponentielles d'ECC qui conduit à des réductions potentielles dans l'implémentation des opérations cryptographiques même avec des clés de taille un peu considérable. **[46]**

  Ces réalisations sont des implémentations matérielles au niveau de l'unité arithmétique et logique, les opérations de base *ECC* sont câblées (des FPGA interfacés avec le système hôte via le bus PCI). Ces prototypes ont été réalisés par *Sun Microsystems Laboratories* **[57]** :

  - Première Génération d'Accélérateur *ECC*
    - Calcul de multiplication de point scalaire sur les courbes *ECC GF(2^m)*
    - Coprocesseur 256-bit dédié
    - Implémentation *ECC* plus rapide (66 MHz, 3..4-cycle non-pipelined,
    - 256x256 multiplications)
    - 6 987 *ECC-163* op/s .
  - Deuxième génération d'Accélérateur *ECC*
    - Calcul de multiplication de point scalaire *ECC* à la puissance modulaire.
    - Processeur 64-bit
    - Support de *ECC GF(p)* et *GF (2^m)*
    - Performance projetée (1.5 GHz, 2-cycle 64x64 pipelined mul)
    - 10,000 *ECC*-163 op/s.
- Pour une taille donnée d'une clé, une sécurité considérablement plus grande est fournie par ECC : Les résultats de comparaison des niveaux de sécurité *ECC* versus *RSA&DSA* présenté sous forme de graphe (voir fig.4.) montrent les tailles de clés et le nombre d'années *MIPS* de sécurité. Avec *ECC* les tailles de clés restent inférieures en réalisant un niveau de sécurité équivalent à *RSA/DSA* qui nécessite des tailles de clé plus supérieures.

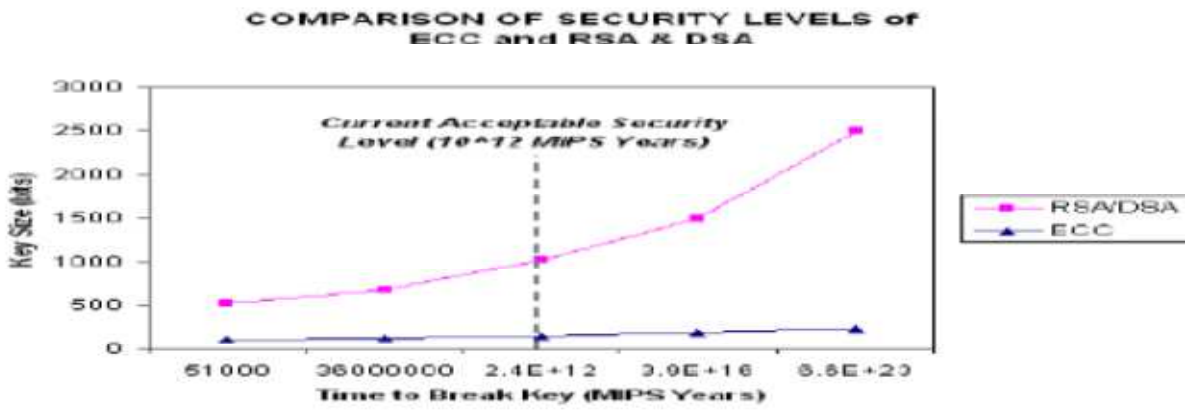

Fig.4. 4 : comparaison du niveau de sécurité entre ECC et RSA/DSA **[58]**

Le tableau suivant donne une comparaison des tailles de clés associés aux niveaux de sécurité et leurs ratios des systèmes *ECC* vs. *RSA/DH/DSA* **[57]**:

Clé Symétrique ou niveau de sécurité	***ECC***	***RSA/DH/DSA***	***Ratio***	***La durée protégée***
80	*160*	1024	6 : 1	jusqu'à 2010
112	*224*	2048	9 : 1	Jusqu'à 2030
128	*256*	3072	12 :1	Après 2031
192	*384*	7680	20 :1	
256	*512*	15360	30 :1	

Tab.4. 1. : Taille de clés et niveaux de sécurité

- Pour un niveau de sécurité donné, la clé d'une petite taille rend également des réalisations compactes possibles, c.-à-d. des opérations cryptographiques plus rapides, s'exécutent sur des petites chips ou des logiciels plus compacts sont possibles. De plus, moins de production de chaleur et moins de puissance d'énergie est particulièrement avantageuse en cas de dispositifs contraints. **[46]**
- Dans une *PKI* basée sur les certificats X.509, une taille typique d'un certificat X.509 ≈ 1 K (≈ 1000 octets) pour *RSA*-2048 bits ou *DSA*, mais en utilisant *ECC*-224 bits, la taille du certificat sera réduite d'environ 20%. Si la CA et l'utilisateur final utilisent tous les deux *ECC*, les certificats seront réduits d'environ 40 %.

Ces caractéristiques d'ECC sont des bonnes motivations pour la large utilisation de l'ECC ces jours. Les résultats montrent que la cryptographie *ECC* est mieux appropriée aux environnements sans fil contraints en ressources avec un niveau de sécurité élevé, donc elle est le meilleur moyenne à utiliser pour fournir un protocole d'authentification amélioré pour les réseaux de mobiles. **[57][46]**

5. Applications d'ECC dans la cryptographie

Soit dans l'environnement *RSA* ou *ECC*, toute théorie trouvée ne peut pas être utilisée directement. Il est nécessaire de définir des standards de structures de données et des algorithmes pour gérer l'information.

Les opérations crypto *ECC* sont adoptées et standardisées par NIST, ANSI, IEEE et IETF. Actuellement, il ya trois applications de *ECC* dans la cryptographie *(ECIES- Elliptic Curve*

Integrated Encryption Scheme ,ECDSA- Elliptic Curve Digital Signature Algorithm, ECDH-Elliptic Curve Diffie-Hellman) **[57]**

5.1. ECIES- Elliptic Curve Integrated Encryption Scheme

ECIES désigne les algorithmes de chiffrement/déchiffrement *ECC* les plus connus. Se sont une variante du schéma de cryptage *ElGamal*. **[57]**

Le principe de cryptage ElGamal est simple, quand Alice veut envoyer un message secret à Bob. Tout d'abord, Bob fabrique une clé publique, Il choisit une courbe elliptique E définie sur un corps fini Fq de telle manière que le problème du logarithme discret soit plus difficile à résoudre. Il choisit aussi un point P sur E. Il choisit un nombre entier secret s et calcule $\boldsymbol{B = sP}$. La courbe E, le corps fini Fq et les points P et B sont publiques et $\boldsymbol{B}$ est la clé publique de Bob. La clé secrète de Bob est $\boldsymbol{s}$. Pour envoyer le message, Alice transforme son message en un point M ∈ E(Fq). Elle choisit un nombre entier secret $\boldsymbol{k}$ et calcule$\boldsymbol{M1 = kP}$.

Elle calcule $\boldsymbol{M2 = M + kB}$.

Elle envoie ***M1*** et ***M2*** à Bob.

Bob déchiffre le message en calculant$\boldsymbol{M = M2 - sM1}$.

Un espion connait la clé publique et les points ***M1*** et ***M2***. Il ne peut pas trouver M si et seulement s'il a résolu le problème du logarithme discret. Donc, la fiabilité de ce genre de crypto-systèmes dépend fortement des progrès fait en matière de résolution du logarithme discret.

Il est important qu'Alice utilise, à chaque fois qu'elle envoie un message Crypté à Bob avec la même clé, un $\boldsymbol{k}$ différent. **[58]**

5.2.ECDSA- Elliptic Curve Digital Signature Algorithm

ECDSA est la variante courbe elliptique de l'algorithme de signature numérique *DSA*.

Pour envoyer un message signé d'Alice à Bob, tous les deux doivent convenir sur les mêmes paramètres elliptiques (une courbe elliptique E d'ordre n, un corps fini F_q, un point de référence P (generator point)).

