RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITÉ Djillali LIABÈS DE SIDI BEL ABBÈS

FACULTÉ DE TECHNOLOGIE
DÉPARTEMENT D'ÉLECTRONIQUE

T H È S E

pour obtenir le titre de

Docteur en Sciences

Spécialité : Électronique
Option : Télécommunications

Présentée par

Hadj GHARIB

ARCHITECTURE D'AUTHENTIFICATION POUR ASSURER LA MOBILITÉ ET LA QUALITÉ DE SERVICE DANS LES RÉSEAUX SANS FIL

---

soutenue le : 24 novembre 2014

Jury :

Président :	Aoued BOUKELIF	Pr	UDL-SBA
Examinateurs :	Fatima DEBBAT	MCA	U-MASCARA
	Bouabdellah KECHAR	MCA	U-ORAN
	Abdelmalek AMINE	MCA	UTM-SAIDA
	Kamel Mohammed FARAOUN	MCA	UDL-SBA
Directeur :	Kamel BELLOULATA	Pr	UDL-SBA


بسم الله الرحمن الرحيم

Dédicace

À mes Parents,

à la mémoire de mon frère,

à ma femme et mes deux enfants,

à mes frères et sœurs

et à tout les êtres chèrs.

Remerciements

Tout d'abord Je remercie ALLAH le tout Puissant qui m'a donné la force et la volonté pour réaliser ce modeste travail.
Je tiens à exprimer ma sincère gratitude à toutes les personnes qui ont rendu cette thèse possible par leurs aides et leurs contributions.
Mes premiers remerciements sont adressés tout d'abord au Professeur Kamel BELLOULATA, directeur de cette thèse pour avoir accepté de m'encadrer, en tant que doctorant, Mes sincères remerciements sont également adressés au professeur Mohamed CHELLALI. Je tiens à lui exprimer mes sincères respects pour m'avoir encouragés au cours des derniers mois de ma thèse. Je n'oublierai jamais ses qualités humaines et mentales qui ont contribué énormément à la progression de mes travaux de recherche.
Je tiens à exprimer ma profonde reconnaissance à Monsieur Nidal ABOUDAGGA docteur de l'UCL de Louvain la neuve pour m'avoir initié au monde de la sécurité informatique.
Je tiens également à remercier les membres de mon jury de thèse. Je suis reconnaissant envers Monsieur Aoued BOUKELIF, professeur à l'université de Sidi Bel Abbès pour avoir bien voulu présider le jury de cette thèse. Mes remerciements vont également aux examinateurs de ma thèse qui ont eu l'amabilité d'examiner ma thèse.
Je tiens à remercier également Monsieur Bouabdellah KECHAR, maître de conférence à l'université d'ORAN, Monsieur Amine ABDELMALEK, maître de conférence à l'université de SAIDA, Monsieur Mohamed kamel FARAOUN, maître de conférence à l'université de Sidi Bel Abbès et à Mademoiselle Fatima DEBBAT, maître de conférence à l'université de MASCARA, d'avoir examiner mon travail.
Mes remerciements chaleureux vont à toutes les personnes avec qui j'ai été amené à discuter et à valider mes travaux de recherche et plus particulièrement, aux membres du laboratoires de mathématiques.
Mes remerciements vont à Nouredine AMROUN pour les pauses café de tout les jours.
Une pensée particulière est adressée au Professeur Ali HAKEM avec qui j'ai partagé mon bureau durant les longues années de ma thèse.
Mes remerciements vont aussi au Docteur sofiane BOUKLI Hacène pour son aide précieuse dans mes travaux de simulations sous ns2. Je garde une place toute particulière pour ma famille, ma mère, mon père, mes sœurs, mes frères. Je voudrais leur exprimer toute ma profonde reconnaissance et je leur remercie du fond de mon cœur parce qu'ils m'ont constamment aidé, malgré la distance, par leur soutien moral et leurs encouragements pour achever cette thèse.
Mes remerciements vont aussi à mes très chers amis (Benali, Yassar, Fethi, Hamidat, Noureddine et Redouane) pour leurs encouragements pour tout les bons moments qu'on a passé ensembles.
Je pense à mes amis d'enfance, à Bounouar, Tahar et les autres et à tous les habitants de mon village Hamadia.

Table des matières

Chapitre 1

Introduction

If privacy is outlawed, only outlaws will have privacy

Phil Zimmermann

Aujourd'hui, les réseaux sans fil ont connu une forte expansion et sont de plus en plus populaires du fait de leur facilité de déploiement. L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information à n'importe quel moment depuis n'importe quel endroit. Cet environnement n'astreint plus l'usager à une localisation fixe, mais lui permet une libre mobilité tout en assurant sa connexion avec le réseau. Il offre des solutions ouvertes pour fournir des services essentiels là où l'installation d'infrastructures n'est pas possible.
Les réseaux sans fil sont généralement classés selon deux catégories : les réseaux sans fil avec infrastructure fixe qui utilisent généralement le modèle de la communication cellulaire et les réseaux sans fil sans infrastructure fixe, appelés aussi réseaux ad hoc. Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle (les réseaux GSM par exemple) mais requièrent une importante infrastructure logistique et matérielle fixe et une installation fastidieuse, tout comme les réseaux filaire classique. En effet, les besoins excessifs de mobilité et de rapidité de déploiement ont mené à l'établissement du schéma de réseau ad hoc. Un réseau ad hoc est un ensemble autonome et coopératif de nœuds mobiles qui se déplacent et communiquent par une transmission sans fil qui ne suppose pas d'infrastructure préexistante. Le réseau ad hoc se forme de manière spontanée et provisoire dès que plusieurs nœuds mobiles se trouvent à portée radio les uns des autres. Les nœuds communiquent, selon la distance qui les sépare, par deux modes de communication : soit les nœuds mobiles peuvent directement communiquer (en transmission ad hoc) car ils sont à portée de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme des relais pour acheminer les paquets à destination. La transmission est multi-sauts. Ainsi, chaque nœud est à la fois utilisateur final et routeur afin de relayer les paquets vers leur destination finale, en raison de la couverture limitée du champ radio disponible pour chaque nœud.
Le choix des éléments relais dans un réseau ad hoc mobile, nommé également par l'instance de standardisation internet (IETF), Mobile Ad hoc Network : MANET, s'effectue par un protocole de routage. Le routage est la méthode d'acheminement des informations d'une source vers une destination à travers un réseau donné. Le

problème du routage consiste à déterminer un acheminement optimal des paquets par rapport à certains critères de performance. Dans les réseaux ad hoc, il s'agit de trouver une méthode d'acheminement pour un grand nombre de nœuds dans un environnement caractérisé par des changements rapides de la topologie du réseau dus à la mobilité des hôtes, ainsi que d'autres caractéristiques comme l'absence d'infrastructure, la limitation de la bande passante, la limitation de source d'énergie, et les modestes capacités de traitement et de mémoire. La question actuelle n'est plus la recherche de la route optimale, mais la recherche du chemin le plus sûr.
Plusieurs stratégies ont été proposées pour sécuriser les protocoles de routage ad hoc. Les mécanismes de sécurité utilisés dans les réseaux filaire et sans fil classiques et qui se basent sur une infrastructure centralisée ne sont pas appropriés à un réseau ad hoc complètement décentralisé. Les solutions qui ont été développées en essayant de les adapter à la nature des réseaux ad hoc s'avèrent coûteuses, lentes et consomment beaucoup de ressources (énergie, capacité de calcul et de stockage), ce qui dégrade les performances globales du réseau.
Dans ce travail, nous nous intéressons aux problèmes de sécurité dans les réseaux ad hoc. Pour cela, nous avons mené une première étude qui porte principalement sur les mécanismes de sécurités qui ont été proposés, et qui se font à l'heure actuelle, dans le but d'assurer un niveau de sécurité optimal dans les réseaux ad hoc.
la plupart des solutions proposées dans la littérature se basent sur des mécanismes cryptographiques très complexes, lents, et très coûteux en termes de consommation deressources pour assurer l'authentification des entités communicantes. Ces solutions ne sont pas, par conséquent, très adaptées à l'environnement ad hoc, et dégradent considérablement les performances du réseau. Afin de pallier aux limites de ces approches, notre objectif consistait donc à proposer une architecture de sécurité efficace et à faible coût sans dégradation significative des performances du réseau. Pour obtenir un bon niveau de sécurité et mieux protéger la stabilité du réseau, nous avons proposé un schéma de sécurité basé sur le protocole d'authentification KERBEROS avec une cryptographie à seuil sur des courbes élliptiques. Notre architecture dégrade, en contre partie, les performances réseau en raison des surcoûts de calcul engendrés par le grand nombre d'opérations cryptographiques effectuées par les nœuds mais ça reste dans la limite acceptable. Nous avons étendu notre contribution en proposant également un mécanisme de quantification de la qualité de service QoS par rapport aux différents niveaux de sécurité.

Chapitre 2

Préliminaires

Sommaire

2.1 Les réseaux sans fil

Au cours de la dernière décennie, nos moyens de communication ont radicalement changé. Nos styles de vie et de travail sont devenues de plus en plus mobile. Par conséquent, nos méthodes traditionnelles de se connecter les uns aux autres aux ressources de données sont devenues non pratique à notre style de vie. Aujourd'hui, la nécessité de la connectivité permanente aux réseaux téléphoniques et informatiques dans les affaires et la vie personnelle est devenue inévitable dans le monde moderne. La nécessité de la mise en réseau persiste dans de nombreuses régions où la connexion filaire est soit coûteux ou impossible ; En outre, la mobilité d'une partie des utilisateurs de réseaux a imposé une nouvelle connectivité sans fil. Récemment la connectivité de téléphonie sans fil s'est avéré être un énorme succès, car elle allie l'accessibilité permanente (n'importe où, n'importe quand) et la mobilité.
Les technologies sans fil offrent les mêmes avantages que les réseaux informatiques. Ainsi, de nombreux protocoles ont été développés pour ces différentes technologies et les chercheurs continuent à les améliorer.
Cette thèse étudie les aspects de sécurité des réseaux sans fil dans différents contextes de mobilité. La sécurité dans les réseaux sans fil, comme dans n'importe quel autre réseau, composé des fonctions fondamentales comme la garantie de la confidentialité, l'intégrité des données, l'authentification des communicateurs, et d'autres fonctions de sécurité avancées telles que la vie privée, l'autorisation, la non-répudiation, la disponibilité et de la comptabilité.
L'objectif de ce travail est l'authentification des entités, car il c'est la principale fonction de construction de la sécurité d'un réseau. Cependant, la conception et le déploiement d'une solution de sécurité cryptographique dans un réseau dépend fortement de ses caractéristiques. Ainsi, nous consacrons la prochaine section de ce chapitre à la description de certaines particularités du réseau sans fil.

2.1.1 Avantages

Il ya beaucoup de raisons d'adopter des services de réseau sans fil, par exemple :

- Mobilité : L'avantage le plus évident de la connectivité sans fil est la mobilité. Nous pouvons utiliser notre téléphone sans fil pour faire un appel tout en voyageant pour des centaines de kilomètres. Nous pouvons accéder aux ressources Internet et les réseaux domestiques de n'importe où, à l'intérieur des bâtiments à l'entreprise ou de l'extérieur.Cette connectivité améliore la productivité des entreprises et le rendement des employés. Les réseaux sans fil peuvent transformer n'importe quel endroit, à tout moment en un bureau de travail.
- Coût : Les appareils sans fil deviennent de plus en plus puissants et moins chers. Les réseaux sans fil réduisent les coûts de câblage et les problèmes liés surtout dans les endroits où câblage est impossible ou peut être dangereux.
- Flexibilité : Le déploiement et le retrait des réseaux sans fil est très facile et rapide. L'administrateur peut ajouter et supprimer des utilisateurs sans intervention physique sur le réseau. L'infrastructure de connexion pour un utilisateur ou des milliers d'utilisateurs est pratiquement la même ; nous avons seulement besoin de déployer des antennes et des stations de base.
- Simplicité d'utilisation : Les dispositifs sans fil peuvent accéder à n'importe quel réseau autorisé sans ajout de modification de configuration.
- Déploiement temporaire : Certains réseaux sans fil peuvent être déployés temporairement, par exemple pendant le temps d'un projet ou lors d'une réunion ou pour une durée d'une tâche bien déterminée (ex : réseaux de capteurs).

2.1.2 Inconvénients

La principale ressource de réseau sans fil est les ondes radio. Les appareils sans fil sont contraints de fonctionner dans une certaine bande de fréquence. Chaque bande a une largeur de bande associée, qui décrit la quantité de flux de données sur une voie de transmission donnée. L'utilisation de la fréquence radio (spectre) est rigoureusement contrôlée par les autorités de régulation comme : La Commission fédérale de la communication (FCC) aux Etats-Unis, le Bureau des communications radio (ERO) en Europe et de l'Union internationale des télécommunications (UIT). Ces organisations allouent les gammes de fréquences de fonctionnement pour chaque type d'application pour éviter les problèmes de chevauchement.
Les réseaux sans fil ne remplacent pas les réseaux filaires. Les réseaux sans fil font ponts pour utilisateurs sans fil pour accéder aux ressources filaires étant donné que les emplacement des serveurs sont fixés.
Habituellement, la vitesse de transmission d'un réseau sans fil est plus lente que celle d'un réseau filaire.
Les ondes radio agissent comme un support de réseau et peuvent souffrir de nombreux problèmes de propagation pouvant interrompre la liaison radio, tels que les interférences multi-trajets, les ombres et les attaques de brouillage.
La sécurité des réseaux sans fil est plus sensible à une série de problèmes qui ne sont pas présents dans les réseaux filaires. Dans les réseaux sans fil, les données ainsi que les cadres de gestion de réseau propagent dans l'air, ce qui les rend facile à être

interceptés.
En outre, le support sans fil est vulnérable à l'injection des messages par les intrus. Les réseaux sans fil ont aussi des limites floues qui ne sont pas évidentes à contrôler. Les appareils sans fil dans le réseau peuvent être la cible d'attaques physiques, par conséquent, les données sensibles partagées avec le réseau pouvaient être extraites.[1]

2.2 Architectures des réseaux sans fil

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité". Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée, ainsi que par le débit et la portée des transmissions.

2.2.1 Avec une infrastructure

Ce mode de fonctionnement est très semblable au protocole Ethernet des réseaux filaires voir figure 2.1. Dans ce mode, un réseau 802.11 est un ensemble de cellules de base appelé Basic Service Set BSS. Chaque cellule BSS comporte un point d'accès (AP)matérialisé par un dispositif d'émission/réception. L'AP donne l'accès au réseau aux machines qui le désirent, on peut le comparer aux concentrateurs (hub) des réseaux fixes. Les APs sont en général câblés entre eux afin de créer un réseau de bornes d'accès. Donc les cellules sont reliées par une infrastructure de communication fixe et interconnectées par un système de distribution afin de former un Extended Service Station ESS. Les BSS d'un ESS sont différenciés via leur BSS Identifier (BSSID) de 6 octets correspondant à l'adresse MAC de l'AP. Cette infrastructure incorpore un portail permettant d'assurer l'interface avec un réseau local.

2.2.2 Sans une infrastructure

Appelé aussi Ad Hoc [39], ce modèle de réseau ne présente aucune infrastructure préexistante ni de site fixe, Contrairement au réseau à infrastructure, les stations dans un réseau Ad Hoc communiquent directement entre elles. L'absence de l'infrastructure ou d'un réseau filaire composé des stations de base, oblige les noeuds mobiles (MN) à se comporter comme des routeurs qui participent à la découverte et à la maintenance des chemins pour les autre hôtes du réseau.

2.3 La sécurité dans les réseaux sans fil

Les réseaux locaux sans fil IEEE 802.11 constituent de nos jours le standard des WLANs le plus largement déployé et utilisé à travers le monde. Les contextes d'utilisation de ces réseaux sont divers et vont principalement du cadre domestique,

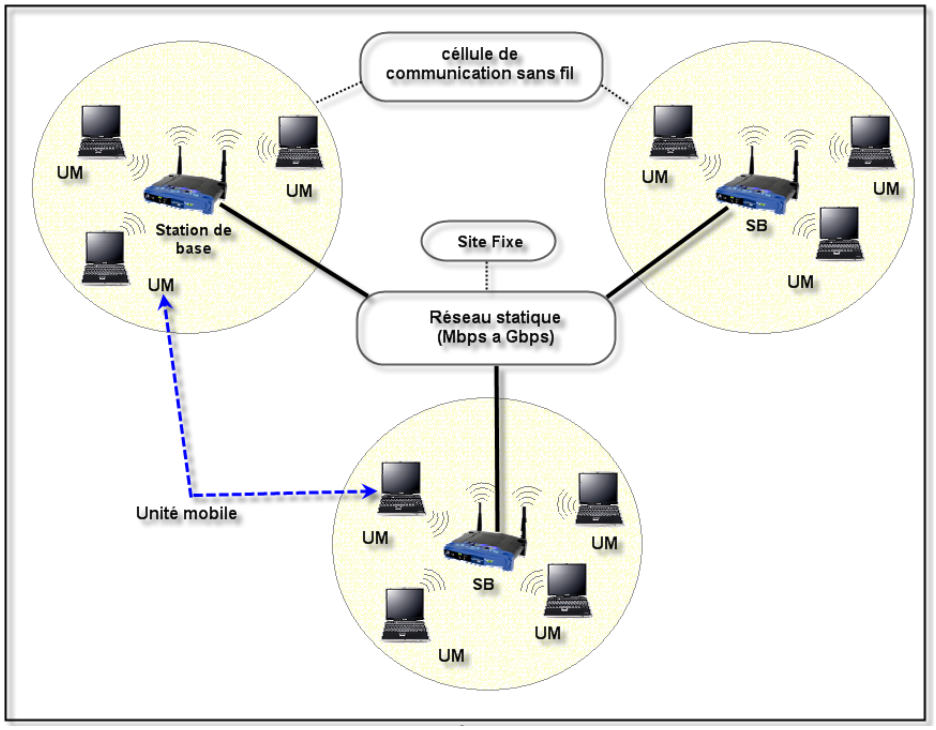

FIGURE 2.1 – Réseaux mobiles avec infrastructure

aux lieux publics (e.g. gares, hôtels, restaurants, etc.) à travers notamment des HotSpots, en passant par le cadre du travail. Poussés précipitamment sur le marché, les WLANs 802.11 n'ont pu intégrer des mécanismes de sécurité robustes qu'après la déferlante des attaques dont ces réseaux ont fait l'objet et la prise de conscience progressive de l'étendue des vulnérabilités dans leur conception initiale. [52]

2.4 Les services de sécurité

L'ISO a defini six services de sécurité : authentification, contrôle d'accès, confidentialité et intégrité des données, non-répudiation et protection contre l'analyse du trafic. Différents types de mécanismes (chiffrement, signature numérique, listes de contrôle d'accès, bourrage ; notarisation...) servent pour assurer ces services. Ils diffèrent par leur sophistication, leurs coûts, les efforts nécessaires pour leur implantation, leur maintenance et leurs besoins en ressources.

2.4.1 Le contrôle d'accès

Le service consiste à empêcher un accès au réseau à tout élément étranger au système. Le contrôle d'accès donne aux participants légitimes un moyen de détecter les messages provenant de sources externes au réseau.

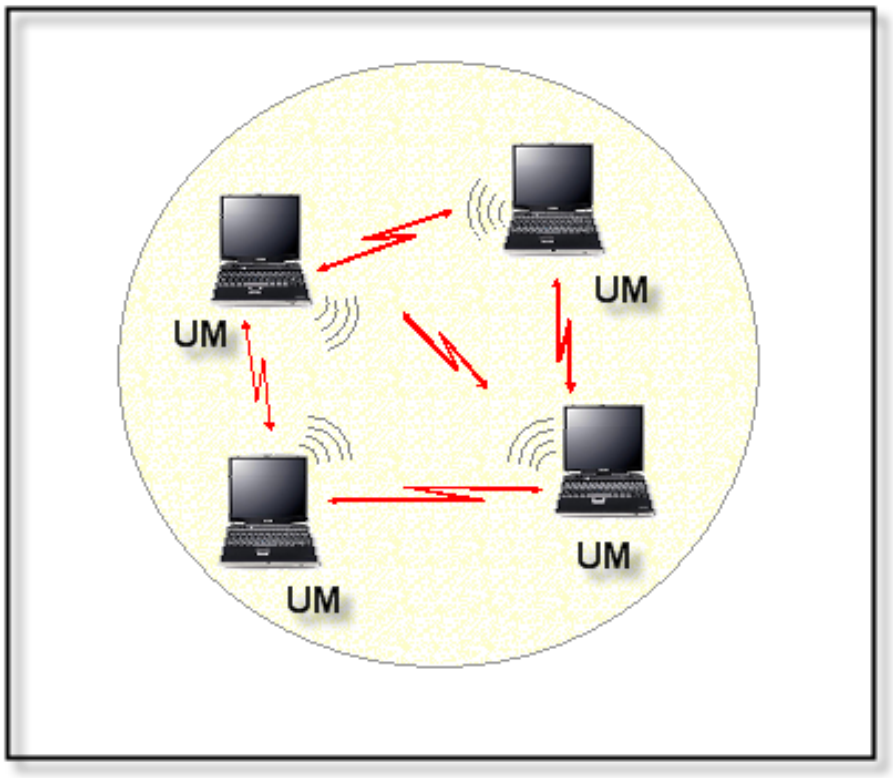

FIGURE 2.2 – Réseaux mobiles sans infrastructure

2.4.2 La disponibilité

Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu en dépit des attaques de dénie de service (DoS) pouvant affecter n'importe couche du réseau.

2.4.3 La confidentialité

Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché. [49]

2.4.4 L'intégrité

Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

2.4.5 La non-répudiation

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

2.4.6 L'authentification

L'Authentification [51], est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.
L'authentification peut se faire de multiples manières, et notamment par la vérification de :

- « Ce que je sais », un mot de passe par exemple,
- « Ce que je sais faire », une signature manuscrite sur écran tactile/digital (de type PDA),
- « Ce que je suis », une caractéristique physique comme une empreinte digitale,
- « Ce que je possède », une carte à puce par exemple.

