la sécurité dans les réseaux mobiles

1.1 Introduction

Avec l'évolution de la technologie, 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.

L'évolution récente des moyens de communication mobile 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, Ces caractéristiques ont un impact direct sur la sécurité de l'information.

Dans ce chapitre, nous allons présenter les réseaux mobiles dont nous allons parler de leurs classifications, leurs générations, leurs caractéristiques et leurs domaines d'applications. Nous allons parler de même de la sécurité des réseaux mobiles tel que les services de la sécurité et ses obstacles, les attaques des réseaux mobiles et enfin les mécanismes de sécurité.

1.2 Généralités sur les réseaux mobiles

1.2.1 Les réseaux informatiques

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau, Les réseaux personnels, ou PAN (Personal Area Network),Les réseaux locaux, ou LAN (Local Area Network),Les réseaux métropolitains, ou MAN (Metropolitan Area Network),Les réseaux régionaux, ou RAN (Regional Area Network) et Les réseaux étendus, ou WAN (Wide Area Network). [1]

1.2.2 Les réseaux sans fil

Un réseau sans fil comme son nom l'indique est un réseau dans lequel au moins deux périphériques (ordinateur, PDA, imprimante, routeur, etc.) peuvent communiquer sans liaison filaire. Les réseaux sans fil ont recours à des ondes radioélectriques au lieu des câbles habituels. Grace aux réseaux sans fil, l'utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu. [2]

1.2.3 Classification des réseaux sans fil

Les réseaux sans fil, se classent en deux catégories : ceux avec infrastructure (les modèles cellulaires), et ceux sans infrastructure ou réseaux Ad hoc. [3]

1.2.3.1 Le mode avec infrastructure

En mode infrastructure chaque nœud (appareil..) 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* (*basic service set*, noté **BSS**) et constitue une cellule. Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement, 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. Cette caractéristique de passer de façon transparente d'un point d'accès à un autre est appelée itinérance (roaming). [2]

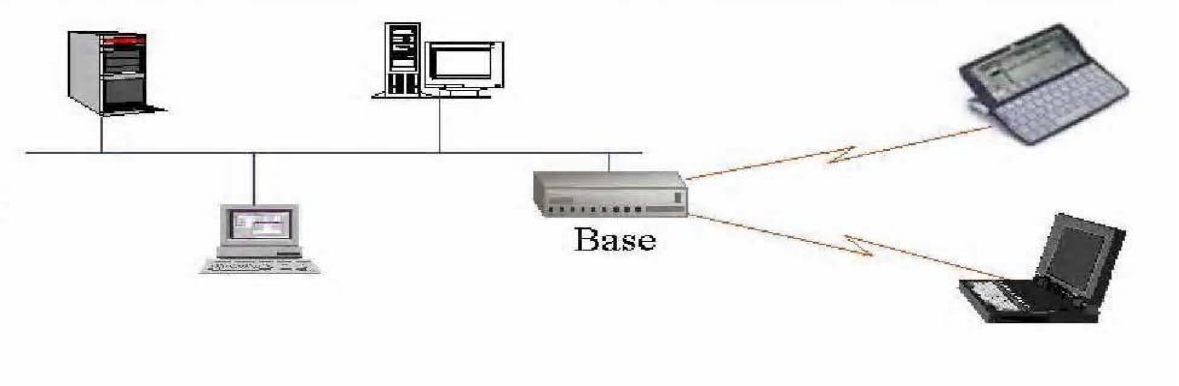

Figure 1.1 : Mode infrastructure.

1.2.3.2 Le mode Ad Hoc

Un réseau mobile Ad hoc, appelé généralement MANET (Mobile Adhoc NETwork) peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil, formant un réseau temporaire, sans l'aide de toute administration centralisée, que ce soit pour sa configuration ou pour sa gestion.

Les MANETs sont des réseaux, à peine initialisés, capables en un temps très court de communiquer indépendamment de la localisation. Dans un réseau Ad hoc les nœuds sont à un instant donné, des nœuds d'extrémité (émetteur et/ou récepteur) ou des nœuds de transfert (routeurs) qui participent à la découverte et à la maintenance des routes pour l'acheminement des paquets de données entre les nœuds d'extrémités. Chaque nœud mobile dans un réseau Ad hoc communique dans son rayon de portée, il est totalement autonome dans son déplacement. Le seul moyen de communication est l'utilisation des interfaces sans fil. [3]

