République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

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

Option :

Administration et Sécurité des Réseaux

Thème

Schéma de détection de l'attaque Sybil dans les réseaux sans fil Ad hoc

Présenté par :
M^{elle} SMAOUN Sarah
M^{elle} ZALIF Nouha

Devant le jury composé de :

Président :	M^r KHENOUS Lachemi	Université Abderrahmane Mira de Béjaïa
Rapporteur :	M^r BAADACHE Abderahmane	Université Abderrahmane Mira de Béjaïa
Examinateurs :	M^r SÂADI Mustapha	Université Abderrahmane Mira de Béjaïa
	M^r AMAD Mourad	Université Abderrahmane Mira de Béjaïa

Année universitaire 2014/2015

Remerciements

Nous remercions Dieu le tout puissant, de nous avoir accordé santé et courage pour accomplir notre cycle d'études

$\mathcal{A}$Au terme de ce travail, nous saisissons cette occasion pour exprimer nos vifs remerciements à toute personne ayant contribué, de près ou de loin, à la réalisation de ce travail.

$\mathcal{N}$ous souhaitons tout d'abord remercier notre encadreur,M^{r}A. BAADACHE qui nous a encadrées avec patience durant la réalisation de ce travail de fin cycle. Ses conseils nous ont été bien utiles, notamment pour la rédaction de ce mémoire.

$\mathcal{N}$ous remercions vivement les membres de jury : M^{r}L. KHENOUS pour l'honneur qu'il nous a fait en acceptant de présider le jury et à M^{r}M. SÂADI et M^r M. AMAD pour avoir accepté d'examiner notre travail.

$\mathcal{U}$n grand merci pour tous les membres de nos familles pour leurs soutiens et leurs encouragements, particulièrement nos parents.

Nous dédions ce modeste travail aux :

$\mathcal{P}$ersonnes les plus chères nos yeux, nos parents.

$\mathcal{N}$os chères sœurs et frères .

$\mathcal{A}$ toute nos familles.

$\mathcal{A}$ nos sincères copines .

$\mathcal{A}$ nos chères amies.

$\mathcal{T}$ous ceux qui sont proches de nos cœurs et dont nous n'avons pas cité leurs noms.

Sarah et Nouha

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AODV	**A**d hoc **O**n **D**emand **D**istance **V**ector
AP	**A**ccess **P**oints
ARAN	**A**uthenticated **R**outing protocol for **A**d hoc **N**etwork
ARP	**A**ddress **R**esolution **P**rotocol
BISS	**B**uilding **S**ecure routing out of an **I**ncomplete **S**et of security Associations
BSS	**B**asic **S**ervice **S**et
CA	**C**ertificate **A**uthority
CBRP	**C**luster **B**ased **R**outing **P**rotocol
CC	**C**entral **C**ontroler
CONFIDANT	**C**ooperation **o**f **N**odes , **F**airness **I**n **D**ynamic **A**d hoc **N**eTworks
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance
DECT	**D**igital **E**nhanced **C**ordless **T**elecommunication
DNS	**D**omain **N**ame **S**ystem
DoS	**D**éni **o**f **S**ervice

DSDV	**D**estination **S**equenced **D**istance **V**ector routing
DSR	**D**ynamic **S**ource **R**outing
ETSI	**E**uropean **T**echnical **S**tandard **I**nstitute
FHSS	**F**requency **H**opping **S**pread **S**pectrum
FSR	**F**isheye **S**tate **R**outing
IBSS	**I**ndependent **B**asic **S**ervice **S**et
IARP	**I**ntrAzone **R**outing **P**rotocol
IERP	**I**ntErzone **R**outing **P**rotocol
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IP	**I**nternet **P**rotocol
HiperLAN	**H**igh **P**erformance **L**ocal **A**rea **N**etwork
HMAC	keyed-**H**ash **M**essage **A**uthentification **C**ode
HomeRF	**Home R**adio **F**requency
LAN	**L**ocal **A**rea **N**etwork
MAC	**M**edia **A**ccess **C**ontrol
MAC	**M**essage **A**uthentication **C**ode
MAE	**M**anet **A**uthentification **E**xtension
MANET	**M**obile**A**d hoc **N**ETwork
MPR	**M**ulti **P**oint **R**elay