Le choix de telle ou telle technique dépend en grande partie de l'usage que l'on souhaite en faire :
authentification de l'expéditeur d'un courriel, authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, authentification des parties lors d'une transaction, etc.
La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

2.4.6.1 Authentification de l'entité distante

Elle garantit que le récepteur est celui souhaité. Son action peut intervenir à l'établissement de la communication ou pendant le transfert des données. Son objectif principal est la lutte contre le déguisement, également appelé usurpation d'identité (spoofing).

2.4.6.2 Authentification de l'origine

Elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité. Comme le précédent, il s'agit d'authentication simple.

2.4.6.3 Authentification mutuelle

Elle assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre.[16]

2.5 Les mécanismes de sécurité

« Il existe deux types de cryptographie dans le monde : la cryptographie qui protège vos documents de la curiosité de votre petite sœur et celle qui empêche les gouvernements les plus puissants de lire vos fichiers. Cet ouvrage s'adresse au dernier cas. »
Bruce Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C.

2.5.1 La cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé. Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

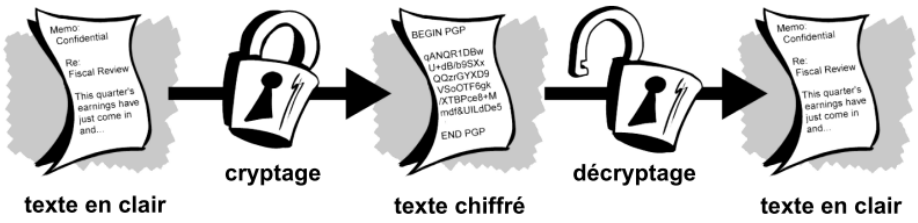

FIGURE 2.3 – La cryptographie

2.5.1.1 cryptographie symétrique

Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants. Ce type de cryptographie fonctionne habituellement suivant deux procédés différents, le cryptage par blocs et le cryptage de "stream" (en continu).

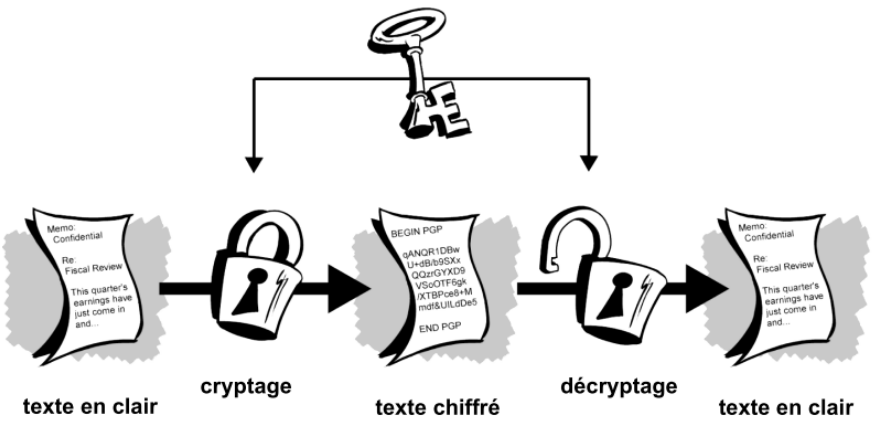

FIGURE 2.4 – Le cryptage symétrique

- Le chiffrement par flot : le cryptage est effectué bit-à-bit sans attendre la réception complète des données à crypter. Une technique de chiffrement, du nom de "One-Time Pad" est utilisé pour chiffrer les flux. C'est le chiffrement inconditionnel le plus sûr. Pour cela, on a besoin d'une chaîne aléatoire de la même longueur que le message d'origine, ce qui n'est pas partique. Le but d'un stream cipher est de générer une chaîne aléatoire à partir d'une clé de longueur courte.
  Une autre technique consiste à "xorer", c'est-à-dire à appliquer un OU exclusif (XOR) au message avec un autre message prédéfini. Bien entendu, cela nécessite que le destinataire (la personne qui décrypte) connaisse le message prédéfini et donc cela rajoute de la complexité au schéma général. Les stream-ciphers sont utilisés aujourd'hui par différentes applications. Pour chiffrer les flux, l'algorithme RC4 est un exemple.
- Le cryptage en blocs (block-cipher) : est au contraire beaucoup plus utilisé et permet une meilleure sécurité. Les algorithmes concernés sont également plus connus (DES, AES, Skipjack...) ; leur nom leur vient du fait qu'ils s'appliquent à des blocs de données et non à des flux de bits (cf. stream-ciphers). Ces blocs sont habituellement de 64 bits mais cela dépend entièrement de l'algorithme utilisé et de son implémentation. De même, la taille de la clé varie suivant l'algorithme et suivant le niveau de sécurité requis ; ainsi, un cryptage de 40 bits (c'est-à-dire utilisant une clé longue de 40 bits) pourra être déclaré faible puisque aisément cassable. Un cryptage de 56 bits (qui est le standard dans le cas du DES) sera qualifié de moyen puisque cassable mais nécessitant pas mal de moyens pour être exploitable (vis-à-vis du temps requis et de la valeur des données). Enfin, un cryptage de 128 bits (valeur standard utilisée par Rijndael alias AES) est plutôt fort à l'heure actuelle.

2.5.1.2 cryptographie assymétrique

Les problèmes de distribution des clés sont résolus par la cryptographie de clé publique. Ce concept a été introduit par Whitfield Diffie et Martin Hellman [13] en 1975. (Il est maintenant prouvé que les services secrets britanniques avaient fait cette même découverte plusieurs années avant Diffie et Hellman et avaient protégé ce secret militaire (sans en faire aucune utilisation)[18]. La cryptographie de clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage : une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète. Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique. D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

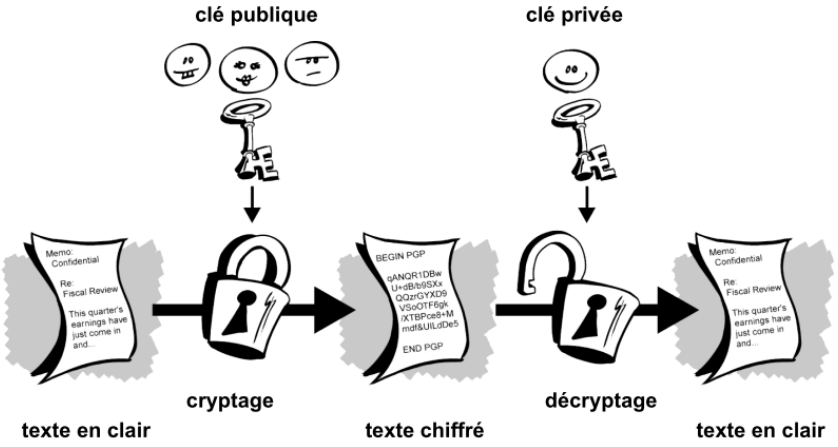

FIGURE 2.5 – Le cryptage assymétrique

2.5.2 Les fonctions de hachages

Une fonction de hachage est une méthode permettant de caractériser une information, une donnée. En faisant subir une suite de traitements reproductibles à une entrée, elle génère une empreinte servant à identifier la donnée initiale. De telles fonctions datent de la fin des années 1980 (algorithme MD2) mais l'idée est plus ancienne, et a germé dès l'apparition des codes correcteurs d'erreurs (théorie de l'information). Une fonction de hachage prend donc en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. On obtient à la sortie une chaîne de caractères hexadécimaux, le condensé, qui résume en

quelque sorte le fichier. Cette sortie a une taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1). Ces fonctions sont très utilisées en informatique et en cryptographie.On les rencontre en navigant sur le Web : les auteurs de logiciels proposent souvent des empreintes sur les pages dédiées aux téléchargements (des fichiers portant l'extension md5 ou sha1, qui contiennent la valeur hachée dudit programme). En comparant l'empreinte de la version téléchargée avec l'empreinte disponible sur le site, l'utilisateur peut s'assurer que sa version n'a pas été corrompue (erreurs de transmission, virus, etc.) Enfin, une fonction de hachage cryptographique doit aussi satisfaire d'autres contraintes. La première stipule qu'il doit être très difficile de retrouver ou génèrer un texte à partir de l'empreinte (on parle alors de fonction à sens unique). Par très difficile, on entend que même avec une armée de machines dédiées à cette tâche, il sera impossible d'effectuer une telle extraction en un temps raisonnable. Une autre caractéristique d'une fonction de hachage cryptographique concerne le comportement de l'empreinte selon le fichier en entrée. La moindre modification dans ce fichier doit engendrer un condensé totalement diffèrent. En outre, le hachage doit rendre impossible la création d'un fichier qui donne la même empreinte qu'un autre préalablement fixé. Cette dernière contrainte est cruciale pour assurer l'intégrité d'un fichier : si elle n'était pas respectée, on pourrait facilement génèrer un fichier corrompu mais valide aux yeux de l'utilisateur.
La fonction de hachages peut être utilisée pour :

1. stockage mots de passe,
2. codes d'authentification de messages (MAC),
3. signatures, chiffrement, "fonction aléatoire"...

On peut classer les fonctions de hachages en deux catégories :

1. Fonctions de hachage sans clé
2. Fonctions de hachage avec clé

Les fonctions de hachage répondent malgré tout à un certain nombre de contraintes. On peut citer :

- la résistance aux collisions : une collision, c'est le fait que deux textes différents donnent la même empreinte.
- la résistance à la préimage : calculer une empreinte via une fonction de hachage, ça doit être facile, on est d'accord. Par contre, partir de l'empreinte pour remonter au texte original, ça, c'est à éviter. On stocke parfois des empreintes de mots de passe plutôt que les mots de passe eux-mêmes, justement parce qu'en cas de piratage, il est compliqué de faire la manipulation inverse !
- la résistance à la seconde préimage : connaissant une chaîne d'entrée et l'empreinte correspondante, il doit être compliqué de trouver une deuxième chaîne d'entrée qui donne la même empreinte (une sorte de « mix » entre les deux premiers critères, si on veut). Attention, si la résistance aux collisions implique nécessairement une résistance à la seconde préimage, cela ne touche pas à la « première » préimage.

2.5.3 La signature numérique

Une signature numérique est un système mathématique pour démontrer l'authenticité d'un message ou d'un document numérique. Une signature numérique valide donne une raison de destinataire à croire que le message a été créé par un expéditeur connu, tel que l'expéditeur ne peut pas nier avoir envoyé le message (authentification et de non-répudiation) et que le message n'a pas été modifié en transit (intégrité). Les signatures numériques sont couramment utilisés pour la distribution de logiciels, les transactions financières, et dans d'autres cas où il est important de détecter la falsification ou l'altération.
Les signatures numériques sont souvent utilisés pour mettre en œuvre les signatures électroniques, un terme plus large qui fait référence à toutes les données électronique qui font objet d'une signature, mais pas toutes les signatures électroniques utilisent des signatures numériques. Dans certains pays, y compris les États-Unis, l'Inde, le Brésil, et les membres de l'Union européenne, les signatures électroniques ont une signification juridique.

Les signatures numériques utilisent un type de cryptographie asymétrique. Pour les messages envoyés à travers un canal non sécurisé, une signature numérique correctement mis en œuvre donne la raison au récepteur de croire que le message a été bien envoyé par l'expéditeur revendiqué. Les signatures numériques sont équivalentes à des signatures manuscrites traditionnelles à bien des égards, mais les signatures numériques correctement mises en œuvre sont plus difficiles à contrefaire que les signatures type manuscrite. Les schémas de signature numérique, dans le sens utilisé ici, sont basés sur des fonctions cryptographique, et doivent être correctement mis en œuvre pour être efficace. Les signatures numériques peuvent également assurer la non-répudiation, ce qui signifie que le signataire ne peut prétendre qu'il n'a pas signé un message, en outre, certains schémas de non-répudiation ajoutent un horodatage à la signature numérique, de telle sorte que même si la clé privée est découverte, la signature reste valide.
Un schéma de signature numérique se compose généralement de trois algorithmes :

1. Un algorithme de génération de clé qui sélectionne une clé privée manière uniforme aléatoire d'un ensemble de clés privées possibles. L'algorithme fournit en sortie de la clé privée et une clé publique correspondante.
2. Un algorithme de signature utilisant une clé privée pour produire une signature d'un message.
3. Un algorithme de vérification de signature qui à partir d'un message, une clé publique et une signature, accepte ou rejette la demande de l'authenticité d'un message.

Deux propriétés principales sont nécessaires. Tout d'abord, l'authenticité d'une signature générée à partir d'un message fixe et la clé privée fixe qui peut être vérifiée en utilisant la clé publique correspondante. Deuxièmement, il est pratiquement impossible de générer une signature valide d'une partie sans connaître la clé privée

de celle-ci.

Fonctionnement :

La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. C'est en effet par l'association de ces deux techniques que nous pouvons obtenir les 5 caractéristiques d'une signature (authentique, infalsifiable, non réutilisable, inaltérable, irrévocable).

Imaginons que Alice souhaite envoyer un document signé à Bob.

1- Tout d'abord, elle génére l'empreinte du document au moyen d'une fonction de hachage.

2- Puis, elle crypte cette empreinte avec sa clé privée.

3- Elle obtient ainsi la signature de son document. Elle envoie donc ces deux éléments à Bob

4- Pour vérifier la validité du document, Bob doit tout d'abord déchiffrer la signature en utilisant la clé publique d'Alice. Si cela ne fonctionne pas, c'est que le document n'a pas été envoyé par Alice.

5- Ensuite, Bob génère l'empreinte du document qu'il a reçu, en utilisant la même fonction de hachage qu'Alice (On supposera qu'ils suivent un protocole établi au préalable).

6- Puis, il compare l'empreinte générée et celle issue de la signature.

7- Si les deux empreintes sont identiques, la signature est validée. C'est Alice qui a envoyé le document et le document n'a pas été modifié depuis sa signature.

8- Dans le cas contraire, cela peut signifier que le document a été modifié depuis sa signature par Alice et ce n'est pas ce document d'origine.

Il ya plusieurs raisons pour signer un tel hachage (ou message digest) au lieu de l'ensemble du document.

- Pour plus d'efficacité : La signature sera beaucoup plus courte et donc permet de gagner du temps car le hachage est généralement beaucoup plus rapide que la signature dans la pratique.
- Pour la compatibilité : Les messages sont généralement des chaînes de bits. Une fonction de hachage peut être utilisé pour convertir une entrée quelconque dans un format de sortie souhaité.
- Pour intégrité : Sans la fonction de hachage, le texte "doit être signé" peut être divisé (séparés) dans des blocs assez petits pour que le schéma de signature peut agir directement. Cependant, le récepteur des blocs signés n'est pas en mesure de reconnaître si tous les blocs sont présents et est ce qu'ils sont dans l'ordre approprié.

2.5.4 Les certificats électroniques

Lors de l'utilisation des systèmes de cryptographie de clé publique, les utilisateurs doivent constamment vérifier qu'ils cryptent vers la clé du bon utilisateur,

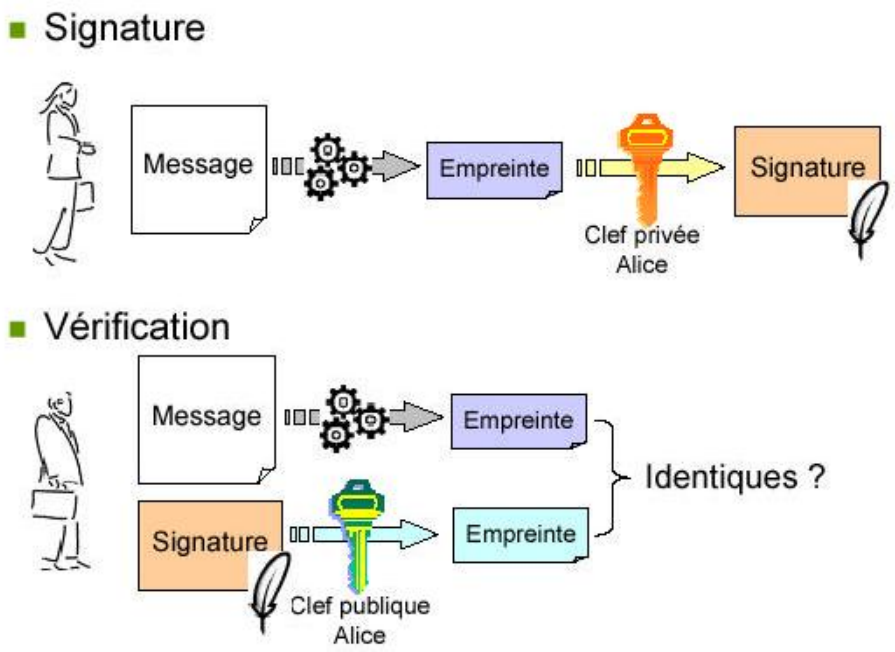

FIGURE 2.6 – Schéma de signature numérique

ce qui constitue un problème. Dans un environnement où le libre échange de clés via des serveurs publics est sécurisé, toute attaque menée par une personne intermédiaire, encore appelée un intercepteur, représente une menace éventuelle. Dans ce type d'attaque, une personne place une fausse clé comportant le nom et l'ID utilisateur du destinataire. Les données cryptées (et interceptées) vers le détenteur réel de cette clé erronée sont dorénavant entre de mauvaises mains.[]

Dans un environnement de clé publique, il est essentiel de s'assurer que la clé publique vers laquelle vous cryptez les données est celle du destinataire concerné et non une contrefaçon. Vous pouvez crypter uniquement vers les clés qui vous ont été distribuées physiquement. Supposons maintenant que vous devez échanger des informations avec des personnes que vous ne connaissez pas, comment savoir que vous êtes en possession de la bonne clé ?

Les certificats numériques ou certificats simplifient la tâche qui consiste à déterminer si une clé publique appartient réellement à son détenteur supposé.

Un certificat correspond à une référence. Il peut s'agir par exemple de votre permis de conduire, de votre carte de sécurité sociale ou de votre certificat de naissance. Chacun de ces éléments contient des informations vous identifiant et déclarant qu'une autre personne a confirmé votre identité. Certains certificats, tels que votre passeport, représentent une confirmation de votre identité suffisamment

importante pour ne pas les perdre, de crainte qu'une autre personne ne les utilise pour usurper votre identité.

Un certificat numérique contient des données similaires à celles d'un certificat physique. Il contient des informations associées à la clé publique d'une personne, aidant d'autres personnes à vérifier qu'une clé est authentique ou valide. Les certificats numériques permettent de contrecarrer les tentatives de substitution de la clé d'une personne par une autre.

Un certificat numérique se compose de trois éléments :

1. Une clé publique.
2. Des informations sur le certificat. (Informations sur l'« identité » de l'utilisateur, telles que son nom, son ID utilisateur, etc.)
3. Une ou plusieurs signatures numériques.

La signature numérique d'un certificat permet de déclarer que ses informations ont été attestées par une autre personne ou entité. La signature numérique ne garantit pas totalement l'authenticité du certificat. Elle confirme uniquement que les informations d'identification signées correspondent ou sont liées à la clé publique. Ainsi, un certificat équivaut en réalité à une clé publique comportant un ou deux types d'ID joints ainsi qu'une estampille agréée par d'autres personnes fiables.

2.5.4.1 Distribution de certificats :

Les certificats sont utilisés lors de l'échange de clés publiques avec un autre utilisateur. Pour un petit groupe de personnes souhaitant communiquer de manière sécurisée, il est facile d'échanger manuellement des disquettes ou des e-mails contenant la clé publique de chaque détenteur. Cette distribution manuelle de clés publiques s'avère limitée. Au-delà d'un certain point, il est nécessaire de mettre en place des systèmes pouvant fournir des mécanismes de sécurité, de stockage et d'échanges nécessaires pour que vos collègues ou d'autres personnes puissent communiquer. Ces systèmes peuvent se présenter sous la forme de référentiels de stockage uniquement, appelés serveurs de certificats ou sous la forme de systèmes structurés offrant des fonctions de gestion de clés, appelés infrastructures de clé publique (PKI).

2.5.4.2 Serveurs de certificats :

Un serveur de certificats, également appelé serveur de clés, est une base de données permettant aux utilisateurs de soumettre et de récupérer des certificats numériques. Un serveur de certificats offre généralement des fonctions de gestion permettant à une entreprise de soutenir sa politique de sécurité (par exemple, autoriser uniquement le stockage des clés répondant à des exigences spécifiques).

2.5.4.3 Infrastructures de clé publique (PKI) :

Une PKI contient les fonctions de stockage de certificats d'un serveur de certificats, mais elle offre également des fonctions de gestion de certificats (émission, révocation, stockage, récupération et fiabilité des certificats). La principale fonction d'une PKI est de présenter l'autorité de certification ou la CA, à savoir une entité humaine (une personne, un groupe, un service, une entreprise ou une autre association) autorisée par une société à émettre des certificats à l'attention de ses utilisateurs informatiques. Une CA fonctionne comme un service de contrôle des passeports du gouvernement d'un pays. Elle crée des certificats et les signe de façon numérique à l'aide d'une clé privée de CA. Ainsi, la CA est l'élément central d'une PKI. A l'aide de la clé publique de la CA, quiconque souhaite vérifier l'authenticité d'un certificat doit vérifier la signature numérique de la CA émettrice et, par conséquent, l'intégrité du contenu du certificat (essentiellement, la clé publique et l'identité du détenteur du certificat).

