Université ABDERRAHMANE Mira Bejaïa

Faculté des Sciences Exactes

Département d'Informatique

MÉMOIRE DE FIN DE CYCLE

En vue de l'obtention du diplôme Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème :

Sécurité contre les attaques liées aux identités dans les réseaux Ad hoc

Présenté par :

- MELOUK Yassamina.
- MOUHLI Souad.

Devant le jury composé de :

Président : M^{r} S.AISSANI.

Examinateur : M^{r} A.BAADACHE.

Promoteur : M^{r} A.ALOUI.

Promotion 2015/2016

Remerciements

Tout d'abord, nous remercions Dieu le tout-puissant qui nous a donné le courage, la force et la volonté pour mener ce travail.

Un grand merci pour nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet.

A nos chères amis qui ont toujours été présents et fidèles.

A notre encadreur ***Mr. ALOUI Abdelouahab*** *pour tout le temps qu'il nous a consacré, pour ces précieux conseils et pour toute son aide et son appui durant la réalisation.*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement.

Enfin, nous tenons aussi à remercier également tous les membres du jury pour avoir accepté d'évaluer notre travail.

Dédicaces

Je dédie ce modeste travail à mes tres chers parents qui ont toujours etaient la pour moi et qui m'ont setenue .

À mes très chères sœurs et a mon frère Rabeh .

À ma belle soeur Lynda.

À tous mes amis .

Souad Mouhli

Je dédie ce modeste travail à mes aimables et respectueux parents qui ont toujours veillés sur mes études.

À mes chers frères : Louanas et Fares et à mes sœurs : Samira et Yamina .

À tous mes amis .

Yassamina Mellouk

Table des matières

Table des Matières **i**

Liste des figures **v**

Liste des tableaux **vi**

Liste des abréviations **vii**

Introduction Générale **1**

1 Généralités sur les réseaux ad hoc **3**

1.1 Introduction 3

1.2 Réseaux mobiles ad hoc 3

1.2.1 definition 4

1.2.2 Normes 4

1.2.3 Applications des réseaux mobiles ad hoc 5

1.3 Modèle mathématique pour les réseaux ad hoc 5

1.4 Caractéristiques des réseaux ad hoc 6

1.5 Routage dans les réseaux ad hoc 7

1.5.1 definition 7

1.5.2 Classification de protocoles de routage 8

1.6 CONCLUSION 10

2 Sécurité dans les réseaux ad hoc **11**

2.1 Introduction 11

2.2 Vulnérabilités des réseaux ad-hoc 11

2.3 Exigences de sécurité 12

2.4 Mecanismes de securité 13
2.5 Attaques dans les réseaux ad hoc 15
2.5.1 Attaques externes 16
2.5.2 Attaques internes 16
2.5.3 attaques passives 16
2.5.4 attaques actives 17
2.6 Attaques possibles dans les protocoles de routage 17
2.6.1 Attaques d'identité 18
2.6.2 Modification, suppression et insertions des messages 18
2.6.3 Rejoue et réordonnancement des paquets 19
2.6.4 Déni de service (Dos) 20
2.7 Solutions de sécurité 20
2.7.1 Protocoles de sécurité 21
2.7.2 Protocoles sécurisés 23
2.8 Conclusion 24

3 Attaques liées aux identités dans les réseaux ad hoc 25
3.1 Introduction 25
3.2 Attaque d'identité 25
3.3 Man in the middle attack 26
3.3.1 Définition 26
3.3.2 Exemple 27
3.4 Spoofing attack 29
3.4.1 Définition 29
3.4.2 Exemple 29
3.5 Sybil attack 30
3.5.1 Définition 30
3.5.2 Exemple 31
3.6 Solutions proposées pour ces attaques 32
3.6.1 Man in the middle attack 32
3.6.2 Spoofing attack 33
3.6.3 Sybil attack 33
3.7 Conclusion 35

4 Proposition d'une technique de détection des attaques d'identités 36
4.1 Introduction 36

4.2 Modèle du réseau 36
4.3 Cryptographie a courbe elliptique 37
4.3.1 Echange de clés par courbes elliptiques 37
4.3.2 Transmission de messages 38
4.4 Challenge 39
4.5 Hypothèses 40
4.5.1 Scénario 1 : pour Spoofing attack 40
4.5.2 Scénario 2 : pour Sybil attack 40
4.6 Solution proposée 40
4.6.1 Spoofing attack 41
4.6.2 Sybil attack 42
4.7 Résultats de simulation 44
4.7.1 Métriques de simulation 44
4.7.2 Analyse et discution des résultats de simulation 44
4.8 Conclusion 46

Conclusion Générale **48**

Bibliographie **50**

Table des figures

1.1 Exemple de reseau adhoc. 4
1.2 Modélisation d'un réseau ad hoc. 6
1.3 Les nœuds cachés 7
1.4 Le chemin utilisé dans le routage entre la source et la destination. . . 8

2.1 Chiffrement symétrique 14
2.2 Chiffrement asymétrique 14
2.3 Classification des attaques dans les réseaux ad hoc. 16
2.4 Les attaques dans les protocoles de routage. 18
2.5 Classification des protocoles de sécurité et sécurisés. 21

3.1 Exemple pour l'attaque d'identité. 26
3.2 Scenario pour l'attaque Man in the middle. 27
3.3 Exemple d'ttaque Man in the middle. 28
3.4 Création de boucles de routage par Spoofing. 30
3.5 Sybil attack public. 32

4.1 La configuration du réseau. 37
4.2 Protocole d'échange de clés. 38
4.3 Protocole transmission de message. 39
4.4 Solution proposée pour spoofing attack. 42
4.5 Solution proposée pour un noeud sybil externe. 42
4.6 Solution proposée pour un noeud sybil interne. 43
4.7 Résultat du nombre d'identités internes. 45
4.8 Résultat du nombre d'identités externes. 45
4.9 Résultat du nombre de nœuds Sybil interne. 46

4.10 Résultat du nombre de nœuds Sybil externe. 46

Liste des tableaux

4.1 Paramètres de simulation 44

Liste des abréviations

AODV	**A**d-hoc **O**n **D**emand Distance **V**ector
ARAN	**A**uthentificated **R**outing protocol for **A**d hoc Network
CA	**C**ertificate **A**uthority
DCA	**D**estriduée **C**ertification **A**uthority
DOS	**D**enial of **S**ervice
DSDV	**D**ynamic **D**estination **S**equenced **D**istance **V**ector
ETSI	**E**uropean **T**élécommunication **S**tandards **I**nstitute
MAC	**M**essage **A**uthentification **C**ode
MAE	**M**anet **A**uthentification **E**xtention
MANET	**M**obile **A**d hoc **N**ETwork
MITM	**M**an in **T**he **M**iddle
PDA	**P**ersonal **D**igital **A**ssistant
SAODV	**S**ecure **A**d hoc **O**n **D**emand **V**ector
SAR	**S**ecurity **A**war Adhoc **R**outing Protocol
SEAD	**S**ecure **A**d hoc **D**istance vector routing
SN	**S**equence **N**umber
SRP	**S**ecure **R**outing **P**rotocole
TCP	**T**ransmission **C**ontrol **P**rotocol
TESLA	**T**imed **E**fficient **S**tream **L**oss-Tolerant **A**uthentication
ZRP	**Z**one **R**outing **P**rotocole

Les systèmes de communication cellulaires sont basés essentiellement sur l'utilisation des réseaux filaires et la présence des stations de base qui couvrent les différentes unités mobiles du système. Les réseaux mobiles "ad hoc" sont à l'inverse, des réseaux qui s'organisent automatiquement de façon à être déployables rapidement, sans infrastructure fixe, et qui doivent pouvoir s'adapter aux conditions de propagation, aux trafics et aux différents mouvements pouvant intervenir au sein des nœuds mobiles. L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calculs portables (les laptops par exemple), poussent aujourd'hui les chercheurs à faire des efforts afin de réaliser le but des réseaux : l'accès à l'information n'importe où et n'importe quand.

Un réseau sans fil ad hoc, ou MANET (Mobile Ad hoc NETwork), est un système autonome composé par un ensemble d'entités mobiles utilisant le médium radio pour communiquer. Il s'auto-organise et opère sans recourir à une infrastructure préexistante ou une administration centralisée. Dans un tel réseau, les nœuds qui sont hors portée radio les uns des autres comptent sur la coopération des nœuds intermédiaires pour acheminer les données à la destination. Bien que simple, rapide et moins coûteux à déployer, un réseau sans fil ad hoc est vulnérable par plusieurs types d'attaques. En effet, à cause de l'ouverture du médium de communication, la mobilité et l'absence d'infrastructure, un nœud malhonnête peut facilement écouter, modifier ou supprimer le trafic passant par lui. Il peut aussi cesser d'acheminer les données, tandis qu'il sollicite les autres nœuds pour lui acheminer ses données.

Des attaques telles que : le brouillage du canal de communication, l'usurpation d'identité, la consommation des ressources et bien d'autres attaques peuvent aussi être menées dans un réseau ad hoc. Ces attaques menacent généralement des services tels que l'authentification des nœuds, l'intégrité et la confidentialité des données, et la disponibilité du réseau.

Pour remédier à ce problème de sécurité, plusieurs approches ont été proposées dans la littérature. Ces approches peuvent être des solutions basées sur la cryptographie, des solutions basées sur la réputation des nœuds ou des solutions qui reposent sur les propriétés des protocoles afin de détecter les comportements malhonnêtes. Malgré cette diversité de solutions, le problème de sécurité reste toujours ouvert et le remède est loin d'être évident.

Dans ce mémoire, on s'est intéressé à l'attaque d'identité (Spoofing attack, Sybil attack, Man in the middle attack), un nœud malicieux peut voler les identités des autres nœuds, il peut utiliser des identités qui n'existent pas dans le réseau dans le

but de mener des attaques. En lançant une telle attaque, un nœud malicieux peut être élu un chef par un ensemble de nœuds, comme il peut orienter le trafic vers lui ce qui a comme conséquence la perturbation du bon fonctionnement du réseau.

Notre mémoire est structuré autour de quatre chapitres. Le premier chapitre, introduit les réseaux sans fil ad hoc, en particulier les caractéristiques, les domaines d'application, les normes de réseaux ainsi que les protocoles de routage, comme on ne peut pas parler de la sécurité sans parler de la cryptographie, le deuxième chapitre donne un aperçu sur les techniques cryptographiques utilisées pour assurer les services de sécurité. Le troisième chapitre se focalise sur les attaques liées aux identités dans les réseaux ad hoc (Spoofing attack, Sybil attack, Man in the middle attack) qui est le sujet de notre travail ainsi que les différentes solutions proposées dans la littérature. Le quatrième et dernier chapitre est consacré à la description de notre solution proposée ainsi que les résultats de la simulation.

Chapitre 1

Généralités sur les réseaux ad hoc

1.1 Introduction

Un réseau ad hoc sans fil est un système composé de nœuds (ordinateur portable, PDA, Netbook, etc.) éventuellement mobiles, qui permet à ses utilisateurs de communiquer via des ondes radio.

Deux types de réseaux sans fil peuvent être distingués :

Le réseau avec infrastructure qui est constitué de plusieurs stations de bases, reliées entre elles par une architecture filaire jouant le rôle d'un routeur pour faire communiquer des nœuds assignés à des stations de bases différentes.

Le réseau sans infrastructure ou ad hoc est un réseau dans lequel chaque nœud peut jouer le rôle d'un routeur , il n'y a pas de stations de bases comme dans le réseau avec infrastructure.

Dans ce chapitre, nous allons présenter les principaux concepts liés au réseau sans fil Ad hoc. Nous commencerons par la définition de ce type de réseaux et son domaine d'application ainsi que quelques caractéristiques, puis nous allons définir le routage dans le réseau ad hoc.

1.2 Réseaux mobiles ad hoc

Dans cette section, nous allons présenter essentiellement les applications, les caractéristiques et le routage dans les réseaux ad hoc.

1.2.1 definition

Les réseaux mobiles ad-hoc, ou réseaux MANET (Mobile Ad hoc Network) consistent en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou d'administration centralisée.
L'infrastructure n'est composée que des stations elles-mêmes qui jouent le rôle d'émetteur, de récepteur et de routeur. Le routage permet le passage de l'information d'un terminal vers un autre, sans que ces terminaux soient reliés directement, ce que montre la figure (1.1)[1].

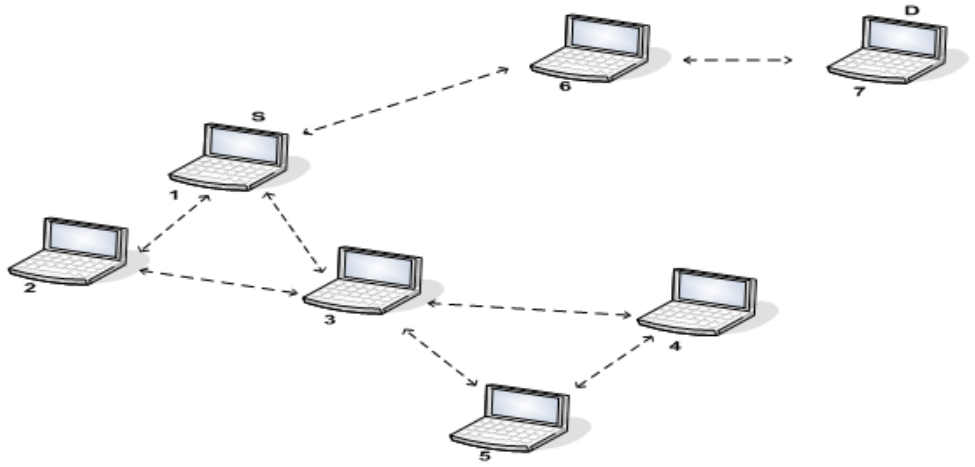

FIG. 1.1 – Exemple de reseau adhoc.

1.2.2 Normes

La norme la plus dominante est l'IEEE 802.11 et ses extensions (IEEE 802.11a, 802.11b, etc.) qui est la référence pour plusieurs produits sur le marché. En plus de la norme IEEE 802.11, il existe la norme européenne HiperLAN (type 1 et 2) et la norme Bluetooth.