OLSR	**O**ptimized **L**ink **S**tate **R**outing protocol
OSPF	**O**pen **S**hortest **P**ath **F**irst
PAN	**P**ersonnal **A**rea **N**etwork
POPA	**P**rinciple **O**f **P**rivilege **A**ttenuation
RDP	**R**oute **D**iscovery **P**acket
RREQ	**R**oute **REQ**uest
RREP	**R**oute **REP**lay
RERR	**R**oute **ERR**or
RSS	**R**eceived **S**ignal **S**trength
RSSI	**R**eceived **S**ignal **S**trength **I**ndication
SAODV	**S**ecure **A**d hoc **O**n demand **D**istance **V**ector
SAR	**S**ecurity **A**ware **R**outing
SEAD	**S**ecure **E**fficient **A**d hoc **D**istance vector routing protocol
SLSP	**S**ecure **L**ink **S**tate **P**rotocol
SNS	**S**ocial **N**etwork **S**ervice
SOSLR	**S**ecure **O**ptimized **L**ink **S**tate **R**outing Protocol
SPINS	**S**ecurity **P**rotocols for **S**ensor **N**etworks
SRP	**S**ecure **R**outing **P**rotocol
SSID	**S**ervice **S**et **ID**entification

TBRPF	**T**opology **B**roadcast based on **R**everse-**P**ath **F**orwarding
TC	**T**opology **C**ontrol
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TESLA	**T**imed **E**fficient **S**tream **L**oss-tolerant **A**uthentication
TIK	**T**esla with **I**nstant **K**ey disclosure
TORA	**T**emporary **O**rdering **R**outing **A**lgorithm
TTL	**T**ime **T**o **L**ive
URL	**U**niform **R**esource **L**ocator
ZRP	**Z**one **R**outing **P**rotocol

Introduction générale

Un réseau sans fil ad hoc est un ensemble de nœuds qui utilisent des liaisons sans fil pour communiquer. Il s'agit d'un réseau où la communication entre nœuds est rendue possible grâce à la coopération entre les nœuds, c'est à dire, des nœuds qui ne se trouvent pas à portée de communication les uns des autres, sollicitent les nœuds intermédiaires pour acheminer les paquets. Un tel type de réseau est caractérisé principalement par l'ouverture et le partage du médium de communication, la mobilité éventuelle des nœuds et l'absence d'infrastructure. Ces caractéristiques rendent le déploiement du réseau facile, moins coûteux et rapide. En contrepartie, ces caractéristiques rendent aussi le réseau très vulnérable aux différentes attaques possibles. En effet, un support sans fil ouvert et partagé permet à n'importe qui à portée de communication d'intercepter, de modifier ou de même supprimer le trafic dans le réseau. En outre, la mobilité et l'absence d'infrastructure rendent difficile l'application des mécanismes de sécurité utilisés en filaire.

Plusieurs classes d'attaques contre les réseaux ad hoc sont répertoriées dans la littérature. Ces attaques visent essentiellement les différents services de sécurité qui sont : l'authentification des nœuds, l'intégrité et la confidentialité des données, la disponibilité du réseau, le contrôle d'accès au support de communication et l'anonymat. Bien que multiples et diversifiées, les solutions de sécurité proposées dans la littérature restent toujours limitées face à la multitude de vulnérabilités exploitées par les attaques. Ces solutions se basent essentiellement sur des outils cryptographiques ou non cryptographiques comme une première ligne de défense et utilisent les systèmes de réputation et de détection d'intrusion comme une deuxième ligne de défense.

Dans notre travail, nous nous sommes intéressés aux attaques liées aux identités qui sont considérées comme une classe bien particulière d'attaques sévères. Cette classe englobe deux types d'attaques à savoir l'attaque de spoofing et l'attaque Sybil. Le spoofing consiste à usurper l'identité légitime d'un nœud donné et l'utiliser à des fins malicieuses, par exemple l'accès à des données confidentielles. Le Sybil, quant à lui, est l'attaque dans laquelle un nœud malicieux se présente dans le réseau en utilisant plusieurs identités.