Alice a une paire de clé consiste d'une clé privée $\boldsymbol{s}$ (un entier choisis aléatoirement de F_q) et une clé publique $\boldsymbol{B = sP}$

Une vue d'ensemble du processus d'ECDSA est définie ci-dessous. **[57] [62]**

Génération de signature

Pour signer un message m par Alice, utilisant la clé privée $\boldsymbol{s}$:

1) Calcule$e = HASH\ (m)$, où le HASH est une fonction de hachage, comme SHA-1.
2) Choisir un nombre entier aléatoire k ∈ [1,1 − n]

3) Calculer r = x1 (mod n), où (x1, y1) = k * P. Si r = 0, passez à l'étape 2
4) Calculer $l = k^{-1}(e + sr)(mod\ n)$.Si l = 0, passez à l'étape 2
5) La signature est la paire (r, s)

Vérification de signature

Pour que Bob authentifie la signature d'Alice, Bob doit avoir la clé publique B d'Alice

1) Vérifier que r et l sont des nombres entiers $\in$ [1,1 − n].Sinon, la signature est invalide
2) Calculer $e = HASH\ (m)$, où le HASH est la même fonction utilisée dans la génération de la signature
3) Calculer $w = l^{-1}\ (mod\ n)$
4) Calculer $u_1 = ew\ (mod\ n)$ et $u_2 = rw\ (mod\ n)$
5) Calculer (x1, y1) = $u_1P + u_2B$
6) La signature est valide si x1 = r (mod n), invalide autrement. **[62]**

Comme une comparaison, un message signé avec une clé *RSA* 1024 bits produit une signature numérique de 128 octets, tandis que le même message signé avec une clé *ECDSA* 192 bits génère une signature numérique de 48 octets. Le peu d'octets de la signature numérique peuvent être enveloppés avec les données dans un seul message.

Les messages signés par *ECDSA* et échangés dans un environnement mobile, peuvent être vérifiés avec une infrastructure *PKI.* On utilise les services *PKI* relatifs au certificat *X .509* basé *ECC* sur des dispositifs mobiles et sur des serveurs. **[57]**

5.3.ECDH- Elliptic Curve Diffie-Hellman

L'objectif principal des protocoles d'échange de clé est de mettre en contact deux ou plusieurs entités communicantes à travers un canal ouvert et non sécurisé, partageant une clé sécrète qui permet de fournir la confidentialité de données et l'intégrité de toute information échangée.

ECDH est le schéma d'échange de clé typique basé sur le mécanisme de *Diffie-Hellman* appliqué aux courbes elliptiques. On trouve certaines implémentations pratiques d'ECDH.

Dans *ECDH key agreement*, deux parties communicantes *a* et *b* se mettent d'accord pour utiliser les mêmes paramètres de courbe elliptique. Elles génèrent leurs clés privées $\boldsymbol{ka}$ et $\boldsymbol{kb}$ et aussi leurs clés publiques correspondantes : $\boldsymbol{Qa = kaG}$ et $\boldsymbol{Qb = kbG}$. Les deux parties échangent leurs clés publiques, ensuite chaque partie multiplie sa clé privée par la clé publique de l'autre partie pour produire un secret commun partagé : $\boldsymbol{ka.Qb = kb.Qa = ka.kb.G}$ (voir la fig.5).**[57]**

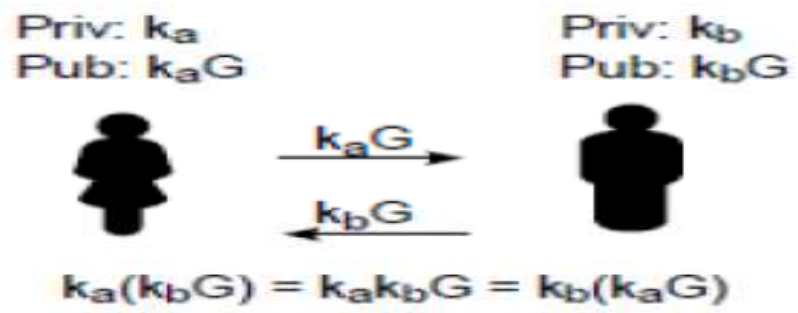

Fig.4. 5 : ECDH key agreement **[58]**

6. Utilisation d'ECC pour échanger la clé secrète AES

6.1.Présentation d'AES

En 1997, le NIST (National Institue of Standards and Technology) a lancé un appel d'offre pour un algorithme de chiffrement symétrique avec un bloc de taille 128 bits et supporte des clés de 128, 192 et 256 bits. Les critères d'évaluation de l'offre comprenaient la sécurité, la puissance de calcul, les contraintes de la mémoire des petits dispositifs (comme la carte à puce), la plateforme logicielle et matérielle et la flexibilité. Un total de 15 algorithmes ont été envoyés et Rijndael (AES) a été sélectionné parmi ces 15 algorithmes.

L'algorithme de Rijndael a été sélectionné pour devenir l'AES en 2001, Rijndael est un acronyme désignant ces créateurs : Joan Daemen et Vincent Rijment.

L'AES utilise des opérations mathématiques comme des substitutions, des permutations et des XORes. Il a plusieurs rounds identiques (de 10 à 14) et leur nombre dépend de la taille de la clé. L'AES opère au niveau octet ce qui permet une implémentation efficace au niveau matérielle et logicielle. L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.

AES a succédé DES et TDES. Il est spécifié actuellement comme le nouveau standard de chiffrement symétrique, il a trois niveaux forts de sécurité : 128 bits, 192 bits et 256 bits. La sécurité 128 bits fournira au mois 30 ans de protection. AES ne fournit pas seulement une sécurité supérieure à TDES mais il délivre aussi une meilleure performance. AES est un bon choix pour un algorithme de chiffrement symétrique.

AES est également un candidat particulièrement approprié pour les dispositifs mobiles limités en ressources de calcul et de stockage. Le monde de la 3G (3ème génération de dispositifs mobiles) a adopté l'algorithme AES pour son schéma d'authentification "Millenage". **[57]**

6.2.ECC le système à clé publique approprié à AES

Selon l'institut national des standards et des technologies NIST, les clés pour les chiffrements symétriques comme AES doivent être échangées avec des crypto systèmes à clé publique forts.

La cryptographie à clé publique fournit les techniques d'agrément de clé qui simplifient énormément la gestion de clé. Aujourd'hui il ya deux types de crypto systèmes à clé publique qui sont considérés sécurisés et efficaces. Ces crypto systèmes, classifiés selon le problème mathématique sur lequel ils se basent, sont : systèmes de factorisation d'entiers (ou RSA est l'exemple le plus connu), systèmes de logarithme discret comme DSA et les crypto systèmes à courbe elliptique ECC.

Les deux principaux benchmarks de comparaison de ces systèmes sont la sécurité et l'efficacité. Les clés publiques ECC ont des tailles plus petites que RSA et DSA/DH. Grace à ces tailles de clés plus petites, ECC surpasse RSA et DSA/DH dans toutes les opérations de niveau de sécurité équivalente.

ECC fournit plus d'efficacité en termes de calcul cryptographique, taille de clé et bande passante. Les implémentations ECC offrent donc des vitesses de calcul plus élevées, une faible consommation d'énergie et une taille de code plus réduite.

ECC évolue linéairement avec *AES* et maintient des tailles de clé relativement plus petites à tous les niveaux de sécurité. Les clés *ECC* pour *AES* 256 bits ont seulement une taille de 512 bits, tandis qu'une clé *AES* 256 bits demande une clé *RSA* de 15360 bits pour une sécurité équivalente, donc ECC ne réduit pas beaucoup la performance. *AES* utilisé en conjonction avec *ECC* permet des solutions de sécurité plus élevées sans dégrader la performance du système même sur des dispositifs mobiles contraints en ressources.

Il est donc fondamental d'utiliser un crypto système ECC pour échanger la clé secrète de l'algorithme de chiffrement symétrique AES. **[57]**

Conclusion

Le crypto système *ECC* offre des clés avec des tailles plus petites comparé aux autres crypto systèmes traditionnels. Les petites clés permettent une économie en calcul CPU, en consommation d'énergie et en bande passante.

La sécurité du crypto système *ECC* est liée à la difficulté de résoudre le problème de logarithme discret, ce qui détermine la force de sécurité de l'ECC.

Le crypto système ECC est utilisé aussi efficacement pour échanger la clé secrète des algorithmes de chiffrement symétriques.

Ces caractéristiques de taille de clé et d'efficacité de sécurité rendent le crypto système *ECC* plus approprié pour les environnements de dispositifs mobiles sans fils contraints en matière de ressources.

Chapitre 5 : Le Protocole Proposé

Introduction

Le principe de base de notre travail est l'élaboration d'un protocole d'authentification adapté aux réseaux de mobiles.

On peut distinguer trois types de protocoles d'authentification pour les réseaux de mobiles, cette distinction est basé sur la méthode cryptographique utilisé (symétrique ou asymétrique).

Les protocoles symétriques sont plus rapides, efficaces et facilement implémentés sur le matériel. Ils sont des simples opérations de substitution et de transposition, ils ne requièrent pas d'opérations mathématiques complexes pour crypter ou décrypter les données. Par conséquent, ils n'exigent pas de grandes dissipations énergétiques durant les phases de chiffrement et de déchiffrement.