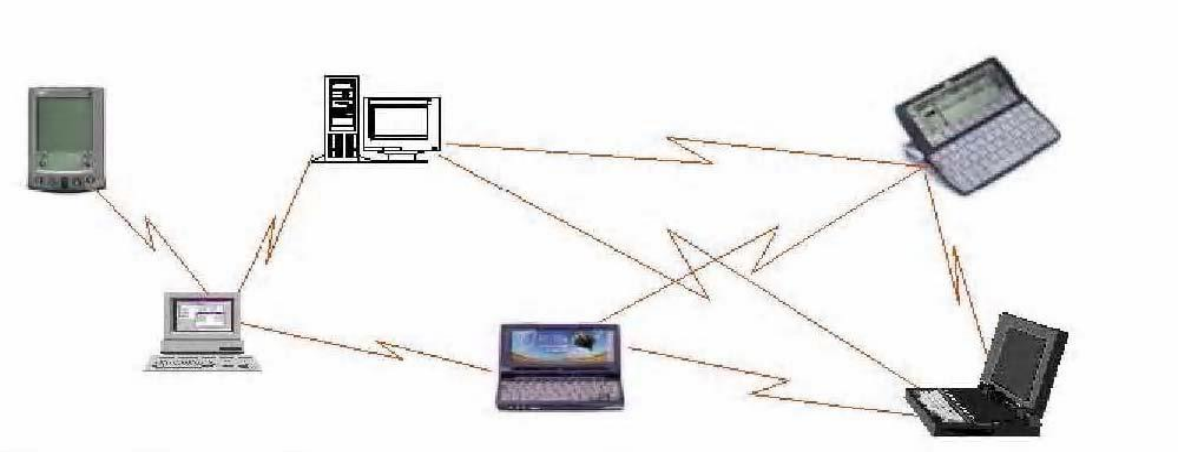

Figure 1.2 : Mode Ad hoc.

1.2.4 Définition des réseaux mobiles

Les réseaux mobiles sont des réseaux sans fil dans lesquels au moins deux terminaux peuvent communiquer sans liaisons filaires. Grace à ce type de réseau, un utilisateur (abonné) a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus au moins étendu, c'est la raison pour laquelle on parle de « mobilité ».[4]

Le réseau 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]

La majorité des réseaux mobiles font partie de la famille des réseaux cellulaires. En effet, Une cellule est une zone géographique dont tous les points peuvent être atteints à partir d'une même antenne. Lorsqu'un utilisateur d'un réseau cellulaire se déplace et change de cellule, le cheminement de l'information doit être modifié. Cette modification s'appelle un changement intercellulaire, ou handover. [6]

1.2.5 L'évolution des réseaux mobiles

Les réseaux mobiles ne cessent de s'évoluer depuis longtemps, Cette évolution peut être classée en cinq générations comme nous allons les décrire ci-dessous :

1.2.5.1 Première Génération (1G)

La première génération de réseaux mobiles est apparue à la fin des années 1970. Elle définit un réseau cellulaire, qui couvre des zones géographiques limitées, c'est-à-dire le territoire de l'opérateur. Le mobile communique par le biais d'une interface radio avec l'antenne centrale, jouant le rôle d'émetteur-récepteur de la cellule. L'émission des données sur l'interface radio est effectuée en analogique essentiellement dédies à la transmission de la voix. La première génération utilise la technique d'accès FDMA (Frequency Division Multiple Access), qui consiste à donner à chaque utilisateur qui le demande une bande de fréquences dans la cellule où il se trouve. [1]

De 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, ETACS (*Extended Total Access Communication* System) est une version améliorée du standard TACS qui permet l'utilisation d'un nombre plus important de canaux de communications. [2]

1.2.5.2 Deuxième Génération (2G)

La deuxième génération (notée 2G) a marqué une rupture avec la 1G grâce au passage de l'analogique au numérique .La norme permet la transmission de la parole et des données simultanément. Elle offre la possibilité aux utilisateurs de partager le même canal de transmission, ceci est possible grâce à l'utilisation de mécanisme de division de fréquence FDMA (Frequency Division Multiple Access) et le mécanisme de division de temps TDMA (Time Division Multiple Access). [2]

De nombreux systèmes 2G ont été développés, D-AMPS (Digital AMPS) compatible avec AMPS lancé par un groupe américain, GSM : lancé par un groupe européen, s'est vite imposé leader des réseaux de téléphonie mobile à l'échelle mondiale .Ce standard a vite donné naissance à ce qu'on l'appelle la génération 2.5 .C'est le réseau GPRS qui permet la transmission des données par paquets.