L'objectif est le gain de plus de ressources réseau que les nœuds légitimes, ce qui conduit bien évidemment à la dégradation des performances du réseau.

Les solutions proposées dans la littérature pour remédier à cette classe d'attaque se basent principalement sur la cryptographie à clé publique et le test des ressources. Ces solutions sont généralement coûteuses en termes d'overhead de communication, de calcul et de stockage. Ceci nous a motivé de proposer un schéma de sécurité basé sur la connaissance de la distance séparant deux nœuds et la direction d'où les paquets sont reçus, pour détecter l'attaque sybil. Notre schéma de sécurité présente l'avantage d'être légère et scalable dans le sens ou aucun matériel n'est nécessaire et aucune coopération entre nœuds n'est exigée pour sa mise en œuvre. Pour prouver son efficacité et évaluer sa performance, nous avons effectué une série de simulation montrant à la fois les avantages et les inconvénients de notre solution.

Notre mémoire est structuré autour de quatre chapitres.Le premier chapitre introduit les réseaux ad hoc, en particulier leurs caractéristiques et les différentes classes de protocoles de routage utilisés. Le chapitre deux, quant a lui, présente un état de l'art sur la sécurité dans les réseaux ad hoc, en particulier, les différentes attaques possibles et les solutions proposées correspondantes. La classe des attaques liée aux identités ainsi que les solutions de sécurité proposées dans la littérature pour y remédier sont présentés dans le chapitre trois. Dans le chapitre quatre, nous décrivons les détails de notre schéma de sécurité contre l'attaque sybil et nous analysons les résultats de simulation. Le mémoire s'achève par une conclusion dans laquelle notre travail est récapitulé et les perspectives sont énumérées.

Chapitre 1

Généralités sur les réseaux ad hoc

1.1 Introduction

Les réseaux sans fil offrent aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. C'est un système de transmission des données conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui composent le réseau. Les réseaux sans fil sont principalement employés lorsqu'il s'agit d'interconnecter des utilisateurs nomades entre eux. Ce système ne pose aucune restriction sur la localisation des usagers. Il utilise des ondes radio plutôt qu'une infrastructure câblée pour communiquer. Ce nouveau mode de communication engendre de nouvelles caractéristiques propres à l'environnement mobile : de fréquentes déconnexions, un débit de communication et des ressources modestes, et des sources d'énergie limitées. Les réseaux mobiles peuvent être classés en deux grandes classes :

- Réseau sans fil avec infrastructure.
- Réseau sans fil sans infrastructure.

Cette deuxième classe de réseaux sans fil constitue la base de notre sujet d'étude, et c'est ce que nous allons développer dans ce présent chapitre. Ce chapitre est décomposé en cinq sections. Dans la section deux nous introduisons les réseaux ad hoc et dans la section trois nous présentons les différentes classes de protocole de routage. Les différentes normes proposées dans l'industrie sont énumérées dans la section quatre. Le chapitre se termine par une conclusion qui récapitule la technologie des réseaux ad hoc.

1.2 Réseau ad hoc

1.2.1 Définition d'un réseau ad hoc

Un réseau mobile ad hoc ou MANET (Mobile Ad hoc NETwork) tel qu'il est définit dans le RFC 2501 [19] est une collection de périphériques équipés d'une technologie de transmission sans fil sans recours à une infrastructure préexistante ou à une administration centralisée. La particularité de ce type de réseau est que chaque nœud peut communiquer avec n'importe quel autre nœud du réseau et qu'il peut jouer les rôles de client et de routeurs. Les nœuds sont libres de se déplacer aléatoirement et s'organisent arbitrairement. La figure 1.1 illustre un exemple d'un réseau ad hoc.