• IEEE 802.11 : Est conçue pour les réseaux locaux, en entreprise ou chez les particuliers. Cette norme s'appuie sur des stations de base reliées à un réseau filaire qui fournit une infrastructure fixe et reliant les utilisateurs mobiles aux ressources de l'entreprise (et éventuellement à l'Internet).

• Bluetooth : Bluetooth a plutôt pour objectif de faire disparaître les câbles

entre les divers équipements numériques (périphériques d'ordinateur tels que clavier, imprimante, modem, ou encore appareil photo numérique, PDA, walkman, etc.). Les équipements Bluetooth ont donc des portées et des débits assez modestes, ainsi qu'une consommation électrique en rapport.

•Hyper LAN : Est une norme européenne standardisée par l'IETSI (European Télécommunication Standards Institute) qui a proposé deux versions d'HyperLAN.

- HyperLAN type 1 : A été conçu comme le pendant européen de 802.11. Cette norme se veut assez similaire dans son utilisation, mais certains choix technologiques ont été faits qui se démarquent nettement de 802.11. Commercialement cependant HiperLAN est resté à l'état de prototype et n'est jamais sorti des laboratoires de recherche.
- HyperLan type 2 : A pour but de concurrencer les versions les plus performantes de 802.11. (802.11a et 802.11b) en offrant des débits aussi élevés et un certain nombre de fonctionnalités supplémentaires. Mais là encore, il est à craindre qu'HiperLAN 2 ne soit jamais commercialisée à grande échelle [2].

1.2.3 Applications des réseaux mobiles ad hoc

Les applications ayant recours aux réseaux ad hoc couvrent un très large spectre, incluant les applications militaires et de tactique, les bases de données parallèles, l'enseignement à distance, les systèmes de fichiers répartis, la simulation distribuée interactive et plus simplement les applications de calcul distribué ou méta-computing. D'une façon générale, les réseaux ad hoc sont utilisés dans toute application où le déploiement d'une infrastructure réseau filaire est trop contraignant, soit parce que c'est difficile à mettre en place, soit parce que la durée d'installation du réseau ne justifie pas de câblage à demeure [3].

1.3 Modèle mathématique pour les réseaux ad hoc

Un réseau ad hoc peut être modélisé par un graphe Gt = (Vt, Et). Où Vt représente l'ensemble des nœuds (les unités ou les hôtes mobiles) du réseau et Et modélise l'ensemble les connexions qui existent entre ces nœuds. Si e = (u,v)$\in$ Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t. La figure (1.2) représente un réseau ad hoc de 10 unités mobiles sous

forme d'un graphe [4].

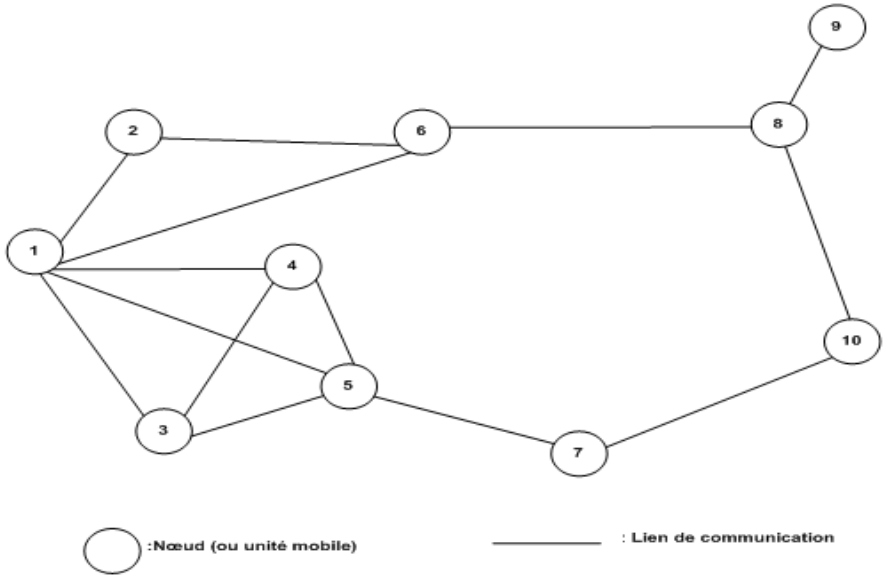

FIG. 1.2 – Modélisation d'un réseau ad hoc.

1.4 Caractéristiques des réseaux ad hoc

Les réseaux mobiles ad hoc sont caractérisés par ce qui suit :

• **Absence d'infrastructure :** Les réseaux mobiles ad hoc se distinguent des autres réseaux mobiles par l'absence d'infrastructure préexistente et de tout génère d'administration centralisée. Les nœuds mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une maniere continue.

• **Topologie dynamique :** Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.

• **Bande passante limitée :** Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.

• **Vulnérabilités :** Les réseaux ad hoc présentent plusieurs failles de sécurité. La liaison sans fil peut permettre à des nœuds non autorisés d'écouter et d'accéder facilement au réseau.

• **Contraintes d'énergie :** Les nœuds mobiles dans les réseaux ad hoc sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources

consommables, la consommation d'énergie devient alors un problème important.

• **Sécurité physique limitée :** Les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

• **Nœuds cachés :** Ce phénomène est très particulier à l'environnement sans fil. Un exemple est illustré par la figure (1.3).
Dans cet exemple, les nœuds B et C ne s'entendent pas, à cause d'un obstacle qui empêche la propagation des ondes. Les mécanismes d'accès au canal vont permettre alors à ces nœuds de commencer leurs émissions simultanément. Ce qui provoque des collisions au niveau du nœud A [3].

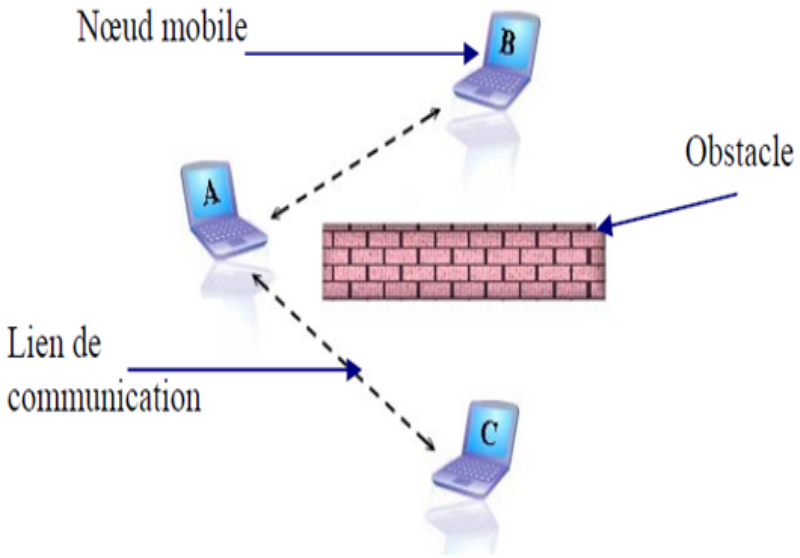

FIG. 1.3 – Les nœuds cachés

1.5 Routage dans les réseaux ad hoc

Les réseaux ad hoc étant de nature multi-sauts, le rôle d'un protocole de routage est de déterminer une route entre un nœud source et un nœud destination.

1.5.1 definition

Généralement, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage

consiste pour un réseau dont les arcs, les nœuds et les capacités sur les arcs sont fixés à déterminer un acheminement optimal des paquets (de messages, de produits .etc.) à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa survabilité en cas de n'importe quelle panne d'arc ou de nœud [5].

Par exemple si on suppose que les coûts des liens sont identiques,le chemin indiqué dans la figure(1.4) est le chemin optimal reliant la station source et la station destination.
Une bonne stratégie de routage utilise ce chemin dans le transfert des données entres les deux stations.

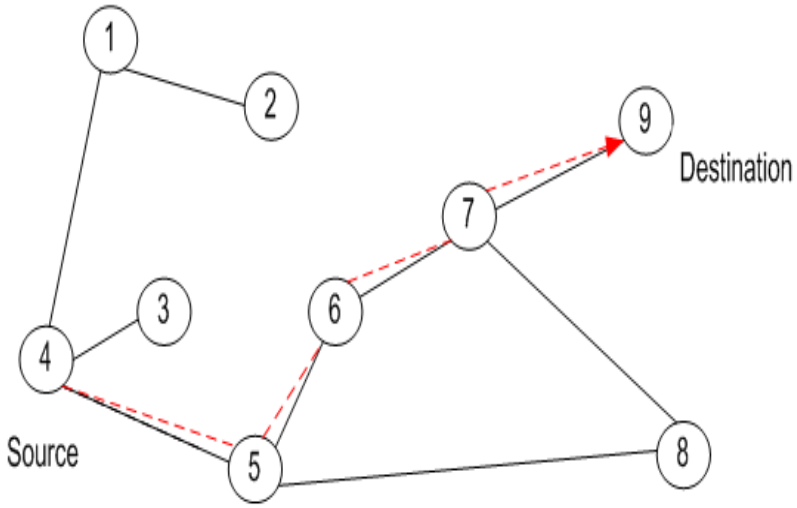

FIG. 1.4 – Le chemin utilisé dans le routage entre la source et la destination.

1.5.2 Classification de protocoles de routage

Les protocoles de routage peuvent être séparés en trois classes : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides.

• **Protocoles de routage proactifs (table driven)**

Dans cette catégorie dite à diffusion de table, les protocoles maintiennent à jour une table de routage dans chaque nœud contenant des informations sur la topologie du réseau. A chaque changement du réseau des messages de mise à jour sont communiqués aux nœuds afin d'avoir une vision globale du réseau. L'avantage de ce

protocole est qu'une route est toujours disponible entre une source et une destination sans pour autant déclencher des mécanismes de recherches de route. Cependant de tels protocoles présentent certaines défaillances dans le cas d'un réseau assez important ou de changements topologiques fréquents ou rapides.

Un exemple de tels protocoles est DSDV (Dynamic destination Sequenced Distance Vector) qui a été conçu spécialement pour les réseaux mobiles. Chaque station mobile maintient une table de routage qui contient toutes les destinations possibles, le nombre de sauts pour atteindre la destination, le numéro de séquences (SN) qui correspond à un nœud destination, permettant de distinguer les nouvelles routes des anciennes et d'éviter la formation de boucles de routage. Les mises à jour des tables sont transmises périodiquement à travers le réseau afin de maintenir la consistance des informations ce qui génère un trafic important qu'il faut limiter[3].

• Protocoles de routage réactifs (à la demande)

Représentent les protocoles les plus récents proposés pour assurer le service de routage dans les réseaux sans fil. Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon leurs besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et ce, dans le but d'obtenir une information spécifique.

Un exemple de tels protocoles est AODV (Ad-hoc On Demand Distance Vector) qui est un protocole réactif fondé sur le principe des vecteurs de distance, c'est-à-dire, dans le cas le plus simple, du nombre de sauts entre l'émetteur et le récepteur. Quand une application a besoin d'envoyer un flot de paquets dans 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, le protocole AODV a pour tâche de trouver la meilleure route [3].

• Protocoles de routage hybride

Est une combinaison entre les protocoles de routage proactif et réactif pour essayer d'apporter les avantages de chacun d'entre eux. Le principe est de connaitre le voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre sauts), et si jamais une application cherche à envoyer quelques choses a un nœud qui n'est pas dans cette zone il faut alors effectuer une recherche réactive à l'extérieur.

Exemple de protocole de routage hybride est ZRP (Zone Routing Protocole)[3].

1.6 CONCLUSION

Après avoir défini l'environnement mobile ad hoc et décrit ses principales applications et caractéristiques, nous avons parlé du routage dans les réseaux ad hoc ainsi que les attaques sur ces protocoles.

A cause des caractéristiques inhérentes de ces réseaux, un vrai problème de sécurité se pose. Dans le chapitre suivant, nous allons présenter les différentes attaques possibles ainsi que les solutions qui existent et qui résolvent le problème de routage dans les réseaux mobiles ad hoc.

Chapitre 2

Sécurité dans les réseaux ad hoc

2.1 Introduction

Un réseau ad hoc est une collection de nœuds, éventuellement mobiles, qui utilisent des liaisons sans fil comme support de communication et ceci sans l'aide d'une infrastructure préétablie ou administration centralisée. Ce réseau est simple, rapide et moins coûteux à déployer. Il est utilisé par plusieurs applications militaires et civiles. Ces applications ont particulièrement des exigences en termes de sécurité.

Cette sécurité n'est pas toujours facile à assurer à cause de multiples vulnérabilités qui sont essentiellement dues aux caractéristiques inhérentes de ce genre de réseau. Les services de la sécurité (l'authentification des participants, la confidentialité et l'intégrité des messages, la disponibilité du réseau, le contrôle d'accès au canal de communication et la non-répudiation) sont menacés par les attaques correspondantes : usurpation d'identité, écoute passive, déni de service et accès non autorisé.

Dans ce chapitre, nous présenterons d'abord les vulnérabilités, les failles exploités pour mener des attaques, et la sécurité des réseaux mobiles ad hoc (exigences de sécurité, mécanismes de sécurité) ensuite nous décriverons les déférentes attaques dans la littérature ainsi que les solutions de sécurité existantes.

2.2 Vulnérabilités des réseaux ad-hoc

Les réseaux ad-hoc sont plus vulnérable que les réseaux filaires à cause de leurs propriétés qui se résument par :

• **Vulnérabilité des canaux de communication :** A cause de l'ouverture et le partage du médium de communication, les messages transitant dans le réseau

peuvent être facilement écoutés et de faux messages peuvent être injectés dans le réseau.

• **Vulnérabilité des nœuds :** Les nœuds peuvent être facilement capturés ou volés et par conséquent tombés sous le contrôle de l'attaquant[6].

• **Manque d'infrastructure :** Etant donné qu'il n'y a pas d'infrastructure, les réseaux Ad hoc ne peuvent utiliser les équipements dédiés à la sécurité dans les réseaux traditionnels tels que les pare-feu ou les serveurs d'authentification. Tous les services de sécurités doivent donc être distribuées et coopératifs [7].