De tels protocoles apparaissaient comme les plus appropriées pour les utiliser dans un environnement mobile sans fil. Cependant, l'authentification par ces protocoles est souvent vulnérable, l'authentification est unidirectionnelle, l'identité et la location de l'utilisateur n'est pas anonyme sans oublie qu'elle besoin d'une troisième partie pour la construction et la distribution de clés.

Plusieurs protocoles asymétriques sont proposés. Ces protocoles sont plus efficaces et moins vulnérables que les protocoles symétriques car un chiffrement asymétrique permet d'autre fonctions de sécurité comme la signature d'un message, alors qu'un chiffrement symétrique ne peut le faire. Cependant, ces protocoles utilisent des clés de grandes tailles et nécessite un temps de calcul plus long et plus de ressources que lors d'un chiffrement symétrique, ceci a cause de la complexité des opérations à effectuer. Donc, il n'est pas encourageant d'utiliser ces protocoles dans un environnement sans fil malgré leurs efficacités en sécurité.

Les protocoles les plus utilisés actuellement sont les protocoles hybrides (mixtes) c.-à-d. ils sont basés sur les deux techniques de cryptographie (asymétrique et symétrique).

Cette méthode mixte est mieux sécurisée et plus efficace, elle présente des solutions intermédiaires, en identifiant un protocole qui doit prendre en charges la sécurité des communications tout en tenant compte des contraintes liées à ces réseaux (mobilité, usage économique de l'énergie,…).

1. Description générale du protocole proposé

Notre protocole d'authentification proposé est un protocole fort (*strong authentication*), l'authentification est réalisée en utilisant des justificatifs obtenus par des moyens de cryptographiques, il appartient à la classe des protocoles hybrides.

Ce protocole dénomme *HAPMON* (pour *Hybrid Authentication Protocol for MObile Networks*) fournit un compromis entre la sécurité et la respecte des contraintes d'environnement mobile.

HAPMON est un protocole d'authentification mutuelle, les deux entités (station mobile MS et le réseau présenté dans le VLR) doivent s'identifier l'un au l'autre en succès pour entrer dans des communications.

HAPMON est une suite de protocoles d'authentification se compose de deux parties : le protocole d'authentification à base de certificat CBA (certificate-based authentication protocol) ; qui s'appuie sur des méthodes cryptographiques asymétriques ; et le protocole d'authentification à base de ticket TBA (the ticket-based authentication protocol) qui s'appuie sur des méthodes cryptographiques symétriques (fig.5.1).

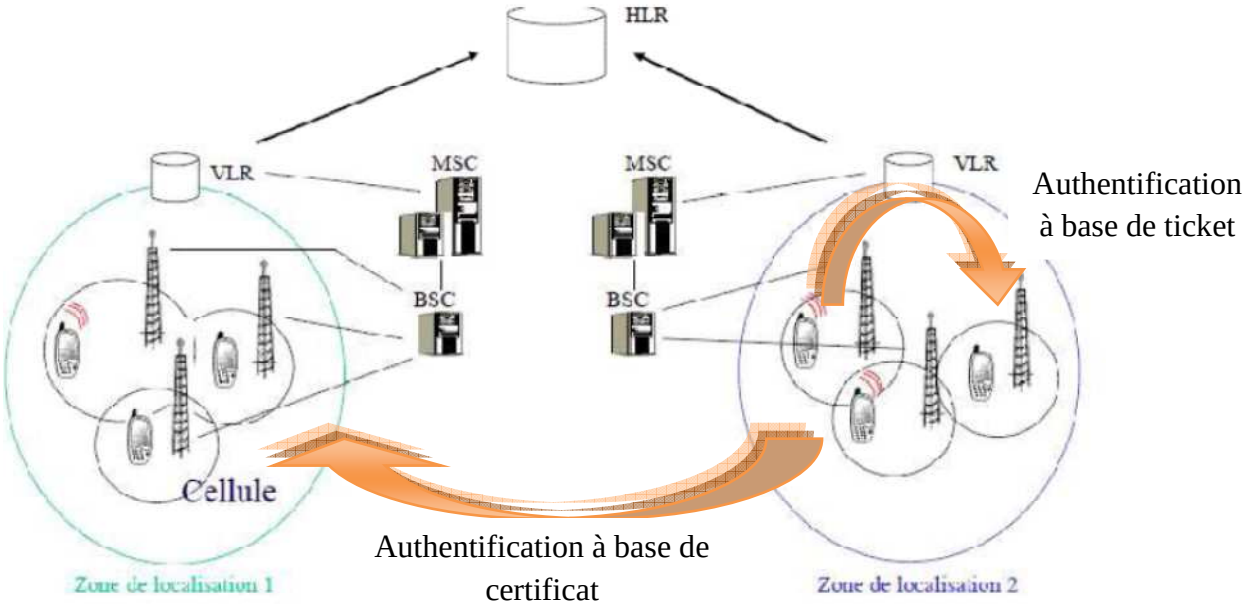

Fig.5. 1 : Le protocole HAPMON

Le protocole CBA est employé dans l'enregistrement, hanhover, et quand le ticket est inadmissible. Si la station mobile MS reste dans la même zone de localisation et demande le service plusieurs fois, alors nous employons le protocole TBA.

HAPMON est fondé sur la cryptographie elliptique parce que la cryptographie à courbes elliptiques est considérée comme une alternative attractive au crypto système *RSA* (le plus utilisé). Elle a été proposée il y a prés de vingt ans, comme une solution particulière aux problèmes des environnements et des dispositifs contraints en ressources, et malgré les tentatives de bon nombre de chercheurs renommés, aucun algorithme n'a été trouvé qui résolve efficacement le problème du logarithme discret elliptique, si ce n'est dans des cas bien

particuliers faciles à détecter. Grace à la difficulté de ce problème, *HAPMON* offre une sécurité avec une compacité et une efficacité inégale.

HAPMON utilise Elliptic Curve Diffie-Hellman (ECDH) pour la génération et l'échange des clés. ECDH est caractérisé par la production des clés secrètes partagées malgré les risques présentés sur le canal sans fil utilisé pour l'échange grâce à la difficulté de résoudre le problème de logarithme discret.

2. Description détaillé du protocole proposé

HAPMON, comme d'autres protocoles d'authentification pour les réseaux de mobiles, a deux phases, la phase d'enregistrement et la phase d'authentification.

2.1.Phase d'enregistrement

Dans cette phase, les nœuds qui demandent les services du réseau sont fournis avec des données qu'ils doivent prouver leur connaissance dans la phase d'authentification comme une preuve d'éligibilité.

La partie responsable sur la phase d'enregistrement est le HLR, une infrastructure de gestion de clés PKI *(public key infrastructure)* à base des certificats électroniques est prise en charge pour la génération des clés publiques/privées et leur distribution à leurs propriétaires à l'initialisation d'une nouvelle entité dans la PKI, ainsi que la publication, révocation et validation des clés publiques.

Avant la génération du certificat, le HLR choisit une courbe elliptique E définie sur un corps fini Fq de telle manière que le problème du logarithme discret soit plus difficile à résoudre. Il choisit aussi un point P (point de référence) sur E.

Le HLR génère par la suite une paire de clés, une clé publique **KU** et une clé privé **KR**.

Il choisit un nombre secret d et calcule $Q = dP$. La courbe E, le corps fini Fq et les points P et Q sont publiques et $\boldsymbol{Q}$ (KU_{MS}) est la clé publique. La clé secrète est $\boldsymbol{d}$ (KR_{MS}).

INPUT: elliptic curve domain parameters (p,E, P, n).
OUTPUT: public key Q and private key d
Select $d \in [1, n-1]$
Compute $Q = dP$.
Return (Q, d).

Elliptic curve key pair generation

Le certificat généré a le format le plus courant actuellement, fourni par le standard X.509v3. Il comprend entre autres : un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification (AC) émettrice du certificat et la signature qui garantit l'authenticité du certificat.