1.2.5.3 Troisième Génération (3G)

La troisième génération s'est implantée au tour des années 2000 avec un très fort déploiement à partir de 2005. Sa normalisation s'est effectuée sous le nom d'IMT 2000(International Mobiles Telecommunication for the year 2000), et du 3GPP. La première ouverture a été celle de NTT DoCoMo au Japon en octobre 2001.

La différence la plus sensible avec la deuxième génération concerne l'introduction du mode paquet à l'exception de la parole téléphonique, qui reste très semblable à celle du GSM. Toutes les informations, en dehors de la parole, sont mises dans des paquets et transportées dans un réseau à transfert de paquets .L'augmentation des débits est assez importante par rapport au GSM. Plusieurs types de modulations ont été étudiés pour l'émission numérique du signal. L'accès au canal radio utilise les techniques FDMA, TDMA et CDMA. [1]

1.2.5.4 Quatrième Génération (4G)

La quatrième génération est une révolution pour les réseaux hertziens par sa totale compatibilité avec le monde IP, de telle sorte qu'il n'y a plus aucune différence entre un réseau fixe et un réseau mobiles. Toutes les applications sont traitées avec le protocole IP, cette génération démarre avec le LTE Advanced(Long Terme Evolution Advanced), a introduit de très hauts débits pouvant aller jusqu'à 100 Mb/s, soit 3 ou 4 fois plus rapides que ceux de la 3G.[1]

Les internautes peuvent envoyer des fichiers lourds sans problème depuis leur utilisation des portables et des téléphones intelligents. Ils se connectent plus rapidement au

web et y naviguent en mode accéléré, en plus ils peuvent visionner des vidéos HD, envoient des courriers avec des pièces jointes et téléchargent des films, etc.

1.2.5.5 Cinquième Génération (5G)

De premières pré-5G sont en cours de réalisation, pour influencer les standards en cours d'étude et pour afficher l'avance technologique du pays qui teste cette nouvelle génération.

La 5G repose sur les trois grandes composantes suivantes :

- La bande étroite, ou NB (NarrowBand), correspondant à l'Internet des objets. Il semble simple de diminuer la capacité d'une communication. En réalité, cette propriété est très complexe à obtenir. Il s'agit de centaines de milliers d'objets connectés sur une même antenne, objets qui ne transmettent parfois pas un seul octet dans l'année, mais qui, dans le cas d'une transmission, doivent disposer instantanément d'un canal, comme les capteurs de détection d'incendie ou de sécurité dans le monde industriel.
- Les missions critiques permettent de prendre en charge des applications dont le temps de réaction est de l'ordre de la milliseconde. L'exemple le plus souvent cité est celui du V2V (Vehicle-to-Vehicle). Si l'application est un système de conduite automatique contrôlé par la 5G, le freinage d'un véhicule doit pouvoir se répercuter sur les véhicules suivants dans un temps de l'ordre de la milliseconde.
- Le haut débit en mobilité doit permettre à des professionnels de travailler dans un train à grande vitesse comme s'ils étaient à leur bureau. De même, un véhicule sur l'autoroute doit permettre à ses occupants, en dehors du conducteur, de regarder une vidéo en très haute définition. [1]

1.2.6 Caractéristiques des réseaux mobiles

Les réseaux mobiles sont caractérisés par ce qui suit : [7]

- **Topologie dynamique :**

Les unités mobiles peuvent se déplacer de façon libre et aléatoire. Par conséquent la topologie du réseau peut se 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 mobiles ont des capacités de stockage faibles et des puissances de calcul limitées. Leur sécurité physique est également faible.

- **Une sécurité physique limitée :**

Les réseaux mobiles comme les autres réseaux sans fil sont plus touchés par le paramètre de sécurité que les réseaux filaires. Cela est justifié par les contraintes et limitations physiques qui font que le contrôle des données transférées.

- **Changement d'échelle :**

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

1.2.7 Type des Terminaux mobiles

Un Terminal mobile est un appareil portable permettant le traitement et l'échange de données. 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 classés par la taille, la forme, le poids, ou par la puissance de calcul. La liste suivante donne quelques exemples des unités mobiles :

- **Smartphone**

Le smartphone ou « téléphone intelligent » désigne un téléphone mobile doté de fonctionnalités évoluées qui s'apparentent à celles d'un ordinateur : navigation sur Internet, lecture de vidéos, de musique, jeux vidéo, courrier électronique, vidéoconférence, bureautique légère. Muni d'un processeur puissant, il embarque une série de capteurs (boussole, accéléromètre, gyroscope, GPS) qui lui permettent de faire fonctionner des applications dédiées à l'activité physique, de navigation assistée ainsi que des jeux que l'on peut contrôler d'un simple mouvement. Les smartphones sont généralement dotés d'un appareil photo-vidéo et d'une caméra frontale dont les performances ne cessent de progresser.