• **Bande passante limitée :** A cause des limitations de bande passante, les communications peuvent facilement être perturbée, l'intrus peut effectuer cette attaque en occupant le support avec ses propres messages, ou tout simplement en perturbant les communications avec du bruit [7].

• **Lien sans fil :** Qui conque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés. A la différence dans les réseaux filaires ou un intrus doit gagner l'accès physique au câble [7].

• **Equivalence des nœuds du réseau :** Comme tous les nœuds du réseau ad hoc participent au routage donc un nœud malicieux peut modifier, ajouter ou supprimer les messages en transit, ce qui entraine une perturbation du réseau [7].

• **Contrainte d'énergie :** La consommation d'énergie constitue un problème important pour des équipements fonctionnant avec une alimentation autonome. Cette dernière vulnérabilité fait que les attaques par dénis de service (DoS), sont possibles [7].

2.3 Exigences de sécurité

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs des machines possèdent uniquement les droits qui leurs ont été donnés. Les considérations de sécurité pour les réseaux ad hoc sont pris en compte tout comme les réseaux conventionnels. Assurer leurs sécurités revient alors à assurer les fonctions suivantes [8] :

• **Authentification :** S'assurer de l'identité des entités en cours de communication. Avec l'authentification, le destinataire sera sûr que le message provient de la source prétendue.

• **Confidentialité :** Assurer que l'information ne peut pas être interprétée par des tiers non autorisés. Les informations de routage doivent aussi, dans certains cas,

rester secrètes.

• **Intégrité :** Assurer que la modification des données transmises sera détectée. On utilise souvent les fonctions de hachage pour assurer l'intégrité.

• **Disponibilité :** Assurer la présence des services du réseau même en présence d'attaques de déni de service. Ces attaques peuvent se présenter au niveau de différentes couches d'un réseau ad hoc. La disponibilité donne aussi une assurance sur la réactivité et le temps de réponse du réseau.

• **Non-répudiation :** Empêcher un nœud de nier l'envoi ou bien la réception d'un message.

• **Contrôle d'accès :** Service de sécurité permettant de déterminer, après avoir authentifié un utilisateur, quels sont ses privilèges et de les appliquer. Ce service a pour but d'empêcher l'utilisation d'une ressource (réseau, machine, données,.etc.) sans autorisation appropriée.

2.4 Mecanismes de securité

Pour mettre en œuvre la sécurité dans les réseaux ad hoc, plusieurs outils ont été utilisés, on peut citer [9] :

• **Chiffrement** Consiste à coder un message en clair pour obtenir un message chiffré. nous avons deux types de chiffrements asymétrique et symétrique :

- Chiffrement symétrique (ou cryptographie à clé secrète) :Consiste à utiliser une même clé partagée entre l'émetteur et le récepteur pour chiffrer et déchiffrer les données.

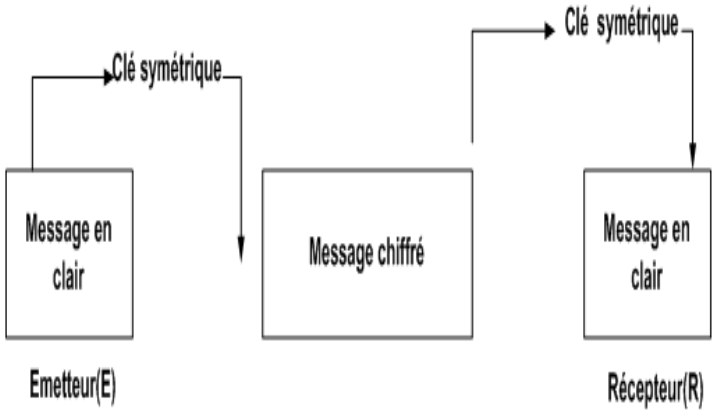

Fig. 2.1 – Chiffrement symétrique

– Chiffrement asymétrique (ou cryptographie à clé publique) :Qui repose sur l'utilisation d'une clé publique qui est diffusée à tout le monde et une clé privée maintenue secrète chez le récepteur. tout message chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante. D'où la confidentialité des messages chiffré avec la clé publique d'un récepteur.

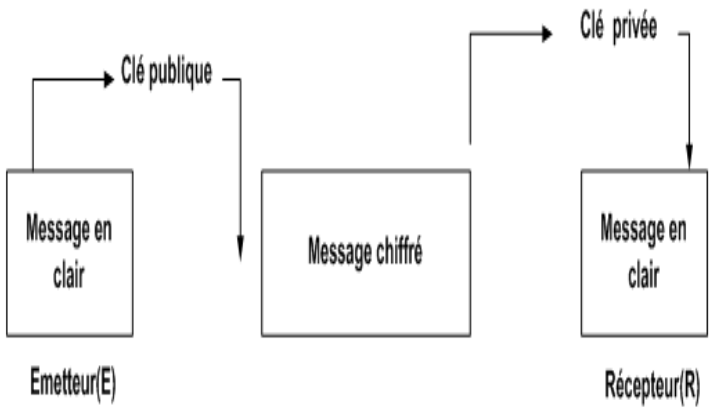

Fig. 2.2 – Chiffrement asymétrique

•**Le hachage :** Il consiste à déterminer une information de taille fixe et réduite (appelée l'empreinte ou le condensé) à partir d'une donnée de taille indifférente.

• **Les fonctions de hachage à sens unique :** Une fonction de hachage à sens unique est une fonction irréversible qui fournit l'empreinte à partir d'une chaine fournie en entrée. La particularité de cette fonction est qu'il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile de retrouver ou déduire la chaîne

initiale à partir de l'empreinte.

• **La signature numérique :** C'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à la clé privée du signataire.

• **Le MAC (Message Authentification Code) :** C'est un code accompagnant des données dans le but d'assurer l'intégrité de ces dernières.

• **Le certificat numérique :** un certificat est un document qui certifie que quelqu'un est le détenteur légitime de quelque chose. Les certificats numériques sont utilisés dans des applications de la cryptographie à clés publiques pour certifier qu'une entité possède une clé.

Un certificat contient deux champs importants : la clé publique d'une entité et son identité. Ces deux champs sont certifiés par un tiers de confiance, appelé l'autorité de certification. Le standard le plus utilisé pour la création des certificats numériques est le X.509 [10].

• **Cryptographie a courbe eleptique :** La cryptographie à courbe elliptique (ECC) est une approche de la cryptographie à clé publique basée sur la structure algébrique des courbes elliptiques sur les corps finis. Les courbes elliptiques sont applicables pour le cryptage, les signatures numériques, sont également utilisés dans plusieurs algorithmes de factorisation entière qui ont des applications en cryptographie, comme Lenstra courbe elliptique factorisation[27].

2.5 Attaques dans les réseaux ad hoc

Une menace dans un réseau de communication est un événement qui pourrait entraîner la violation d'un ou plusieurs services de sécurité. La mise en œuvre effective d'une menace est appelé attaque. Une variété d'attaques de sécurité est possible dans les réseaux ad hoc [11].

La classification des attaques qu'on trouve dans la littérature peuvent être classées par leurs sources (Interne, externe), par leurs effets (passive, active),ce que illustre la figure(2.3) :

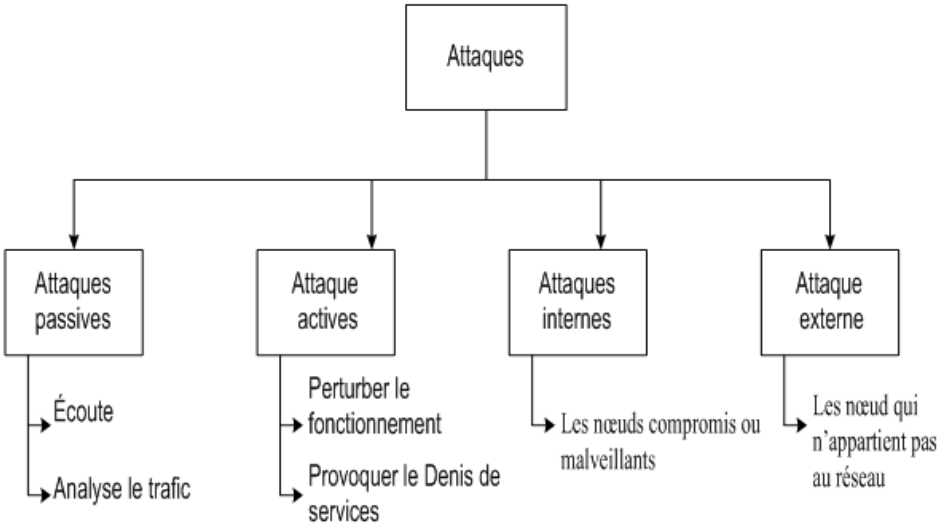

FIG. 2.3 – Classification des attaques dans les réseaux ad hoc.

2.5.1 Attaques externes

Cette catégorie inclus les attaques lancées par un nœud qui n'appartient pas au réseau ou bien qui n'est pas autorisé. Par exemple, un groupe de nœuds qui partagent une clé pour chiffrer ou déchiffrer des messages échangés entre les membres du groupe. Une attaque externe consiste à prendre connaissance de la clé partagée afin de l'utiliser pour mener des attaques contre les membres du groupe [8].

2.5.2 Attaques internes

Cette catégorie inclus les attaques lancées par des nœuds compromis ou malveillants. Par exemple, un membre de ceux qui partagent une clé commune, lance des attaques pour perturber le bon fonctionnement du réseau [8].

2.5.3 attaques passives

Les attaques passives se limitent à l'écoute et l'analyse du trafic échangé. Ce type d'attaques est plus facile à réaliser (il suffit de posséder le récepteur adéquat) et il est difficile à détecter puisque l'intrus n'apporte aucune modification sur les informations échangées. L'intention de l'intrus peut être la connaissance des informations confidentielles des utilisateurs ou bien la connaissance des nœuds importants dans

le réseau, en analysant les informations de routage, pour se préparer à une attaque active [8].

2.5.4 attaques actives

Un intrus tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service [8].
Par exemple parmi les attaques actives les plus connues, on peut citer :

- La modification :modifier les messages est une attaque contre l'intégrité, par exemple altérer les contenu du message.
- L'interception :intercepter les messages est une attaque contre la confidentialité, par exemple écouter le trafic dans le réseau pour en prendre connaissance.
- La fabrication :la fabrication des messages et leurs insertion dans le réseau est une attaque d'authentification, par exemple insertion des messages de réponses aux requêtes de découverte de routes.
- L'interruption :un atout du système est détruit ou devient non disponible, c'est une attaque contre la disponibilité.

2.6 Attaques possibles dans les protocoles de routage

Dans cette partie nous allons parler sur les attaques concernant les protocoles de routage, et pour cela nous avons opté pour la classification illustrée dans la figure(2.4) :

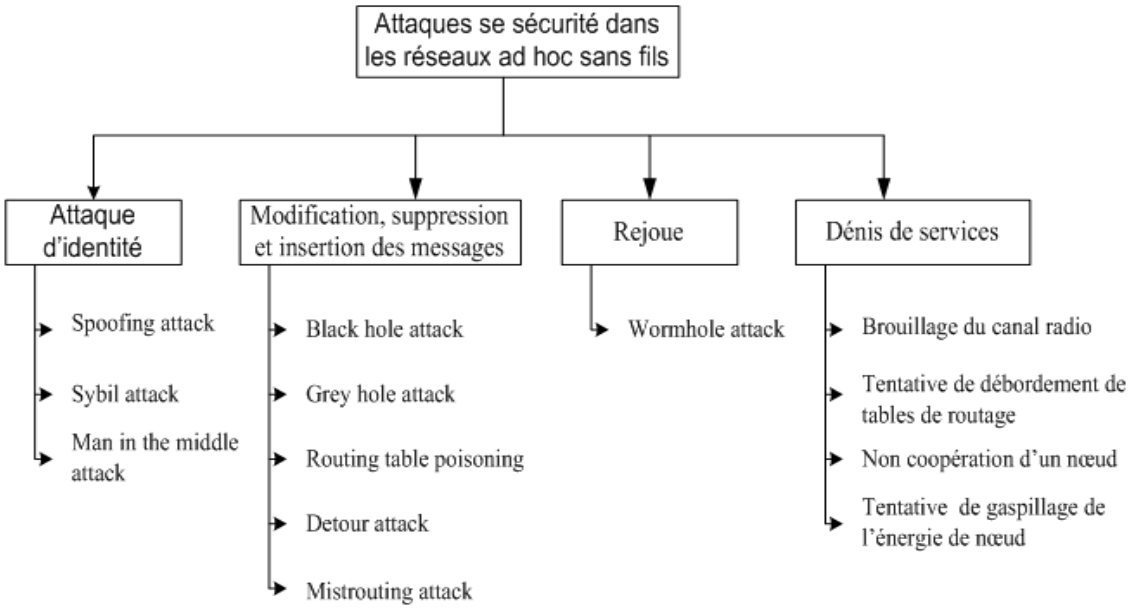

FIG. 2.4 – Les attaques dans les protocoles de routage.

2.6.1 Attaques d'identité

Dans cette classe d'attaque, un intrus usurpe l'identité d'un autre nœud afin de l'utiliser pour mener des attaques contre les autres nœuds du réseau. Un nœud peut usurper facilement l'identité d'un autre nœud, ceci peut être fait en changeant sa propre adresse IP MAC ou toute autre identité définie dans la couche application avec celle d'un autre nœud légitime. Certaine procédures fortes d'authentification peuvent être employée pour empêcher cette attaque[12].
On peut avoir plusieurs modèles de l'attaque d'identité :

- Spoofing attack
- Sybil attack
- Man in the middle attack

Dans ce genre d'attaque rentre la notion de malveillance des nœuds sur quoi s'intéresse notre étude, qu'on va expliquer en détail dans le chapitre suivant.

2.6.2 Modification, suppression et insertions des messages

• **Par modification :** En absence de contrôle d'intégrité sur les messages transmis, un nœud malicieux peut rediriger le trafic vers lui ou causer un déni de service,

simplement par la modification de certains champs des paquets de contrôle utilisés par les protocoles de routage.
On peut classer les attaques comme suit :

- Routing Table Poisoning : Un nœud malicieux peut provoquer des boucles de routage ou lancer un déni de service en changeant la liste des nœuds indiqués dans le paquet.
- Misrouting attack :un nœud malicieux envoie des paquets de données à des destinations fausses. Ce type d'attaque est effectué en modifiant l'adresse finale de destination du paquet de données.