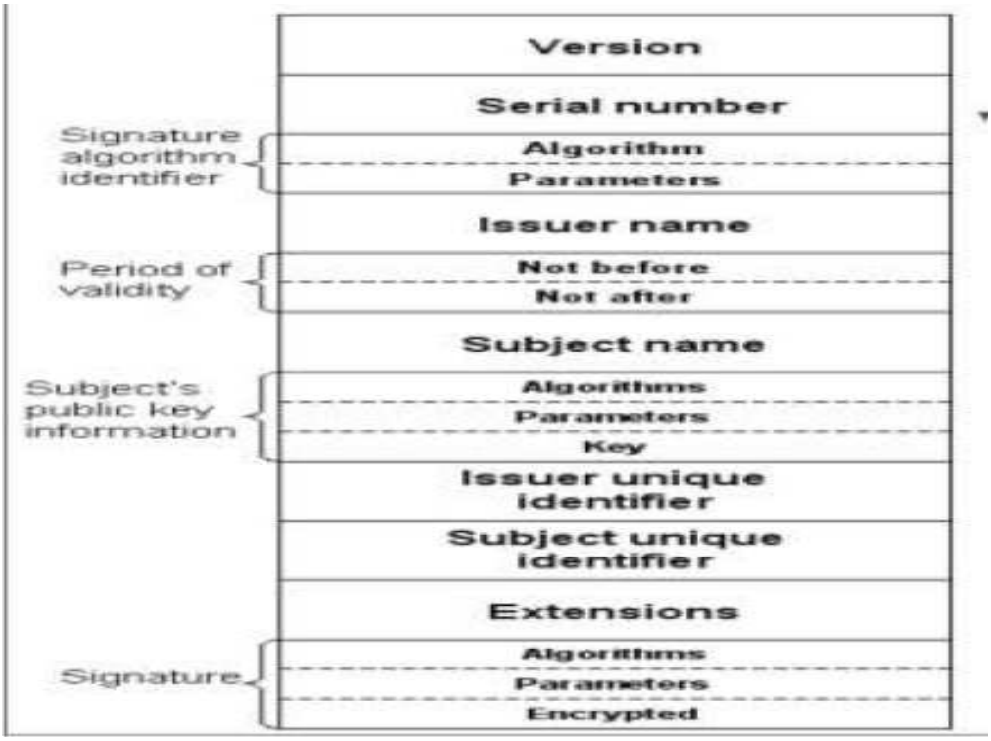

Fig.5. 8 : Le certificat **[50]**

La signature est apposée par HLR (AC) en utilisant sa clé privée KR_{HLR}. La clé publique de HLR KU_{HLR} stocké dans le VLR et les nœuds mobiles à la fois, est employée pour vérifier la validité des certificats.

Le HLR génère aussi pour MS une clé ***ki*** utilisée dans le chiffrement des données avant la vérification du certificat pour que rien ne soit envoyé en claire sur le réseau.

Cette clé est équivalente à la clé ***ki*** du réseau GSM.

À la fin de cette phase, le certificat, la clé privée de MS KR_{MS}, la clé ***ki*** et la clé publique d'HLR KU_{HLR} sont stockés dans le nœud qui demande les services du réseau d'une manière sécurisé et les données du VLRs sont mises à jour.

2.2.La phase d'authentification

La deuxième phase, phase d'authentification, commence après que la première phase a été achevée avec succès. Dans cette phase d'authentification, le nœud mobile et le VLR se changent mutuellement les preuves fournis par le HLR dans la phase d'enregistrement.

La phase d'authentification est une suite de deux protocoles, protocole d'authentification à base de certificat et le protocole d'authentification à base de ticket.

L'emploie de l'un de protocole ou l'autre est dépend principalement de la localisation d'unité mobile au moment de demande de service et d'autres considérations.

2.2.1. Authentification à base de certificat

Ce protocole est utilisé en cas d'enregistrement, handover et fin de délais d'un ticket. C'est un protocole d'authentification asymétrique basé sur *Elliptic Curve Integrated Encryption Scheme (ECIES)*. On peut expliquer le fonctionnement de ce protocole dans trois étapes :

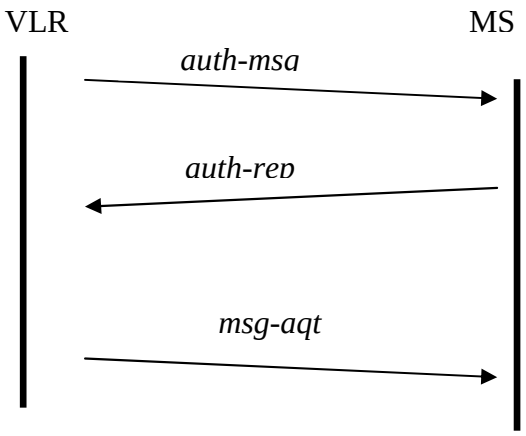

Fig.5. 3 : Le protocole CBA

Etape 1 :

A chaque demande de service par MS, le VLR utilise le TID de MS pour trouver les données associées au MS comme la courbe elliptique, point de référence P et la clé partagé***ki***.

Le VLR génère un message d'authentification *auth-msg* qui contient un point aléatoire R1, R1= aP, de la courbe elliptique et leur certificat *CertVLR*. Ce message est crypté par ***ECIES*** en utilisant la clé partagée entre le réseau et l'unité mobile ***ki*** fournis dans la phase d'enregistrement. Le message crypté est envoyé au MS.

A la réception du message crypté, MS le décrypte en utilisant la clé ***ki*** puis, elle vérifie la validité du *CertVLR* par $\boldsymbol{KU_{HLR}}$, si elle est valide, MS fait le processus suivant :

- Elle calcule la clé partagée avec le VLR $\boldsymbol{k_c}$, $k_c = KR_{MS}KU_{VLR}$ (KU_{VLR} est consulté du certificat).
- Elle calcule $R1` = R1 + k_c$
- Elle choit un $b \in GF(p)$ et calcule bP = R2.

Pour répondre sur le message d'authentification envoyé par VLR, MS construit un message de réponse *auth-resp* qui contient leur certificat *CertMS*, $R1`$ et R2.

Auth-resp = (CertMS, $R1`$, $R2$) est chiffré par ***ECIES*** en utilisant la clé $\boldsymbol{KU_{VLR}}$.

Etape 2 :

VLR décrypte le message par son clé privé $\boldsymbol{KR_{VLR}}$, il vérifie la validité de *CertMS* en utilisant $\boldsymbol{KU_{HLR}}$, si elle est valide, il :

- Calcule la clé commune avec MS k_c, $k_c = KR_{VLR}KU_{MS}$ (KU_{MS} est consulté du certificat).
- Calcule R1= $R1`$- k_c.

Si R1 trouvé est équivalent à R1 envoyé, ceci implique que la clé secrète de MS est valide, ce n'est pas d'un cas d'usurpation d'identité. Donc VLR a bien authentifié MS. Il va envoyer un acquittement d'authentification au MS et génère la *clé de la prochaine session*.

En suite le VLR:

- Calcule $R2`= R2 + k_c$.

Le VLR génère en suite un ticket qui est une structure de donnée contient : le ID de MS, la date de création, la date d'invalidation de ticket et la signature du VLR.

Ms-id: F904.6001.B270.9845
The issue date: 10/11/2011
The end-date: 15/11/2011
VLR-sign: D0F4

Fig.5. 4 : Le ticket

le VLR envoi le message d'acquittement qui contient (ticket,$R2`$) crypté par $\boldsymbol{KU_{MS}}$.

Pour la préparation à la prochaine session, Le VLR calcule la nouvelle clé par Elliptic Curve Diffie-Hellman **ECDH** à partir de *R2*.

$k_1 = aR2$.

Etape3 :

Après la réception du message d'acquittement MS le déchiffre par sa $\boldsymbol{KR_{MS}}$, elle déchiffre $R2`$ pour trouver R2, $R2 = R2`- k_c$.

Si R2 trouvé correspond au R2 envoyé, ceci implique que la clé secrète de VLR $\boldsymbol{KR_{VLR}}$ est valide, ce n'est pas d'usurpation d'identité de VLR. Donc MS a bien authentifié le VLR.

la MS va enregistrer le ticket et calcule la nouvelle clé par **ECDH** à partir de *R1*.

$k_1 = bR1$.

2.2.2. *Authentification à base de ticket*

Ce protocole est utilisé en cas de demande de service au sien de la même zone de localisation où le ticket est valable. C'est un protocole d'authentification symétrique basé sur l'algorithme *Advanced Encryption Standard (*AES*).*

On peut expliquer le fonctionnement de ce protocole dans deux étapes :

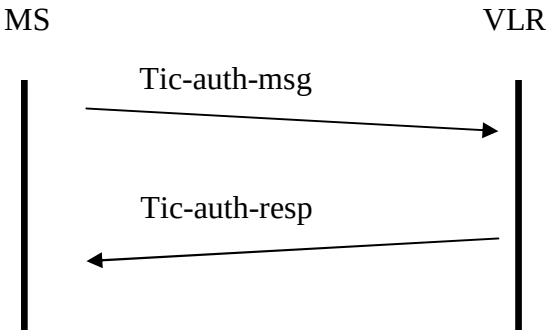

Fig.5. 5: Le protocole TBA

Etape 1 :

A chaque demande ou réception d'un service par l'unité mobile, elle construit un ticket authentication message *Tic-auth-msg* contien R1= aP (a est choisis aléatoirement), et le ticket générer par le VLR à la fin d'exécution du CBA. Le message en suite est crypté par l'algorithme AES utilisant la clé k_0 généré pandant la dernière session (on change la clé à chaque session pour augmenter la sécurité).