- **PDA**

Les PDA sont des appareils de la taille d'un téléphone mobile, mais possédant généralement un large écran tactile à la place d'un écran plus petit et offrant la possibilité de réaliser des calculs, de stocker et de récupérer de l'information pour un usage personnel ou professionnel. [8]

- **Micro portable**

Est un ordinateur personnel, Il est plus léger et ses dimensions limitées permettent un transport facile. Ils intègrent une unité centrale, un écran dépliable, une souris, ainsi que certains périphériques.

- **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. [7]

1.2.8 Domaine d'application des réseaux mobiles

Les réseaux 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 :

1.2.8.1 M-Commerce et M-business

M-Business est considéré comme un sous-ensemble des affaires électroniques. Lorsque les activités de commerce électronique sont effectuées via un appareil mobile sur un réseau mobile, cela s'appelle M-Business. Si les transactions de commerce électronique sont effectuées via des appareils mobiles, cela s'appelle M-Commerce, M-Commerce n'est impliqué que dans les transactions monétaires qui sont exécutées par transfert d'informations sans fil à l'aide d'appareils mobiles. M-Business comme un terme générique de M-Commerce, mais qui couvre la prise en charge supplémentaire des processus d'échange non financier entre les entreprises via les services d'informations mobiles. [9]

1.2.8.2 M-Learning

Le M-Learning est également la combinaison de technologies mobiles et d'une pédagogie appropriée pour permettre aux apprenants d'interagir avec les environnements d'apprentissage et les autres apprenants, à tout moment et en tout lieu. L'apprentissage mobile est effectivement une sous-catégorie du concept plus large d'E-Learning. L'apprentissage mobile est l'intersection de l'informatique mobile et de l'apprentissage en ligne: des ressources accessibles où que vous soyez, de fortes capacités de recherche, une interaction riche, un support puissant pour un apprentissage efficace et une évaluation basée sur les performances - l'apprentissage en ligne indépendamment de l'emplacement dans le temps et l'espace. Un avantage clé de l'apprentissage Mobile est son potentiel pour augmenter la productivité en rendant l'apprentissage disponible partout et à tout moment. [10]

1.2.8.3 M-Banque et M-Payment (Paiement sur mobile)

Le M-Banking comme étant la réalisation d'opérations de gestion d'un compte bancaire via les réseaux mobiles avec des outils mobiles (téléphones mobiles ou PDA). Il s'inscrit dans la continuité du développement des canaux de distribution électroniques à distance et la banque multi-canal. [11]

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 et l'infrarouge. 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. [12]

1.3 La sécurité des réseaux mobiles

1.3.1 La sécurité informatique

La sécurité informatique est l'ensemble de politiques et de mécanismes de protection et de contrôle mis en œuvre pour réduire les vulnérabilités d'un système contre les menaces accidentelles ou intentionnelles pour éviter les erreurs, afin d'assurer le bon fonctionnement de système. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information [13]

1.3.2 La sécurité des réseaux

La sécurité est une fonction incontournable des réseaux. Puisqu'on ne voit pas son correspondant directement, il faut l'authentifier. Puisqu'on ne sait pas par où passent les données, il faut les chiffrer. Puisqu'on ne sait pas si quelqu'un ne va pas modifier les informations émises, il faut vérifier leur intégrité. Nous pourrions ajouter une longue suite de requêtes du même genre qui doivent être prises en charge par les réseaux. Globalement, on peut diviser la sécurité des réseaux en deux parties : la sécurité à l'ouverture de la session et la sécurité lors du transport de l'information. Les techniques pour réaliser ces deux formes de sécurité sont extrêmement diverses, et il s'en invente de nouvelles tous les jours. [1]

1.3.3 Les services de sécurité

- **La confidentialité** : elle assure la protection des données contre les attaques non autorisées.
- **L'authentification** : elle assure celui qui se connecte est celui qui correspond au nom indiqué.
- **L'intégrité** : elle garantit les données reçues qui sont exactement celles qui ont été émises par l'émetteur autorisé.
- **La non-répudiation** : elle assure un message qui a été bien envoyé par une source spécifiée et reçu par un récepteur spécifié.
- **Le contrôle d'accès** : qui a pour fonction de prévenir l'accès à des ressources sous des conditions définies et par des utilisateurs spécifiés. [1]

On peut les expliquer dans les 7 points suivants :

1. Le message ne doit parvenir qu'au destinataire.
2. Le message doit parvenir au bon destinataire.
3. L'émetteur du message doit pouvoir être connu avec certitude.
4. Il doit y avoir identité entre le message reçu et le message émis.
5. Le destinataire ne peut pas contester la réception du message.
6. L'émetteur ne peut pas contester l'émission du message.
7. L'émetteur ne peut pas accéder à certaines ressources que s'il en a l'autorisation.