2.5.4.4 Formats de certificats

Un certificat numérique est en réalité un ensemble d'informations permettant d'identifier une clé publique, signé par un tiers de confiance, afin de prouver son authenticité. Un certificat numérique peut se présenter sous différents formats.
PGP reconnaît deux formats de certificat :

- ⋆ Certificats PGP
- ⋆ Certificats X. 509

2.6 Attaques et vulnérabilités dans les réseaux sans fil

L'utilisation des liens sans fil facilite considérablement les attaques contre les réseaux ad hoc, que ce soit à travers de simples écoutes ou d'attaques plus nuisibles comme le dysfonctionnement intentionnel d'un service (déni de service). Contrairement aux réseaux filaires où les attaquants doivent avoir un accès physique au réseau ou bien outrepasser plusieurs couches de défense telles que les pare-feu et les passerelles, dans les réseaux sans fil, il suffit que l'attaquant soit dans le champ de transmission d'un nœud pour pouvoir intercepter les communications de ce dernier. Enfin, dans certains contextes comme celui des réseaux de capteurs, les nœuds ont une faible protection physique et peuvent donc être capturés, corrompus et détournés à des fins malfaisantes.
La majorité des réseaux autonomes et auto-organisés, et tout particulièrement les réseaux sans fil ad hoc, s'appuient sur des algorithmes coopératifs nécessitant l'implication de tous les nœuds du réseau, et ce, afin d'assurer le fonctionnement de la majorité des services. Prenons l'exemple des protocoles de routage qui sont plus vulnérables dans les réseaux ad hoc que dans les réseaux avec infrastructure, car chaque nœud doit faire office de routeur pour ses voisins. Des nœuds pourraient par exemple

décider de supprimer ou de modifier les informations de routage qu'ils reçoivent de leurs voisins ou bien injecter de fausses informations de routage. Ces comportements peuvent s'avérer préjudiciables pour le bon fonctionnement du réseau dans la mesure où le routage constitue l'un des noyaux de base du fonctionnement des réseaux informatiques. Un autre comportement malveillant, plus facile à réaliser, mais tout aussi néfaste pour le bon fonctionnement du réseau est le comportement dit égoïste d'un nœud [31]. Autrement dit, certains nœuds pourraient refuser de router les paquets des autres afin de préserver leurs ressources matérielles.[6]

2.6.1 Classification des attaques

Dans les réseaux ad hoc, selon le niveau d'intrusion des actions menées par un attaquant, on distingue généralement deux catégories d'attaques : les attaques passives et les attaques actives.[2]

2.6.2 Attaque passive

L'adversaire ne fait que surveiller les canaux de communication. Une écoute se produit lorsqu'un attaquant capture un nœud et étudie le trafic qui le traverse sans en altérer le fonctionnement. Les données analysées aident l'intrus à agir plus tard. Un adversaire passif ne fait que menacer la confidentialité des données.

2.6.3 Attaque Active

Une attaque est active lorsqu'un nœud non autorisé altère des informations de routage en transit par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations dans le fonctionnement du réseau.

2.6.4 Attaque externe ou interne

En outre, selon le domaine d'appartenance d'un nœud, les attaques actives peuvent elles mêmes être classées en deux catégories, à savoir les attaques externes et internes. Tandis que les attaques externes sont réalisées par des nœuds qui n'appartiennent pas au domaine du réseau, les attaques internes sont menées par des nœuds compromis qui sont autorisés à participer au fonctionnement du réseau. Etant donné que les attaquants font d'ores et déjà partie du réseau de nœuds autorisés, les attaques internes sont généralement plus pernicieuses et difficiles à détecter que les attaques externes.

2.6.5 Attaque individuelle ou attaque distribuée

En effet, les attaques peuvent être de type individuelles ou par collusion ou appelée également distribuée. Les attaques individuelles sont menées par un seul nœud attaquant. Puisque les capacités de communication et de calcul de l'attaquant sont en général similaires à celles des autres nœuds du réseau, ces attaques demeurent relativement simples, et sont d'autant plus limitées que des mécanismes de sécurité

sont mis en œuvre. En revanche, rien n'empêche à des nœuds attaquants de mutualiser leurs informations et leurs ressources, en exploitant les connexions qu'ils ont entre eux. Ces attaques par collusion, issues de plusieurs nœuds répartis à différents endroits dans le réseau, sont généralement plus évoluées et plus dangereuses. Par ailleurs, en raison de l'intervention de plusieurs nœuds intermédiaires, leur détection et l'identification précise de leur origine sont rendues plus complexes.

2.6.6 Description des principales attaques

2.6.6.1 Replay ou rejeu

un nœud malicieux réinjecte des messages dans le réseau. Des anciens messages continuent à circuler ce qui occupe de la bande passante et peut même affecter la justesse de la topologie.

2.6.6.2 Spoofing ou usurpation d'identité

consiste à se faire passer pour quelqu'un d'autre en utilisant son identité. L'attaquant se présente en utilisant l'identité d'un nœud légitime et peut ainsi communiquer avec les nœuds du réseau sans être rejeté.

2.6.6.3 Le déni de service

denial of services (DoS), apparaissent comme les attaques les plus faciles à réaliser par un attaquant. La criticité de telles attaques dépend fortement du contexte d'utilisation. Les modèles de dénis de services qui suivent se dégagent plus particulièrement dans le cas de réseau sans fil ad hoc :

- Brouillage du canal radio pour empêcher toute communication.
- Tentative de débordement des tables de routages des nœuds servant de relais.
- Non-coopération d'un nœud au bon fonctionnement du réseau dans le but de préserver son énergie. L'égoïsme d'un nœud est une notion propre aux réseaux ad hoc. Un réseau ad hoc s'appuie sur la collaboration sans condition de ses éléments. Un nœud refusant de jouer le jeu peut mettre en péril l'ensemble.
- Tentative de gaspillage de l'énergie des nœuds. L'attaque consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et ainsi de lui faire consommer toute son énergie. Cette attaque est référencée aussi par l'appellation sleep privation torture attack, un scénario de torture par privation du sommeil.

2.6.6.4 Brouillage (jamming)

Le jamming est une attaque très connue qui s'en prend à la communication sans fil. En effet, vu la sensibilité du média sans fil au bruit, un nœud peut provoquer un déni de service en émettant des signaux à une certaine fréquence pour interférer avec les fréquences radio employées par les nœuds du réseau.[54]

2.6.6.5 attaque du trou noir (Black Hole Attack)

Dans ce cas de figure, un nœud malhonnête tente d'exploiter les failles des protocoles de routage afin de se faire élire comme faisant partie du plus court chemin vers le nœud dont il veut intercepter les paquets. Il pourra donc recevoir les paquets destinés à ses victimes et les supprimer afin de réaliser un déni de service ou bien utiliser son positionnement sur ces routes et lancer par exemple les premières étapes d'une attaque de l'homme du milieu.

2.6.6.6 Rushing attack

Cette attaque s'appuie sur le fonctionnement des protocoles de routage réactifs et plus précisément sur la diffusion des paquets de demande de route. Dans ces protocoles, les nœuds ne tiennent compte que du premier paquet reçu et suppriment toutes les autres copies d'une même demande de route. Dans l'attaque Rushing, l'attaquant exploite cette propriété en devançant les autres nœuds dans l'envoi des paquets de demande de route. Cela est possible en ne respectant pas, par exemple, les délais de transmission des paquets de demande de route tels qu'ils ont été spécifiés par le protocole de routage ou bien en ne respectant pas les délais d'accès aux médias de communication. Un des moyens de contrer cette attaque est de permettre aux nœuds de sélectionner de manière aléatoire la copie de demande de route à relayer. Autrement dit, chaque nœud attend une période de temps t avant de sélectionner aléatoirement une copie d'une demande de route reçue durant cette période de temps.

2.6.6.7 Attaque Wormhole

L'attaque du trou de ver est une attaque particulièrement difficile à contrer. Elle peut être lancée par un attaquant externe et être réussie même en présence d'un système d'authentification et de chiffrement. Une version simple de cette attaque est de faire croire à deux de ses voisins qu'ils sont eux aussi voisins en relayant leurs paquets. Une version plus élaborée de cette attaque nécessite la présence d'au moins deux nœuds malveillants formant une collusion et se trouvant généralement dans des zones géographiquement séparées. Le but de cette version de l'attaque est de former un tunnel entre ces deux nœuds. Ce tunnel est construit de telle sorte que chaque paquet capturé à l'une des extrémités du tunnel soit relayé, à travers ce tunnel, vers le deuxième attaquant se trouvant à l'autre bout du tunnel. Celui-ci à son tour les relaie localement, selon le type du paquet reçu, à ses voisins.
Prenons l'exemple de la figure 2.7. Les paquets hello émis par un nœud A sont capturés par une des extrémités du tunnel X et envoyés vers l'autre extrémité du tunnel Y. Dans ce cas de figure, si le nœud B diffuse, à son tour, le message hello à ses voisins, ces derniers seront induits en erreur quant à l'appartenance du nœud A à leur voisinage.[6]

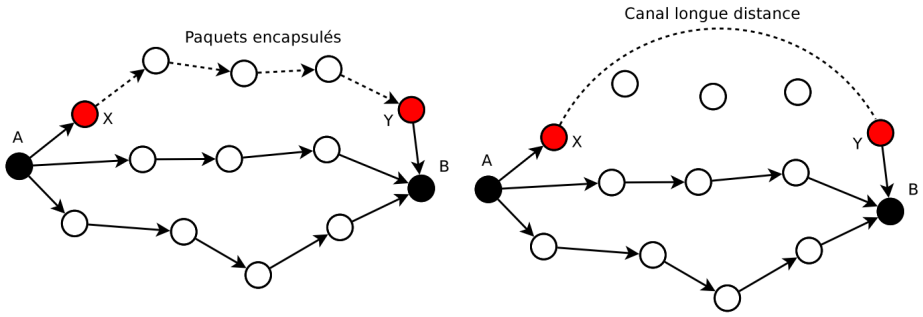

FIGURE 2.7 – Attaque Wormhole

2.6.6.8 Attaque Sybille

L'attaque Sybille a tout d'abord été introduite et décrite par Douceur [14] dans le contexte des réseaux pair-à-pair. Elle a été définie initialement comme le fait qu'un nœud malveillant (Sybil node) parvienne à posséder illégitimement plusieurs identités et simule un ensemble de nœuds associés à ces identités. Par la suite, plusieurs variantes sont apparues dans différentes situations. Elle est considérée comme une attaque très difficile à prévenir ou à détecter dans de nombreux contextes. L'attaque Sybille est également efficace contre les algorithmes de routage, l'agrégation de données, les algorithmes de vote, la répartition équitable des ressources, la détection de nœuds malveillants, etc. Par exemple, pour attaquer un protocole de routage, l'attaque Sybille peut donner l'illusion à un nœud de posséder plusieurs chemins vers une destination alors que tous ces chemins traversent la même entité physique. Afin de se prémunir contre l'attaque Sybille, il faudrait trouver le moyen de vérifier si l'identité d'un nœud est la seule réellement utilisée par son dispositif physique.

2.7 Le routage dans les réseaux ad hoc

Les réseaux ad hoc sont multi-sauts. Il peut donc arriver qu'un mobile veuille communiquer avec un autre qui n'est pas dans sa portÉe de communication directe. Les messages vont devoir être transmis de proche en proche jusqu'à la destination : c'est ce que l'on appelle "le routage". La technique la plus basique est l'inondation, où chaque mobile ré-émet tous les paquets qu'il reçoit pour la première fois. Évidemment, l'inondation consomme beaucoup de ressources (bande passante et énergie) et n'est pas optimale. De nombreux protocoles de routage ont donc été proposés pour rendre les communications multi-sauts plus efficaces (moins de réémissions, chemins plus courts, etc.) que l'inondation basique.[12]

2.7.1 Contraintes de routage dans les réseaux ad hoc

L'accomplissement de la tâche de routage, inhérente à tout réseau, est compliqué dans les réseaux ad hoc par l'utilisation de communications via radio : la radio est en effet le médium le plus hostile à la propagation de l'information, du fait notamment des interférences entre utilisateurs et de la complexité du traitement du signal. D'autre part, le routage ad hoc est aussi compliqué par la mobilité des éléments susceptibles d'acheminer le trafic (c'est-à-dire les utilisateurs eux-mêmes). N'ayant pas été prévus pour ces dernières complications, les algorithmes de routage classiques ne peuvent donc pas être utilisés tels quels. Ils doivent être optimisés (si ce n'est entièrement revus) pour être efficaces dans les réseaux ad hoc : s'adapter aux communications radio en réduisant au maximum le trafic de contrôle nécessaire au bon fonctionnement du réseau, et en même temps rester en mesure de suivre dynamiquement la mobilité des éléments du réseau. Ce sont ces contraintes qui sont au fondement des algorithmes de routage ad hoc.

2.7.2 Routage à plat

Les protocoles de routage "à plat" considèrent que tous les nœuds sont égaux voir figure 2.8. La décision d'un nœud de router des paquets pour un autre dépendra de sa position et pourra être remise en cause au cours du temps.

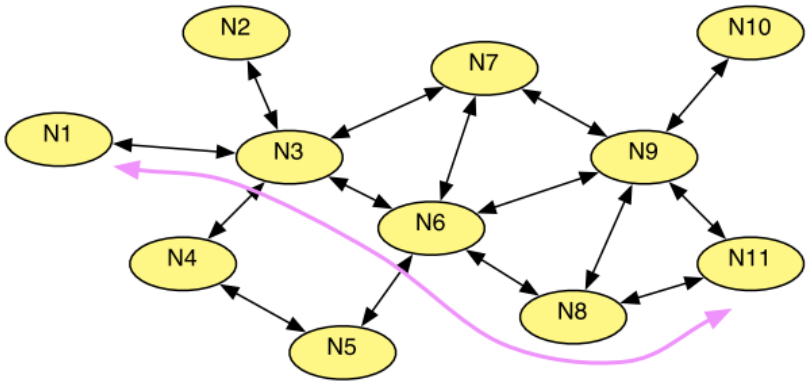

FIGURE 2.8 – Routage à plat

2.7.3 Routage hiérarchique

Les protocoles de routage hiérarchique fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du

réseau. Par exemple, un mobile pourra servir de passerelle pour un certain nombre de nœuds qui se seront attachés à lui. Le routage en sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Un exemple est donné sur la figure 2.9, où le nœud N3 passe par les passerelles P1, P2 et P3 pour atteindre N7. Dans ce type de protocole, les passerelles supportent la majeure partie de la charge du routage (les mobiles qui s'y rattachent savent que si le destinataire n'est pas dans leur voisinage direct, il suffit d'envoyer à la passerelle qui se débrouillera). Dans les réseaux où certains nœuds s'avèrent très sédentaires et disposent de suffisamment d'énergie par exemple réseau d'ordinateurs portables reliés au secteur.

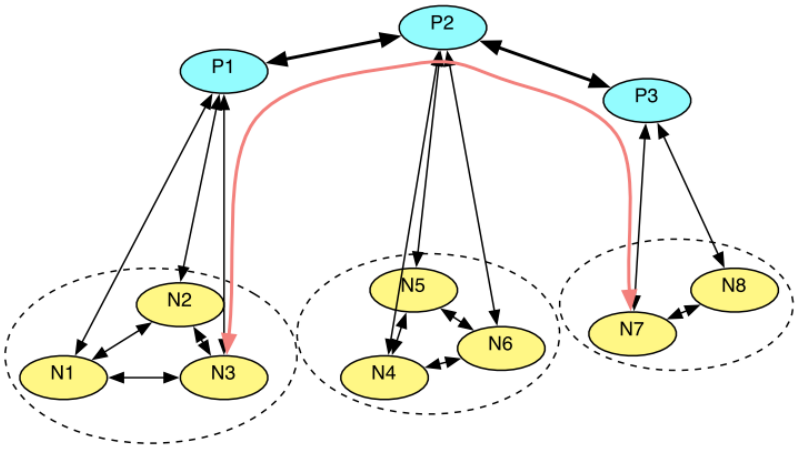

FIGURE 2.9 – Routage hiérarchique

2.7.4 Mécanismes de routage

Il existe une grande diversité de techniques ou encore architectures de routage ad hoc ; ainsi, les protocoles de routage dans les réseaux ad hoc peuvent être classés suivant plusieurs critères, citant par exemple : la consommation de l'énergie, le rôle de chaque nœud dans le réseau, le nombre de messages émis, ... etc.

2.7.5 L'inondation

L'inondation ou la diffusion pure, consiste à faire propager un paquet (de données ou de contrôle) dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins. Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau (voir la figure 2.10). Notons que les nœuds peuvent être amener à appliquer - durant l'inondation - certains traitements de contrôle, dans le but d'éviter certains problèmes, tel que le bouclage et la

duplication des messages.
Le mécanisme d'inondation est utilisé généralement dans la première phase du routage plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination. Un paquet de requête de route est inondé par la source afin qu'il atteigne la station destination. Il faut noter que l'inondation est très coûteuse surtout dans le cas ou le réseau est volumineux (latence, surcharge des messages...etc.), c'est pour cela les protocoles de routage essaient de minimiser au maximum la propagation des paquets inondés en rajoutant d'autres paramètres de diffusion.

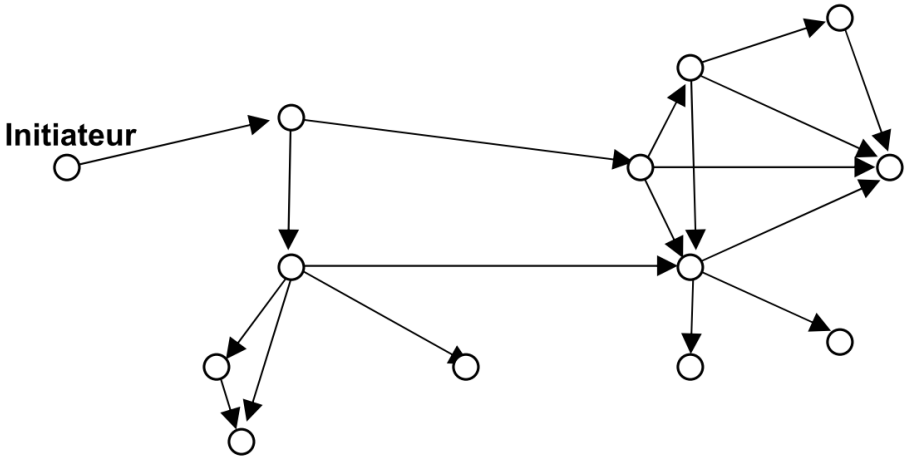

FIGURE 2.10 – Le mécanisme d'inondation

2.7.6 Les différentes familles de protocoles de routage MANET

Dans les travaux menés à l'IETF, plusieurs familles de protocoles de routage ad hoc se sont rapidement dégagés. Chaque protocole peut ainsi être classifié en tant que réactif, proactif, ou hybride. On peut différencier ces protocoles par la méthode utilisée pour découvrir le chemin entre le nœud source et le nœud destination.

2.7.7 Les protocoles proactifs

La méthode proactive identifie en temps réel un sous-ensemble des liens entre les éléments du réseau qui soit suffisant pour que toute paire d'éléments du réseau soit connectée à chaque instant (éventuellement à travers plusieurs liens consécutifs). En efiet, les protocoles proactifs recherchent à intervalle régulier les différentes routes disponibles dans le réseau. Leur principe de base est de maintenir à jour les tables de routage, de sorte que lorsqu'une application désire envoyer un paquet à un autre mobile, une route soit immédiatement connue. Les messages à portée globale ne doivent alors contenir que l'information sur les liens appartenant à ce sous- ensemble, au

lieu de toute l'information sur tous les liens, ce qui constitue une économie certaine. Afin d'identifier de manière distribuée le sous-ensemble de liens essentiels pour que chaque paire d'éléments du réseau soit connectée, les algorithmes de sélection ou d'auto proclamation de relais sont réutilisés. Avec un algorithme d'auto proclamation, il est par exemple suffisant que chaque nœud relais envoie périodiquement un message à portée globale contenant l'information à propos de tous ses liens avec tous ses voisins pour qu'il soit garanti que chaque nœud du réseau possède assez d'information pour trouver un chemin jusqu'à tout autre élément dans le réseau.
Dans le contexte des réseaux ad hoc les nœuds peuvent apparaître ou disparaître de manière aléatoire et la topologie même du réseau peut être changée ; cela signifie qu'il va falloir un échange continuel d'informations pour que chaque nœud ait une image à jour du réseau. Les tables sont donc maintenues grâce à des paquets de contrôle, et il est possible d'y trouver directement et à tout moment un chemin vers les destinations connues en fonctions de divers critères. On peut par exemple privilégier les routes comportant peu de sauts, celles qui offrent la meilleure bande passante, ou encore celles où le délai est le plus faible. L'avantage premier de ce type de protocole est d'avoir les routes immédiatement disponibles quand les applications en ont besoin, mais cela se fait au coût d'échanges réguliers de messages (consommation de bande passante) qui ne sont certainement pas tous nécessaires (seules certaines routes seront utilisées par les applications en général). Le protocole OLSR est un exemple type de cette catégorie.[12]

2.7.8 Optimized Link State Routing (OLSR)

OLSR [8] est un protocole proactif à état de liens. Afin de maintenir à jour les tables de routage, chaque nœud implémentant OLSR diffuse régulièrement des informations sur son propre voisinage. Ces informations sont suffisantes pour permettre à chaque nœud de reconstruire une image du réseau et de trouver une route vers n'importe quelle destination. Mais contrairement à des protocoles tels qu'OSPF, cette diffusion ne se fait pas par une simple inondation (où chaque nœud retransmet simplement chaque nouveau paquet qu'il reçoit) ; OLSR optimise la diffusion grâce au système des relais multi-points (Multi-Points Relays : MPR). Chaque nœud choisit dans ses voisins directs un sous-ensemble minimal de nœuds qui lui permettent d'atteindre tous ses voisins à deux sauts (voir figure 2.11). La diffuusion des informations sur les liens utilisées pour le routage se fait ensuite uniquement par les relais multi-points ; la couverture totale du réseau est assurée tout en limitant sensiblement le nombre de ré-émissions. Afin de choisir ses relais multipoints, un nœud a besoin de connaitre complètement la topologie de son voisinage à deux sauts ;cela est réalisé grâce à l'envoi périodique de paquets hello contenant la liste des voisins à un saut connus. aximum la propagation des paquets inondés en rajoutant d'autres paramètres de diffusion.