Tic-auth-msg = $(\text{ticket}, R1)_{k0}$

Après la réception du message, le VLR utilise le TID pour trouver la clé k_0 et le ticket de MS et vérifier si ce dernier est valable. Si le ticket est valable et valide, MS est donc authentifiée avec succès au VLR.

Le VLR construit *ticket authentification response Tic-auth-resp* qui contient R2= bP (b est choisis aléatoirement) et R1. Le cryptage est aussi réalisé par AES en utilisant toujours la clé k_0 $(R1, R2)_{k0}$.

Si le ticket est invalide ou non valable (heur date), le VLR demande de MS de refaire le protocole d'authentification à base de certificat CBA.

Etape 2:

Après la réception du message *Ti-auht-resp*, l'unité mobile utilise le k_0 pour décrypter le message, ensuite elle vérifier si R1est correct. Si oui, ce signifier que le VLR a la clé partagé correcte, donc MS a authentifié le réseau et elle construit la clé de la prochaine session K_1, K_1 est calculé à base d' **ECDH**, $K_1 = aR2$

Le VLR calcule aussi la clé de la prochaine session K_1 à base d' **ECDH** , $K_1 = bR1$.

3. Analyse de sécurité

Les performances de *HAPMON* seront évaluées par rapport aux conditions de sécurité suivantes :

3.1.Confidentialité

Dans *HAPMON*, tous les messages échangés entre les MS et le réseau sont chiffrés, rien et envoyé en claire. Le chiffrement est réalisé par ***ECIES*** en cas d'authentification à base de certificat et par ***AES*** en cas d'authentification à base de ticket. Donc la confidentialité des messages échangés est totalement assurée.

L'utilisation de la clé de session fondée sur la cryptographie elliptique ne donne pas aux intrus le temps pour calculer la clé à cause de la difficulté de résolution du problème de logarithme discrète, ce qui augmente la confidentialité des messages.

3.2.Non-répudiation

Même sans employer la signature numérique, le protocole proposé peut assurer la non-répudiation au moyen de certificat électronique et la vérification de la domination de la clé privée. Cette technologie permet de prouver l'identité d'un nœud par la prouve de la possession de la clé privée associé à la clé publique indiquée dans le certificat.

HAPMON fournit la non-répudiation d'origine des données envoyées par le MS au réseau et vice versa.

3.3.Authentification mutuelle explicite

Par contre plusieurs protocoles d'authentification comme celui des réseaux GSM, Notre protocole assure une authentification mutuelle.

Dans *HAPMON*, l'authentification mutuelle est explicitement exprimée, elle consiste à confronter aux attaques de type Man-in-the-Middle.

L'authentification mutuelle entre MS et VLR est accomplie, si chaque un des deux a prouvé à l'autre qu'il possède la clé partagée correcte $\mathbf{K_c}$.

3.4.Resistance à l'attaque par dictionnaire

Le protocole proposé est capable d'assurer la protection contre l'attaque par dictionnaire sur la clé partagée. Même avec la connaissance de la courbe elliptique, le point de référence et la clé publique de MS et du VLR, un adversaire ne peut pas effectuer l'attaque par dictionnaire pour obtenir la clé de session, parce que le temps qu'il faudrait pour trouver la clé de session (temps de résolution du problème du logarithme discrète) est jugé supérieur au délai de sécurité voulu.

Conclusion

La difficulté de sécuriser un réseau de mobiles est due à la limite des capacités des nœuds de réseau en matière de ressource. En particulier, un protocole d'authentification dédié aux réseaux de mobile est un problème qui a été abordée par de nombreux chercheurs, mais les résultats n'atteint pas encoure à l'optimale.

Dans ce travail, on a présenté un protocole d'authentification dédié aux réseaux de mobiles, il appartient à la famille des protocoles hybrides.

Ce protocole, consiste à assurer une authentification mutuelle entre le réseau et les nœuds mobiles, ce qui mène à une confiance totale pendant les communications entre eux.

Le protocole est caractérisé par l'introduction de la cryptographie elliptique, qui est basé sur la difficulté de résolution du problème de logarithme discret. Cette difficulté détermine la force de sécurité de notre protocole.

Chapitre 6 : Implémentation Et Analyse Des Performances

Introduction

A fin d'évaluer les performances de schéma d'authentification proposé, nous avons implémenté son fonctionnement sous J2ME. Nous avons attitré la bibliothèque Bouncy Castle comme un fournisseur des opérations de la cryptographie elliptique.
A fin de tester les performances de notre protocole, nous avons choisi de le comparer avec les protocoles elliptiques et non elliptiques les plus connus.

1. Présentation de J2ME

La plateforme Java 2, Micro Edition (J2ME) est la 2ème révolution dans l'histoire de Java, l'utilisation du Java sur les serveurs était la 1 ère révolution de Java **[57]**. La deuxième révolution est l'explosion des petits dispositifs Java.
J2ME est une JRE (Java Runtime Environment) pour les appareils embarqués comme les téléphones portables, agendas électroniques, systèmes de navigation et autres. Il est constitué d'un ensemble d'API standards définis par un groupe d'experts. Il fournit la puissance et les avantages de la technologie Java pour des dispositifs embarqués ou mobiles ; c.-à-d. une interface utilisateur flexible, un modèle de sécurité robuste, une palette de protocoles réseaux intégrée et une gestion des applications locales et réseaux. **[65]**

J2ME est divisée en configurations, profils et des APIs optionnelles (extensions) qui fournissent des informations spécifiques sur les différentes familles de dispositifs. Des configurations et des profils permettent de personnaliser le JRE. Les configurations sont constituées d'une machine virtuelle et d'un ensemble minimal de classes. Elles fournissent ainsi les fonctionnalités de base pour des dispositifs aux caractéristiques semblables. Actuellement, il existe 2 configurations J2ME, CLDC (Connected Limited Device Configuration) et CDC (Connected Device Configuration).
La CLDC est conçue pour des dispositifs à la capacité de mémoire restreinte, pour des processeurs lents et des connexions au réseau intermittentes, y est associée une machine virtuelle, KVM, prévue pour ces ressources limitées.
La configuration CDC, contenant une machine virtuelle CVM, est adressée à appareils plus conséquents, tels des PDA avancés, des TV numériques interactives, des tablettes d'accès à Internet…**[57] [65]**

Alors que les configurations fournissent le fondement d'une application, les profils définissent leur structure. La couche profil est ajoutée au sommet d'une configuration. Elle définit un ensemble d'APIs et de spécifications nécessaire pour développer des applications pour une

famille particulière de dispositifs mobiles. Il s'agit de bibliothèques de classes conçues pour une configuration donnée et apportant des fonctionnalités et spécificités supplémentaires.
Il existe deux profils de référence J2ME; Fondation destiné à la CDC et MIDP (Mobile Information Device Profile), destiné à la CLDC.

Le profil Fondation est une spécification pour les dispositifs qui supportent une connexion réseau riche dans l'environnement J2ME. Ce profil ne supporte pas l'interface utilisateur.

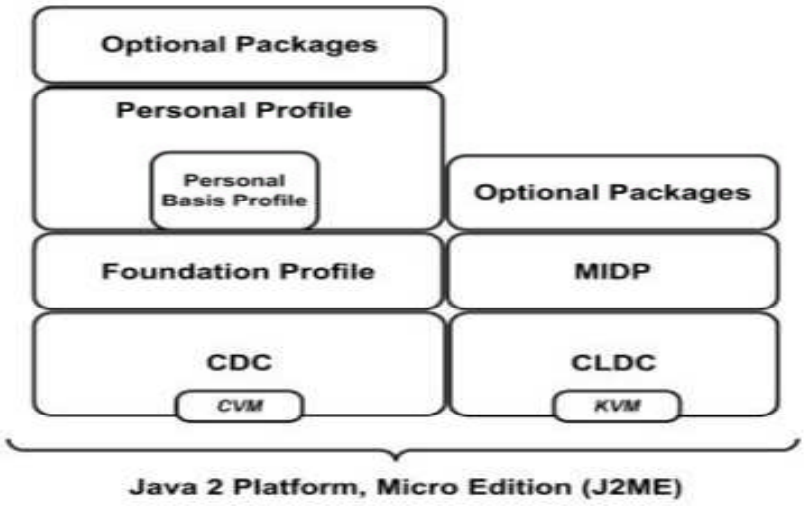

Fig.6. 1. L'architecture de J2ME **[57]**

Autres profils peuvent s'ajouter au dessus du profil fondation pour ajouter l'interface utilisateur et autres fonctionnalités. Ces profils sont *Personal Basis Profile* et *Personal Profile*. La combinaison de *CDC + Foundation Profile + Personal Basis Profile + Personal Profile* est désignée comme la génération future de l'environnement d'exécution de l'application personnelle Java **[57]**.
Le profil MIDP répond à des exigences de mémoire (128 ko de mémoire volatile, 8ko de mémoire persistante, 32ko de mémoire volatile pour la machine virtuelle), d'affichage (96×54 pixels), Des capacités d'entrée de données (*keypad*, *keyboard*, ou *touch screen*) et des connexions réseau bidirectionnelle, probablement intermittente. Le monde J2ME actuellement est couvert par *MIDP* sur les petits dispositifs et *Personnal Profile* sur les dispositifs les plus puissants.