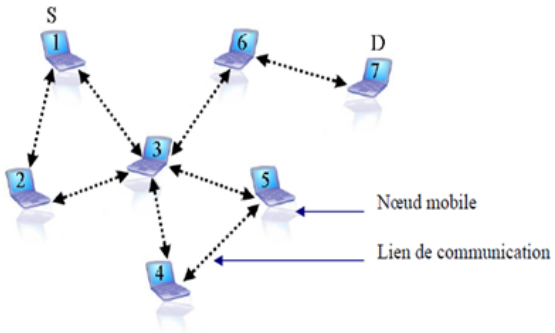

FIGURE 1.1 – Exemple d'un réseau ad hoc

Comme il est illustré dans la figure 1.2, la topologie du réseau peut changer à tout moment, elle est donc dynamique, aléatoire et imprévisible.

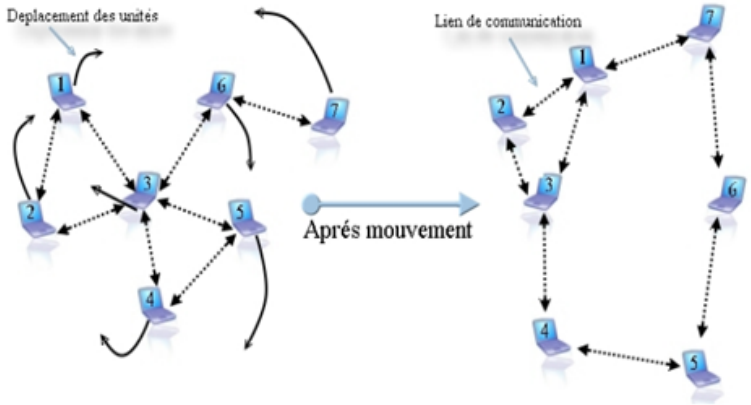

FIGURE 1.2 – Changement de topologie des réseaux ad hoc

1.2.2 Modélisation

Un réseau ad hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$, où : V_t représente l'ensemble des nœuds du réseau et E_t représente l'ensemble des connections qui existent entre ces nœuds. Si $e = (u, v) \in E_t$, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t.

La figure 1.3 représente un réseau ad hoc de 7 unités mobiles sous forme d'un graphe.

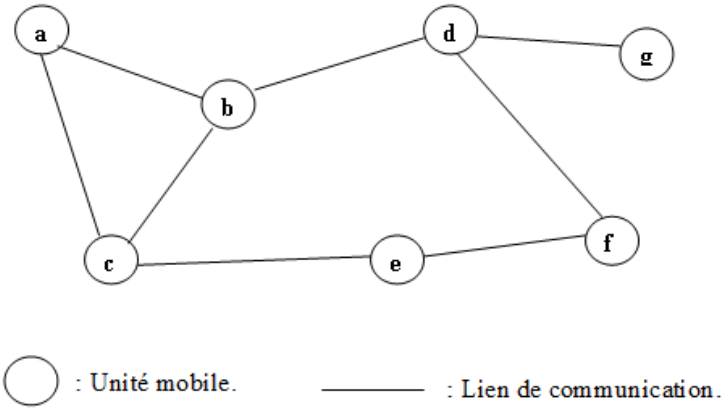

FIGURE 1.3 – Modélisation d'un réseau ad hoc

1.2.3 Caractéristiques des réseaux ad hoc

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

- **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.
- **Bande passante limitée :** Un 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.
- **Contraintes d'énergie :** Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources épuisables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.
- **Absence d'infrastructure :** Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.

- **Coût réduit :** Les réseaux ad hoc peuvent être facilement déployés dans des endroits ou le cablâge est difficile. Ce qui réduit considérablement le coût d'installation.
- **Hétérogénéité des nœuds :** Les nœuds ad hoc peuvent correspondre à une multitude d'équipements qui ne disposent pas forcément les mêmes propriétés physiques et logicielles, mais elles doivent inter-opérer pour établir un réseau commun.
- **Interférences :** Les liens radios ne sont pas isolés. Deux transmissions simultanées sur une même fréquence ou utilisant des fréquences proches peuvent s'interférer [27].