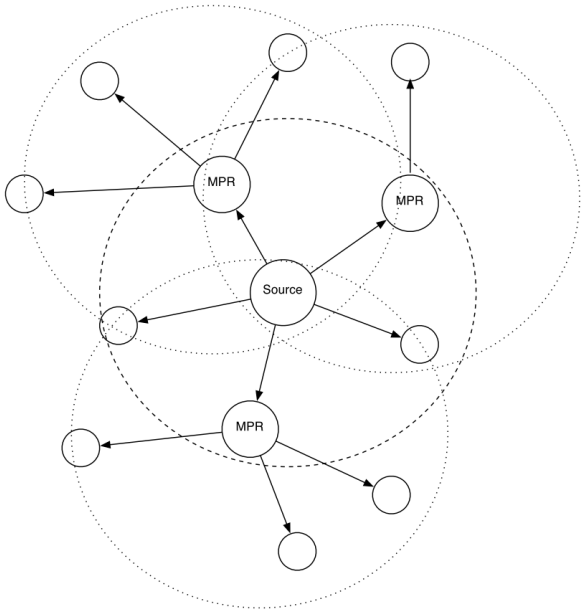

FIGURE 2.11 – Relais multipoints

2.7.9 Le protocole DSDV (Destination Sequenced Distance Vector)

Le protocole DSDV est basé sur l'algorithme distribué de Bellman-Ford [40] Chaque nœud du réseau maintient dans sa table de routage un ensemble d'informations pour chaque destination contenant :

- L'adresse du destinataire : l'identifiant du prochain nœud vers cette destination.
- Le nombre de sauts (nœuds) pour l'atteindre.
- Le plus grand numéro de séquence reçu pour cette destination. Il est utilisé pour permettre au nœud mobile de faire la distinction entre les anciennes routes et les nouvelles routes découvertes.

Afin de maintenir la consistance des tables de routage dans une topologie qui change rapidement, chaque nœud du réseau transmet périodiquement sa table de routage à ses voisins directs. Lors d'une nouvelle diffusion, le nœud incrémente un numéro de séquence et le transmet avec sa table de routage. Celui-ci est utilisé par les autres nœuds pour valider la mise à jour de leur table de routage et éviter les boucles. Afin de limiter le trafic occasionné par toutes ces mises à jour, il existe deux types de mise à jour :

- Des mises à jour complètes ;
- Des mises à jour incrémentales.

Dans la mise à jour complète, la station transmet la totalité de la table de routage aux voisins. Dans les mises à jour incrémentales, seules les nouvelles entrées ou celles qui ont subi un changement, par rapport à la dernière mise à jour, sont envoyées. Cela permet de limiter les informations échangées.

2.7.10 Les protocoles réactifs

La méthode réactive se fonde sur une économie plus poussée, et identifie en temps réel un sous-ensemble de liens suffisant pour acheminer le trafic utilisateur du moment. Les protocoles réactifs ou encore "On Demand " entreprennent la recherche d'une route uniquement avant de transmettre un paquet. Leur principe est de ne rien faire tant qu'une application ne demande pas explicitement d'envoyer un paquet vers un nœud distant. Seuls les liens dont on a besoin, font l'objet d'information de routage. Pour cela, les messages à portée globale ne sont plus envoyés périodiquement, mais seulement à la demande, lorsque du trafic utilisateur doit être acheminé vers une destination vers laquelle un chemin n'est pas connu à ce moment-là. Dans ce cas, un message à portée globale est diffusé dans tout le réseau, en tant que requête pour établir un tel chemin. La destination (ou un nœud connaissant un chemin vers la destination) recevra alors cette requête diffusée, et pourra y répondre pour établir un chemin, envoyant une réponse rebroussant le chemin pris depuis la source de la requête. Cela permet d'économiser de la bande passante et de l'énergie. Une fois que ce chemin est trouvé, il est inscrit dans la table de routage et peut être utilisé. En général, cette recherche se fait par inondation (un paquet de recherche de route est transmis de proche en proche dans tout ou partie du réseau). L'avantage majeur de cette méthode est qu'elle ne génère du trafic de contrôle que lorsqu'il est nécessaire et donc elle réduit de manière drastique la quantité d'information de routage à transmettre, si un nombre réduit de chemins sont utilisés à travers le réseau, et que les nœuds ne sont pas trop mobiles. Les principales contreparties sont que l'inondation est un mécanisme coûteux qui va faire intervenir tous les nœuds du réseau en très peu de temps et qu'il va y avoir un délai à l'établissement des routes. Le protocole AODV est un exemple de protocole de routage ad hoc qui utilise certaines de ces techniques de réduction de la quantité d'information de routage.

2.7.11 Ad-hoc On Demand Distance Vector (AODV)

AODV [38] est un protocole basé sur le principe des vecteurs de distance et appartient à la famille des protocoles réactifs. Les protocoles à vecteur de distance sont en général sujets au problème de boucle et de comptage à l'infini de l'algorithme de Bellman-Ford qu'ils utilisent (certaines parties du réseau se trouvent isolées du reste, et les nœuds les composant vont croire qu'ils peuvent atteindre les nœuds desquels ils sont coupés en passant par leurs voisins. Il s'en suit un phénomène de bouclage dans lequel les nœuds injoignables se voient attribuer des distances de plus en plus grandes). Dans le cas d'AODV, ces problèmes sont résolus par l'utilisation de numéros de séquence pour les messages de contrôle. Quand une application a

besoin d'envoyer des paquets sur le réseau et qu'une route est disponible dans la table de routage, AODV ne joue aucun rôle. S'il n'y a pas de route disponible, il va par contre en rechercher une. Cette recherche commence par une inondation de paquets Route Request (RREQ). Chaque nœud traversé par un RREQ en garde une trace dans son cache et le retransmet. Quand les paquets de recherche de route arrivent à la destination (ou à un nœud intermédiaire qui connait lui-même une route valide jusqu'à la destination), alors un paquet de réponse est généré (RREP) et il est envoyé par le chemin inverse, grâce aux informations gardées dans les caches des nœuds traversés par les RREQ (voir figure 2.12). AODV dispose d'un certain nombre de mécanismes optimisant son fonctionnement. L'inondation se fera par exemple au premier essai dans un rayon limité autour de la source, et si aucun chemin n'est trouvé, alors seulement elle sera étendue à une plus grande partie du réseau. En cas de rupture de certains liens, AODV va essayer de reconstruire localement les routes affectées en trouvant des nœuds suppléants (cette détection de rupture peut d'ailleurs se faire grâce à un mécanisme optionnel de paquets hello diffusés aux voisins directs uniquement). Si une reconstruction locale n'est pas possible, alors les nœuds concernés par la rupture des routes utilisant ce lien sont prévenus de sorte qu'ils pourront relancer une nouvelle phase de reconstruction complète.

2.7.12 Dynamic Source Routing (DSR)

DSR [27] est un autre protocole réactif. Il se différencie des autres en particulier parce qu'il pratique le source routing : l'émetteur précise dans l'en-tête de chaque paquet la liste des nœuds qu'il devra traverser pour atteindre sa destination. Ce type de routage présente certains avantages particulièrement intéressants ; il autorise en particulier la source à conserver dans sa table de routage plusieurs chemins valides vers une même destination. Le choix du chemin emprunté pourra donc être fait indépendamment pour chaque paquet, et permettre un meilleur équilibrage de la charge du réseau ou une meilleure réactivité aux pannes / changements de topologie (plutôt que de tout de suite en construire une nouvelle quand une route est brisée, on en a d'autres à disposition immédiate). Dans la pratique, DSR est structuré en deux sous-parties complémentaires : la recherche de route et la maintenance de route. La recherche de route se fait par inondation : un paquet de recherche est diffusé de proche en proche jusqu'à la destination. Au fur et à mesure, les identifiants des nœuds traversés sont ajoutés dans le paquet de recherche de route. Quand elle reçoit ce paquet, la destination sait donc déejà quel chemin il a emprunté, et obtient ainsi (en l'inversant) la route pour retourner à la source. À la réception par la destination de paquets de recherche ayant suivi des chemins différents, la destination répond sur les chemins inverses, et la source aura ainsi finalement plusieurs chemins valides pour l'atteindre. figure 2.13

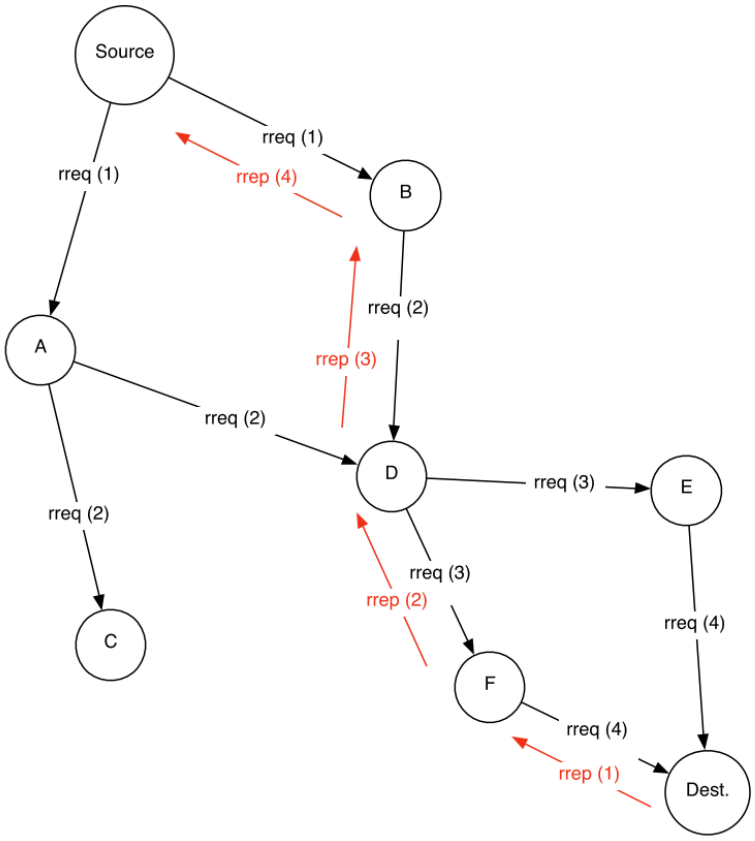

FIGURE 2.12 – Recherche de route par inondation (AODV)

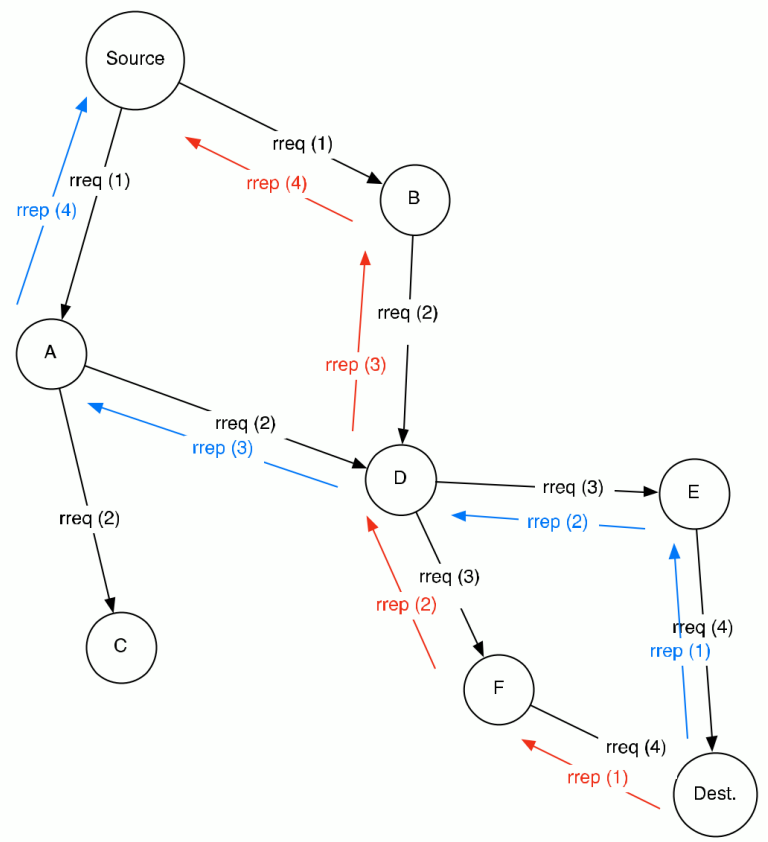

FIGURE 2.13 – Recherche de route par inondation (DSR)

2.7.13 Les protocoles hybrides

Les protocoles hybrides combinent les approches réactive et proactive. Le principe est de connaître notre voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre sauts), et si jamais une application cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, d'effectuer une recherche réactive à l'extérieur. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée (un nœud qui reçoit un paquet de recherche de route réactive va tout de suite savoir si la destination est dans son propre voisinage. Si c est le cas, il va pouvoir répondre, sinon il va propager de manière optimisée la demande hors de sa zone proactive). Selon le type de trafic et les routes demandées, ce type de protocoles peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l ensemble de réseau pour chercher une route vers un nœud éloigné.

2.7.14 Le protocole ZRP (Zone Routing Protocol)

ZRP [23] définit pour chaque nœud une zone de routage (zone radius), qui inclut tous les nœuds dont la distance minimale (en nombre de sauts) à ce nœud est d. Les nœuds qui sont exactement à distance d sont appelés nœuds périphériques. Pour trouver une route vers des nœuds situés à une distance supérieure à d, ZRP utilise un système réactif, qui envoie une requête à tous les nœuds périphériques. Pour cela, ZRP met en œuvre deux types de fonctionnement : IARP (IntrAzone Routing Protocol) et IERP (IntErzone Routing Protocol).
Basé sur un protocole à vecteur de distance, IARP permet, en utilisant une technique proactive, de trouver toutes les routes jusqu'à une distance d. IERP quant à lui, permet d'établir les routes vers les nœuds à plus de d sauts d'une façon réactive.
Le processus de recherche de route fonctionne de la façon suivante :

- si une route est connue, cela signifie que la destination est à moins de d sauts. Cette route est la route retournée par le protocole ;
- si aucune route n'est connue, cela signifie que le nœud est situé à une distance supérieure à d. Dans ce cas, le nœud envoie une requête par IERP à tous les nœuds périphériques ;
- si un nœud périphérique a connaissance d'une route disponible, il renvoie une réponse. Dans le cas contraire, le protocole se poursuit récursivement jusqu'à obtention d'une route.[6]

2.8 Qualité de service 'QoS' dans les réseaux sans fil

La Qualité de Service (QoS) regroupe un ensemble de mécanismes et de technologies capables d'assurer un bon acheminement des données, pour différents types de trafics, entre les entités du réseau.
Les réseaux informatiques n'ont pas été initialement prévus pour prendre en compte

les paramètres de QoS. Les ressources en bande passante étaient limitées. De ce fait les premières générations de réseaux ont soufert de faibles niveaux de débits et ont subi des délais considérables pénalisant la transmission des données.
Les groupes de recherche ont été contraint de mettre en place de nouveaux mécanismes de gestion des retransmisssions et de correction d'erreur afin d'être en accord avec les principes fondamentaux d'Internet (simplicité, fiabilité, universalité).
Afin de garantir cette qualité de service, trois protocoles se sont imposés : [15]

1. Intserv (Integrated Service, protocole inclus dans RSVP (Ressource Reservation Protocol))
2. Diffserv (Differentiated Services)
3. MPLS (Multi-Protocol Label Switching)

Les modèles de qualité de service IntServ/RSVP [57] et DiffServ [5] ont été proposés par l'IETF pour fournir des garanties aux besoins des services temps réel dans les réseaux filaires. D'un coté, l'application du modèle IntServ dans MANET s'avère inadaptée à l'environnement ad hoc. Ceci est justifié du fait que les capacités des nœuds mobiles sont trop variables et limitées pour supporter un traitement complexe et gérer les réservations ainsi que les états des communications en cours. De plus, une réservation dans les réseaux filaires est différente de celle d'un réseau mobile sans fil, car les liens sont partagés, limités, et susceptibles à des variations spatio-temporelles. D'un autre coté, le modèle DiffServ semble le mieux adapté aux réseaux mobiles. Pour résoudre le problème de passage à l'échelle, ce modèle utilise une granularité par classe, où aucune signalisation pour la réservation de ressources n'est utilisée. Cependant, dans ce modèle le cœur du réseau est supposé bien dimensionné, et un administrateur de domaine est nécessaire. Ces deux contraintes restent difficiles à satisfaire.

Le modèle FQMM [53] repose sur une architecture réseau plate (non hiérarchique), constituée d'une cinquantaine de nœuds mobiles, formant un domaine DiffServ. Il combine les propriétés des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride : par flux, pour les trafics prioritaires, et par classe pour les autres trafics. Dans le réseau, les nœuds peuvent avoir des rôles différents suivant les trafics existants : nœud d'entrée du trafic, intermédiaire ou de sortie. Les nœuds d'entrée permettent de marquer et classifier les paquets, qui seront ensuite relayés par les nœuds intermédiaires suivant leurs PHB (Per Hop Behavior), jusqu'à arriver au nœud destinataire. Ce modèle repose essentiellement sur la couche IP, où les fonctionnalités sont séparées en deux grands plans : le plan relayage de données et le plan contrôle et gestion. Les techniques d'ordonnancement et de gestion de mémoires tampons sont étudiées. Dans ce modèle, le protocole de routage est supposé fournir des routes ayant suffisamment de ressources. L'avantage d'une telle approche est la possibilité d'interfacer le réseau avec l'Internet, vu les mécanismes de qualité de services offerts qui sont proches des protocoles filaires. Cependant, plusieurs mécanismes ainsi que l'interaction avec la couche MAC

restent à définir pour s'adapter aux conditions variables du réseau ad hoc.[32]

2.8.1 Les métriques de QoS dans les MANET

La plupart des applications informatiques requièrent généralement une configuration matérielle minimale pour bien fonctionner. Les applications déployées dans un réseau spécifient en plus les contraintes que le réseau doit satisfaire pour que leur exécution corresponde à un niveau de qualité bien défini. Du point de vue du réseau, ces critères se traduisent en général en termes de capacité, de disponibilité, de latence et de fiabilité. Selon le type de réseau, ces concepts abstraits sont traduits en grandeurs mesurables identifiées sous le terme général de métrique. Les stations d'un réseau mobile ad hoc concentrent toutes les fonctionnalités liées au routage. De ce fait, toutes les métriques généralement prises en compte par les routeurs pour assurer le routage doivent pouvoir être prises en compte par toute station dans un MANET. Aux métriques qui caractérisent les liaisons sans-fil en général, peuvent s'ajouter des métriques liées à la spécificité des réseaux mobiles ad hoc. En effet, les stations d'un MANET sont en général caractérisées par des ressources limitées. L'état interne de la station, notamment son autonomie énergétique peut influer directement sur son aptitude à participer au routage. La mobilité des nœuds induit également la nécessité de considérer des métriques telles que la stabilité d'une liaison ou sa durée de vie. [24].

2.8.2 Les métriques caractérisant les stations

Certaines métriques sont utilisées soit pour décrire l'état interne d'une station, soit pour caractériser cette dernière vis-à-vis de ses voisins ou de l'ensemble du réseau [35] :

- La charge résiduelle de sa batterie ou l'autonomie énergétique d'une station peut être associée à une métrique permettant de l'évaluer par rapport aux autres stations. En effet, l'épuisement de la batterie d'une station entraîne sa déconnexion du réseau, ce qui peut engendrer la disparition de plusieurs liaisons. Les conséquences peuvent aller jusqu'à la déconnexion d'une partie du réseau si la station concernée était le seul pont qui la reliait au reste du MANET. La durée de vie d'une station est également une métrique parfois associée à l'autonomie énergétique de cette station.
- La capacité disponible du buffer de transmission d'une station est une métrique liée au trafic généré ou retransmis par une station. Elle permet par exemple de déterminer les stations les moins chargées pour la retransmission des paquets.
- La mobilité ou la stabilité d'une station par rapport à son voisinage a également inspiré des métriques permettant de caractériser les stations d'un MANET.
- La capacité d'adaptation d'une station face à la mobilité ou à la densité dans son voisinage peut également être associée à des métriques susceptibles de

jouer un rôle dans le choix des nœuds retransmetteurs de paquets.

2.8.3 Les métriques caractérisant les liaisons

La grande majorité des métriques étudiées dans les MANET caractérisent plutôt les liaisons entre les stations [35] :

- Le débit minimum disponible sur une liaison ou sur une route est l'une des métriques ayant fait l'objet d'un très grand nombre d'études. Il correspond à la capacité d'une route entre une station source et une station destination. Bien que la règle permettant de calculer cette capacité sur une route constituée de plusieurs liaisons soit assez claire, la valeur obtenue dépend des valeurs des capacités de chaque liaison. Le problème est que cette valeur dépend de tellement de facteurs dans les réseaux sans fil en général, et dans les MANET en particulier, qu'aucune des méthodes d'estimation proposées jusqu'à présent ne fait l'unanimité.
- Le délai de bout-en-bout est le temps qui s'écoule entre le moment où un paquet est enregistré pour un envoi par la source et le moment où il est intégralement reçu par la destination.
- La gigue est la variation entre la valeur maximale observée sur le délai de bout-en-bout et le délai de transmission minimum observé.
- La robustesse d'une liaison qui est généralement associée à la valeur estimée ou effectivement mesurée du taux de perte de paquets sur une liaison.
- La stabilité d'une liaison ou d'une route est également une métrique intéressante. On peut aussi bien la corréler à la stabilité des stations impliquées qu'à leur durée de vie.