Le package *MIDlet* définit les applications MIDP, les interactions entre ces applications, et l'environnement dans lequel l'application s'exécute. Une application MIDP est appelée *MIDlet*,

elle est le pendant des applets ou servlets pour J2ME. Plusieurs *MIDlets formant* une suite, peuvent être empaquetées ensemble pour partager des ressources d'une seule JVM.
Des bibliothèques personnelles peuvent être ajoutées par les constructeurs, au-dessus des profils. Par exemple le paquetage le plus courant est celui gérant la technologie Bluetooth. Mais ces fonctionnalités sont souvent propriétaires et leur utilisation limite donc la portabilité. **[65]**

2. Présentation de bouncy castle

Bouncy Castle est une librairie qui implémente différents services cryptographiques. Il est Australien d'origine donc il n'est pas concerné par les restrictions américaines sur l'exportation des logiciels cryptographiques.
Bouncy Castle existe en deux implémentations, une en Java et l'autre en C#. Il contient aussi une API légère (*lightweight*) appropriée à l'environnement mobile J2ME/MIDP.
Bouncy Castle est un package libre et open-source, il ressemble à la librairie C *openssl* qui est conforme aux différents standards en vigueur. *Bouncy Castle* n'est pas installé de base sur les plateformes java. Le package BC peut être téléchargé du site *http://www.bouncycastle.org/* dans un seul module comprenant le provider JCE, l'API lightweigth, J2ME et JDK, ou dans des modules séparés.
La version Java de la librairie est essentiellement un "provider" pour le "Java Cryptography Extension" (JCE), autrement dit, une implémentation d'algorithmes de chiffrement, de signatures numériques, de "Message Authentication Codes" (MAC), de fonctions de hachage, d'algorithmes de génération de clés, etc. L'API suit donc l'interface définit dans la "Java Cryptography Architecture" (JCA). **[66]**
En dehors du provider, Bouncy Castle propose aussi plusieurs librairies supplémentaires, la plus importante est la librairie contenant les classes de tests.
Bouncy supporte aussi les services suivants **[57]**:

- Les certificats X.509 : Le provider Bouncy Castle peut lire les certificats X.509 (v1, v2 ou v3). En plus des classes dans le package org.bouncycastle.asn1.x509 pour la génération de certificat, une autre classe JCE est fournie dans le package org.bouncycastle.x509, et elle supporte les certificats RSA, DSA et ECDSA.
- Support de classes pour les courbes EC : Le package BC a aussi des classes supplémentaires pour supporter les courbes elliptiques (clés et paramètres EC). Nous trouvons ces classes dans les packages suivants : org.bouncycastle.jce.spec, org.bouncycastle.jce.interfaces, et org.bouncycastle.jce.

3. Modèle d'implémentation

A fin de valider notre travail, on a recourir au J2ME qui est, actuellement, le meilleur environnement pour tester des applications destiné aux environnements mobiles. Plus qu'il permet de développer des applications tout en respectant les ressources disponibles, il fournit aussi des packages qui offrent des services réseaux aux développeurs. Donc il est adéquat pour implémenter notre proposition.

Nous avons assigné le VLR comme un serveur, les stations mobiles comme des clients et la communication entre eux est s'établie par l'intermédiaire des sockets.

```
import javax.microedition.io.*;
import javax.microedition.midlet.*;
import java.io.*;

public class Server extends MIDlet implements Runnable {

public static int MYECHOPORT;

public void run() {
ServerSocketConnection s = null;
try {
s = (ServerSocketConnection)Connector.open("socket://:" +
MYECHOPORT);
} catch(IOException e) {
        ……..
}
while (true) {
try {
   // Wait for a connection.
SocketConnection sc = (SocketConnection) s.acceptAndOpen();
//traitement de socket
handleSocket(sc);
} catch(IOException e) {
      ……..
}
}
}

public static void handleSocket(SocketConnection incoming)
throws IOException {
        ……..
        ……..
                        }
}//server
```

Server Socket

```
import javax.microedition.io.*;
import javax.microedition.midlet.*;
import java.io.*;

public class Clien extends MIDlet implements Runnable {

public static int MYECHOPORT;

public void run() {
String address;
SocketConnection sock = null;
DataInputStream din = null;
DataOutputStream dout = null;
Try{
sock = (SocketConnection) Connector.open("socket://" +
address + ":" + MYECHOPORT);
din = sock.openDataInputStream();
dout = sock.openDataOutputStream();
} catch(IOException e) {
      ……
}

// Just send and receive a few messages,
String response = null;
try {
dout.writeUTF("message");
response = din.readUTF();
} catch(IOException e) {
      ……
}

}//client
```

Client Socket

4. Analyse de performances et de sécurité

A fin de bien apparaitre les performances de notre proposition, on va le comparer avec les protocoles basés sur la cryptographie elliptique et la cryptographie classique les plus renommés. Ils sont **[65]** :

- Aziz et al's protocol: conçu pour empêcher les accès non autorisés dans les réseaux sans fil, il est basé sur le crypto-système RSA. La taille de la clé est 1024 bits.
- Beller-Chang-Yacobi's protocol: crée à fin d'assurer l'ésotérique et l'authentification sur les systèmes de communications mobiles, il est basé sur Rabin crypto-système. La taille de la clé est 1024 bits.
- Aydos protocol: proposé pour les réseaux de 3ème génération, il est basé sur une bibliothèque ECC (crée spécialement à cette fin) qui est capable d'accomplir des opérations de génération et de vérification de signature ECDSA sur lesquelles le protocole est basé. La taille de la clé est 192 bits.

La charge de calcule, l'exigence en espace de stockage et bande passante mesurés à coté des stations mobiles sont les paramètres de comparaison à effectuer.

Récemment, il est prouvé qu'un système RSA de 1024 bit et un système ECC de 160 bits offrent le même niveau de sécurité. C'est pour cette raison, on a implémenté notre système avec une clé de 192 bits et plus qui offre une sécurité semblable, plutôt très forte.

Les résultats obtenus sont résumés dans le tableau suivant :

Protocole		***Bande passante (bits)***	***Stockage (bits)***
Beller-Chang-Yacobi (1024-bit)		8320	5120
Aziz-Diffie (1024-bit)		8680	2176
Aydos (192-bit)		1922	1632
HAPMON (192-bit)	TBA	1256	1400
	CBA	2168	1664

Tab.6. 1. : Les résultats obtenus

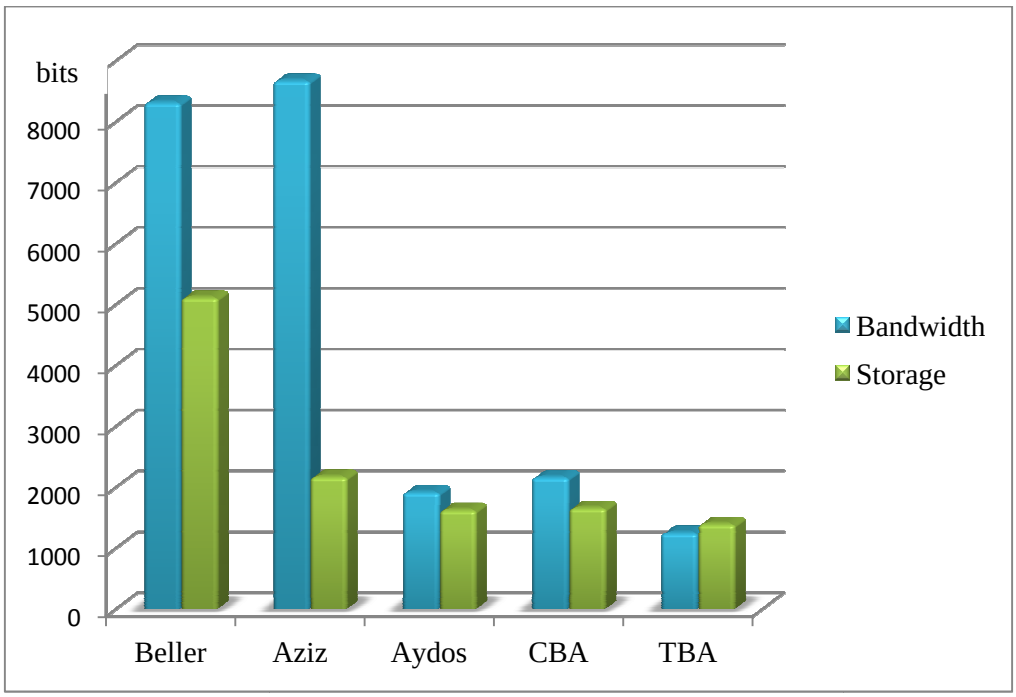

Fig.6. 2 : Comparaison de HAPMON avec d'autres protocoles.