1.2.4 Domaines d'applications des réseaux mobiles ad hoc

Les applications ayant recours aux réseaux ad hoc couvrent un très large spectre. Parmi ces applications on trouve :

- **Applications militaires :** Si les premiers travaux dans le contexte des réseaux ad hoc ont été menés dans une optique militaire, c'est en partie dû à leur mode de fonctionnement particulièrement bien adapté aux environnements hostiles et mobiles. Ainsi, les communications entre soldats, véhicules et engins aérodynamiques deviennent autonomes et spontanées.
- **Opérations de secours :** Ils peuvent être utilisés pour la mise en communication d'unités de secours, lorsqu'une catastrophe naturelle (telle qu'un tremblement de terre, une inondation) a détruit les infrastructures de télécommunications et que l'établissement d'une liaison satellite pour chaque entité en communication représente un coût trop élevé.
- **Travail collaboratif :** Ils peuvent être utilisés pour la mise en place instantanée d'un réseau reliant plusieurs ordinateurs entre eux. Ils s'avèrent particulièrement utiles lors de l'organisation d'événements tels que des colloques, des réunions ou des conférences afin de proposer un réseau de partage de l'information.
- **Réseaux de capteurs :** De tels réseaux sont constitués d'équipements de taille réduite qui embarquent un système de communication sans fil. Ces équipements, disséminés dans un environnement potentiellement hostile ou inaccessible, sont chargés de mesurer certaines propriétés physiques (telles que la température, la pression, la lumière, les sons, etc.) et de les transmettre à une station de base [10].
- **Réseaux véhiculaires :** Les objectifs envisagés par un tel usage sont, entre autres, de permettre aux véhicules d'obtenir des informations locales sur les conditions de circulation, des informations touristiques, une téléphonie entre véhicules, et un accès à l'Internet [37].

1.2.5 Avantages et inconvénients des réseaux ad hoc

Les réseaux ad hoc présentent les avantages suivants :

- **Pas de câblage :** L'un des avantages des réseaux ad hoc est l'absence du câblage, ce qui facilite et rend rapide le déploiement de ce genre de réseau.
- **Mobilité :** Les nœuds dans un réseau ad hoc peuvent se déplacer d'une manière libre et arbitraire. Ceci représente un avantage car aucune restriction n'est exigée concernant la mobilité des usagers.
- **Extensibilité :** L'une des propriétés les plus importantes d'un réseau ad hoc est la possibilité de l'étendre et d'augmenter sa taille très facilement et sans nécessiter trop de moyens.
- **Coût :** Le déploiement d'un réseau ad hoc ne nécessite pas d'installer des stations de base. Les unités mobiles sont les seules entités physiques nécessaires pour déployer un tel réseau. Ce qui réduit considérablement le coût.

Les réseaux ad hoc présentent les inconvénients suivants :[44]

- **Topologie imprévisible :** L'activité permanente et les déplacements fréquents des nœuds d'un réseau ad hoc peut causer un changement la topologie d'une manière aléatoire et imprévisible.
- **Collision :** Les risques de collisions augmentent avec l'augmentation du nombre de nœuds qui partagent le même médium de communication.
- **Sécurité :** A cause de l'utilisation d'un support de communication ouvert et partagé, la mobilité et l'absence d'infrastructure, Un réseau ad hoc devient de plus en plus vulnérable, ce qui pose un sérieux problème de sécurité.

1.3 Routage dans les réseaux ad hoc

Dans cette section, nous allons mettre l'accent sur les différents protocole de routage utilisés dans les réseaux ad hoc.

1.3.1 Définition

Le routage est l'opération qui consiste à trouver un chemin entre deux nœuds distants. La découverte de ce chemin peut se faire selon un certain critère de performance (bande passante, délai,etc.).Bien évidemment, la conception et l'implémentation d'un protocole de routage doit prendre en considération les contraintes suivantes :

- La minimisation de la charge du réseau.
- Offrir un support pour pouvoir effectuer des communications multipoints fiables.
- Assurer un routage optimal.
- Offrir une bonne qualité concernant le temps de latence.

1.3.2 Protocoles de routage

Le but principal d'un protocole de routage est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités, ce qui assure l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes est plus complexe. Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être classés en trois catégories : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides(voir figure 1.4).