Chapitre 3

Architecture d'authentification utilisant la cryptographie à seuil dans Kerberos pour MANETs

Sommaire

3.1 Introduction

L'utilisation des technologies sans fil augmente progressivement et les risques liés à l'utilisation de ces technologies sont considérables. En raison de leur topologie ayant une évolution dynamique et l'environnement ouvert sans une politique

contrôle centralisée d'un réseau traditionnel, un réseau mobile ad hoc (MANET) est vulnérable à la présence des noeuds malveillants et les attaques. La solution idéale pour surmonter une myriade de problèmes de sécurité dans les MANET est l'utilisation d'une l'architecture d'authentification fiable. Dans ce chapitre, nous proposons un nouveau système de gestion de clé basé sur la cryptographie à seuil de dans Kerberos pour les MANETs, le schéma proposé utilise la cryptographie à courbe elliptique, procédé qui consomme moins de ressources et parfaitement adapté au environnements sans fil. Notre approche montre une force et une efficacité contre les attaques connus.[21]

3.1.1 Contexte

Un réseau mobile ad hoc est formé par une population de noeuds sans fil sans infrastructure préexistante de réseau ou une administration centrale. Cette nature, le rends facile à déployer en particulier dans les environnements où il est difficile de mettre en œuvre un réseau régulier. Les réseaux MANET peuvent être utilisés dans des applications civiles et militaires où la sécurité des échanges doit être assurée.

3.1.2 Motivation

L'authentification des utilisateurs est une importante mesure de sécurité pour protéger les données confidentielles. Sans un moyen de vérifier un utilisateur, l'accès aux données peut être accordée à des utilisateurs ou des groupes qui ne sont pas normalement autorisés. Si le nombre de noeuds est petit, l'authentification noeud à noeud est relativement facile à mettre en œuvre, mais si le nombre de noeuds devient important, une stratégie de sécurité totale doit être soigneusement mis en place. L'introduction d'un tiers de confiance (Trusted third party ou TTP) est fortement recommandée. Pirzada et McDonald dans [41] ont utilisé un TTP basée sur Kerberos, d'où on a inspiré notre idée. Bien que ce modèle est largement utilisé, il a hérité toutes les faiblesses du système d'authentification Kerberos [4], telles que les attaques par devinnetes et les attaques par rejeu et la présence d'un point de défaillance unique qui constitue la fiablesse majeure du système d'où la nécessité d'une disponibilité permanente d'un serveur central. Lorsque le serveur Kerberos est en panne , personne ne peut être identifitié pour accéder à un tel service. Pour remedier à ça on a procédé à une répartition des serveurs d'authentification en utilisant une cryptographie à seuil sur des courbes elliptiques qui produit moins de calculs le rendant bien souhaité pour les MANET.

3.1.3 Travaux connexes

Le Schéma de partage de secret a été introduit par Shamir dans [44]et maintenant il est largement utilisé dans de nombreux potocols cryptographiques comme outil de sécurisation de l'information [58, 3, 22, 10, 43, 36, 33]. Zhou et al. dans [58] ont proposé l'utilisation de cryptographie à seuil pour garantir la sécurité dans les réseaux Ad-Hoc et ont énuméré les défis dans la conception d'un tel système. Dans

[3] Azer et al. ont décrit une étude sur une technique d'authentification basée sur le même principe et ont décrit également certains défis à prendre en compte.
Dans [22] Govindan et Mohapatra présentent une étude détaillée sur les différentes approches de calcul de confiance orientées MANET. Une approche sur la gestion des clés distribuées et authentification en déployant les concepts de la cryptographie basée sur l'identité et le partage du secret à seuil a été proposé dans [10]. Dans [43] un schéma basé cryptographie à seuil avec RSA pour les MANET utilisant le partage de secret vérifiable (VSS) est présenté. Un autre schéma présenté dans [36] propose un système de gestion de clés des certificats à clé public entièrement distribuée basée sur des graphes de confiance et cryptographie à seuil. Dans [33], les auteurs utilisent une signature à seuil dans les MANET regroupés en clusters anonymes. Cependant, aucun de ces travaux ci-dessus utilise Kerberos [34] comme TTP en cryptographie à seuil dans les MANET.
Au meilleur de nos connaissances, notre architecture de sécurité proposée est la première dans laquelle l'authentification est basée sur la distribution des serveurs Kerberos (TGS) combinée avec cryptographie à seuil dans les réseaux mobiles ad hoc (MANET).

3.1.4 Défis et enjeux

La principale vulnérabilité des MANETs vient de leur architecture ouverte. Contrairement aux réseaux câblés qui ont des routeurs dédiés, chaque nœud mobile dans un réseau ad hoc peut fonctionner comme un routeur et achemine les paquets pour les autres nœuds [55]. Le canal sans fil est accessible aux utilisateurs légitimes du réseau et aussi pour les attaquants malveillants. La sécurité des réseaux sans fil est sensible à une série de problèmes inexistants dans les réseaux filaires. Dans les réseaux sans fil, les flux de données propagent dans l'air, ce qui les rend facile à être intercepté par des intrus faisant des écoutes indiscrètes, pouvant aussi injecter des messages malveillants. Les réseaux sans fil ont aussi des limites floues difficiles à contrôler. Les appareils sans fil dans le réseau peuvent être la cible d'attaques physiques. Par conséquent, les secrets et les données sensibles pourraient être extraites. La capacité de calcul d'un nœud mobile est aussi une contrainte du moment que le nœud ne peut pas effectuer des tâches de calcul intensif tel que le calcul cryptographique asymétrique en raison des sources d'énergie limitées des batteries. La topologie du réseau est très dynamique en tant que les nœuds rejoignent et quittent fréquemment le réseau. Le canal sans fil est également soumis à des interférences et des erreurs qui affectent la bande passante et les délais de transmission. Malgré cette dynamique, les utilisateurs mobiles peuvent demander à tout moment et n'importe où des services de sécurité lors des déplacents d'un endroit à un autre.
La solution de sécurité doit tenir compte de tous ces aspects pour la performance et la qualité de service souhaité.
La solution idéale doit prendre en considération :

- La collaboration de tout les nœuds mobiles pour contrecarrer les attaques.
- La solution doit s'étendre sur toutes les couches du réseaux, chaque couche

contribue à une ligne de défense.
- La solution de sécurité doit déjouer les menaces internes et externes.
- Enfin et surtout, la solution de sécurité doit être très bien pensée et adaptée au réseau à sécuriser.

3.1.5 Organisation du chapitre

Le chapitre est organisé comme suit : d'abord, nous présentons un bref aperçu du système d'authentification Kerberos et le cryptosystème à seuilElGamal . Ensuite, nous présentons notre modèle proposé suivi d'une analyse de la sécurité. Enfin, nous comparons notre proposition avec les schémas à basés seuil-RSA.

3.2 PRELIMINAIRES

3.2.1 Le protocole d'authentification Kerberos

Kerberos est un protocole d'authentification réseau créé par MIT utilisant une cryptographie à clé symétrique pour authentifier les utilisateurs à des services réseau. Kerberos utilise des tickets au lieu de mots de passe, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.

3.2.1.1 Kerberos credentials

Kerberos a deux types d'informations d'identification (credentials) : Les tickets et les authentificateurs. Un ticket est utilisé par un utilisateur pour s'authentifier auprès d'un serveur à partir duquel il demande un service, il contient l'ID du serveur (Identifier), l'ID de l'utilisateur, un horodatage, une durée de vie, et une clé de session chiffrée par la clé du serveur d'authentification. Un authentificateur est utilisé pour prévenir les attaques par rejeu. En général, un authentificateur contient l'ID de l'utilisateur et un horodatage chiffré avec une clé de session partagée entre l'utilisateur et le serveur d'authentification

3.2.1.2 Les Échanges Kerberos :

Le protocole Kerberos est composé de trois échanges : le serveur d'authentification (AS), Le service de délivrance de tickets (TGS) et le serveur d'application (AP). L'échange AS permet au client d'obtenir des informations d'identification pour prouver son identité au TGS. L'échange TGS permet au client de s'authentifier auprès du TGS et obtenir un ticket de service pour le service souhaité. L'échange AP est effectué entre le client et le service pour authentifier le client avant de lui accorder l'accès aux ressources. voir figure 3.1

3.2.2 Partage de clé secrète de Shamir

Partage de secret se rapporte à des méthodes pour la diffusion d'un secret au sein d'un groupe de participants (appelé aussi associés), dont chacun est affecté une

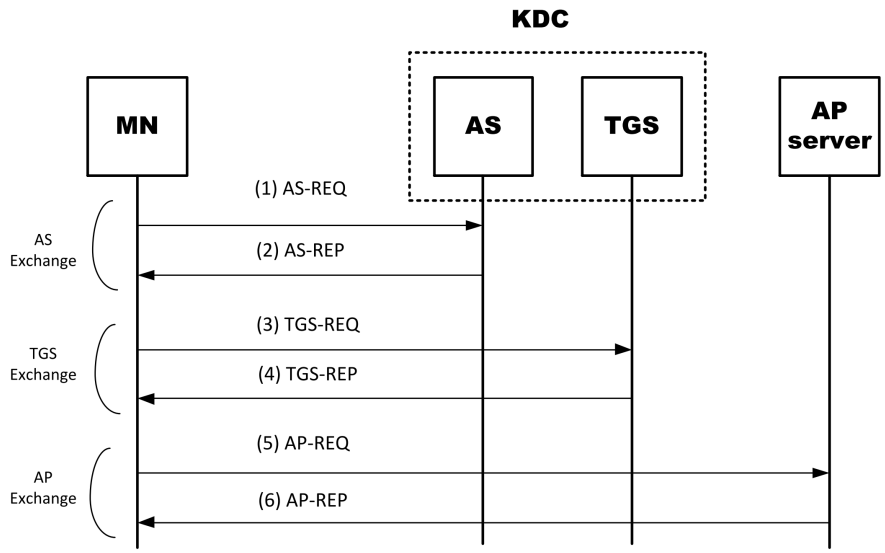

FIGURE 3.1 – Les échanges du protocole Kerberos

part du secret. Le secret peut être reconstruit si un nombre suffisant de pièces est réuni. Dans le cas de partage de secret (k, n), le secret est distribué aux participants n, et tout k de ces n participants peut reconstruire le secret, mais n'importe quelle collection de moins de k actions partielles ne peut obtenir aucune information sur le secret [11].

- La phase de négociation :

- Soit s un secret de certains $\mathbb{Z}_p$, p : premier
- Sélectionner un polynôme aléatoire
  $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots f_{k-1} x^{k-1}$
  sous la condition que : $f(0) = s$:
- Choisir $f_1, \ldots, f_{k-1} \leftarrow \mathcal{R}\ \mathbb{Z}p$ aléatoirement
- Définir $f_0 \leftarrow s$
- Pour $i \in [1, n]$, partage le secret $s_i = (i, f(i))$ à la i^{th} partie
  Le secret s peut être reconstruit à partir de chaque sous-ensemble de k participants par la formule de Lagrange,
  Étant donné de k points (x_i, y_i), $i = 1, \ldots, k$,

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} (mod\ p)$$

Et

$$s = f(0) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{-x_j}{x_i - x_j} (mod\ p)$$

Tout sous-ensemble d'un maximum de $k-1$ part ne peut avoir d'informations sur le secret.

3.2.3 ElGamal Cryptosystème à Seuil avec courbes elliptiques

Le Cryptosystème ElGamal est basé sur la difficulté de résoudre le problème de logarithme discret [17]. Nous supposons que nous avons un tiers de confiance (TTP) - Kerberos dans notre cas - que met en place le système.
phase 1 : La génération des clés pour (t, n)

- Choisir une grand nombre premier : un nombre premier p tel que $p = 2q + 1$, q aussi premier.
- Trouver un générateur g d'ordre q.
- Choisir un nombre aléatoire $a \in \mathbb{Z}q$ et calculer $y = \beta^x$.
- Calculer un polynôme aléatoire de degré $t-1$
  $f(x) = a + \sum_{j=1}^{t-1} a_i x^i \ mod\ p$, les a_i sont choisis aléatoirement.
- Calculer les n parties de a : $s_i = f(x_i)$ pour chaque utilisateur i.
  La clé publique est $pk = (p, g, \beta)$ et et la clé privée principale est $sk = (x)$
  La clé privée principale n'est donnée à personne.

phase 2 : Chiffrement

- Choisir un nombre aléatoire $k \in \mathbb{Z}q$ et calculer $c_1 = g^k mod\ p$.
- Calculer $c_2 = m\beta^k mod\ p$.
- Le cryptogramme est : $c = (c_1, c_2) = (g^k, m\beta^k)$

phase 3 : Décryptage
Pour déchiffrer un message chiffré $c = (c1, c2)$, les t participants doivent demander au TTP de leurs parties de décryptage de ce message chiffré.
Le TTP cacule $d_i = c_1^{s_i} = \left(g^k\right)^{s_i} mod\ p$ pour chaque utilisateur i qui demande la partie de décryptage.
Supposons que I est l'ensemble des t participants qui ont demandé une partie de décryptage. Une fois que chaque utilisateur dispose de sa partie de décryptage $d_i = g^{k s_i} = g^{kf(x_i)}$, les utilisateurs coopèrent pour calculer :
$d = \prod_{i \in I} d_i^{\Lambda_i} \equiv \prod_{i \in I} \left(g^{kf(x_i)}\right)^{\Lambda_i} \equiv \prod_{i \in I} g^{kf(x_i)\Lambda_i} \equiv g^k \sum_{i \in I} f(x_i)\Lambda_i \equiv g^{kf(0)} \equiv g^{ka}\ (mod\ p)$
Les participants doivent coopérer pour :

- Calculer les Λ_i valeurs et
- Calculer g^{ka}

Le texte en clair est calculée comme :[45]
$m = c_2 d^{-1} = \left(m\beta^k\right)\left(g^{ka}\right)^{-1} = m g^{ka} g^{-ka} = m\ mod$
phase 4 : Seuil ElGamal avec Courbes elliptiques
Cette opération peut se faire en convertissant un message à un point sur une courbe elliptique et vice-versa, en utilisant la méthode de Koblitz [28, 37].

phase 5 :
Enfin, nous utilisons la formule d'interpolation de Lagrange pour récupérer le message.

3.3 NOTRE PROPOSITION

Notations	Descriptions
MN	Nœud Mobile
AS	Serveur d'authentification
TGS	Le service de délivrance de tickets
ID_x	l'identité de x
TKT_x	Ticket de l'entité x
T^i	Horodatage $i = ', '', ''', '''', '''''$
E_k	chiffrement par la clé k
$K_{x,y}$	la clé partagée entre x et y
$AUTH_{x,y}$	Authentificateur entre x et y

TABLE 3.1 – Notations utilisées dans ce chapitre

Le noeud mobile envoie un ticket spécifiant les ressources souhaitées et un authentificateur au serveur d'authentification crypté avec la clé MN/AS (pré-distribué via un canal sécurisé lors de la phase d'inscription ou d'enregistrement). L'AS confirme l'identité de MN, s'il est valide, il répond au MN avec une version modifiée de l'horodatage dans l'authentificateur chiffré avec la clé MN/AS. Dans cette phase, au lieu d'utiliser un seul TGS, nous utilisons le Cryptosystem à seuil ECC-ElGamal pour diviser le TGS en plusieurs parties pour permettre une authentification à seuil, cela signifie qu'un seul TGS ne peut pas garantir l'achèvement du processus d'authentification sans la participation d'un nombre prédéfini d'autres TGS.

3.3.1 Détails de la proposition

1. Le MN (Mobile Node) demande un TGT (Ticket Granting Ticket), le MN envoies un message au AS pour demander un service, ce TGT comprend le ID_{MN} et le ID_{TGT}.
2. L'AS accorde un TGT pour MN. L'AS vérifie l'identité de MN. Si MN est valide, l'AS crée un ticket TGT tgs et génère une clé de session $K_{MN,TGS}$ chiffrée par la clé du MN K_{MN} pour protéger la communication entre MN et TGS, et envoies tout cela à MN. Le ticket TGS comprend le ID_{MN}, le ID_{TGS} - des TGS participants-, un horodatage, la période de validité du Ticket, et la clé de session $K_{MN,TGS}$. Le K_{MN} n'est connu que par le MN et l'AS.

Algorithm 3.1: TGS distribués

1 MN envoies une requette TGT au AS, $MN \rightarrow AS : ID_{MN} \parallel ID_{TGS} \parallel T^{'}$
2 AS accorde un TGT to MN et si ID_{MN} est validé continuer sinon rejet de la requette : $AS \rightarrow MN : ID_{MN} \parallel TKT_{TGS} \parallel E_{kMN}[K_{MN,TGS} \parallel T^{''} \parallel ID_{TGS}]$
$TKT_{TGS} = E_{KTGS}[K_{MN,TGS} \parallel ID_{MN} \parallel T^{''} \parallel ID_{TGS}]$
3 **repeat**
4 $MN \rightarrow TGS : ID_{AP} \parallel TKT_{TGS} \parallel AUTH_{MN,TGS}$
$AUTH_{MN,TGS} = E_{K(MN,TGS)}[ID_{MN} \parallel T^{'''}]$
5 $TGS \rightarrow MN : \ ID_{MN} \parallel TKT_{AP} \parallel E_{K(MN,TGS)}[K_{MN,AP} \parallel T^{''''} \parallel ID_{TGS}]$
$TKT_{AP} = E_{KAP}[K_{MN,AP} \parallel ID_{MN} \parallel ID_{AP} \parallel T^{''''}]$
6 $MN \rightarrow AP : TKT_{AP} \parallel AUTH_{MN,AP}$
$AUTH_{MN,AP} = E_{K(MN,AP)}[ID_{MN} \parallel T^{'''''}]$
7 $AP \rightarrow MN : \ E_{K(MN,AP)}[T^{'''''}]$
8 $k = k + 1$
9 **until** $k = r$ *(r : le min de TGS participants)*
10 $k < n$ (n : nombre total de $TGSs$)

3. Après avoir reçu le message des TGS participants, le MN décrypte le message pour obtenir le ticket TGS et $K_{MN,TGS}$. Quand il demande un ticket AP, le MN doit envoyer un message de demande au TGS, comprennant l'ID de l'AP, le ticket TGS et l'authentificateur $AUTH_{MN,TGS}$ crypté par la clé $K_{MN,TGS}$.
4. Les TGS participants accordent un ticket AP à MN. Dès la réception de la requette de MN, les $TGSs$ décryptent le ticket TGS en utilisant ses propres clés secrètes pour obtenir $K_{MN,TGS}$, puis ils l'utilisent pour déchiffrer $AUTH_{MN,TGS}$, cela peut confirmer la ligitimité du MN, ensuite ils génèrent une clé de session $K_{MN,AP}$ pour la communication de service de entre MN et AP, puis ils créent un ticket AP, qui comprend l'ID de MN, l'ID_{AP}, un nouveau horodatage, une période de validité du ticket AP et K MN, AP. Puis les TGS chiffrent le ticket AP en utilisant K_{AP} et la clé de session $K_{MN,AP}$ en utilisant $K_{MN,TGS}$ et les envoie à MN qui peut déchiffrer le message à l'aide de $K_{MN,TGS}$ pour obtenir Ticket AP et $K_{MN,AP}$.
5. Le MN transmet le ticket AP pour le serveur d'application avec un nouvel authentificateur $AUTH_{MN,AP}$.
6. AP décrypte ticket AP et $AUTH_{MN,AP}$ séparément, et juge si les demandes sont authentiques en comparant les informations contenant dans toutes les précendentes communications et plus précisément les horodateurs pour empêcher une attaque de relecture.

3.3.2 Avantages de notre architecture proposée

Notre système garantit la disponibilité du service ; dans le traditionnel Kerberos les KDCs sont des points de défaillance unique, en divisant le TGS en n parties et

au moins k pièces sont nécessaire à la réalisation de l'opération d'authentification, faisant ça, nous fournissons une garantie déterministe de sécurité. En outre, notre architecture basée sur les courbes elliptiques avec une cryptographie à seuil peut offrir une sécurité équivalente à d'autres schémas avec une réduction du temps de traitement et avec une taille de clé plus petite [48].Voir tableau 3.2

RSA	Courbes elliptiques
1024	160
2048	224
3072	256

TABLE 3.2 – Tailles de clé en bits pour des niveaux équivalents

3.4 ANALYSE

3.4.1 Mesure du niveau de sécurité pour les TGS distribués

En supposant que les nœuds TGS distribués sont anonymes et un adversaire ne peut pas découvrir leurs identités, la meilleure approche pour l'adversaire est de compromettre autant de nœuds que possible dans un laps de temps donné, en espérant que suffisamment de nœuds TGS figurent parmi les nœuds compromis. L'équation suivante résume cette situation [56] , qu'on a simulé avec le langage R [47].

$$\text{Le niveau de sécurité} = 1\text{-} \frac{\sum_{c}^{i=k} \binom{n}{i} \binom{M-n}{c-i}}{\binom{M}{c}}$$

On insiste sur le fait que si la différence entre n et k est trop grande, la sécurité du système peut se détériorer.Voir figure 3.2

3.4.2 Complexité de calcul

Les calculs dans notre proposition dépendent des opérations des clés, telles que le cryptage, le décryptage, la distribution et la vérification des clés. La génération de la clé principale utilise le partage de secret à seuil, et la complexité de calcul vient du nombre de participants.

3.4.3 Temps de traitement

D'après les résultats présentés dans [20, 19, 29]. Il est très clair que l'utilisation de la cryptographie avec des courbes elliptiques est très approprié pour les environnements sans fil. Comme le montre la figure 3.3. Au niveau de la sécurité 192

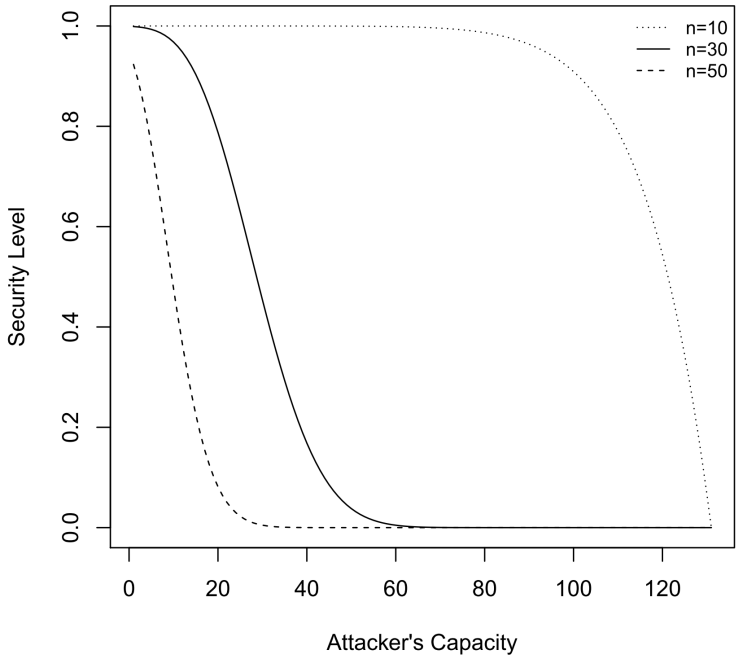

FIGURE 3.2 – Le niveau de sécurité

bits, ECCEG-TC est à peu près de 2 à 3 fois plus rapide qu'avec les opérations de génération des clés privés de 1024 bits de RSA ce qui est plus que le niveau de sécurité requis, voir tableau 3.2.