• **Par suppression :** Dans ce type d'attaque, l'intrus supprime tous ou certains paquets.
On peut trouver deux types :

- Trou noir (Black holes) : Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou " trou noir " dans le réseau. L'attaquant supprime tous les paquets (contrôle de données).
- Trou gris (Gray holes) :C'est un cas particulier du trou noir dans lequel l'attaquant supprime les paquets de données et transmet ceux de contrôle.

• **Par insertion :** Dans ce type d'attaque, l'intrus peut insérer de nouveaux messages dans le but de perturber le bon fonctionnement du réseau.
On peut avoir un modèle de l'attaque par insertion :

- Détour attack : l'attaquant ajoute un certain nombre de nœuds Virtuels dans une route pendant la phase de découverte de route. Par conséquent, le trafic est détourné a d'autre routes qui semblent être plus courtes et pourraient contenir des nœuds malicieux [12].

2.6.3 Rejoue et réordonnancement des paquets

Rejouer les paquets dans un réseau ad hoc est une attaque différente de celle de rejoue dans les réseaux filaire classique en terme de temps et d'espace. Les nœuds malveillants peuvent se déplacer dans le réseau pour rejouer les paquets de données. Un nœud malveillant pourrait se déplacer aussi loin que possible du nœud destination avant de rejouer les paquets de données afin d'impliquer plusieurs nœuds intermédiaires et d'épuiser leurs ressources tout en transmettant les paquets. Les attaques de rejouer (rediffusion) sont généralement évités en utilisant une certaine forme de mécanisme de fraîcheur comme l'utilisation des numéros de séquence[12].

On peut avoir un modèle de l'attaque de rejoue :

– Wormhole attack :la conséquence d'une telle attaque peut être la falsification de l'information du voisinage.

2.6.4 Déni de service (Dos)

Apparaissent comme les attaques les plus faciles à réaliser par un attaquant. Des attaques par déni de services peuvent être réalisées en utilisant des connaissances internes de réseaux pour attaquer le support de transmission. Les nœuds du réseau font délibérément tomber les paquets au lieu de les transmettres, ainsi de ne pas intervenir dans la communication des nœuds voisins.
On peut avoir plusieurs modèles de déni de service :

– 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. 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 de nœuds ayant une autonomie de batterie faible ou cherchant à rester autonome (sans recharge) le plus longtemps possible. Ces nœuds se caractérisent par leur propension à passer en mode veille le plus souvent possible. 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.
– Dispersion et suppression du trafic en jouant sur les mécanismes de routage[12].

2.7 Solutions de sécurité

Plusieurs solutions ont été proposées dans la littérature pour pallier les problèmes de sécurité dans les réseaux ad hoc. Dans ce qui suit, nous allons présenter quelques protocoles de sécurité, et quelques protocoles sécurisés (les protocoles de sécurité conçus pour sécuriser des protocoles non sécurisé).
Nous avons opté pour la classification illustrée dans la figure(2.5) :

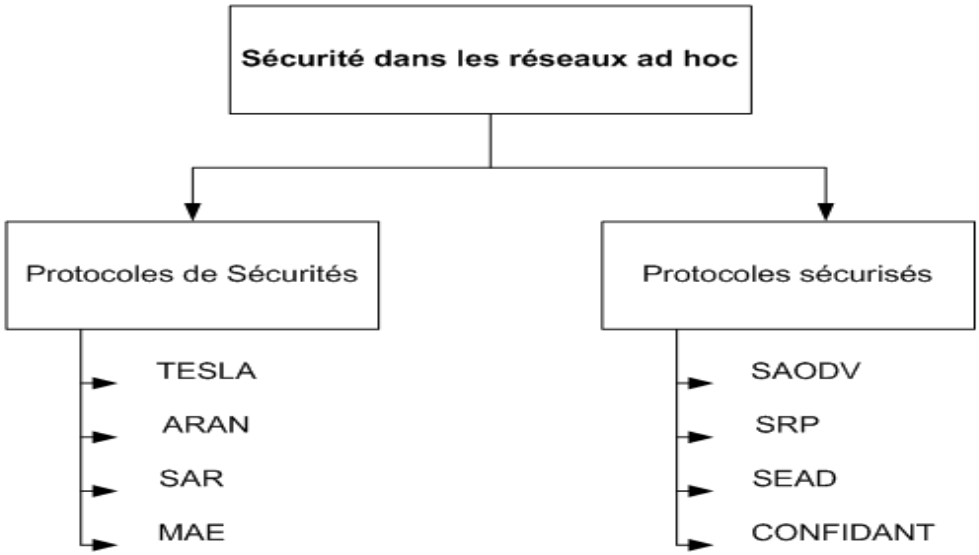

FIG. 2.5 – Classification des protocoles de sécurité et sécurisés.

2.7.1 Protocoles de sécurité

Dans cette classe, nous allons citer les protocoles suivants :

• **TESLA (Time Efficient Stream Loss tolerant Authentication)**

Ce protocole a été proposé par Perrig et al. Il permet d'authentifier les messages avec un MAC dépendant d'une clé secrète qui n'est divulguée par l'émetteur du message qu'après un délai d'attente, La valeur est calculée de manière à ce qu'on soit sûr que le destinataire a reçu le message avant la divulgation de la clé, cette condition garantie l'intégrité du message. La clé secrète utilisée pour le MAC est issue d'une chaîne de clés. Un élément de la chaîne ki est calculé de la manière suivante :
Ki = h (ki+1) où h est une fonction de hachage. L'élément initial kn est choisi par l'émetteur. Ce dernier va utiliser ces clés par ordre croissant, en commençant par k1. En réception, le destinataire pourra vérifier la relation suivante : ki-1 =h (ki) où ki est la clé dernièrement reçue et ki-1 correspond à la clé précédente. Cette condition assure que la clé ki fasse bien partie de la chaîne de clé de l'émetteur, ce qui assure l'authentification du paquet[13].

• **ARAN (Authenticated Routing protocol for Ad hoc Network)**

Ce protocole, proposé par Sanzgiri et al, se contente de l'authentification des nœuds de bout en bout par l'utilisation des certificats préétablis distribués par un serveur de confiance. Chaque nœud transmettant un message de demande de route doit le signer. Le paquet de demande de route RREQ ; D ; CertS ; NS ; tkpriv(S) envoyé par

le nœud source S à destination de D contient le certificat de l'émetteur CertS, une valeur aléatoire NS et un estampillage t. Ce paquet est signé à l'aide de la clé privée de la source kpriv(S). Le premier voisin recevant le paquet vérifie la validité de la signature et la validité du certificat de S avant de rajouter son certificat et signer le message avec sa signature. Chaque nœud intermédiaire vérifie la signature et le certificat du nœud du quel il a reçu le message et les remplacent par sa signature et son certificat et ainsi de suite jusqu'à ce que le message atteigne la destination. L'inconvénient de cette méthode est qu'elle utilise l'authentification saut par saut en vérifiant à chaque fois le certificat, ce qui augmente considérablement le calcul au niveau de chaque nœud ainsi que la taille des messages[6].

- **SAR (Security aware Ad hoc Routing protocol)**

L'idée principale du protocole de routage sécurisé SAR est de protéger le mécanisme d'établissement de la route contre la participation des nœuds malicieux. Pour cela, il introduit la notion de hiérarchie de confiance : chaque nœud a un niveau de confiance qui change progressivement en fonction de son comportement. Si le nœud participe dans la découverte des chemins alors son niveau de confiance augmente. Dans le cas où il annonce des informations de routage invalides ou il ne fait pas suivre le trafic dans le temps prévu, son niveau de confiance diminue.
Ce niveau de confiance permet de restreindre le mécanisme de découverte de la route seulement aux nœuds légitimes. L'initiateur de la route inclut dans le message RREQ une métrique de sécurité indiquant le niveau de confiance minimal que doit posséder le nœud pour participer à la découverte de la route. Cette idée peut être réalisée par le partage d'une clef secrète entre les nœuds possédant le niveau de confiance adéquat. Les messages RREQ seront ensuite chiffrés par cette clé[14].

- **MAE (Manet Authentification Extension)**

MAE, met en place un service de certification auto-organisé qui soit configurable suivant la politique de sécurité et adapté aux réseaux ad hoc. Dans ce modèle, l'autorité de certification (CA) est distribuée à l'aide de la cryptographie à seuil, qui permet de distribuer la clé privée de CA. MAE présente les dispositifs habituels permettant de certifier les clés publiques et aussi la gestion de la révocation des certificats. Son principal avantage et qu'il s'adapte à tous les protocoles du routage qu'ils soient proactifs ou réactifs [15].

2.7.2 Protocoles sécurisés

Dans cette classe nous citons à titre d'exemple les protocoles sécurisés suivants :

• **SAODV(Secure Ad hoc On demand Distance Vector)**

A été proposé comme une extension du protocole AODV en lui ajoutant un modèle de gestion de la réputation. Chaque nœud possède une idée formé des valeurs de confiance, de méfiance et d'incertitude à propos de chaque autre nœud. Suit a des événements positifs et négatifs résultant de l'interaction entre nœud, la réputation correspondante pour chaque nœud est incrémentée ou décrémentée [16].

• **SRP (Secure Routing Protocol)**

Un protocole de routage sécurisé (SRP, Secure Routing Protocol) doit être capable d'établir une communication entre deux nœuds même en présence de nœuds malicieux. Il doit aussi avoir la capacité de détecter les nœuds malicieux et d'avertir les autres nœuds légitimes du comportement de ces nœuds. Les nœuds légitimes vont donc écarter les chemins contenant des nœuds malicieux. Un nœud malicieux peut exploiter cette propriété pour lancer une attaque blackmail contre un nœud légitime. Pour lutter contre cette attaque, on doit avoir une hiérarchie de confiance. Le protocole doit aussi garantir la confidentialité des informations de routage pour empêcher un nœud malicieux de connaître les nœuds importants du réseau. Sinon ces nœuds seront des candidats pour une attaque en déni de service[17].

• **SEAD (Secure Ad hoc Distance vector routing)**

Ce protocole, proposé par Hu et al, est une version sécurisée du protocole de routage DSDV. Il est conçu pour protéger le numéro de séquence et le nombre de sauts dans les messages de mise à jour contre la modification. Il propose que chaque nœud calcule une suite de hachés (h0, h1,..., hn) en appliquant une fonction de hachage H tel que h0=x et hi=H (hi-1) avec 0¡i¡=n, x est une valeur initiale choisie aléatoirement. La suite de hachés est organisée en segments de m éléments chacun : (h0, h1, h2,..., hm-1), (hkm, hkm+1, hkm+2,..., hkm+m-1),..., hn où k= n/m-i, m étant le diamètre maximal du réseau et i le numéro de séquence. Il est à noter que la valeur hn est distribuée aux autres nœuds de telle sorte que chacun aura le haché final de tous les autres nœuds, qu'il stocke dans l'entrée correspondante de la table de routage.
Pour un numéro de séquence i et un nombre de sauts j, la valeur hn-mi+j correspond au haché à ajouter dans le message de mise à jour. Ceci permet au récepteur de vérifier l'authenticité de l'émetteur du message de mise à jour en appliquant successivement la fonction H, m* i-j fois sur le haché reçu et de comparer la valeur obtenue à celle stockée dans la table de routage (hn).

De cette manière, un attaquant ne peut jamais diminuer le nombre de sauts ou augmenter le numéro de séquence[18].

• **CONFIDANT**

Le système CONFIDANT, propose par Bucchegger et le Boudec, a pour but de détecter et exclure les nœuds malveillants dans un réseau ad hoc ; il est composé de plusieurs modules :

- Le contrôle : son rôle est de collecter des informations de première main sur le comportement des nœuds dans les réseaux. Les observations servent à classifier directement un nœud comme bienveillant ou malveillant.
- Le système de récupération :il se charge de combiner les informations de seconde main avec les informations de première main en une réputation locale sur chacun des nœud qui sert à son tour à décider si un nœud doit être considéré comme malveillant.
- Le gestionnaire de confiance : ce dernier décide à quel moment un message d'alarme doit être envoyé aux autres nœuds de confiance afin de les avertir du comportement malveillant d'un nœud. C'est aussi lui qui décide si le contenu d'un message d'alarme sera en considération ou ignoré.
- Le gestionnaire de chemins : il manipule la topologie vue par le nœud en fonction des degrés de confiance des autres nœuds afin d'éliminer les nœuds malveillants du réseau.
- Le protocole de routage : il exploite l'information de la topologie pour trouver des chemins valides et fiables. Principalement, il peut se baser sur le système de réputation pour refuser de router des paquets en provenance des nœuds malveillants[9].

2.8 Conclusion

Dans ce chapitre, nous avons présenté la sécurité dans les réseaux ad hoc, et dans lequel nous avons énuméré les différents services de la sécurité et les différentes attaques possibles ou la plupart de ces attaques ciblent la fonction principale des MANETs à savoir le routage, ainsi que quelques solutions existantes dans la littérature.

En conclusion, la sécurité des réseaux ad hoc reste toujours un challenge à cause des vulnérabilités de la communication sans fil.

Dans notre prochain chapitre, nous allons focaliser notre étude sur l'attaque d'identité (Spoofing attack, Sybil attack, Man in the middle attack).

Chapitre 3

Attaques liées aux identités dans les réseaux ad hoc

3.1 Introduction

Dans un réseau sans fil ad hoc, l'absence d'une autorité de certification centrale, qui assigne des identités aux nœuds du réseau, rend la gestion des identités difficile. Une attaque d'identité est lancée quand un nœud malveillant participe au réseau avec des identités multiples pour déformer le réseau et perturber son bon fonctionnement.

Dans ce chapitre nous allons détailler l'attaque d'identité ainsi que ces différents types (Man in the middle attack, Spoofing attack, Sybil attack) puis la problématique posés par ce type d'attaque qui a conduit à plusieurs initiatives ainsi que les solutions proposées pour ces attaques dans la littérature.