Le besoin 1 correspond à un service de confidentialité, les besoins 2 et 3 à un service d'authentification, le besoin 4 à un service d'intégrité des données, les besoins 5 et 6 à un service de non-répudiation et le besoin 7 au contrôle d'accès.

1.3.4 Les obstacles de sécurité dans les réseaux mobiles

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

1.3.4.1 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, ces ressources sont limitées dans une unité mobile.

Ces ressources limitées ont un impact important sur la sécurité du terminal.

• Espace Mémoire et de stockage limité:

Un mobile est un dispositif minuscule avec un espace de stockage limité. 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:

Elle 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 terminal. En application d'une fonction ou d'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 de la sécurité 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). [14]

1.3.4.2 La mobilité

Comparant un environnement statique, le 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, des sous-systèmes et 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. [14]

1.3.4.3 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. Il ne permet pas 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, il ne nécessite pas de sa présence physique, il est capable de faire des attaques contre les vulnérabilités naturelles du medium en restant en dehors du domaine attaqué. 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, il existe toujours des techniques pour les contourner. [14]

1.3.5 Attaques sur les réseaux mobiles

Il existe une variété d'attaques qui peuvent atteindre l'infrastructure d'un réseau, On peut classer les attaques sur les réseaux mobiles dans comme suit:

1.3.5.1 Attaques sur les unités mobiles

Les unités mobiles sont exposées aux attaques beaucoup plus 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 être exposée à plusieurs risques comme :

- **Vol**

Si un appareil est 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. [7]

- **Attaques par dénie 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. Ceci est provoqué par l'envoi des données excessives à une unité connectée au réseau. Un appareil mobile, par le fait de sa capacité de traitement limitée, peut-être plus facilement rendu inutilisable par l'envoi massif de trafic de l'attaquant. [7]

- **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. Ils se présentent sous forme de quelques lignes de code en langage machine binaire qui se greffent sur un programme utilisé sur le système de l'unité mobile cible, afin de modifier le comportement l'appareil. Le virus peut être tout entier contenu dans ce greffon, ou il peut s'agir d'une simple amorce, dont le rôle va être de télécharger un programme plus important qui sera le vrai virus. 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.[13]

- **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'une autre unité mobile afin de pouvoir recevoir ses messages ou d'avoir des privilèges qui ne lui sont pas accordés. [15]

1.3.5.2 Attaques sur l'interface radio [17]

L'interface radio par leur nature plus vulnérable aux attaques que l'interface filaire. Le support de transmission étant partagé. Les attaques sur l'interface radio peuvent être soit passives (l'attaquant n'écoute que passivement les communications entre l'appareil mobile et la station de base) soit actives (en plus d'écouter, l'attaquant injecte ou modifie les données).

- **Attaques 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. C'est une attaque dangereuse qui touche la confidentialité et l'intégrité des informations, elle est désignée aussi écoute clandestine des transmissions sans fil, elle a pour objectif d'extraire des informations confidentielles. Les attaques sur l'interface radio par interposition peuvent être comme suit : [7]

- ***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.
- ***Active*** : en plus de l'écoute, l'attaquant injecte ou modifie les données transmises.

- **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.

1.3.5.3 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 découverte.

L'attaquant pourrait envoyer un signal "occupé" à l'unité mobile à chaque fois qu'il demande un service. Aussi, il est possible que le BTS répond 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 dénie de service puisqu'elle bloque les utilisateurs légitimes d'employer le réseau. [18]

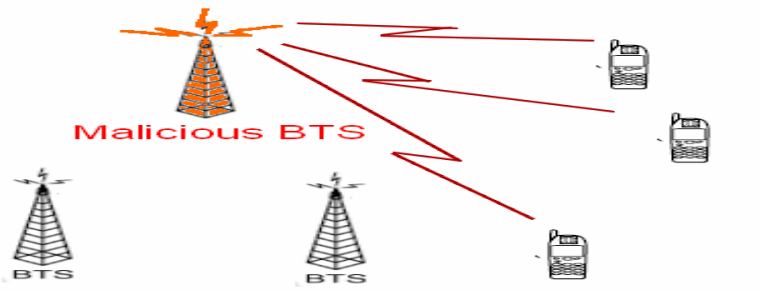

Figure 1.3 : Attaque sur les BTS.