3.4.4 La prévention des attaques de devinettes

Notre système est résistant aux attaques de devinettes, l'introduction de l'horodatage chiffrés dans les messages échangés, rendent la tâche difficile pour un attaquant essayant d'entrer les mots de passe deviné[30, 9, 7, 42].

3.4.5 La prévention des attaques de rejeu

Nous utilisons un horodatage synchronisée intégrée dans le message dans une fenêtre de temps de réception pour empêcher la les attaque de rejeu ; cette contremesure garantit la fraîcheur des messages dans une session.

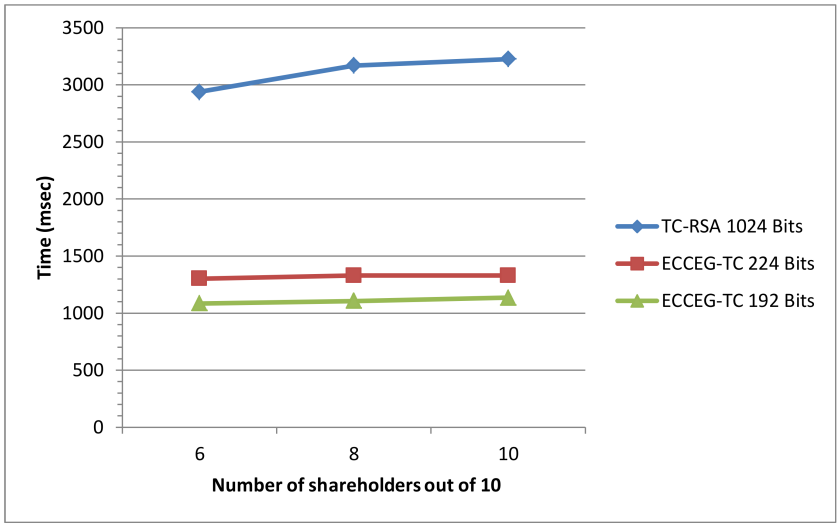

FIGURE 3.3 – Temps de traitement

3.5 Impact de la population des nœuds

Dans ce que va suivre toutes les simulations sont faites avec un algorithme ECCEG-TC avec une clé de 192 bits.
Comme le montre la figure 3.4, le temps de latence augmente sous-linéairement avec l'augmentation de la taille du réseau. Il a été observé, par exemple, pour un réseau MANET de 100 nœuds avec une latence d'environ 0,8 s pour le seuil t = 3 et 1 s pour t = 8. nous remarquons que notre schéma de sécurité augmente légèrement la latence mais reste acceptable par rapport à d'autres schémas plus gourmands.

3.6 Impact de la densité du réseau

La densité du réseau a des influences directes sur le nombre de nœuds dans le voisinage du demandeur ainsi que de l'allocateur. On observe dans la figure 3.5 un temps de latence de plus en plus significatif lorsque la densité est faible. Dans ce cas, le nombre de voisins d'un seul saut est faible, conduisant à de nombreuses recherches en élargeant le cercle en particulier lorsque le seuil est élevé. La latence augmente également lorsque la densité est élevée en raison de l'augmentation du nombre de messages échangés pouvant provoquer des collisions. A noter que la valeur moyenne du temps de latence reste inférieure à 3 secondes, ce qui bien en pratique.

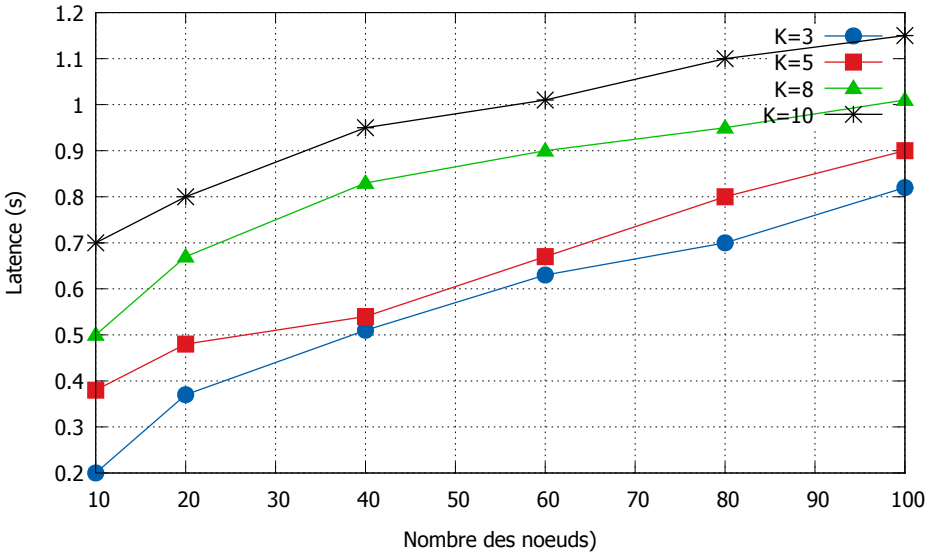

FIGURE 3.4 – Variation de la latence en fonction de la population des nœuds

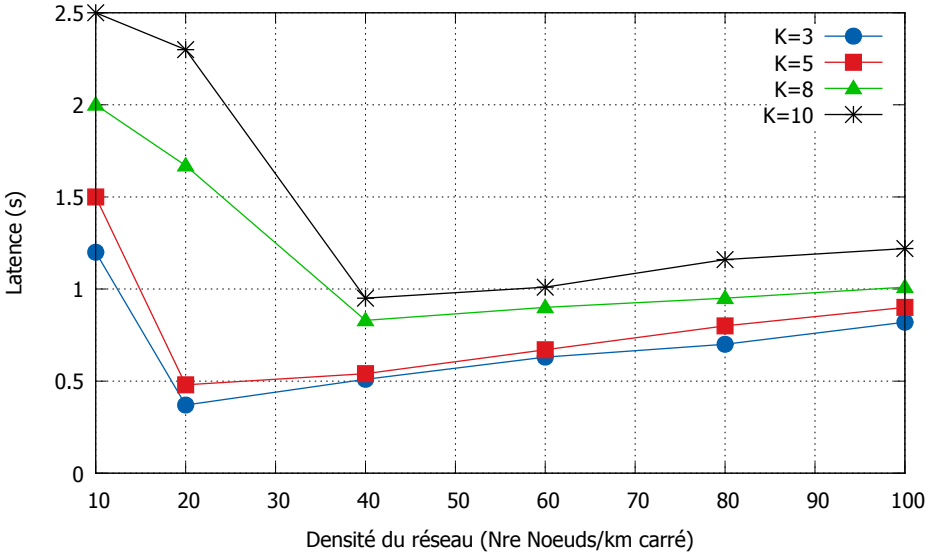

FIGURE 3.5 – Variation de la latence en fonction de la densité du réseau

3.7 Impact de la mobilité du réseau

Il a été observé que la mobilité d'un noeud n'a pas d'effet significatif sur les temps d'attente (figure 3.6). C'est parce que les vitesses simulées étaient inférieures à 20 m/s, et que le temps d'attente moyen est inférieur à 2 secondes, un tel retard pour un mouvement de nœud ne dépasse pas 20 m/s, et ce, dans la plupart du temps ne rompt pas les liens. Dans certains cas particuliers, la mobilité peut avoir un impact positif ou négatif sur la latence.

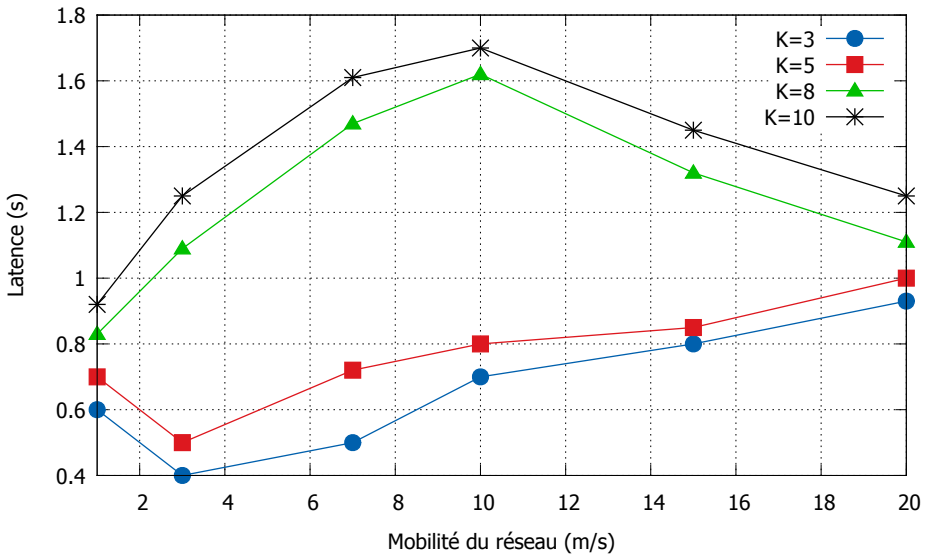

FIGURE 3.6 – Variation de la latence en fonction de la mobilité du réseau

3.8 Conclusion

Il a été démontré que l'utilisation du système d'authentification à base de RSA dans des environnements sans fil n'est pas préférable. Le schéma d'authentification proposé sur la base du cryptosystème à seuil d'ElGamal sur des courbes elliptiques offre à la fois la disponibilité et le niveau de sécurité fort requis dans les réseaux mobiles ad hoc et s'est avéré être une meilleure méthode pour la défense contre les attaques de devinettes hors ligne et les attaques de rejeu. En utilisant une cryptographie à courbe elliptique, notre système est efficace et facile à mettre en œuvre dans les appareils mobiles.

Chapitre 4

L'authentification et la qualité de service (QoS)

Sommaire

Avec le développement de l'économie et de la société, le service exige toujours plus de sécurité et de qualité. Cependant, puisque les services de sécurité induisent toujours la consommation de ressources supplémentaires, la QoS peut se dégrader évidemment. Il est important et essentiel de trouver des solutions optimales qui peuvent non seulement atteindre le niveau suffisant de sécurité, mais aussi répondre à des QoS aussi élevées que le système peut supporter. Dans ce chapitre, nous proposons une fonction agissant sur la QoS pour évaluer le délai de bout-en-bout induit par la sécurité dans le réseau de communication. En outre, un algorithme d'optimisation multiobjectifs basé le système immunitaire artificiel est utilisé pour obtenir des paramètres optimaux à la fois pour la sécurité et la qualité de service. Les simulations montrent que le modèle proposé est éfficace pour atteindre un équilibre optimal entre la sécurité et la qualité de service.

4.1 Introduction

Traditionnellement, la qualité de service (QoS) et la sécurité avaient été considérés comme des fonctionnalités distinctes dans le réseau de communication. Cependant, avec le développement de la recherche, il a été découvert que les deux sont fortement corrélés l'une de l'autre. D'une part, pour avoir une qualité de service

stable le service a besoin de suffisamment de protection pour résister à des attaques divers et éviter la congestion du réseau en raison d'une attaque réussie. D'autre part, le service de sécurité a toujours un impact évident sur la qualité de service, tel que le retard supplémentaire causé par procédure de chiffrement ou d'authentification. Il est très important et essentiel pour assurer la sécurité d'un réseau sans fil, en particulier un réseau Ad hoc, de moment que le canal sans fil est ouvert et les informations se propagent dans l'air et un attaquant peut facilement intercepter des informations sensibles sur le réseau. De plus, la bande passante limitée du canal sans fil augmente l'impact de la sécurité sur la QoS grandement. Par conséquent, cet impact doit être mieux considéré pour bien satisfaire les exigences des nouvelles technologies de réseaux.

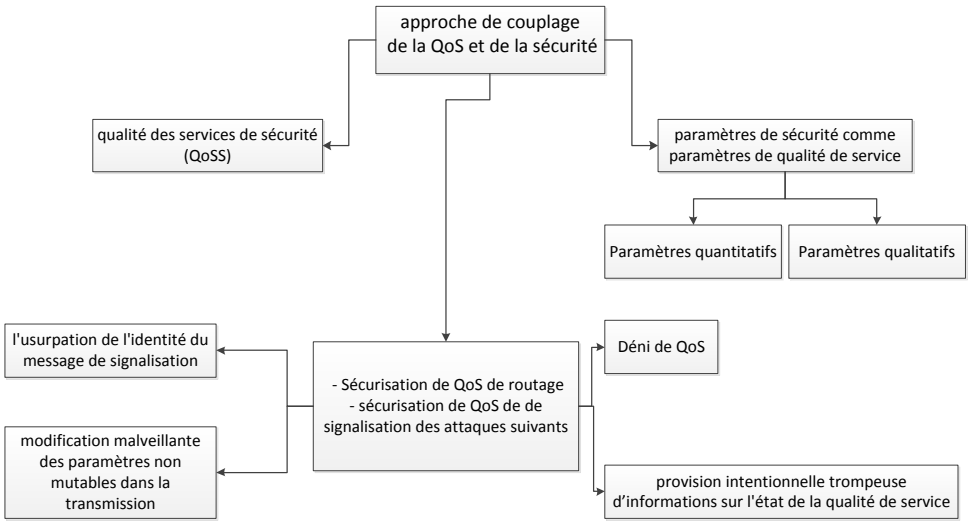

FIGURE 4.1 – Approche de couplage de la QoS et de la sécurité

4.1.1 Optimisation multi-objectif

L'optimisation multi-objectif est une branche de l'optimisation combinatoire, elle est utilisée fréquemment dans nombreux secteurs de l'industrie concernés (Télécommunications, Transport, Environnement, Mécanique, Aéronautique, ...). Comme le suggère le nom, un problème d'optimisation multi-critère consiste à optimiser plusieurs fonctions objectif simultanément. C'est difficile de résumer des objectif en un

objectif unique, car il existe des conflits entre ces objectif. En général, Les objectifs de l'optimisation sont contradictoires, c'est-à-dire que l'objectif est de trouver des bons compromis parmi toutes les solutions. Ces problèmes peuvent être NP-complets. Dans la partie suivante, je vais présenter la définition mathématique d'un problème d'optimisation multi-objectif.

4.1.1.1 Définition : Problème multi-objectif

Etant donné $X = (x_1, x_2, ..., x_n)$ est le vecteur des variables de décision. Il satisfait les contraintes ci-dessous :

$$g_i(X) \geq 0, i = 1, 2, ..., k \quad (1)$$

$$h_i(X) = 0, i = 1, 2, ..., l \quad (2)$$

Supposons r objectifs, et tous ces objectif sont conflictuels, la fonction optimale est : $f(X) = (f_1(X), f_2(X), ..., f_r(X))$
Trouver $X^* = (x_1^*, x_2^*, ..., x_n^*)$, optimiser $f(X^*)$ sous les contraintes (1) et (2). Les solutions qu'on obtient sont les solutions Pareto efficiency ou un optimum de Pareto.

4.1.1.2 Définition : L'optimum de Pareto

L'optimum de Pareto est un concept en économie. Ce terme est nommé d'après Vilfredo Pareto, un économiste italien qui a utilisé le concept dans ses études d'efficacité économique et la répartition des revenus. Un optimum de Pareto est un état dans lequel nous ne pouvons pas améliorer le bien-être d'un individu sans détériorer d'un autre. Nous pouvons dire que le vecteur $X^* \in F$ est un optimum de Pareto, si pour chaque $X \in F$, soit $\forall i \in I(f_i(X) = f_i(X^*)), I = \{1, 2, ..., r\}, soit \exists j \in I, f_j(X) > f_j(X^*)$. Sachant que $F = \{X \in R^n | g_i(X) \geq 0, i = 1, 2, ..., k; h_j(X) = 0, j = 1, 2, ..., l\}$ En général, l'optimisation multi-objectif donne un ensemble de solutions, plus d'une solution. Dans un ensemble de solutions P, on sélectionne un ensemble de solutions non dominées. Dans l'espace de recherche, les solutions non dominées sont les solutions Pareto optimal. L'ensemble de solutions non dominées forme Pareto frontier. L'objectif d'optimisation multi-objectif est de trouver un ensemble de solutions non dominées et proche du Pareto frontier.

4.1.1.3 Définition : Relation de dominance

P est un ensemble de solutions, il existe k objectifs : $f_1(), f_2(), ..., f_k()$. Pour chaque individu dans l'ensemble P. Il y a trois relations entre les deux solutions x et y. Pour x et y, soit x domine y, soit y domine x, soit x et y ne se domine pas leur même. Nous pouvons donc définir la relation ci-dessous :

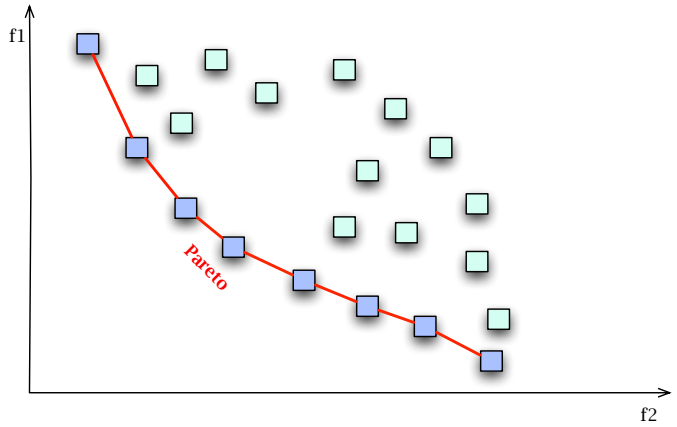

FIGURE 4.2 – La frontière de Pareto

– **La dominance :**
Une solution x et une solution y appartiennent à l'ensemble P, x domine y si et seulement si : $\forall i \in \{1, 2, ..., k\} : f_i(x) \leq f_i(y) et \exists j \in \{1, 2, ..., k\} : f_j(x) < f_j(y)$. Nous notons y $\prec$ x.
Si la solution x domine la solution y, nous disons que x est la solution non dominée et y est la solution dominée par x. Le symbole $\prec$ représente la relation dominée.

– **Non relation :**
Une solution x et une solution y appartiennent à l'ensemble P, nous disons que la solution x et la solution y sont non relation si et seulement s'il n'existe pas la relation dominée entre elles.

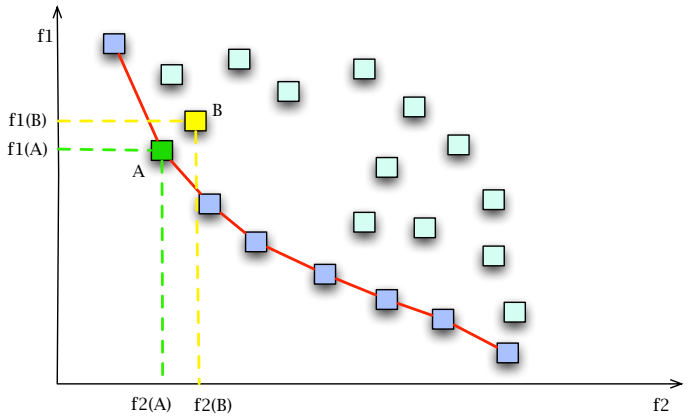

FIGURE 4.3 – La relation de dominance

4.2 Classification des niveaux de sécurité

Le niveau de sécurité indique le niveau de protection fourni par l'authentification pour l'analyse quantitative de la sécurité. La classification des niveaux de sécurité est indiquée dans le tableau 4.1 suivant les fonctions de sécurité : l'intégrité, l'authentification, la confidentialité et la disponibilité des ressources. L'authentification diffère d'un niveau à un autre voir figure 4.4 on part d'une simple authentification à une authentification forte.