3.2 Attaque d'identité

Comme nous avons défini dans le chapitre précèdent, l'attaque d'identité est une attaque ou l'intrus usurpe l'identité (adresse IP ou MAC par exemple) et les privilèges d'un autre nouds afin de mener son attaque dans le réseau, ce que illustre la figure(3.1) :

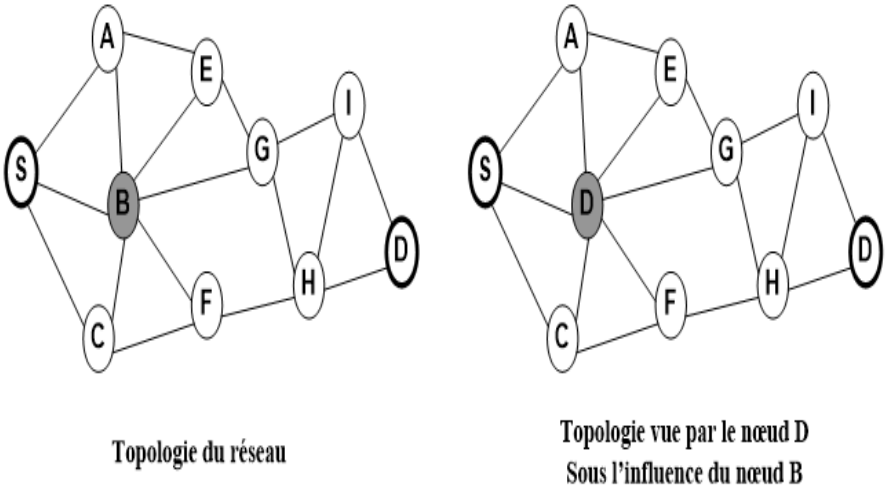

FIG. 3.1 – Exemple pour l'attaque d'identité.

Cette categorie d'attaques inclut :

- Man in the middle attack.
- Spoofing attack.
- Sybil attack.

Dans ce qui suit nous allons détailler ces types d'attaques.

3.3 Man in the middle attack

Dans cette partie nous allons définir et donner un exemple pour l'attaque Man in the middle.

3.3.1 Définition

L'attaque de l'homme du milieu (HDM) ou Man In The middle (HITM), est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre.

MITM est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. Elle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données, tout en masquant à chaque acteur de l'échange la réalité de son

interlocuteur. Pour mettre en œuvre l'échange réseau approprié, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine devienne un des points de passage [4].

Donc L'objectif principal de cette attaque est de détourner le trafic entre deux machines. Cela pour intercepter, modifier ou détruire les données transmises au cours de la communication, ce que nous allons illustrer dans la figure(3.2) :

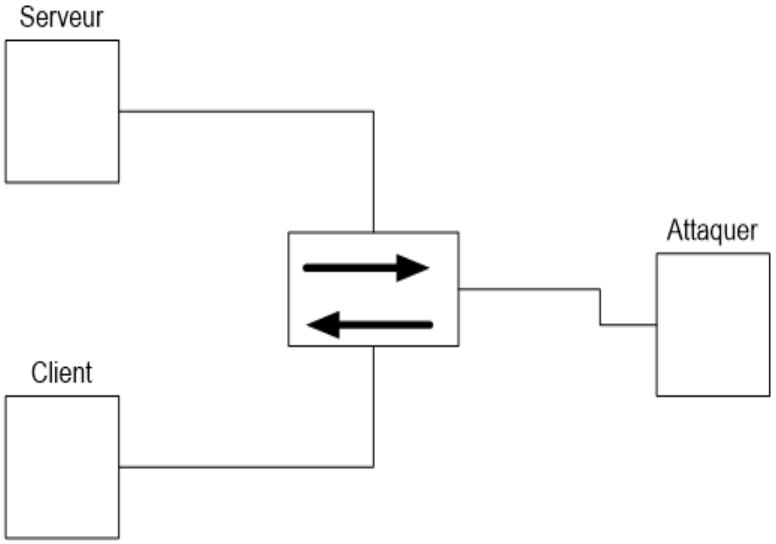

FIG. 3.2 – Scenario pour l'attaque Man in the middle.

3.3.2 Exemple

Il existe plusieurs exemples sur l'attaque man in the middle (injection, key exchanging, downgrade attack, feltring), dans ce qui suit nous allons définir l'exemple key exchanging (échange de clés).

Key exchanging (échange de clés de Diffi Hellman) : Modification de la clé publique échangée par serveur et client. Lorsque le client reçoit le message il ne peut pas s'assurer que c'est bien le serveur qui lui a envoyé et non pas un intrus (MITM), il y'a pas de moyens malheureusement, l'attaque MITM peut exploiter ce point faible pour tromper le serveur et le client.

Alice c'est le serveur, Bob est le client, et Eve attaquant de type man in the middle (MITM). Alice et Bob choisissent respectivement X et Y, Eve choisit Z. Alice envoie le message 1 a Bob, Eve l'intercepte et envoie le message 2 a Bob avec

les valeurs correctes de g et de n (qui de tout façon sont publiques), suivies de Z au lieu de X, elle renvoie aussi le message 3 a Alice. Ensuite Bob envoie le message 4 à Alice ; Eve l'intercepte également et le conserve. Maintenant chacun d'eux se plonges dans l'arithmétique modulo.

- Alice calcule la clé secrète gXZmod n, et Eve fait de même (pour les messages échangés avec Alice)
- Bob calcule gYZmod n et Eve fait de même chose (pour les messages échangés avec Bob)

Pensant qu'elle dialogue avec Bob, Alice va créer une clé de session (en réalité avec Eve) et Bob fait de même. Dans ce protocole chaque message que le serveur envoie au cours de la session chiffrés et capturé par l'attaquant (MITM), conservé, modifié au besoin et transmis au client comme le montre la figure(3.3).

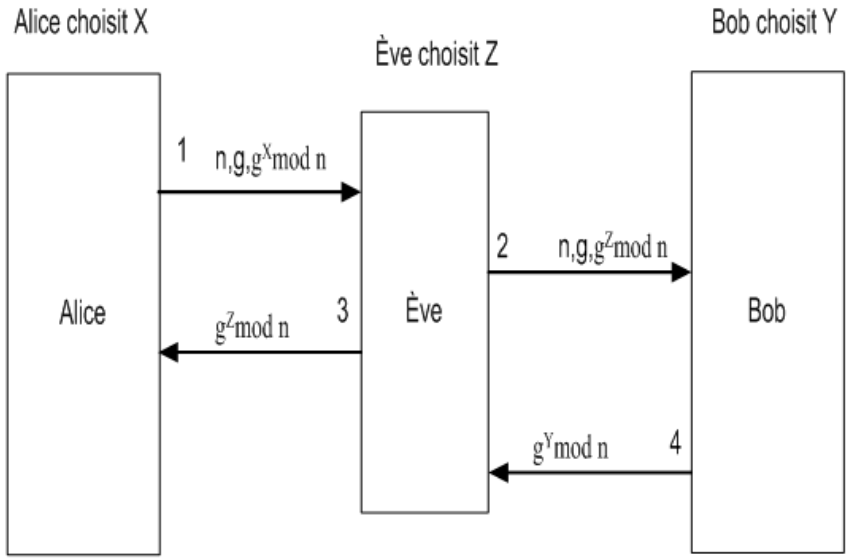

FIG. 3.3 – Exemple d'ttaque Man in the middle.

De la même façon dans l'autre direction, l'attaquant (MITM) intercepte tous les messages provenant du client, et destinés au serveur : ces messages peuvent donc être malicieusement modifié puis envoyé au serveur. Le serveur et le client ne s'en apercevront jamais qu'ils sont bernés par un intrus (MITM), ils pensent qu'ils sont liés par un canal sécurisé.

3.4 Spoofing attack

Dans cette partie nous allons definir et donner un exemple pour l'attaque Spoofing.

3.4.1 Définition

L'IP Spoofing signifie usurpation d'adresse IP, l'attaquant prend l'identité d'un autre nœud dans le réseau d'où il reçoit les messages qui sont destinés à ce nœud. Il peut ainsi recevoir les paquets destinés aux nœuds légitimes, diffuser de fausses informations de routage (envoyer par exemple de faux paquets de contrôle à la place du nœud légitime).

Cette attaque peut être utilisée de deux manières différentes :

- La première utilité de l'IP Spoofing va être de falsifier la source d'une attaque. Par exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée pour éviter de localiser la provenance de l'attaque.
- L'autre utilisation de l'IP Spoofing va permettre de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux[8].

3.4.2 Exemple

Nous avons choisis la création de boucles de routage que nous allons definir ci-dessous.

- **Création de boucles de routage par Spoofing**

  Un nœud malicieux change son adresse IP ou son adresse MAC afin de se faire passer pour un autre nœud légitime du réseau. L'intrus ensuite peut lancer ses attaques avec l'identité de ce nœud. L'usurpation d'identité peut conduire à des boucles de routage. Dans la figure 3.4.1 chacun des nœuds A, B, C, D possède une route vers la destination X. Pour former une boucle de routage, le nœud malicieux M change son adresse MAC pour qu'elle corresponde à celle de A, puis il annonce à B une route vers X avec une métrique meilleure (un nombre de sauts plus petit ou un numéro de séquence plus récent) que celle de la route à travers C. B met à jour alors sa table de routage en sauvegardant la nouvelle route vers X à travers A (figure 3.4.2). L'intrus répète le même processus avec le nœud C en usurpant l'identité du nœud B. C enregistre alors la nouvelle route vers X à travers B (figure 3.4.3). De cette façon une boucle est

formée et aucun paquet de l'un des quatre nœuds A, B, C, D ne peut arriver à X [8].

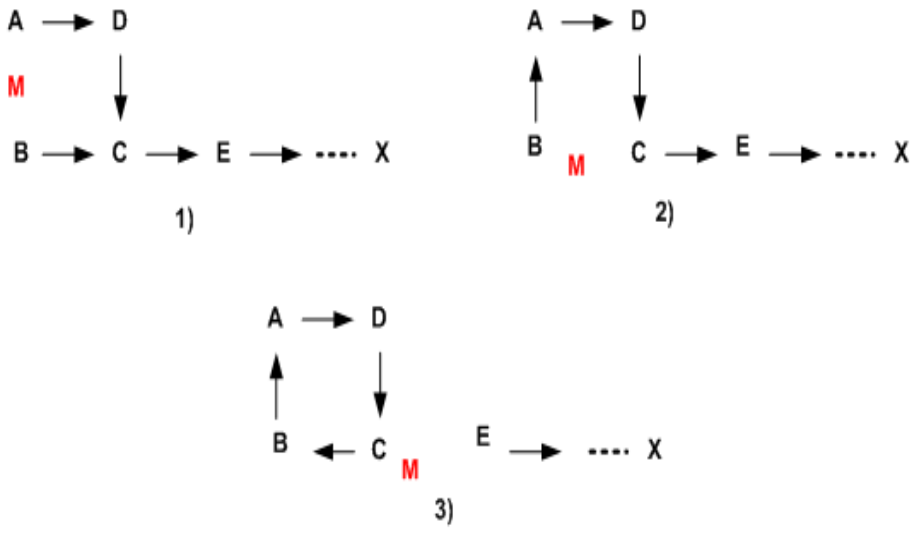

FIG. 3.4 – Création de boucles de routage par Spoofing.

3.5 Sybil attack

Dans cette section nous allons definir l'attaque Sybil et donner un exemple pour cette attaque.

3.5.1 Définition

L'attaque Sybil est une attaque par laquelle un nœud contrôle une fraction substantielle du système en présentant des identités multiples. Un attaquant génère un grand nombre d'identifiants. A partir de ce grand nombre d'identifiants, l'attaquant peut extraire un ensemble spécifique d'identifiants, lui permettant de compromettre la disponibilité ou l'intégrité du réseau. Elle est considérée comme une attaque très difficile à prévenir ou à détecter.

Pour donner une bonne description nous classifions l'attaque Sybil en deux catégories, le premier est la présentation des identités multiples simultanément, le second est la présentation des identités multiples exclusivement.

– La première, nous le décrivons comme suit : un ou plusieurs attaquants généré certaines identités. Ces derniers envoi ces identité fictives instantanément aux

nœuds attaqué et jouant le rôle d'intermédiaires.

– La seconde, un seul attaquant neutralise certains nœuds et se présente avec leurs identités respectives dans le réseau.

L'attaque Sybil 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[20].

3.5.2 Exemple

Nous allons definir dans ce qui suit Sybil attack public en créant de nouvelles identités.

– **Sybil attack public en créant de nouvelles identités (création de nouvelles attaques)**

Dans cet exemple le nœud compromis qui effectue l'attaque Sybil présent à tous ces voisins les nœuds fictifs qu'il a générés. Le nœud F déclare aux nœuds C, E, G qu'il possède d'autre voisins X et Y. ainsi, les cibles de l'attaque sont tous les voisins de l'attaquant. Logiquement les identités créées X et Y devraient avoir des voisins différents de ceux de F. dans notre cas, X doit être le voisin de E et Y doit être le voisin de G. si c'est le cas il devrait y avoir des communications entre ces nœuds. Pourtant, il n'ya aucun trafic entre ces nœuds donc les faux nœuds sont virtuellement a la même place que le nœud corrompu (à l'origine de l'attaque)[8].

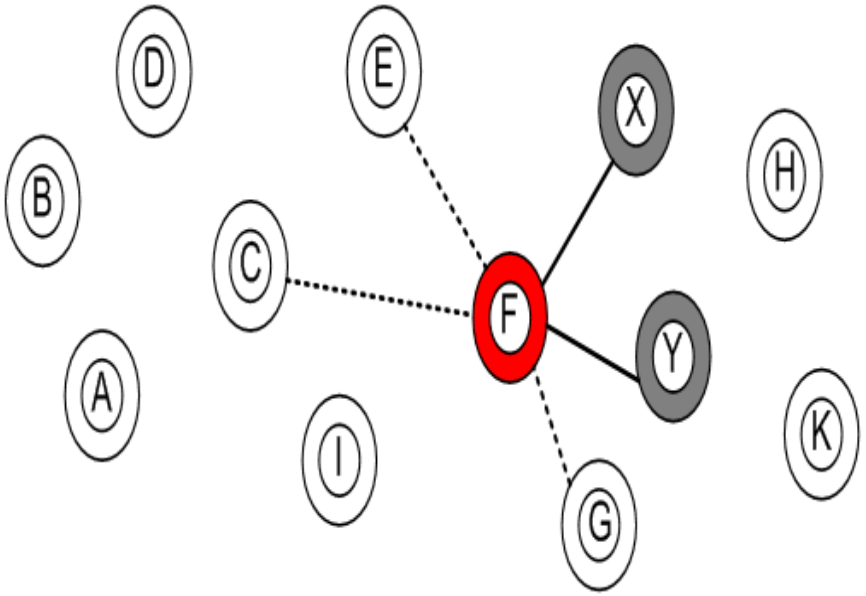

FIG. 3.5 – Sybil attack public.