- **Détournement d'une session**

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

1.3.5.4 Attaques sur le réseau cœur

Le réseau cœur est considéré la base des réseaux 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 mobile. [17]

- **Dénie de service distribué (DDoS)**

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. Comme les virus informatique ne concernent pas seulement les ordinateurs, ils touchent les réseaux informatiques ainsi que les réseaux mobiles, donc ils sont considérés le moyen principale pour réaliser ce type d'attaque. Un attaquant équipé par des virus peut envoyer des paquets de commande à tous les nœuds de réseau pour demander des services de réseau cœur. Avec la limitation des capacités de traitement des requêtes; la cible sera immédiatement bloqué et par conséquent le réseau sera bloqué. [18]

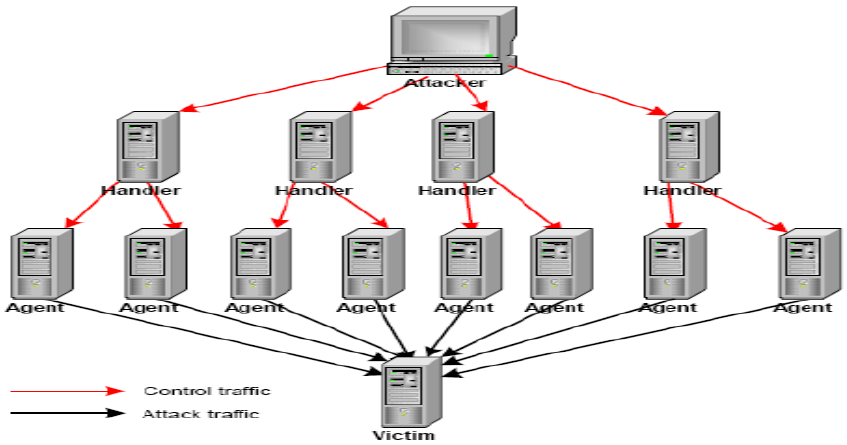

Figure 1.4 *:* Attaque Dénie de service distribué.

- **L'attaque par force brute**

Généralement les mots de passe de la plupart des logiciels sont stockés et cryptés dans un fichier. Pour obtenir un mot de passe, il suffit 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 moins 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. [19]

1.3.6 Mécanismes de bases pour la sécurité

Afin de remédier les problèmes des attaques décrits au-dessus, plusieurs mécanismes de base sont proposés à savoir :

1.3.6.1 La cryptographie

La cryptographie est la science d'écriture et de lecture de messages chiffrés. En effet, elle joue un rôle essentiel dans toutes les communications sécurisée en chiffrant un message dit texte clair, pour obtenir un texte dit crypté, à l'aide d'une clé on utilise des moyens matériels ou logiciels conçus à cet effet. La cryptographie est un traitement fait sur une donnée qui sera transmise à un destinataire, à travers un canal peu sécurisé en présence d'adversaire. [25].

Dans le deuxième chapitre, nous expliquerons ce mécanisme en détail.

1.3.6.2 L'antivirus

La majorité des solutions antivirus actuelles sont réactives. Elles sont activées seulement après la détection d'une activité malveillante au niveau d'un nœud du réseau. Le traitement proactif ferme les services vulnérables avant l'infection, et bloque ainsi la propagation des logiciels malveillants. Le risque peut être partiellement atténué par

l'installation de logiciels antivirus pour les unités mobiles. Cependant, les antivirus ne corrigent pas les attaques de système d'exploitation et de réseau. Ils enlèvent tout simplement les fichiers et répertoires infectés à partir de l'appareil mobile.