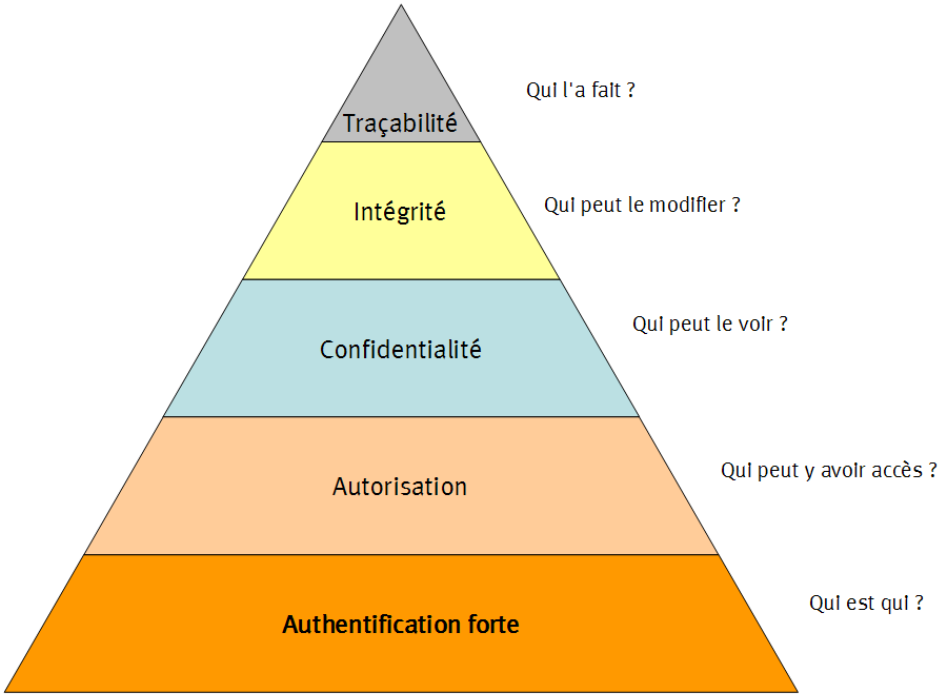

FIGURE 4.4 – Représentation de l'authentification forte sous forme pyramidale

Niveau de sécurité i	Services de sécurité			
	Intégrité	authentification	Confidentialité	Disponibilité
1 (Faible)	Non	Oui	Non	Non
2 (Moyen)	Non	Oui	Faible	Faible
3 (Élevé)	Non	Oui	Moyen	Moyen
4 (Très Élevé)	Oui	Oui	Élevé	Élevé

TABLE 4.1 – Classification des niveaux de sécurité

4.3 Analyse de performances du système proposé

Dans cette section, nous présentons deux services de sécurité : chiffrement et authentification. Leurs effets sur la sécurité et QoS sont étudiés séparément.
Il est bien connu que l'authentification de l'utilisateur et le cryptage des données sont deux mécanismes de sécurité principales, et ils déterminent principalement le niveau de sécurité requis. Le cryptage des données est un facteur clé de ce niveau. Le niveau de sécurité est différent en utilisant différents algorithmes de chiffrement avec la même longueur de clé, ou en utilisant le même algorithme de chiffrement avec différentes longueur de la clé. Toutefois, il apporte aussi plus de temps de latence qui est l'élément principal de la QoS [25]. L'authentification est un autre facteur de niveau de sécurité. elle peut non seulement entraîner des surcôuts de calcul ce qui est évident, mais aussi d'augmenter la probabilité de perte de service.
Si la communication de bout en bout est constitué de chiffrement et de déchiffrement de données, la transmission de données et de l'authentification, le temps de retard T est égale à la somme du temps de cryptage et de décryptage, le temps de transmission et le temps d'authentification. Etant donné que l'authentification et le cryptage ont un impact sur la sécurité, il est supposé que le niveau de sécurité peut être déterminée par au moins avec le niveau de chiffrement et le niveau de sécurité d'authentification. Le dernier temps de retard R et le niveau de sécurité N peut être exprimée comme :

$$R = t_{trans} + t_{auth} + t_{enc}$$
$$N = min(l_{enc}, l_{auth})$$

Où, t_{trans} est le retard engendré par la transmission. t_{enc} est le temps de chiffrement et de déchiffrement. t_{auth} est le temps d'authentification dans chaque transmission de paquet. l_{enc} et l_{auth} sont les niveaux de sécurité de cryptage et d'authentification respectivement.

4.3.1 La sécurité et la mobilité :

La sécurité et la mobilité semblent être en contradiction l'une de avec l'autre. la sécurité est habituellement appliquée par une autorité centrale statique qui est généralement en charge de la sécurisation du système en considération, soit qu'il s'agisse d'un réseau de communication, un système d'exploitation, ou le système d'accès à la chambre forte d'une banque. Dans ce cas, parce que les utilisateurs sont statiques ainsi, leurs emplacements sont prévisibles, ils sont plus susceptibles d'être disponibles, et le système peut facilement effectuer les contrôles appropriés. Dans cette partie, nous allons montrer que cette intuition peut être trompeuse : la mobilité est loin d'être un obstacle, et peut être utile pour établir des associations de sécurité entre deux nœuds mobiles d'un même réseau.

4.3.2 Le chiffrement

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de

(dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel. Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. Pour vérifier l'intégrité ou l'authenticité d'un document, on utilise respectivement un Message Authentication Code (MAC) ou une signature numérique. On peut aussi prendre en considération l'analyse de trafic dont la communication peut faire l'objet, puisque les motifs provenant de la présence de communications peuvent faire l'objet d'une reconnaissance de motifs. Pour rendre secrète la présence de communications, on utilise la stéganographie. La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme. Dans notre travail, nous avons continué à adopter un schéma de chiffrement basé sur les courbes élliptiques avec des clés de tailles 160, 224 et 256 bits.(voir tableau 3.2).

4.3.2.1 Effet de cryptage sur la sécurité :

Le niveau de chiffrement d'un système de sécurité donné est liée à la sécurité de algorithme deployé et la longueur de clé. Il est supposé que l'algorithme de chiffrement est assez difficile à casser, ce qui signifie qu'il n'ya pas de meilleure façon pour déchiffrer la session du système de chiffrement que par attaque exhaustive. Par conséquent, il n'est pas difficile de calculer le degré de complexité de l'attaque. Si la longueur de clé est de 8 bits, il ya $2^8 = 256$ clés possibles, l'attaquant doit essayer 256 fois pour obtenir la bonne clé. Lorsque la longueur de clé est k_{long}, il doit essayer de $2^{k_{long}}$ fois. Par conséquent, nous pouvons conclure que plus la longueur de la clé est importante, plus le nombre d'essais sera nécessaire, ce qui indique que le niveau de sécurité le plus élevé.
Nous pouvons supposer que le niveau de sécurité est égale à 1 lorsque la longueur de la clé est la plus courte possible. Le niveau de sécurité de chiffrement l_{enc} peut être notée :

$$l_{enc} = 2^{\frac{k_{long}}{k_{min}}} - 1 \text{ [26]}$$

Où, k_{min} est la plus courte longueur de clé.

4.3.2.2 Effet de cryptage sur le retard :

Avec l'utilisation des ECC pour crypter et décrypter le même message, le temps de chiffrement et de déchiffrement augmente linéairement avec la longueur de la clé.

4.3.3 L'authentification

Afin de valider l'identité des utilisateurs et assurer la sécurité du système, l'authentification est toujours utilisée comme un processus initial pour autoriser les utilisateurs d'établir et de maintenir des communications fiables. En rejetant les utilisateurs non autorisés, l'authentification peut protéger les données de réseau et les utilisateurs.
Pour tester la qualité de service dans le modèle proposé dans le chapitre 3 nous

avons procédé à des tests sur les échanges Kerberos avec des TGS distribuées en utilisant un schéma basé sur la cryptographie à seuil avec courbes élliptiques avec des clés de taille différentes.

4.3.3.1 Effet de l'authentification sur Retard

Très peu de travaux ont été réalisés dans l'analyse quantitative de la qualité de service. Il est très difficile de quantifier avec précision l'authentification ou les métriques de sécurité, telles que l'intégrité des données et la confidentialité des données. Par conséquent, nous utilisons le taux d'authentification, qui est défini comme temps d'authentification en une minute pour évaluer quantitativement le niveau de sécurité.
Il est généralement admis que plus le temps d'authentification est élevé, plus le niveau de sécurité est élevé (sauf deni). Comme les changements de taux d'authentification, le niveau de sécurité change en conséquence. Pour plus de simplicité, il est supposé que le taux d'authentification est proportionnel au niveau de la sécurité, nous proposons une fonction linéaire adaptée pour décrire la relation entre l'authentification et le niveau de sécurité. Elle est présentée comme suit :

$$l_{auth} = r_{auth} * e$$

Où l_{auth} est le niveau de sécurité d'authentification, et r_{auth} est le taux d'authentification, e est un coefficient de proportionnalité du taux d'authentification.

4.3.3.2 Effet du taux d'authentification sur le retard :

Le service d'authentification est toujours fourni au début d'une communication. Une fois que l'authentification est terminé, les processus de communication suivants ne sont pas essentiellement affectées par l'authentification. le retard engendré par l'authentification est le temps entre l'envoi d'une demande d'authentification et de la réception de la réponse, il est proportionnel à la vitesse d'authentification.

4.4 Simulations

Les simulations se concentrent principalement sur l'évaluation de l'impact de la sécurité sur la qualité de service. L'algorithme a été implémenté autour de la bibliothèque de programmation par contraintes java Choco [46].

4.4.1 Les hypothèses et les paramètres

Des simulations sont effectuées avec un PC core2duo de 2.0 GHZ, les paramètres permettant d'évaluer la sécurité et de retard sont indiquées dans le tableau suivant 4.2. Le problème a été testé avec plusieurs instances basées sur celles proposées par [50] et par [26]

Paramètres du retard et le niveau de sécurité pour RSA			
k_{min}	e	r_{auth}	k_{long}
128	9e+005	[0..0.2]	[0..2048]

TABLE 4.2 – Paramètres pour le retard et le niveau de sécurité

Paramètres du retard et le niveau de sécurité pour ECC-EG			
k_{min}	e	r_{auth}	k_{long}
56	9e+005	[0..0.2]	[0..256]

TABLE 4.3 – Paramètres pour le retard et le niveau de sécurité

4.4.2 Impact du niveau de sécurité sur le retard

L'impact du niveau de sécurité sur le retard est représenté sur la figure 4.5. la longueur de clé et Le taux d'authentification à des valeurs optimales sont présentées dans la figure 4.6 et la figure 4.7.

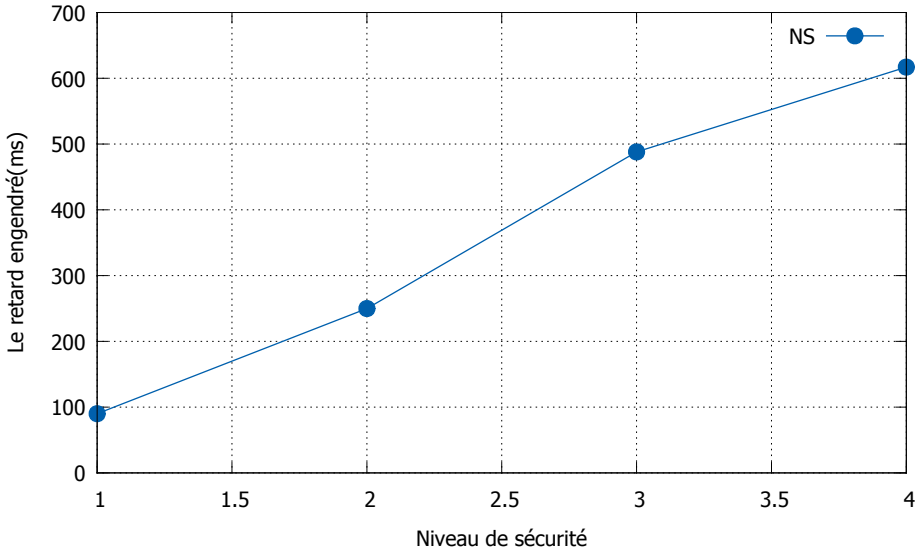

FIGURE 4.5 – Niveau de sécurité vs modification du retard

La figure 4.5 montre que le retard augmente avec l'augmentation du niveau de sécurité. Cette évolution s'explique par l'augmentation de la longueur de la clé et le taux d'authentification, ce qui provoque plus de temps de chiffrement et d'authentification. Quand le niveau de sécurité change un délai supplémentaire s'ajoute.
Évidemment, la vitesse de progression du niveau de sécurité est plus grande que

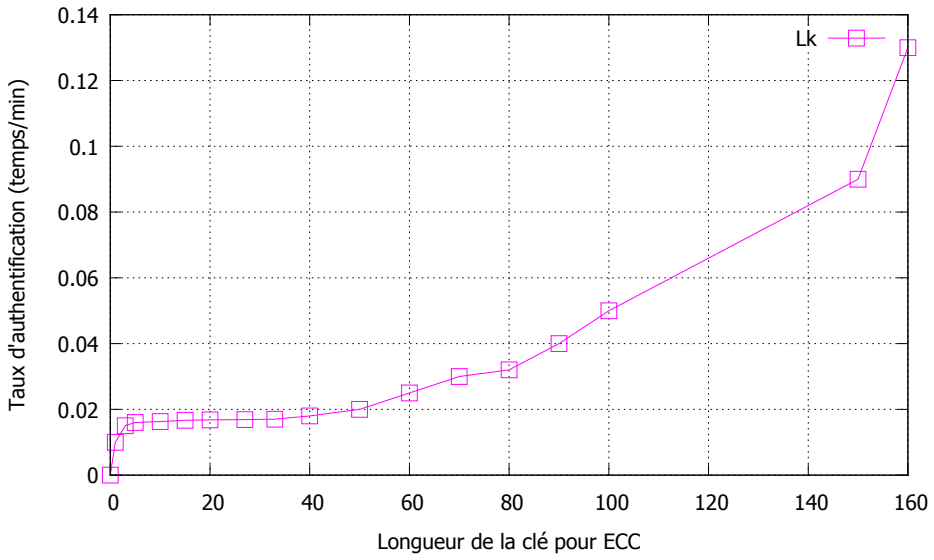

FIGURE 4.6 – Longueur de la clé vs taux d'authentification pour un ECC crypto-système

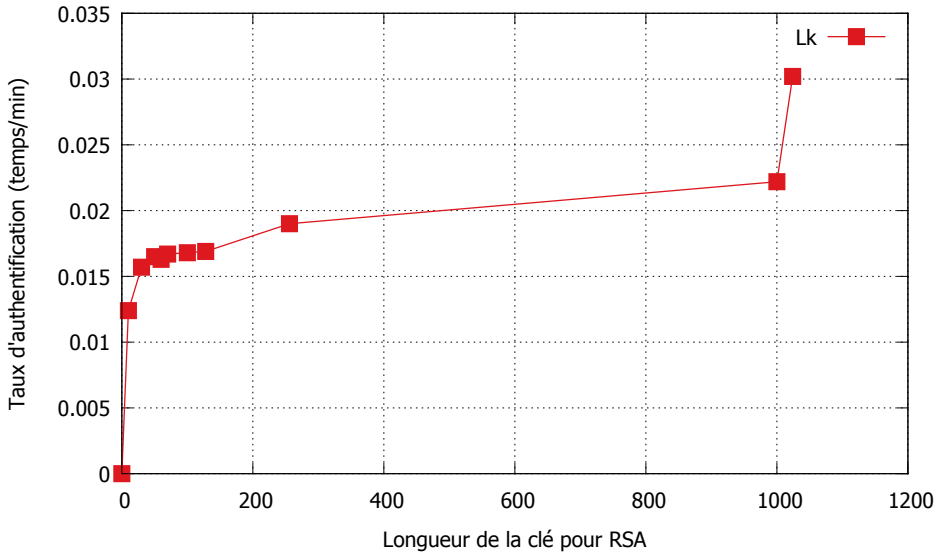

FIGURE 4.7 – Longueur de la clé vs taux d'authentification pour un RSA crypto-système

celle de retard. Le niveau de cryptage a une croissance exponentielle avec la longueur de la clé, et le niveau de sécurité de l'authentification est proportionnel au taux d'authentification. De plus, l'impact de la sécurité sur le retard est principalement causé par le cryptage, et il présente une variation linéaire avec une longueur de clé.

Les figures 4.6 et 4.7 révèlent que le taux d'authentification augmente essentiellement avec longueur de clé. Afin d'obtenir un niveau aussi élévé que possible, leurs augmentations deviennent semblables. En outre, du moment que le chiffrement est indépendant de l'authentification, il existe plusieurs combinaisons optimales entre k_{long} et r_{auth} pour un niveau de sécurité donné.

4.5 Conclusion

Dans ce chapitre, nous avons étudié l'impact quantitatif de la sécurité sur la QoS à l'aide d'une approche basé sur l'optimisation multiobjetives à contraintes. Les sorties de cette fonction sont utilisées pour modifier les paramètres de qualité de service d'origine avant qu'elles ne soient exécutées par les fonctions QoS de l'application connexes. Le rendement du système est analysé par rapport au retard engendré et le niveau de sécurité de bout en bout. En outre, on a étudie les impacts de cryptage et d'authentification sur le niveau de sécurité. Enfin, pour obtenir le délai minimum et un niveau de sécurité élevé, nous avons utilisé un algorithme immunitaire pour optimiser la longueur de clé et le taux d'authentification. Les simulations montrent que le modèle proposé est efficace pour obtenir des solutions optimales dans différentes configurations.

Chapitre 5

Conclusion

La sécurisation des échanges dans les réseaux Ad hoc reste un problème majeur. Elle se heurte souvent à la difficulté de proposer des mécanismes cryptographiques relativement robustes face aux différentes attaques possibles, causées par les intrusions externes et les nœuds compromis sans pour autant affecter les performances globales du réseau ad hoc et des protocoles de routage de manière trop prononcée.

Dans ce travail, nous avons étudié les problèmes de sécurité dans les réseaux mobiles Ad hoc d'un point de vue théorique. Cette étude a révélé un nombre de difficultés liées à l'absence d'infrastructure centralisée, la contrainte d'énergie, la topologie dynamique, la bande passante, les ressources limitées, etc. De nombreux travaux de recherche proposent des schémas de sécurité qui conviennent aux caractéristiques des réseaux ad hoc. Bien que des solutions répondent à un ensemble d'exigences de sécurité, il n'en demeure pas moins que les solutions les plus efficaces et les plus complètes sont coûteuses.

Notre travail focalisait sur une nouvelle architecture d'authentification dans le but de proposer une solution de sécurité efficace qui permette de préserver les performances globales du réseau. Nous étions attirés par l'efficacité et la rapidité de traitement des fonctions cryptographiques basées sur les courbes elliptiques. En effet, cette approche est beaucoup plus légère et beaucoup moins coûteuse que les schémas basés RSA. L'idée de base de notre solution était de mettre en place un système d'authentification à base de KERBEROS qui permet aux nœuds de s'authetifier de façons sécurisée. Pour plus d'efficacité, nous avons intégré notre schéma d'authentification dans une extension de sécurité du protocole de routage AODV. L'intégration de notre schéma d'authentification dans le protocole KERBEROS a permis aux nœuds voisins d'échanger les messages de contrôle HELLO de manière sécurisée, efficace, et moins coûteuse. En effet, le mécanisme des a permis de réduire le nombre d'opérations cryptographiques utilisées.

Cela a permis de réduire le nombre de paquets perdus, et de préserver les ressources des nœuds, prolongeant ainsi, la durée de vie du réseau. Un autre point fort de notre solution est que la facilité et la rapidité de la manipulation des courbes élliptiques permettent un gain d'espace et de temps non négligeable, ce qui permet d'accélérer les fonctionnalités de routage, notamment, la génération et le traitement des messages échangés, et par conséquent, cela contribuera énormément à l'amélioration des performances du réseau et son bon fonctionnement. En effet, les premiers résultats de l'intégration des courbes élliptiques à AODV sont très satisfaisants et très encourageants et montrent que le nouveau protocole amélioré offre de bonnes

performances en termes de coût et de routage, tout en garantissant un bon niveau de sécurité.
L'objectif de notre approche est aussi d'empêcher d'une part les attaques sur les messages de contrôle, et de fournir d'autre part, un support fiable pour la détection des comportements malveillants. Pour cela, nous avons développé une deuxième ligne de défense qui consiste en un mécanisme de sécurité à la fois préventif et réactif pour contrer l'attaque de devinnettes et les attaques de rejeu.
Le mécanisme que nous avons proposé permet d'augmenter le niveau de sécurité et de renforcer la robustesse de notre solution face à ce type d'attaques. En effet, ce mécanisme permettra de détecter l'occurrence de ces deux attaques dans le réseau.
Les résultats de la simulation montrent clairement que le schéma de sécurité que nous avons proposé réalise un compromis entre la robustesse et l'efficacité en termes de sécurité et les performances globales du réseau. Notre approche est donc bien adaptée au contexte ad hoc. Elle présente une bonne solution pour sécuriser l'échange des informations tout en respectant les contraintes et les limitations imposées par cet environnement.
Nous envisageons de valider par simulation le deuxième volet de notre étude qui est l'impact de la sécurité sur la qualité de service. A la fin de ce travail de recherche, nous pouvons dire que la sécurisation des échanges dans les réseaux ad hoc reste un vrai challenge. Les recherches continuent dans ce domaine afin d'améliorer et d'optimiser de plus en plus les solutions de sécurité existantes afin de rendre les réseaux ad hoc plus fiables, plus performants et plus sécurisés à faible coût.

Annexe A

Les courbes elliptiques

Introduction

L'utilisation des courbes elliptiques dans le domaine de la cryptographie est très répandue notamment pour donner des critères de primalité ou pour crypter un message... En ce qui nous concerne, nous allons plus particulièrement nous interessé au cryptage d'un message via les courbes elliptiques avec les différents protocoles existants. L'utilisation des courbes elliptiques pour crypter des messages se voit surtout dans le domaine de la cryptographie à clé publique, qui est une catégorie de protocoles cryptographiques faisant intervenir des clés (servant au cryptage) disponibles aux yeux de tous.

Dans un premier temps, on va mettre en place les outils mathématiques nécessaires concernant les courbes elliptiques et puis nous verrons comment crypter un message.

A.1 Outils mathématiques

A.1.1 Les courbes elliptiques

A.1.1.1 Définition générale

Soit K un corps de caractéristique $\neq 2$, 3 et soit x^3+ax+b sans racine multiple avec a et $b \in K$. Une courbe elliptique définie sur K est l'ensemble des (x, y) tel que $\begin{cases} x, y \in K \\ x^3+ax+b=y^2 \qquad (1) \end{cases}$, plus un élément noté $\mathcal{O}$ appelé point à l'infini.

Si K est un corps de caractéristique 2 alors une courbe elliptique définie sur K est l'ensemble des points vérifiant $y^2+cy=x^3+ax+b$ ou $y^3+xy=x^3+ax^2+b$ auquel on ajoute un point à l'infini $\mathcal{O}$.

Si K est un corps de caractéristique 3, une courbe elliptique sur K est définie par l'ensemble des points tels que $y^2=x^3+ax^2+bx+c(3)$ et d'un point à l'infini $\mathcal{O}$.