3.6 Solutions proposées pour ces attaques

3.6.1 Man in the middle attack

Il existe différents moyens pour se prémunir de l'attaque MITM [21] :

- obtenir la clé publique de son interlocuteur par un tiers de confiance. Si les deux interlocuteurs possèdent un contact en commun (le tiers de confiance) alors ce dernier peut servir d'intermédiaire pour transmettre les clés. Les infrastructures à clés publiques sont des systèmes ou des organismes qui permettent de vérifier la validité des clés en se basant principalement sur des certificats ;
- vérifier le niveau de confiance qui a été accordée à la clé que l'on a en sa possession : certains logiciels comme GnuPG (est une implémentation de l'algorithme RSA) proposent de mettre la clé publique en ligne sur un serveur. Sur ce serveur, d'autres utilisateurs peuvent faire connaître le degré de confiance qu'ils accordent à une clé. On obtient ainsi un graphe qui relie les différents utilisateurs ;
- utilisation de hachage et la signature pour transmission des messages ;
- authentification avec un mot de passe ou autre système avancé.

3.6.2 Spoofing attack

Les conséquences d'une telle attaque est l'usurpation d'identité et prise de contrôle du serveur cible. Pour éviter ce genre d'attaque il faut :

- Le filtrage IP : Le filtrage IP consiste en la mise en place de règles de contrôle d'accès portant sur l'adresse IP source des paquets entrant dans un équipement ou une application, qui a alors la possibilité de comparer l'adresse IP source du paquet entrant avec une liste d'adresses autorisées (adresses unitaires ou réseau tout entier). Le paquet IP sera accepté seulement si l'adresse fait partie de cette liste. Dans le cas contraire, le paquet sera rejeté (émission d'un refus ou poubellisation). A noter que d'autres contrôles ou traitements sur le paquet peuvent être appliqués avant de l'accepter définitivement, mais ceci est hors de ce propos. Le concept de filtrage IP est également à la base de la notion de cloisonnement des réseaux : telle machine ne peut communiquer qu'avec telle autre machine.
- Les signatures dans les messages protègent effectivement le réseau contre les attaques d'usurpation d'identité. Toutefois, si un adversaire a réussi à prendre le contrôle d'un nœud légitime ou à s'emparer de sa clé privée, il peut générer des messages signés correctement avec son identité ; un tel nœud est appelé un nœud compromis.
- Ne pas utiliser uniquement l'adresse IP comme méthode d'authentification on ajoute un autre mécanisme d'authentification comme un login et un mot de passe ;
- Vérifier que son système n'a pas des numéros de séquence TCP facilement prédictible, Une solution consiste à refuser les paquets TCP SYN successifs depuis une même adresse pour éviter que le pirate prédise le comportement du générateur de numéros de séquences.

3.6.3 Sybil attack

Pour éviter ce genre d'attaque plusieurs solutions ont été propsées.

- Piro et al. [22] ont montré que la mobilité peut être utilisée pour améliorer la sécurité de la surveillance du trafic sur le réseau pour détecter un attaquant Sybil, qui utilise un certain nombre d'identités réseau simultanément. Ils montrent que cette détection peut être faite par un seul nœud, ou par de multiples nœuds de confiance pour améliorer la précision de la détection. Ils étendent encore la détection pour surveiller les collisions au niveau MAC

de différencier une seule usurpation de l'attaquant beaucoup d'adresses et un groupe de nœuds voyageant en proximité étroite.

- Zhou et al [23] considèrent que les autorités de certification distribuées (DCA) régimes qui sont basées sur la cryptographie à seuil, ne peut pas vaincre attaques Sybil et de résoudre le problème, ils proposent un système DCA multiples clé basée sur la cryptographie, qui est invulnérable aux attaques Sybil, et réalise la communication inférieure latence frais généraux et modéré par rapport avec le schéma à seuil.
- Le document [24] propose SAND (Sybil Attaque Découverte de Quartier élastique), un algorithme qui utilise des détecteurs de l'univers pour aider les nœuds pour déterminer quel univers est réel. L'idée principale est que chaque message transmis par le nœud contient ses coordonnées. Si un nœud reçoit un message dont les coordonnées ne sont pas correspondre à la puissance du signal reçu, les réponses de nœud avec un message de conflit, ce qui aide à détecter fictive les nœuds.
- Le document [25] propose une détection d'une technique d'attaque Sybil dans laquelle les nœuds peuvent déterminer localement leurs emplacements par des variations d'intensité du signal reçu et informer les voisins sur l'emplacement met à jour en conséquence. Ensuite le nœud vérifie la position de chaque nœud voisin et assure en outre que chaque emplacement physique est délimitée par une seule identité à un moment donné.
- Dans [26], les auteurs proposent une approche composée de deux éléments, une sécurité composant qui explore le réseau variable dans le temps topologie et son information statistique, et de la géométrie pour détecter l'existence d'attaques Sybil dans le réseau ad hoc sans fil, et un composant de visualisation qui intègre les résultats de détection et fournit un mécanisme pour illustrer les modèles de topologie anormaux et de localiser de fausses identités.
- Le document [27] propose une méthode de détection à base d'empreintes digitales à identifier les attaques d'usurpation d'identité et les attaques Sybil dans les réseaux sans fil. L'idée principale est qu'un seul nœud ne peut pas communiquer en utilisant deux identités différentes, parce que les empreintes digitales des identités ont été classées comme appartenant au même nœud.

3.7 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur l'attaque d'identité, dans laquelle un intrus usurpe l'identité d'un autre nœud. Apres avoir spécifié l'attaque d'identité, et montré comment ces types d'attaques peuvent perturber le fonctionnement du réseau et dégrader ces performances, nous avons présenté quelques solutions proposées dans la littérature qui visent à lutter contre ces types d'attaques.

Dans le chapitre suivant, nous allons détailler notre proposition et mener une série de simulation pour montrer son efficacité .

Chapitre 4

Proposition d'une technique de détection des attaques d'identités

4.1 Introduction

Notre objectif dans ce chapitre est de proposer une méthode de détection d'une attaque identités, en particulier l'attaque Spoofing et l'attaque Sybil, et pour cela nous allons utiliser la cryptographie a courbe elliptique et le challenge.
Dans ce qui suit, nous allons d'abord introduire le modèle de réseau sur lequel notre solution est implémentée, nous présenterons ensuite un certain nombre d'hypothèses relatives à la fiabilité de notre solution et enfin nous détaillerons et discuterons les résultats de la simulation.

4.2 Modèle du réseau

Le réseau, dans lequel notre solution est implémentée, est une collection de nœuds mobiles reliés par des liaisons sans fil, qui coopérent ensemble pour rendre la communication possible entre tout pair de nœuds dans le réseau.

Les nœuds de réseau doivent se mettre d'accord sur une clé secrète .

Pour mener son attaque, un nœud malicieux doit d'abord usurper l'identité du nœud source ou le nœud destination, ensuite il envoie des messages en se faisant passer pour l'un des nœuds pour empêcher les deux nœuds source et destination de communiquer l'un avec l'autre, ce que montre la figure(4.1).

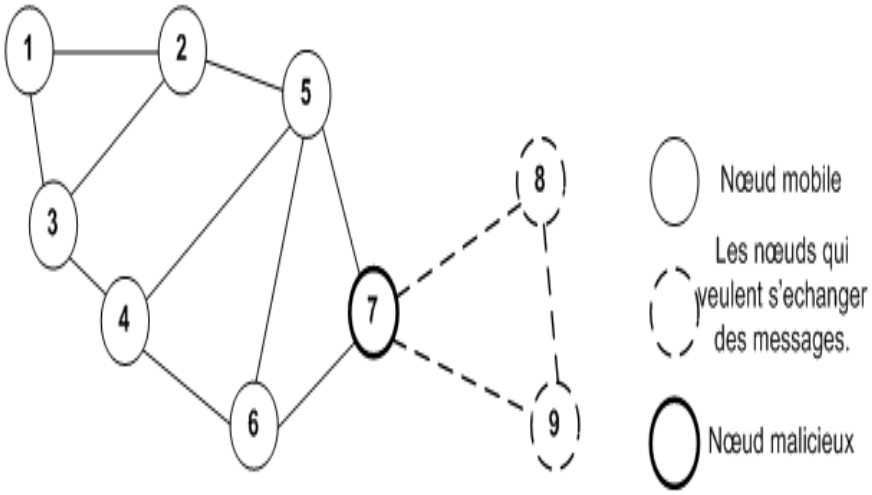

FIG. 4.1 – La configuration du réseau.

4.3 Cryptographie a courbe elliptique

La différence des algorithmes de chiffrement à base de courbes elliptiques par rapport aux algorithmes basés sur les entiers comme RSA ou El-Gamal est que, pour les vaincre, il faut résoudre un problème de logarithme discret sur une courbe elliptique est réputé être un problème plus difficile que le problème similaire dans les entiers modulos n. C'est pourquoi on estime qu'une clé de 200 bits (qui mesure, pour une courbe elliptique, la taille du corps fini K de cette courbe) pour les chiffres basés sur les courbes elliptiques est plus sûre qu'une clé de 1024 bits pour le RSA. Comme les calculs sur les courbes elliptiques ne sont pas bien compliqués à réaliser, c'est un gros avantage pour les cartes à puces où on dispose de peu de puissance, et où la taille de la clé influe beaucoup sur les performances [27].

4.3.1 Echange de clés par courbes elliptiques

Il s'agit d'un échange de clés à la manière de Diffie-Hellman, c'est-à-dire sans se les communiquer directement.

Alice et Bob se mettent d'accord ensemble et publiquement sur une courbe elliptique E(a,b,K), c'est-à-dire qu'ils choisissent un corps fini K (par exemple, Z/pZ), et une courbe elliptique y2=x3+ax2+b. Ils choisissent aussi ensemble, et toujours publiquement, un point P situé sur la courbe.

Ensuite Alice et Bob choisissent secrètement KA et KB, Alice envoie à Bob KAP,

et Bob envoie à Alice KBP, ils sont capable de calculer kA(kBP)=kB(kAP)=(kAkB)P, ce point de la courbe elliptique consiste la clé secrète ((kAkB)P.

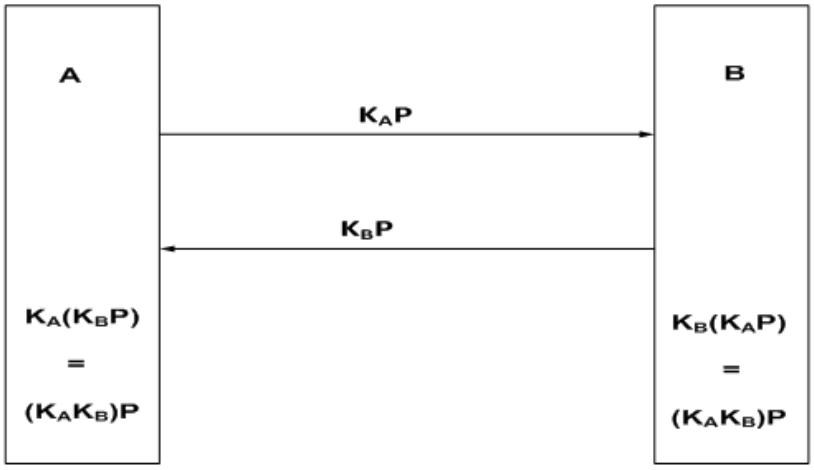

FIG. 4.2 – Protocole d'échange de clés.

4.3.2 Transmission de messages

On suppose cette fois qu'Alice veut envoyer à Bob un message en utilisant un algorithme de chiffrement par courbes elliptiques. Bob commence par fabriquer une clé publique de la façon suivante.
Il choisit une courbe elliptique E(a,b,K), un point P de la courbe, et un entier kB. Sa clé publique est constituée par la courbe elliptique E(a,b,K) et par les points P et kBP de cette courbe elliptique. Sa clé privée est l'entier kB, qu'on ne peut pas retrouver même connaissant P et kBP, par la difficulté de résoudre le problème du logarithme discret sur une courbe elliptique. Lorsqu'Alice veut envoyer de façon secrète un message M de la courbe elliptique à Bob, voici l'échange qui se passe :

- Alice prend connaissance de la clé publique (E,a,b,K), P et kBP de Bob.
- Alice choisit secrètement et aléatoirement un entier n.
- Alice calcule nP et M+nkBP et envoie ces deux points à Bob.
- Avec sa clé secrète kB, Bob calcule nkBP à partir de nP, puis il calcule (M+nkBP)-nkBP. Il retrouve ainsi M. comme le montre la figure (4.3).

Si quelqu'un espionne les échanges, on ne connait pas de chemin plus facile que de calculer kB pour retrouver M : c'est encore une fois le problème du logarithme discret à résoudre.