Le système antivirus/Antispam analyse et bloque la propagation des malwares (virus, vers et cheval de Troie..),et des messages de spam entre deux utilisateurs du même opérateur, en plus, un scan des vulnérabilités sera utilisé dans ce composant pour localiser et aider à corriger les faiblesses applicatives de l'appareil mobile. Cela aidera à réduire considérablement les risques de l'exploitation d'une faille de sécurité existante. [20]

1.3.6.3 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). **[7]**

1.4 Conclusion

La sécurité au sein des réseaux mobiles reste un challenge très difficile à réaliser, car il hérite le problème de sécurité des réseaux filaires plus les problèmes liés aux spécificités des réseaux mobiles telles que la limitation des ressources en terme d'énergie, de la puissance de traitement et de mémoires disponibles ; aussi la présence du support sans fil sans oublier des caractéristiques physiques des unités mobiles. Pour cela, toutes les solutions proposées pour ces réseaux doivent respecter ces contraintes qui font un obstacle dur pour assurer la sécurité de ces réseaux. En effet, Malgré la diversité des mécanismes de sécurité, ils ne sont pas tous applicables dans les réseaux mobiles à cause de ses contraintes. Nous préjugions que la cryptographie est le mécanisme clé pour une telle situation.

Dans le chapitre suivant nous allons présenter une vue globale de la cryptographie moderne en mettant le point sur les concepts de base et les méthodes de chiffrement symétriques et asymétriques utilisés.

Chapitre 02

Chapitre 02 : La cryptographie

2.1 Introduction

La sécurité informatique est devenue une préoccupation majeure pour tous ceux qui sont intéressés par l'informatique et la plupart des développeurs se concentrent sur les techniques de cryptage pour fournir de bons résultats. En effet, la cryptographie, ou l'art de chiffrer est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois de la physique, on l'utilise lorsqu'il y a un échange sensible de données.

Dans ce chapitre nous allons décrire le concept de la cryptographie et ses deux types à savoir la cryptographie symétrique et asymétrique ainsi que les algorithmes de chiffrement les plus utilisés.

2.2 Définition de la cryptographie

Le terme cryptographie vient en effet de deux mots grecs : Kruptus qu'on peut traduire comme secret et Graphein pour écriture. La cryptographie est l'art de cacher l'information pour qu'elle soit incompréhensible, elle désigne l'ensemble des techniques qui permettent de chiffrer les messages, son objectif principale est de permettre à deux personnes **Alice** et **Bob** de communiquer à travers un canal peu sécurisé de telle sorte qu'un opposant **Eve** ne puisse pas comprendre ce qui est échangé, on utilise une clé appelée clé de chiffrement pour le processus de chiffrement. Pour rendre l'information à nouveau compréhensible on utilise une clé appelée clé de déchiffrement pour le processus de déchiffrement. [21]

2.3 Terminologie [21] [22]

Les principaux termes utilisés dans la cryptographie sont :

Cryptologie : C'est une science mathématique regroupant la cryptographie et la cryptanalyse.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Cryptosystème : un Cryptosystème est constitué d'un algorithme cryptographique ainsi que toutes les clés possibles et tous les protocoles qui le font fonctionner.

Cryptogramme : **Texte chiffré** : **Ciphertext** : est le résultat de l'application d'un chiffrement d'un texte clair.

Texte clair : Plaintext : le message à chiffrer.

Chiffrement: la fonction permettant de transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a crée le message et ainsi que le destinataire.

Déchiffrement : la fonction permettant de retrouver le texte clair à partir du texte chiffré.

Clé : une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement).On distingue généralement deux types de clefs :

Clés symétriques : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou à clé secrète.

Clés asymétriques : il s'agit de clés utilisées dans le cas du chiffrement asymétrique ou à clé publique. Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

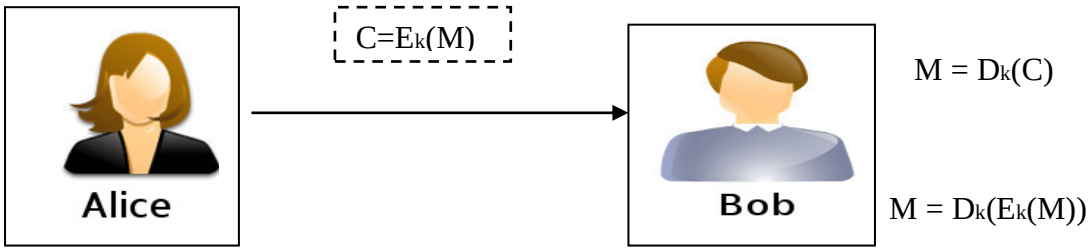

Figure 2.1 : Une représentation d'un Cryptosystème.

- M représente le texte clair.
- C est le texte chiffré tel que $C=E_k(M)$.
- K est la clé de chiffrement et déchiffrement (dans le chiffrement symétrique).
- E(x) est la fonction de chiffrement.
- D(x) est la fonction de déchiffrement.