A.1.2 Définition dans $\mathbb{R}$:

Soit E une courbe elliptique sur $\mathbb{R}$, soient P et Q deux points de E, on définit $-P$ et $P+Q$ par les règles suivantes :

1. si P est le point à l'infini $\mathcal{O}$, alors $-P$ vaut $\mathcal{O}$ et $P+Q=Q$, c'est-à dire que $\mathcal{O}$ est l'élément neutre pour l'addition. On va désormais supposer que ni P, ni Q n'est le point à l'infini.

2. Le point $-P$ est le point ayant la même abscisse mais l'ordonnée opposée *ie* si $P=(x,y)$, $-P=(x,-y)$. On peut remarquer que si P est sur la courbe elliptique, $-P$ l'est aussi d'après (1).

3. si P et Q ont des abscisses différentes, la droite (PQ) et E s'intersectent en un troisième point R sauf si la doite est tangente à la courbe en P auquel cas $R=P$ ou si celle-ci est tangente à E en Q auquel cas $R=Q$. On définit alors $P+Q$ par $P+Q=-R$ (le point de même abscisse que R et d'ordonnée opposée).

4. si $Q=-P$ (*ie* si P et Q ont la même abscisse mais des ordonnées opposées), alors $P+Q=\mathcal{O}$.

Montrons maintenant qu'il y a exactement trois points d'intersection entre (PQ) et E qui sont P, Q et $P+Q$.

Soient (x_1,y_1), (x_2,y_2) et (x_3,y_3) les coordonnées respectives de P, Q et $P+Q$. On veut exprimer (x_3,y_3) en fonction de x_1, y_1, x_2, y_2. Supposons que P et Q ont des abscisses différentes *ie* supposons que $P\neq Q$ et $P\neq -Q$ et posons $y=\alpha x+\beta$, l'équation de la droite (PQ) non verticale d'après ce qu'on vient de supposer. On a alors $\begin{cases}\alpha=\frac{y_2-y_1}{x_2-x_1}\\ \beta=y_1-\alpha x_1\end{cases}$.

On a $\begin{cases}(x,y)\in(PQ)\\ (x,y)\in E\end{cases}$

$$\Leftrightarrow\begin{cases}y=\alpha x+\beta\\ (\alpha x+\beta)^2=x^3+ax+b \text{ (car } \mathbb{R} \text{ est de caractéristique } \neq 2 \text{ et } 3)\end{cases}.$$

On en déduit qu'on a un point (x,y) appartenant à E et à (AB) si et seulement si x est racine de l'équation $x^3-(\alpha x+\beta)^2+ax+b=0(*)$. On sait que cette équation a déjà 2 racines qui sont x_1 et x_2 puisque ce sont les abscisses des points P et Q (qui sont supposés appartenir à E et (AB) et on sait aussi que la somme des racines d'un polynôme de degré n en x est égale à l'opposé du coefficient du terme en x^{n-1} d'où la troisième racine de $(*)$ est tel que : $x_3=\alpha^2-x_1-x_2$. Par conséquent, on a $P+Q=(x_3,-\alpha x+\beta)=(x_3,y_3)$ tel que :

$$\begin{cases}x_3=(\frac{y_2-y_1}{x_2-x_1})^2-x_1-x_2\\ y_3=-y_1+\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)\end{cases}$$

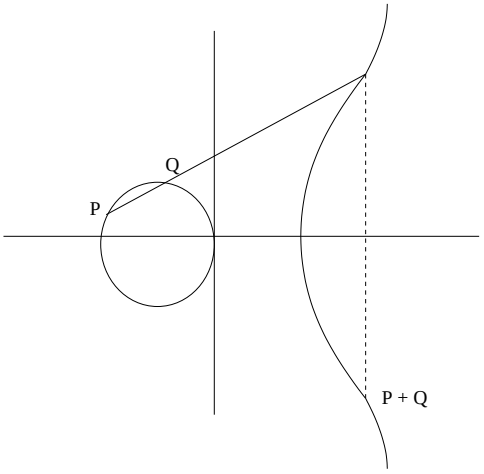

FIGURE A.1 – $P + Q$ sur la courbe elliptique $y^2 = x^3 - x$

Supposons à présent que $P = Q$, l'expression de $P + Q$ n'est pas très différente. Le coefficient directeur de (AB) α devient la valeur de la dérivée $\frac{dy}{dx}$ en P. On a $(1) \Leftrightarrow x^3 + ax^2 + b = y^2 \Leftrightarrow (3x^2 + a)dx = 2ydy \Leftrightarrow \frac{dy}{dx} = \frac{3x^2+a}{2y}$. Pour se ramener au cas $P = Q$, on fait tendre Q vers P *i.e.*, on fait tendre x_2 vers x_1. D'où

$$\begin{cases} x_3 = (\frac{3{x_1}^2+a}{2y_1})^2 - 2x_1 \\ y_3 = -y_1 + \frac{3{x_1}^2+a}{2y_1}(x_1 - x_3) \end{cases}$$

A.1.3 Extension à $\mathbb{F}_p$

L'expression de $P+Q=(x_3,y_3)$ où P et Q sont des points de E reste valable à l'exception près que la division par n est remplacer par la multipication de l'inverse de n dans $\mathbb{F}_p$ et que les calculs se font mod$p$ *i.e.* on a :

$$\bullet \begin{cases} x_3 = ((y_2-y_1)(x_2-x_1)^{-1})^2 - x_1 - x_2 \\ y_3 = -y_1 + (y_2-y_1)(x_2-x_1)^{-1}(x_1-x_3) \end{cases} \text{ si } P \neq Q$$

$$\bullet \begin{cases} x_3 = ((3{x_1}^2+a)(2y_1)^{-1})^2 - 2x_1 \\ y_3 = -y_1 + (3{x_1}^2+a)(2y_1)^{-1}(x_1-x_3) \end{cases} \text{ si } P = Q.$$

A.1.4 Autres outils

Pour crypter un message via les courbes elliptiques, on travaille de façon générale dans le corps à q éléments $\mathbb{F}_q$ où $q=p^r$ avec p premier. Dans notre cas, on va plutôt se placer dans $\mathbb{F}_p$ pour simplifier avec p premier supposé grand et on va considérer une courbe elliptique E définie sur ce corps.

A.1.4.1 Calcul de kP

On va présenter une méthode de calcul rapide de kP où $k \in \mathbb{F}_p$ et $P \in E$. Cette méthode est indispensable puisqu'elle est à la clé de la cryptographie untilisant les courbes elliptiques. En effet, pour crypter un message grâce à une courbe elliptique E, voici les différentes étapes :

1. codage de message en clair en faisant correspondre à chaque unité de message m_i un point $P_i \in E$

2. cryptage en calculant pour chaque P_i, kP_i où $k \in \mathbb{F}_p$ est une clé secrète.

Les étapes de décryptage dépendent ensuite des algorithmes utilisés.

Voici donc l'algorithme de calcul de kP, $k \in \mathbb{F}_p$, $P \in E$ étant donnés :

Si Q_1 et $Q_2 \in E$, on sait calculer Q_1+Q_2, l'idée est de diminuer le nombre d'opérations permettant d'arriver à kP en faisant obtenir autant que possible les puissances de 2 :

Début :
Etape 1 : on écrit $k=2^s t$ avec t impair. On a donc $kP=2^s tP$. On calcule assez rapidement $2^s tP$ en calculant $2P$, puis $4P$, ..., $2^s P = P_1$.

Etape 2 : il reste à calculer tP_1 :

$t' \leftarrow t$
$P' \leftarrow P_1$

Tant que $t' \neq 1$ faire
écrire : $t' = 2^{s_1} + t_1$
$P_{tmp} \leftarrow P'$
$P' \leftarrow 2^{s_1} P'$
$t' \leftarrow t_1$
fin Tant que

$P' \leftarrow P' + P_{tmp}$
Fin

En fait l'algorithme calcule kP en écrivant $kP = 2^s(\sum_{i=0}^{S_1} a_i 2^i)P$ avec $a_i \in \{0, 1\}$

Bibliographie

[1] Nidal Aboudagga. *Authentication Management for Secure Seamless Mobility.* PhD thesis, Université Catholique de Louvain, 2008. (Cité en page 6.)

[2] KHADIDJA AYAD. Sécurité du routage dans les réseaux ad hoc mobile. *memoire de magistère Ecole Nationale Supérieure d'Informatique*, 2012. (Cité en page 19.)

[3] Marianne A Azer, Sherif M El-Kassas, and Magdy S El-Soudani. Threshold cryptography and authentication in ad hoc networks survey and challenges. In *Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on*, pages 5–15. IEEE, 2007. (Cité en pages 38 et 39.)

[4] Steven M Bellovin and Michael Merritt. Limitations of the kerberos authentication system. *ACM SIGCOMM Computer Communication Review*, 20(5) :119–132, 1990. (Cité en page 38.)

[5] Steven Blake, David Black, Mark Carlson, Elwyn Davies, Zheng Wang, and Walter Weiss. An architecture for differentiated services. *rfc 2475, December*, 1998. (Cité en page 33.)

[6] AIT-SALEM Boussad. *Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques.* PhD thesis, Université de Limoges, 2011. (Cité en pages 19, 21 et 32.)

[7] Zhenchuan Chai, Zhenfu Cao, and Rongxing Lu. Threshold password authentication against guessing attacks in ad hoc networks. *Ad Hoc Networks*, 5(7) :1046–1054, 2007. (Cité en page 46.)

[8] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot, et al. Optimized link state routing protocol (olsr). *RFC 3626*, 2003. (Cité en page 26.)

[9] Ricardo Corin, Sreekanth Malladi, Jim Alves-Foss, and Sandro Etalle. Guess what ? here is a new tool that finds some new guessing attacks. Technical report, DTIC Document, 2003. (Cité en page 46.)

[10] Hongmei Deng, Anindo Mukherjee, and Dharma P Agrawal. Threshold and identity-based key management and authentication for wireless ad hoc networks. In *Information Technology : Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, volume 1, pages 107–111. IEEE, 2004. (Cité en pages 38 et 39.)

[11] Haimabati Dey and Raja Datta. A threshold cryptography based authentication scheme for mobile ad-hoc network. In *Advances in Networks and Communications*, pages 400–409. Springer, 2011. (Cité en page 41.)

[12] Dominique Dhoutaut. *Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l'expérimentation.* PhD thesis, Laboratoire CITI, INSA de Lyon, 2003. (Cité en pages 22 et 26.)

[13] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6) :644–654, 1976. (Cité en page 12.)

[14] John R Douceur. The sybil attack. In *Peer-to-peer Systems*, pages 251–260. Springer, 2002. (Cité en page 22.)

[15] Khaled Dridi. *Spécification du protocole MAC pour les réseaux IEEE 802.11 e à différentiation de services sous contrainte de mobilité*. PhD thesis, Université Paris-Est, 2011. (Cité en page 33.)

[16] Danièle Dromard and Dominique Seret. *Architecture des réseaux*. Pearson Education France, 2013. (Cité en page 10.)

[17] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology*, pages 10–18. Springer, 1985. (Cité en page 42.)

[18] James H Ellis. The history of non-secret encryption. *Cryptologia*, 23(3) :267–273, 1999. (Cité en page 12.)

[19] Levent Ertaul and Nitu J Chavan. Rsa and elliptic curve-elgamal threshold cryptography (ecceg-tc) implementations for secure data forwarding in manets. *Threshold*, 7(8) :9, 2007. (Cité en page 45.)

[20] Levent Ertaul and Weimin Lu. Ecc based threshold cryptography for secure data forwarding and secure key exchange in manet (i). In *NETWORKING 2005. Networking Technologies, Services, and Protocols ; Performance of Computer and Communication Networks ; Mobile and Wireless Communications Systems*, pages 102–113. Springer, 2005. (Cité en page 45.)

[21] Hadj Gharib and Kamel Belloulata. Authentication architecture using threshold cryptography in kerberos for mobile ad hoc networks. *Advances in Science and Technology Research Journal*, 8(22) :12–18, 2014. (Cité en page 38.)

[22] Kannan Govindan and Prasant Mohapatra. Trust computations and trust dynamics in mobile adhoc networks : a survey. *Communications Surveys & Tutorials, IEEE*, 14(2) :279–298, 2012. (Cité en pages 38 et 39.)

[23] Zygmunt J Haas, Marc R Pearlman, and Prince Samar. The zone routing protocol (zrp) for ad hoc networks. *draft-ietf-manet-zone-zrp-04. txt*, 2002. (Cité en page 32.)

[24] Lajos Hanzo and Rahim Tafazolli. A survey of qos routing solutions for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, 9(2 2nd) :50–70, 2007. (Cité en page 34.)

[25] Wenbo He and Klara Nahrstedt. An integrated solution to delay and security support in wireless networks. In *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, volume 4, pages 2211–2215. IEEE, 2006. (Cité en page 56.)

[26] Huawang Zeng Jianyong Chen, Cunying Hu. A novel model for evaluating optimal parameters of security and quality of service. *Journal of Computers*, 5(6) :973–978, 2010. (Cité en pages 57 et 58.)

[27] David B Johnson, David A Maltz, Josh Broch, et al. Dsr : The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5 :139–172, 2001. (Cité en page 29.)

[28] Neal Koblitz. *A course in number theory and cryptography*, volume 114. Springer, 1994. (Cité en page 42.)

[29] K Lauter. The advantages of elliptic curve cryptography for wireless security. *Wireless Communications, IEEE*, 11(1) :62–67, 2004. (Cité en page 45.)

[30] Chun-Ta Li and Yen-Ping Chu. Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks. *IJ Network Security*, 8(2) :166–168, 2009. (Cité en page 46.)

[31] Sergio Marti, Thomas J Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265. ACM, 2000. (Cité en page 19.)

[32] Rabah Meraihi. *Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc*. PhD thesis, École nationale supérieure des télécommunications, 2005. (Cité en page 34.)

[33] SangJae Moon. Anonymous cluster-based manets with threshold signature. *International Journal of Distributed Sensor Networks*, 2013, 2013. (Cité en pages 38 et 39.)

[34] Clifford Neuman, Sam Hartman, Tom Yu, and Kenneth Raeburn. The kerberos network authentication service (v5). *Network*, 6649 :6806, 2005. (Cité en page 39.)

[35] Patrick Sondi Obwang. *Le Routage à Qualité de Service dans les Réseaux Mobiles Ad Hoc*. PhD thesis, Université de Bourgogne Président du jury Eric Gressier-Soudan, Conservatoire National des Arts et Métiers, 2011. (Cité en pages 34 et 35.)

[36] Mawloud Omar, Yacine Challal, and Abdelmadjid Bouabdallah. Reliable and fully distributed trust model for mobile ad hoc networks. *Computers & Security*, 28(3) :199–214, 2009. (Cité en pages 38 et 39.)

[37] Bh Padma, D Chandravathi, and P Prapoorna Roja. Encoding and decoding of a message in the implementation of elliptic curve cryptography using koblitz's method. *International Journal on Computer Science & Engineering*, 2(5), 2010. (Cité en page 42.)

[38] Charles Perkins, E Belding-Royer, Samir Das, et al. Rfc 3561-ad hoc on-demand distance vector (aodv) routing. *Internet RFCs*, pages 1–38, 2003. (Cité en page 28.)

[39] Charles E Perkins. *Ad hoc networking*. Addison-Wesley Professional, 2008. (Cité en page 6.)

[40] Charles E Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *ACM SIGCOMM Com-*

puter Communication Review, volume 24, pages 234–244. ACM, 1994. (Cité en page 27.)

[41] Asad Amir Pirzada and Chris McDonald. Kerberos assisted authentication in mobile ad-hoc networks. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26*, pages 41–46. Australian Computer Society, Inc., 2004. (Cité en page 38.)

[42] Na Ruan, Takashi Nishide, and Yoshiaki Hori. Elliptic curve elgamal threshold-based key management scheme against compromise of distributed rsus for vanets. *Journal of Information Processing*, 20(4) :846–853, 2012. (Cité en page 46.)

[43] Sajal Sarkar, Bapi Kisku, Sudip Misra, and Mohammad S Obaidat. Chinese remainder theorem-based rsa-threshold cryptography in manet using verifiable secret sharing scheme. In *Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on*, pages 258–262. IEEE, 2009. (Cité en pages 38 et 39.)

[44] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11) :612–613, 1979. (Cité en page 38.)

[45] Web site. Cours, dernier accès le, 14/02/2014. https://www.scs.carleton.ca/sites/default/files/course_page/secretsharing.pdf. (Cité en page 42.)

[46] Web site. Choco solver, dernier accès le, 17/05/2014. http://www.emn.fr/z-info/choco-solver/. (Cité en page 58.)

[47] Web site. language r, dernier accès le, 17/05/2014. http://www.r-project.org/. (Cité en page 45.)

[48] Web site. Site du nsa, dernier accès le, 17/05/2014. http://www.nsa.gov/business/programs/elliptic_curve.shtml. (Cité en page 45.)

[49] Web site. Wikipédia, dernier accès le, 17/05/2014. http://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information. (Cité en page 8.)

[50] Web site. test, dernier accès le, 19/05/2014. http://www.tik.ee.ethz.ch/sop/download/supplementary/testProblemSuite/. (Cité en page 58.)

[51] Richard E Smith. *Authentication : from passwords to public keys*. Addison-Wesley Longman Publishing Co., Inc., 2001. (Cité en page 9.)

[52] Christian Tchepnda. *Authentification dans les réseaux véhiculaires opérés*. PhD thesis, Télécom ParisTech, 2008. (Cité en page 7.)

[53] Hannan Xiao, Winston KG Seah, Anthony Lo, and Kee Chaing Chua. A flexible quality of service model for mobile ad-hoc networks. In *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*, volume 1, pages 445–449. IEEE, 2000. (Cité en page 33.)

[54] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang. Jamming sensor networks : attack and defense strategies. *Network, IEEE*, 20(3) :41–47, 2006. (Cité en page 20.)

[55] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks : challenges and solutions. *Wireless Communications, IEEE*, 11(1) :38–47, 2004. (Cité en page 39.)

[56] Seung Yi and Robin Kravets. Moca : Mobile certificate authority for wireless ad hoc networks. In *2nd Annual PKI Research Workshop Pre-Proceedings*, volume 51, page 65, 2003. (Cité en page 45.)

[57] Lixia Zhang, Steve Berson, Shai Herzog, and Sugih Jamin. Resource reservation protocol (rsvp)–version 1 functional specification. *Resource*, 1997. (Cité en page 33.)

[58] Lidong Zhou and Zygmunt J Haas. Securing ad hoc networks. *Network, IEEE*, 13(6) :24–30, 1999. (Cité en page 38.)

Table des figures

Liste des tableaux

Liste des Algorithmes

الملخص

الهدف من هذه الأطروحة هو توفير مصادقة جديدة
البنيان تتكيف مع الشبكات اللاسلكية وخاصة الشبكات العشوائية.
لهذا استخدمنا نموذج يستند إلى بروتوكول المصادقة تحسين انقسامات
الطرف TGS لمخطط قاعدة البيانات KDC باستخدام التشفير على عتبة
على المنحنيات الإهليجية

يتجنب اقتراحنا نقطة الفشل الواحدة التي عادة ما تحدث

في مخططات قاعدة البيانات KDC

الأطروحة المقدمة تركز على المجالات التالية:
أولا، هذه هي المرة الأولى التي يجمع فيها نظام مصادقة بين بروتوكول
المصادقة KERBEROS
مع توزيع TGSمع مخطط تشفير **الجمل** مع عتبة على المنحنيات الإهليجية.
ويخصص المحور الثاني لنمذجة الأمن كمعامل في نوعية
الخدمة .لذا نقترح مقاييس جديدة لقياس تأثير عنصر ما على الأخر.
وأخيرا، نقدم وجهات نظر التوثيق والأمن للتنقل في
الشبكات العشوائية.
كل هذا العمل تم تنفيذه في محاكاة ns2 و الذي سمح لنا
إجراء التحقق من الدقة في شروط الشبكة الحقيقية.

Résumé : L'objectif de cette thèse est de fournir une nouvelle architecture d'authentification adaptée aux réseaux sans fil et plus particulièrrement les réseaux Ad hoc.
Nous utilisons pour cela un schéma basé sur le protocole d'autentification KERBEROS amélioré par la divisions de la partie TGS à l'aide d'une cryptographie à seuil sur des courbes élliptiques. Notre proposition a permet d'éviter le point de défaillance unique habituellement touvé dans les schémas de base de KERBEROS.
Les contributions présentées se concentrent sur les axes suivants :
Tout d'abord, c'est la première fois qu'un schéma d'authentification combine à la fois le protocole d'autentification KERBEROS avec un TGS distribué à l'aide du schéma de seuil d'ELGAMAL sur des courbes élliptiques.
Le second axe est consacré à la modélisation de la sécurité en tant que paramètre dans la qualité de service. Nous proposons donc également des métriques afin de mésurer l'impact d'un élément sur l'autre.
Enfin, nous présentons Les perspectives de l'authentification et de la sécurité pour la mobilité dans un réseau ad hoc.
L'ensemble de ces travaux a été implémenté dans le simulateur ns2, ceci ayant permis d'effectuer une validation en conditions réelles du réseau.

Mots clés : Authentification, Kerberos, cryptographie à seuil, courbes élliptiques

Authentication architecture to ensure mobility and QoS in wireless networks

Abstract : The objective of this thesis is to provide a new authentication architectur adapted to wireless networks especially Ad hoc networks.
For this we use a model based on the authentication protocol improved the divisions of the TGS party to the KDC scheme using a threshold cryptography on elliptic curves. Our proposal avoids single point of failure usually Locate in the KDC database schemas. The papers presented will focus on the following areas :
First, this is the first time an authentication scheme combines the KERBEROS authentication protocol with TGS distributed with the threshold ElGamal scheme on elliptic curves.
The second axis is devoted to modeling of security as a parameter in the quality of service. We therefore propose metrics to measure the impact of an element on the other.
Finally, we present the perspectives of authentication and security for mobility in an ad hoc network.
All of this work has been implemented in the ns2 simulator, which allowed it to perform validation in real network conditions.

Keywords : Authentication, Kerberos, threshold cryptography, elliptic curves