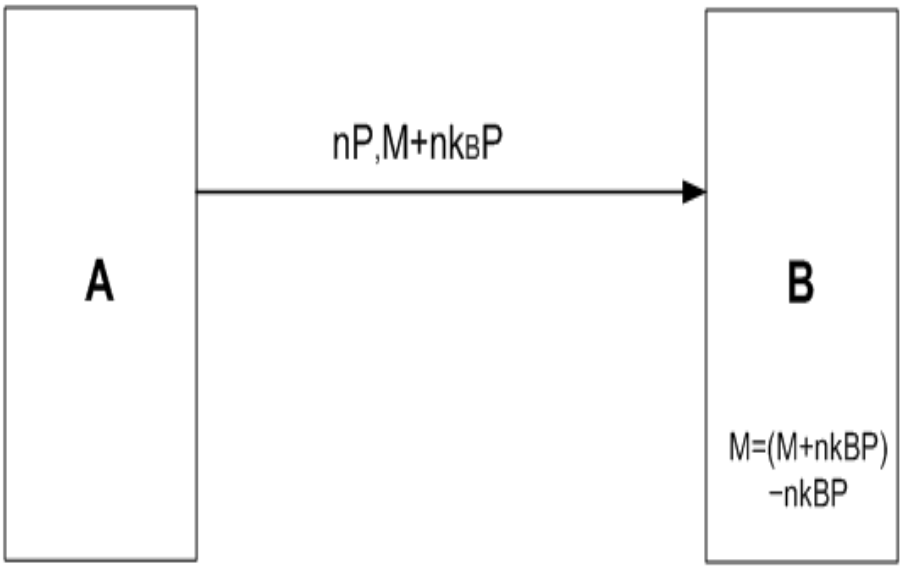

FIG. 4.3 – Protocole transmission de message.

4.4 Challenge

Le challenge est une opération de calcul qui nécessite une grande quantité de calcul à résoudre, mais il est facile à vérifier. Le challenge utilisé dans notre solution consiste à : que idD soit l'identité de nœud de détecteur, id(ni) l'identité du ni de nœud voisin, sn(ni) un numéro de séquence pour le ni voisin et r(ni) nombre aléatoire. Pour chaque noeud voisin ni, le challenge est de trouver x(ni) tels cette :

y (ni) = H (idD || id (ni) || sn (ni) || r (ni) || x (ni))

Où :

- H est la fonction de hachage .
- || : est l'opérateur de concaténation .
- y(ni) : le résultat de la fonction de hachage du nœud ni.
- y(ni) : le résultat de la fonction de hachage du nœud ni.

Le nœud détecteur D envoie à son ni voisin :Sn(ni), r(ni) et y(ni).

Le nœud ni, doit trouver une solution x(ni) et l'envoie au nœud détecteur D dans un délai ne dépassant pas le temps de calculs. Un nœud Sybil avec plusieurs identités recevra autant de challenges que les identités qu'il a, et il ne peut répondre à toutes ces challenges reçus, en raison du temps du calcul ts (qui est court)[28].

4.5 Hypothèses

Dans le réseau sur lequel notre solution est mise en œuvre, d'abord, nous allons décrire un réseau ad hoc dit neutre (sans aucune attaque), on suppose que les nœuds sont homogènes, la même capacité physique, énergétiques et de communication.

De plus, nous supposons que les liaisons sans fil sont bidirectionnelles. En effet, notre solution nécessite un bidirectionnel échange de paquets pour envoyer le défi et recevoir son résultat, et une clé qui est partagée dans le réseau pour assurer l'authentification

4.5.1 Scénario 1 : pour Spoofing attack

Nous allons la décrire pour un simple scénario pour l'attaque Spoofing composé de 3 nœuds, Soient A, M et B trois nœuds (M est un nœud malicieux).

- On suppose que le nœud A partage une clé secrète KP avec le nœud B.
- On suppose qu'un des nœuds du réseau effectue le Spoofing attack (le nœud malicieux M), M génère une fausse identité, ce nœud malicieux présente ces identités virtuelles a l'un de ses voisin en jouant le rôle d'intermédiaire.

4.5.2 Scénario 2 : pour Sybil attack

- Attaque externe : On suppose qu'un nœud externe du réseau effectue le Sybil attack, le nœud malicieux génère plusieurs fausses identités, ce nœud malicieux présente ces identités Virtuelles à l'un de ses voisins en jouant le rôle d'intermédiaire. Et on suppose qu'il existe une clé qui est partagée dans le réseau.
- Attaque interne : La déférence entre ce cas et le cas précédent est que le nœud malicieux est interne du réseau, et pour cela nous avons ajouté le challenge.
  On suppose que les noeuds ont le meme temps de calcul pour repondre au challenge.

Nous notons que ces hypothèses sont toutes raisonnables et pratiquement réalisables.

4.6 Solution proposée

Le mécanisme propose de détecter parmi les nœuds du réseau les nœuds malicieux. Les nœuds de réseau se mettent d'accord sur une courbe elliptique E (a, b,

k), c'est-à-dire choisissant un corps finis K et une courbe elliptique

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

Ils choisissent ensemble une clé K et un point P situé dans la courbe.
On suppose que tous les nœuds du réseau partagent une clé secrète KP pour chiffrer et déchiffrer les message échangés entre eux.

En utilisant une fonction de hachage h( ) et en chiffre le haché par la clé KP pour éviter la modification des messages passant par d'éventuels intrus M.

Dans le but de faciliter la compréhension de notre approche, nous allons la décrire pour un simple scénario pour l'attaque Spoofing composé de trois nœuds, ensuite nous la généraliserons pour l'attaque Sybil.

4.6.1 Spoofing attack

Notre solution doit assurer les points suivants :

- B doit recevoir le message envoyé par A ;
- M doit être empêché de jouer le rôle de A ;
- M ne pourra pas modifier le message passé par lui ;

• msg : le message en claire .
• idA : l'identité de l'émetteur A .
• e : le chiffrement de hachage avec la clé KP, donc e=encrypter KP (H1), et H1=h (msg).
A, B, veux vérifier l'intégrité et pour cela le nœud B il déchiffre e avec la clé KP, décrypter KP(e)= H2 ; si le H2= H1 alors c'est bien A qui la envoyé le message, il n'ya pas d'intrus, sinon il existe une attaque Spoofing.

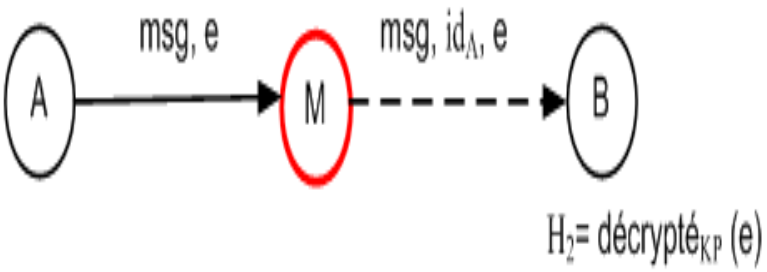

FIG. 4.4 – Solution proposée pour spoofing attack.

4.6.2 Sybil attack

- **1er cas : attaque externe**

Le nœud malicieux est un nœud externe de réseau, il ne connaît pas la clé KP qui est partagée dans le réseau. La solution c'est la même pour Spoofing attack sauf que dans l'attaque Sybil un nœud malicieux usurpe plusieurs identités comme le montre la figure (4.5).

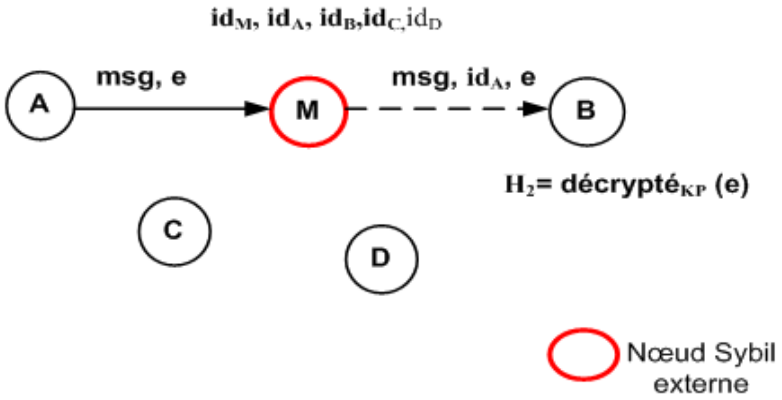

FIG. 4.5 – Solution proposée pour un noeud sybil externe.

- **2ème cas : attaque interne**

Dans cette solution tous les nœuds appartiennent au même réseau, le nœud malicieux M prend connaissance de la clé KP partagée dans le réseau donc l'échange de messages n'est pas sécurisé. C'est pour cela que nous avons ajouté un challenge.
Y (ni) : le résultat de la fonction de hachage du nœud ni.
Y (ni) = H (idD || id (ni) || sn (ni) || r (ni) || x (ni))
x (ni) : le nœud ni doit trouver une solution x (ni) et l'envoi au nœud détecteur(D).
Soit D le nœud détecteur et M un nœud malicieux, le nœud détecteur envoi un challenge a son voisin (les nœuds qui prennent connaissance de la clé KP). Lorsque le nœud malicieux M reçois le challenge il peut juste calculer la fonction de challenge pour seulement son identité a l'instant ts, lorsque il termine le calcul pour les autres identités (puisque M est un nœud Sybil il connaît toutes les identités des autres nœuds), il dépasse le temps de calcul, donc le nœud détecteur D refuse ses messages puisque il a accepté déjà les messages des autres nœuds a l'instant ts, comme le montre la figure (4.6).

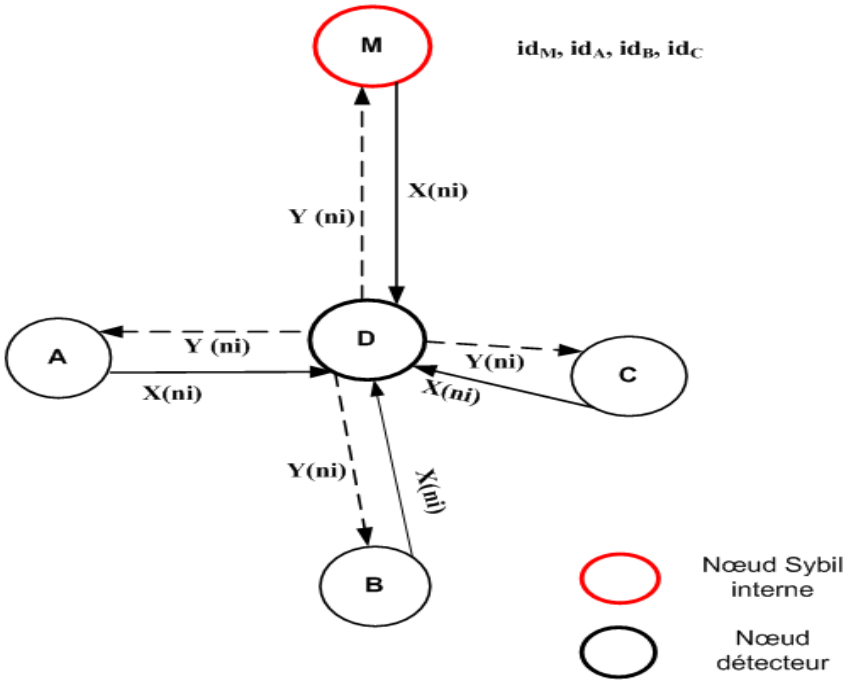

FIG. 4.6 – Solution proposée pour un noeud sybil interne.

4.7 Résultats de simulation

Pour montrer l'efficacité de notre solution dans la prévention de l'attaque Sybil, nous avons effectué une série de simulation en utilisant le langage JAVA. Les paramètres de simulation sont énumérés dans le tableau (4.1).

Paramètre	Valeur
Taille du réseau	1 km * 1 km
Portée	50 m
Taille du paquet	1024 bits
Nombres de nœuds	20
Temps de simulation	10 secondes

TAB. 4.1 – Paramètres de simulation

4.7.1 Métriques de simulation

Afin de mesurer la performance de notre solution, nous allons considérer les métriques suivantes :

- Le nombre d'identités pour un seul nœud Sybil.
- Le nombre de nœuds Sybil.

Les deux métriques sont mesurées pour montrer l'efficacité de notre solution.

4.7.2 Analyse et discution des résultats de simulation

L'objectif de notre solution et de détecter les nœuds Sybil qui sont soit interne, ou bien externe du réseau, et empêcher leurs communication dans le réseau.

Dans le but de monter que notre solution protège efficacement contre l'attaque Sybil, nous allons présenter les figures suivantes telles qu'elles sont mesurées dans les deux cas :

- Pour un seul nœud Sybil.
- Pour plusieurs nœuds Sybil.

• Pour un seul nœud Sybil

Les deux figures illustrent le résultat de simulation du nombre d'identités par raport au temps.

nous remarquons que le nombre d'identités usurpées par le nœud Sybil augmente avec le temps.

Les deux courbes obtenue du nombre d'identités usurpées par un nœud Sybil par rapport au temps est alors croissante et ça dans les deux cas (interne, externe) :

– Le cas où le nœud Sybil est interne.

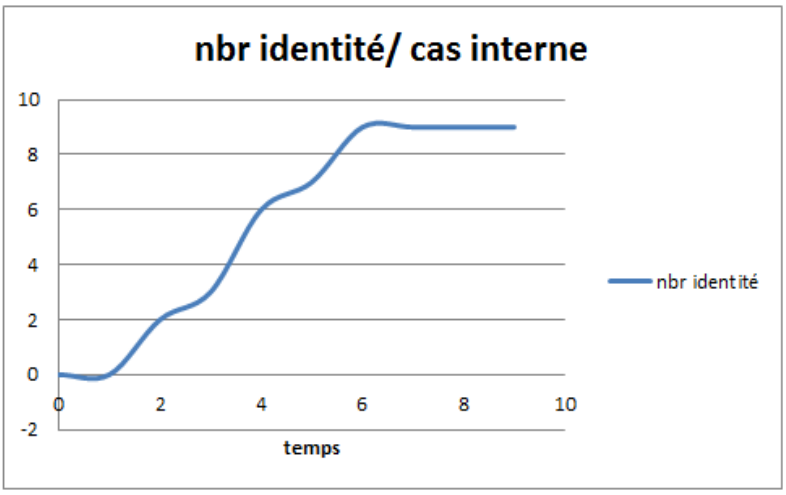

FIG. 4.7 – Résultat du nombre d'identités internes.

– Le cas où le nœud Sybil est externe.