A partir de la figure ci-dessus, on peut observer la grande différence entre HAPMON, basé sur la cryptographie elliptique, et les protocoles non elliptiques (Aziz & Beller). Cette différence clarifie bien l'impacte de l'introduction de la cryptographie elliptique dans la sécurisation des réseaux de mobiles.

On peut observer aussi, la petite différence entre notre protocole d'authentification à base de certificat (**CBA**) et le protocole elliptique *d'Aydos*. Cette différence s'explique par le fut qu'Aydos utilise uniquement ECDSA et opère sur des points d'une courbe elliptique pour authentifier les nœuds du réseau. Il est considéré comme un protocole symétrique, par contre CBA (protocole asymétrique), il est basé sur l'utilisation du certificat qui est une structure de données très complexe et exigeante.

L'analyse de la charge de calcul dans ces protocoles nous permet de dresser le tableau ci-dessous.

Les significations des symboles ci-dessus sont comme suit :

PKE: Public Key Encryption

PKD: Public Key Decryption

eP : Point Multiplication

ECDSAV: Elliptic Curve Digital Signature Algorithm Verification

SKE: Secret Key Encryption or Decryption

ECIES: Elliptic Curve Integrated Encryption Scheme

ECAES: elliptic curve AES.

Protocole		**Charge de calcule**
Beller		2 PKE + 1PKD + Pre-computation
Aziz		3 PKE + 2 PKD
Aydos		1 eP + 1 ECD-SAV + 2 SKE +1 SHA
HAPMON	CBA	1 ECAES dec + 2 ECIES
	TBA	1 ECAES enc + 1 ECAES dec

Tab.6. 2 : Résultat d'analyse de la charge de calcule

Il est clair que notre schéma à un modeste charge de calcul comparant aux autres puisqu'il nécessite, à coté des stations mobiles, uniquement une opération de cryptage par ECAES et 2 opérations cryptage/décryptage ECIES dans le cas de protocole d'authentification à base de certificat (CBA) et uniquement une opération de cryptage et une autre de décryptage par ECAES dans le cas de protocole d'authentification par ticket(TBA). Les autres protocoles sont basés sur la cryptographie classique (RSA, Rabin, SHA) qui nécessite des opérations très complexes.

Conclusion

Dans ce chapitre, on a effectué quelques mesures de performances pour évaluer l'efficacité et la sécurité du schéma proposé (HAPMON), on a réalisé notre implémentation en utilisant l'environnement J2ME, on a basé sur des métriques de base tels que l'exigence en matière d'espace de stockage et de bande passante et la charge de calcule.

Les résultats obtenus démontrent que notre schéma a de meilleures performances par rapport aux autres. Ces performances sont obtenues grâce à l'introduction de la cryptographie elliptique, cependant la fiabilité de notre proposition est totalement dépendue de cette cryptographie.
Les résultats montrent aussi que notre schéma est capable d'offrir un niveau de sécurité adapté à l'enjeu de la communication dans un environnement mobile.

Conclusion générale et perspectives

Les réseaux de mobiles prennent une place de plus en plus prépondérante dans les réseaux de communications sans fil. L'existence d'un certain nombre de contraintes (liberté totale de mouvement, vulnérabilité du medium, limite de ressources…) rendant difficile la tâche de conception et de développement des mécanismes de sécurité.

Dans ce travail, on a analysé le problème de sécurité dans les réseaux de mobiles. On a trouvé que l'authentification est la brique de base de la sécurité. En conséquence, nous nous sommes intéressés à la proposition d'un schéma d'authentification toute en respectant les contraintes de l'environnement mobile.
L'étude, qui a porté sur l'analyse des protocoles existants, nous a permis de faire ressortir un ensemble de problèmes. Afin de les résoudre, nous avons conçu un nouveau protocole d'authentification que nous avons appelé HAPMON.

HAMPON se base sure une idée qui diffère des autres protocoles d'authentification de la même famille. C'est une suite de deux protocoles, l'un est basé sur le certificat et l'autre est basé sur le concept de ticket, où le choix d'un tel protocole dépend de certains paramètres.
L'idée de base consiste à intensifier le contrôle dans le premier protocole puis le soulager pendant le deuxième qui est le fréquemment utilisé.

HAPMON est basé sur la technique de cryptographie à courbe elliptique ECC, ce qui représente l'un des points forts de notre protocole. Le crypto système ECC a l'avantage d'offrir les tailles de clé les plus petites comparé aux autres crypto systèmes traditionnels, mais avec le même niveau de sécurité. Cette caractéristique rend le crypto système ECC plus attractif sur les dispositifs mobiles sans fil contraints en ressources, il permet une économie en calcul CPU, en consommation d'énergie et en bande passante.

Les résultats de comparaison avec des protocoles elliptiques et non elliptiques selon un certain nombre de paramètres mesurés à coté des stations mobiles encouragent et montrent les performances et la validité de notre schéma. HAPMON a montré qu'il n'est pas capable de garantir uniquement l'authentification, mais il assure aussi les conditions principales de la sécurité telles que la confidentialité, l'intégrité et la non-répudiation.

Tant que la plupart des dispositifs mobiles sont équipés par les moyens d'acquisition de données biométriques (caméra…), comme perspectives à notre travail, nous prévoyons de nous orienter vers l'authentification par des systèmes biométriques qui sont de plus en plus utilisés

depuis quelques années. Il est prouvé qu'ils sont capables d'éviter la fraude d'une manière simple et efficace.

En conclusion, notre travail a permis de résoudre un certain nombre de problèmes rencontrés dans le processus d'authentification dans les réseaux de mobiles. Notre proposition présente des performances plus optimales par rapport à d'autres protocoles étudiés.
L'amélioration et l'enrichissement des mécanismes de sécurité dans les réseaux de mobiles, permettent le succès des services offerts et donc une plus large utilisation de ce type de réseau.

Références

[1] : ATHMANI Samir ; *Protocole de sécurité pour les réseaux de capteurs sans fil* ; mémoire de magistère ; P : 9-13; 2010.

[2] : Guy Pujolle ; *les réseaux, Edition 2011* ; livre ; P : 195-218.

[3] : www.ComentCaMarche.net; site de documentation informatique ; 2005.

[4] : THIERRY Bohbot ; *Les Reseaux Sans Fil Et Les Problemes De Securite* ; rapport de mastère ; P : 1-12 ; 2009-2010.

[5] : Pujolle, Vivier, Al agha ; *Réseaux De Mobiles Et Réseaux Sans Fils* ; livre ; 2001.

[6] : Sidi-Mohammed SENOUCI ; *Application De Techniques D'apprentissage Dans Les Réseaux Mobiles* ; thèse de doctorat ; université de pierre et marie curie – paris 6 ; 2003

[7] : JOCHEN Schiller ; *Mobile Communication* ; livre, Second edition, P : 1-23 2003.

[8] : Samuel Pierre *; Réseaux et systèmes informatiques mobiles* ; livre ; P : 3-35 ; 2002.

[9] : Nicolas SIMON ; *Sécurité Dans Les Smartphones* ; mémoire de Licencié en Informatique ; Université Libre De Bruxelles ; P : 11-37 ; 2006-2007.

[10] : http://3lrvs.tuxfamily.org/582.pdf, mars 2011.

[11] : Antoine Gnansounou ; *Architecture Et Fonctionnement Des Reseaux Mobiles Gsm* ; Cour, 2009.

[12] : M. BENJAMIN Savouré ; *la téléphonie mobile : Technologies, Acteurs et usages* ; mémoire de mastère 2 de recherche ; P : 5-22 ; 2005-2006.