2.4 Objectif de la cryptographie

Les principaux objectifs garantis par l'application de la cryptographie sont [23]:

- **La confidentialité**:

  Le message chiffré ne doit pas être compréhensible que par les destinataires légitimes. Il ne peut pas être déchiffré par un intrus.

- **L'intégrité :**

  Le destinataire peut vérifier le message reçu qui n'a pas été modifié en chemin par l'utilisation de mécanisme de la signature électronique.

- **L'authentification**:

  Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.

- **La non répudiation**:

  Un expéditeur ne peut pas nier d'avoir envoyé un message et le destinataire ne peut pas nier de l'avoir reçu.

2.5 Classification de cryptographie

Dans la cryptographie moderne toute la sécurité est basée sur la clé et non dans les détails des algorithmes utilisés. On trouve principalement deux grandes familles de cryptographie moderne : la cryptographie symétrique ou à clé secrète et la cryptographie asymétrique ou à clé publique.

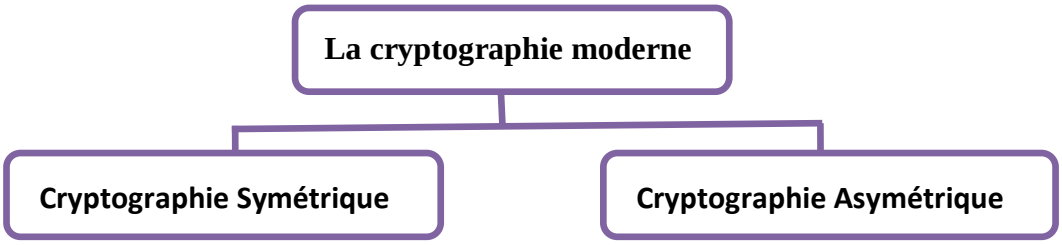

Figure 2.2: Les méthodes de la cryptographie moderne.

2.5.1 Cryptographie symétrique

Cryptographie symétrique utilise une même clé secrète pour chiffrer et déchiffrer des données dont elle assure la confidentialité. Les algorithmes symétriques sont très rapides en termes de calcul, cependant ils posent le problème de distribution de clés entre un émetteur et un récepteur. Le partage d'une clé avec chaque entité communicante dans un groupe de n entités est difficile et conduit à un grand nombre de clés à gérer. [24]

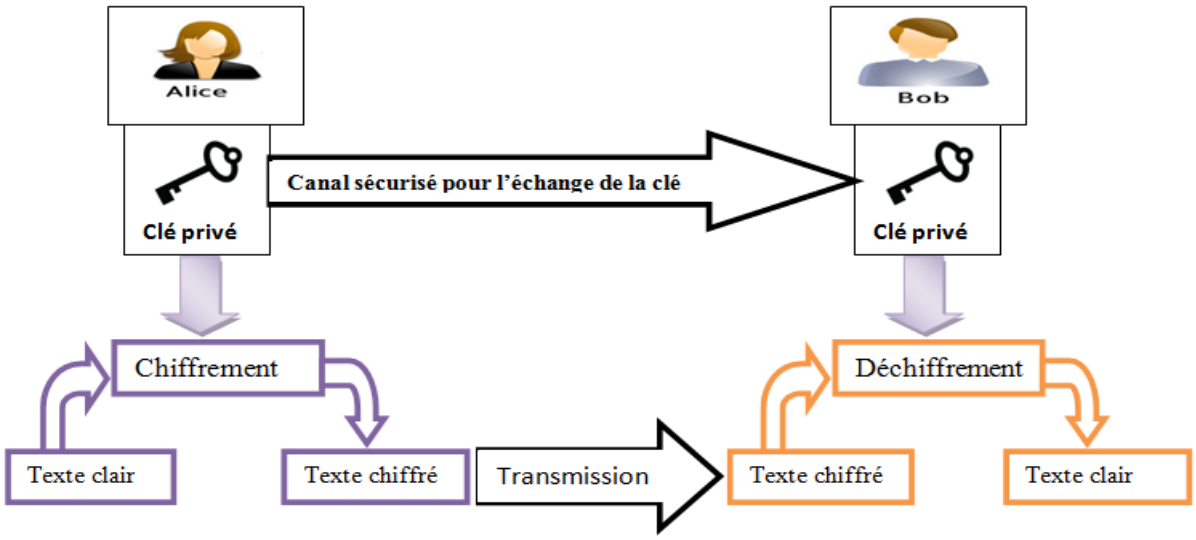

Figure 2.3 : Principe d'un chiffrement à clé secrète (symétrique).