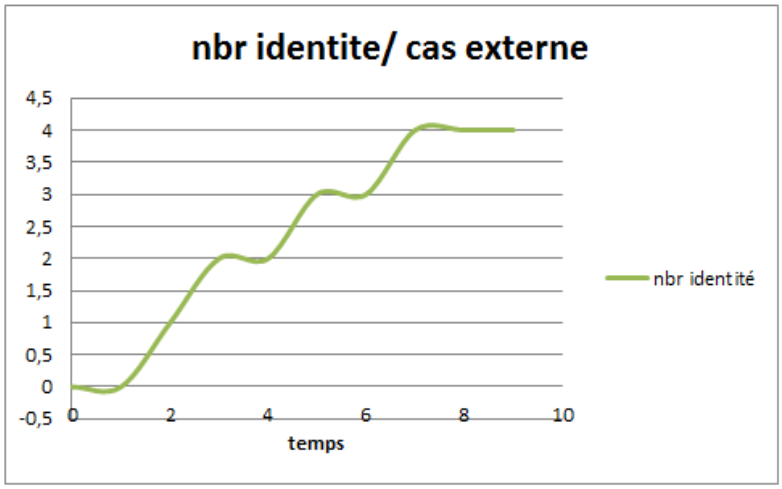

FIG. 4.8 – Résultat du nombre d'identités externes.

• **Pour plusieurs nœuds Sybil**

Les deux graphes suivants sont une représentation du nombre de nœuds Sybil par rapport au nombre de nœuds présent dans le réseau.

Nous remarquons d'après les graphes obtenus suite à la simulation, une augmentation du nombre de nœuds Sybil par rapport aux nœuds du réseau et sa dans les

deux cas(interne, externe).Et ce la montre que la solution est efficace pour detecter les noeuds sybil.

– Le cas où les nœuds Sybil sont internes

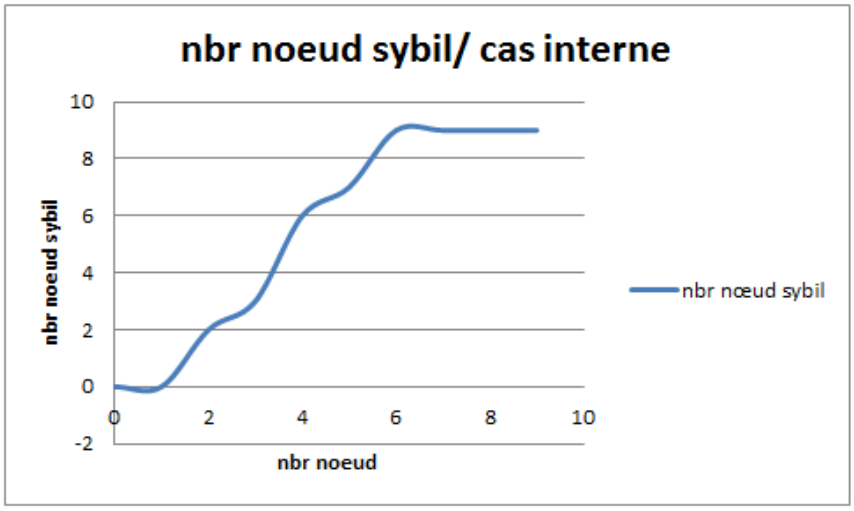

FIG. 4.9 – Résultat du nombre de nœuds Sybil interne.

– Le cas où les nœuds Sybil sont externes

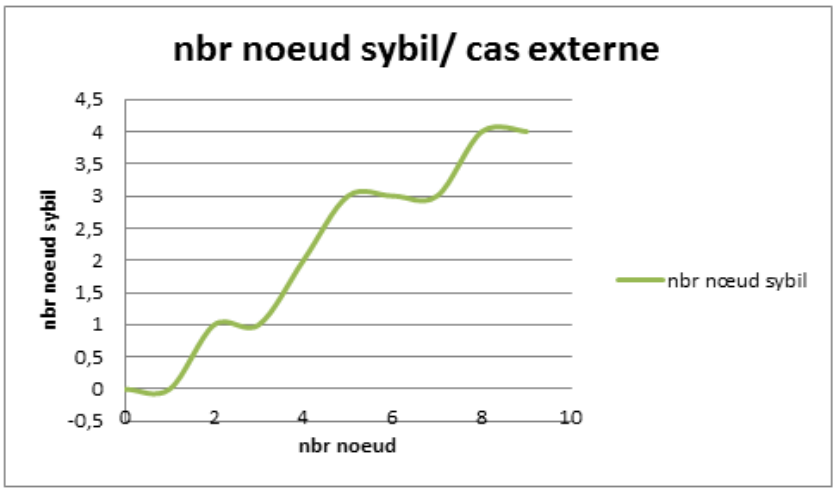

FIG. 4.10 – Résultat du nombre de nœuds Sybil externe.

4.8 Conclusion

Dans ce chapitre, nous avons proposé une approche pour lutter contre les attaques liées aux identités dans les réseaux Ad hoc (Spoofing attack, Sybil attack)

qui consiste à détecter les noeuds Sybil, et empécher la perturbation de la communication entre les nœuds légitimes dans un réseau. Pour se protéger contre cette attaque, nous avons proposé une solution qui se base sur la cryptographie à courbe elliptique et le challenge. Les résultats de simulation montrent que la solution proposée est efficace pour prévenir contre ce type d'attaques.

Un réseau ad hoc est une collection de nœuds mobiles qui communiquent entre eux via des liaisons sans fil. Il est simple, rapide, moins couteux à déployer, et facilement vulnérable par plusieurs types d'attaques à cause de ses caractéristiques inhérentes. En effet, un nœud malicieux peut écouter le trafic, le modifier ou même le supprimer.

En se comportant ainsi, un nœud malicieux vise les différents services de sécurité qui sont essentiellement l'authentification des participants, l'intégrité, la confidentialité des données et la disponibilité du réseau. Les solutions de la littérature, bien que multiples, ne font face qu'a un nombre limité de ces attaques.C'est pourquoi la sécurité dans les réseaux ad hoc reste toujours un problème ouvert.

Dans ce mémoire, nous nous sommes intéressés à la sécurité dans les réseaux mobiles ad hoc. En particulier, nous nous sommes focalisés sur les attaques liées aux identités dans les réseaux ad hoc (Spoofing attack, Sybil attack et Man in the middle attack), dont la conséquence est la perturbation du fonctionnement du réseau. Dans une telle attaque, le nœud malhonnête usurpe l'identité d'un autre nœud et l'utilise pour se faire passer pour lui.

Il existe deux variantes de cette attaque, la première variante est le Spoofing dans lequel un attaquant usurpe une seule identité et l'utilise pour avoir des privilèges qui ne lui sont pas accordés. La deuxième variante est le Sybil dans lequel un seul nœud prétend être plus qu'un seul en utilisant simultanément plusieurs identités différentes dans le réseau afin d'avoir la capacité de monter plus aisément des attaques.

Après avoir introduit les réseaux mobiles ad hoc et présenter une revue de littérature sur la sécurité dans ces réseaux, nous avons résumé les approches de sécurité proposées pour se protéger contre les attaques liées aux identités dans les réseaux ad hoc.

Dans ce travail, nous avons proposé une solution pour se protéger contre l'attaque Spoofing et l'attaque Sybil, on utilisant la cryptographie a courbe elliptique pour un nœud malicieux qui est externe du réseau, et nous avons ajouté un challenge dans le cas ou le nœud malicieux est interne du réseau. Après plusieurs simulations et plusieurs variations dans les paramètres de simulation, nous avons démontré la performance de notre solution.

En perspectives, nous souhaitons de :

- Simuler en implémentant le notre approche sous d'autres simulateurs comme NS 2, J-Sim, ...etc.
- Introduire la notion de mobilité dans notre solution.

– Enfin, mettre en pratique notre solution dans une application réelle des réseaux ad hoc.

Bibliographie

[1] G.PUJOLLE, " les réseaux ", livre, paris, 8 ème édition 2014.

[2] K.OUDIDI, " Routage et Qualité de Service dans les réseaux sans fil spontanés ", Thèse, Université Mohammed V - Souissi, 16 juillet 2010.

[3] M.FARIKHA, " Réseaux ad hoc : routage, qualité de service et optimisation ", livre, paris, lavoisier, 2010.

[4] A.BAADACHE, " sécurité de routage dans les réseaux mobiles ad hoc", thèse, magister en informatique, université de Bejaia, octobre 2005.

[5] N.DAUJEARD, J.CARSIQUE, R.LADJADJ, A.LALLEMAND, " LE ROUTAGE dans les réseaux mobiles Ad hoc ", mémoire d'informatique, 2002/2003.

[6] A. BAADACHE, "Sécurité contre l'attaque de suppression de paquets dans les réseaux mobiles ad hoc", thèse en informatique Réseaux et Systèmes Distribués, université de Bejaia, 08-07-2012

[7] W.STALLING "cryptography and network security, principal and practice ", edition prentice hall, 1999.

[8] O.CHEIKHROUHOU, " Sécurité des réseaux ad hoc ", thèse, Diplôme National d'Ingénieur en Génie Informatique Université de Sfax, Tunisienne, soutenu le 4 juillet 2005.

[9] A.PERRIG, and D.JOHNSON, "Wormhole attacks in wireless network", IEEE journal on Selected Areas in communications, 24(2) : 370-380, Feb 2006.

[10] R. HOUSLEY, W. POLK, W. FORD and D. SOLO, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC : 3280, Network Working Group, Apr, (2002).

[11] D. DJENOURI, L. KHALLADI and N. BADACHE, "A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys, vol 7, no 4, pp. 2-28, (2005).

[12] PO-WAH YAU, SHENGLAN HU and CHRIS J. MITCHELL, Attaques et vulnerabilities sur les réseaux ad hoc : [Malicious attacks on ad hoc network routing protocols Information Security Group, Royal Holloway, University of London Egham, Surrey TW20 0EX, UKP.Y au, S.Hu, C.Mitchell@rhul.ac.uk].

[13] A. PERRIG, R. CANETTI, D. TYGAR and D. SONG. The TESLA Broadcast Authentication Protocol. RSA Crypto Bytes, vol 5, no 2, pp. 2-13, (2002).

[14] S. Yi, P. NALDURG, and R. KRAVETS : "A security-aware ad hoc routing protocol for wireless networks", in : The 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002.

[15] R.S. PUTTINI, L. ME, and R.T.SOUSA, certification and authentification services for securing Manet routing protocols, In proceeding of the IFIP TC6 International conference on Mobil and Wireless Communication Networks, 2003.

[16] M.HAUSPIE, Contributions a l'étude des gestionnaires de services distribués dans les réseaux ad hoc, thèse de doctorat, université des sciences et technologies de Lille, 2005.

[17] S. GUPTE, M. SINGHAL : "Secure routing in mobile wireless ad hoc networks", ad hocNetworks 1 ,pp.151-174, 2003.

[18] Y. C. HU, D. B. JOHNSON and A. PERRIG. SEAD : Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, vol 1, no 1, pp.175-192, (2003).

[19] S. BUCHEGGER and J.Y. BOUDEC, "Self-policing mobile ad hoc network by reputation system. IEEE Communications Magazine", vol. 43, no. 7, pp. 101-107, 2005.

[20] S.ABBAS, M.MERABTI and D.LLEWELLYN-JONES. "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks". Second International Conference on Developments in eSystems Engineering, pages 190-195, (2009).

[21] http ://www.infosec.gov.hk, consulté le 23/06/2016.

[22] C.PIRO, C.SHIELDS and B.N.LEVINE, " Detecting the Sybil Attack in Ad hoc Networks". In Proceedings of IEEE/ACM International Conference on Security and Privacy in Communication Networks (SecureComm'06), pages 1-11, August,(2006).

[23] H.ZHOU, M.W.MUTKA and L.M.NI. "Multiple-keyCryptography-based Distributed Certificate Authority in MobileAd-hoc Networks ". Global Telecommunications Conference(GLOBECOM'05), pages 1681-1685, (2005).

[24] V.ADNAN, N.MIKHAIL, T.S´EBASTIEN and D.SYLVIE. "Universe Detectors for Sybil Defense in Ad Hoc Wireless Networks ". Proceedings of the 10th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'O8), Springer-Verlag, pages 63-78, (2008)..

[25] S.ABBAS, M.MERABTI and D.LLEWELLYN-JONES. "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks ". Second International Conference on Developments in eSystems Engineering, pages 190-195, (2009).

[26] W.WANG and A.LU. "Visualization Assisted Detection of Sybil Attacks in Wireless Networks ". In Proceedings of the 3rd international workshop on

Visualization for computer security. Pages 51-60, (2006).

[27] R.LERCIER," Courbes elliptiques et cryptographie" ,Sécurité des systèmes d'information,2004.

[28] W.MI, L.HUI, Z.YAN-FEI and C.KE-FEI. "TDOA-based Sybil attack detection scheme for wireless sensor networks". Journal of Shanghai University (English Edition), vol 12, no 1, pp. 66-70, (2008).

Résumé

L'absence d'une autorité de certification centrale dans les réseaux ad hoc sans fil qui les rend vulnérables aux attaques ciblant les identités des noeuds. Le Spoofing et le Sybil sont des attaques sévères dans lequel le même nœud physique survient dans le réseau en utilisant une ou plusieurs identités différentes. Le nœud malicieux peut causer plusieurs problèmes dans le réseau, comme l'annonce de fausses informations sur le voisinage ou par malveillance. Dans ce mémoire, nous proposons une solution qui est basée sur la cryptographie à courbe elliptique et le challenge. Apres simulation, Nous avons démontré l'efficacité et la performance de notre solution.

Mots clés : Réseau Ad hoc, Sécurité de routage, Attaque Spoofing, Attaque Sybil, Attaque Man in the middle.

Abstract

The absence of a central certification authority in wireless ad hoc networks makes them vulnerable to attacks targeting identities nodes. Spoofing and Sybil are severe attack in which the same physical node occurs in the network using one or more different identities. The malicious node can cause several problems in the network, such as the announcement of false information about the neighborhood or maliciously consensus. In this memory, we propose a solution that is based on elliptic curve cryptography and challenge. Through simulation, we have shown the efficiency and the performance of our suggested solution.

Key words: Ad hoc network, Routing security, Spoofing Attack, Sybil Attack, Man in the middle Attack.