[13] : GARAH Messaoud ; *Minimisation De La Probabilité D'échec Du Handover Dans Les Reseaux Cellulaires Mobiles*, thèse de doctorat ; université de BATNA ; P : 10-28 ; 2010.

[14]: Boyinbode O. K. and Akinyede R. O.; *Mobile Learning: An Application Of Mobile And Wireless Technologies In Nigerian Learning System*; article; IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.

[15]: www.convertigo.com/fiche-mcommerce.pdf, février 2011.

[16] : Emin Islam Tatlı; *Security in Context-aware Mobile Business Applications*; thèse de doctorat, université Mannheim(Turk) ; P: 11-15; 2008.

[17] : Achraf AYADI ; *Innovation Technologique Dans Les Reseaux Mobiles Et Creation De La Valeur: Cas De La Banque Mobile* ; article ; Laboratoire de Management Interdisciplinaire Transculturel GET/Institut National des Télécommunications France; 6-8 octobre 2004.

[18] : Wen-Chen Hu, Chung-wei Lee et Weidong Kou; *Advances In Security And Payment Methods For Mobile Commerce*; livre; P: 194; 2004.

[19]: www.extelia.fr/servicemobile.pdf, 2011.

[20]: Nguyen Tien Thinh ; *Système D'exploitation Pour Les Mobiles* ; Travail Personnel Encadré, institut de la francophonie pour l'informatique ; P : 9-13 ; Juillet 2009.

[21]: YANG XIAO, XUEMIN SHEN & DING-ZHU DU, **"**Wireless Network Security**"**, livre, P: 181- 242, 2007.

[22]: Abdesselem BEGHRICHE ; **"**De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc**"**, mémoire de magistère; P : 1-18, 2008-2009.

[23] : D^{r}. Nada Meskaoui, Nagi Wakim ; **"**Une approche techniques biométriques/agents pour la Sécurité des réseaux informatique**"** ; Rapport ; 2006.

[24]: Robert Eriksson; Security and usability in the mobile context, mémoire de mastère, 2007.

[25]: Laurent Bloch & Christophe Wfhugel, **"**Sécurité informatique : Principes et méthode**"** livre, édition 2, P : 4- 32, 2009.

[26]: Eva Blomqvist, "Security In Sensor Networks", Rapport, Helsinki University of Technology Control Engineering Laboratory, P: 14-29, 2003.

[27] : Cédric Llorens, Laurent Levier & Denis Valois, **"**Tableaux de bord de la sécurité réseau**"**, livre, édition 2, P : 3-145, 2006.

[28] : Ahmed Serhrouchni; **"** Mesure de la sécurité "logique" d'un réseau d'un opérateur de télécommunications**"** ; thèse de doctorat; école nationale supérieurs de la télécommunication Paris, P : 21-33, 2005.

[29] : Mourad BAGHDADI ; **"**Gestion de la mobilité dans un réseau de senseurs sans fil WSN**"** ; Thèse ; école supérieurs des communications, Tunus, 2005.

[30] : http://www.ssi.gouv.fr/archive/fr/reglementation/netsec_fr.pdf , **"**Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne**"**, rapport, 2011.

[31] : Gay pujolle et Davor Males, **"**WI-FI par la pratique**"**, livre, P : 79-101, septembre 2002.

[32] : Noureddine CHAIB, **"**La sécurité des communications dans les réseaux VANET**"**, mémoire de magistère, P : 11-28, 2010.

[33] : François LESUEUR ; **"**Sécurité dans les réseaux Pair-à-Pair**"** ; Rapport ; 2006.

[34] : Amélie Désandré, Benjamin Kittler, Romain Loutrel et Thomas Renaudin ; **"**Sécurité Informatique**"** ; Rapport, Novembre 2004.

[35]: Ali I. Gardezi, **"**Security In Wireless Cellular Networks**"**, article, April 23, 2006.

[36]: Igor Bilogrevic, Murtuza Jadliwala and Jean-Pierre Hubaux, **"**Security Issues in Next Generation Mobile Networks: LTE and Femtocells**"**, article, Laboratory for computer Communications and Applications (LCA1) EPFL Lausanne Switzerland, 2010.

[37]: Alaaedine CHOUCHANE, **"**Detection and Reaction against DDoS Attacks in Cellular Networks**"**, projet de fin d'étude, The Communication Networks and Security Research Laboratory, l'école supérieur de communication de Tunis, P: 4-23, 2006- 2007.

[38]: http://www.securiteinfo.com/Le+Grand+Livre+Ge+La+Sécurité+Informatique.pdf, **"**Le grand livre de la sécurité informatique**"**, livre, P : 1-62, 18 février 2002.

[39]: Praphul Chandra ; **"**Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security**"**, livre, P: 1-158; 2005.

[40]: SOSA CARBAJAL, Carla Lisette ; **"**Evolution Des Réseaux Sécurisés, Projet Bibliographique**"** ; Université Des Sciences Et Technologies De Lille 1; P : 1-27, 2009-2010.

[41] : http://www.efort.com/SECURITE_MOBILE_EFORT.pdf, **"**Sécurité Mobile 2G, 3G et 4G: Concepts, Principes et Architectures**"**, rapport, P : 1- 10, 2010.

[42] : Michel Riguidel, **"**La sécurité des réseaux et des systèmes**"**, rapport, ENST PARIS, P: 28-29, 2005-2006.

[43]: Saikat Chakrabarti, Venkata C. Giruka and Mukesh Singhal; *Security in Distributed, Grid, Mobile and Pervasive Computing, livre, P: 87-108*, 2006.

[44]: John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary; **"**Wireless Sensor Network Security: A Survey**"**; livre; 2006.

[45] : Z. MAMMERI ; Sécurité dans les réseaux; Cours de Réseaux, Université Paul Sabatier (Toulouse III) ; 2008.

[46]: P.G.RAJESWARI, K.THILAGAVATHI, "A Novel Protocol For Indirect Authentication In Mobile Networks Based On Elliptic Curve Cryptography ", Article, Journal of Theoretical and Applied Information Technology, 2009

[47] : Dhia Hachicha, Conception et développement d'un système d'authentification forte par SMS; projet de fin d'études, école supérieur de communication du Tunus ; 2005.

[48] : Joseph Illand ; La sécurité des systèmes d'information : un enjeu réaffirmé ; Fonctionnaire de Sécurité de Défense ; 2003.

[49]: Steve Schneider, Verifying Authentication Protocols in CSP, article, IEEE Transactions On Software Engineering, VOL. 24, NO. 9, September 1998.

[50]: Anand R. Prasad and Seung-Woo Seo ; Security in Next Generation Mobile Networks: SAE/LTE and WiMAX; livre, P: 14-18; 2011.

[51]: Solanki Jigar, Akpakpo Brunel, Authentification D'utilisateur : Gestion Des Identites, cours, Universite Sciences Et Technologies Bordeaux 1 ; 2007.

[52] : Caline Villacres , L'Authentification de A à Z ; rapport ; 2003.

[53] : Pascal Gachet ; Sécurité et PKI ; livre ; P : 17-24 ; 2002.

[54] : Carine BERNARD, L'utilisation De La Signature Électronique Au Cnrs, rapport de stage, 2004.

[55] : Jean-Luc Archimbaud ; Certificats (électroniques) Pourquoi ? Comment? rapport (V3), Décembre 2000.

[56]: Ivan Stojmenović, Handbook of wireless networks and mobile computing, livre, P: 315-318; 2002.

[57] : EUSCHI Salah, " La Sécurité des Applications M-commerce : Problématiques et solutions ", mémoire de magistère, université de ouargla, 2011.

[58]: Hagler Michael, " Courbes elliptiques et cryptographie ", raport, 19 février 2006.

[59]: GUILLAUME Dubach, " Courbes elliptiques et cryptographie asymétrique", Article, Séminaire De Mathématiques Des Elèves, 18 mars 2009.

[60]: Robert Rolland, " Courbes elliptiques et cryptographie", rapport, C.N.R.S., Institut de Mathématiques de Luminy.

[61]: Nicolas Méloni," Arithmétique pour la Cryptographie basée sur les Courbes Elliptiques", Thèse de Doctorat, Université Montpellier II, 24 septembre 2007.

[62]: Anoop MS, "Elliptic Curve Cryptography, An Implementation Guide", article, 2002.

[63]: Thierry Favre, " Cryptographie et courbes elliptiques", Projet de semestre, 31 mai 2011.

[64]: Michael Morrison, Wireless Java with J2ME in 21Days, P: 1- 123, livre, 2001.

[65]: M. Aydos, T. Yanik, an K. Ko, High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor ,IEE Proceedings: Communications,Oct 2001.

[66]: **www.bouncycastle.org,** le site officiel de bouncy castle, mai 2012.