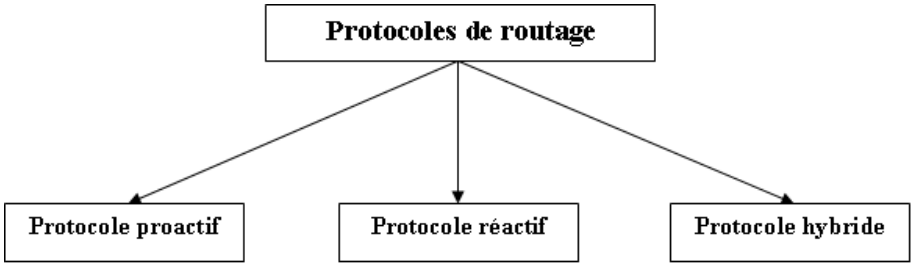

FIGURE 1.4 – Catégories des protocoles de routage

Protocoles proactifs

Le principe des protocoles proactifs est de maintenir à tout instant une vue globale et cohérente de la topologie du réseau, et de construire les meilleurs chemins existants entre les nœuds avant qu'ils ne soient requis, avec en particulier une table de routage indiquant par quel voisin passer pour atteindre un destinataire. Les routes sont sauvegardées même si elles ne sont pas utilisées. Afin de traiter les changements de topologie, la mise à jour de ces tables est assurée par la diffusion périodique des messages de contrôle à travers le réseau. Il existe plusieurs protocoles de routage, ceux-ci pouvant être distingués par le nombre de tables maintenues par chaque nœud, et par la façon dont les mises à jour sont diffusées lorsque des changements topologiques sont détectés. Les deux principales méthodes utilisées sont : la méthode état de lien ("Link State") et la méthode du vecteur de distance ("Distance Vector"). Parmi les protocoles proactifs les plus connus : DSDV, OLSR, FSR, TBRPF. L'avantage des protocoles proactifs est qu'ils offrent de bonnes performances en termes de temps de réponse, puisque lorsqu'un nœud souhaite communiquer, il dispose immédiatement des informations de routage nécessaires. En contrepartie, leur principal inconvénient est leur coût en termes d'utilisation de la bande passante. Ce coût, qui est dû à l'échange permanent de messages de contrôle nécessaires à la maintenance des tables de routage [5]. Dans ce qui suit nous allons présenté OLSR,

un exemple typique des protocoles de routage proactif.

OLSR (Optimized Link State Routing Protocol)[24] OLSR, proposé par Jacquet et al. est un protocole de routage proactif à état de liens inspiré du protocole de routage filaire OSPF (Open Shortest Path First). OLSR opère sur la base d'échanges périodiques de message de contrôle afin d'accomplir les opérations de découverte et de maintenance de la topologie du réseau. Il est fondé sur le concept de relais multi-point (MPR pour Multi Point Relay) qui représente un sous-ensemble de nœuds spécifiquement sélectionnés, il est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts (tous les voisins des voisins) pour assurer les opérations de génération et de retransmission des messages de contrôle pendant le processus d'inondation. Ce mécanisme d'inondation contribue à réduire la charge réseau en nombre de diffusions de messages de contrôle. Dans OLSR, deux types de messages de contrôle sont introduits :

- Les messages " HELLO " contiennent la liste de leurs voisins pour s'informer du proche voisinage et permettre ainsi à chacun de choisir son ensemble de relais multipoints.
- Les messages " TC " (Topology Control) déclarent les sous-ensembles de voisinage que constituent les relais multipoints. Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints. Ces informations offrent une carte de réseau contenant tous les nœuds et un ensemble partiel des liens, mais suffisant pour la construction de la table de routage.

Protocoles réactifs

Ce sont des protocoles dans lesquels la mise à jour ou le contrôle des routes se fait à la demande, une route n'est établie que lorsqu'elle est demandée par le nœud source. Lorsque qu'un nœud demande une route vers un destinataire, il initie un processus de découverte de chemin par inondation du réseau. Le processus prend fin lorsque la route est découverte ou lorsque toutes les permutations de route ont été exploitées sans succès. Une fois la route est établie, celle-ci est maintenue par une procédure de maintenance jusqu'à ce qu'elle ne soit plus utilisée ou que le destinataire ne soit plus joignable. Actuellement les protocoles réactifs les plus connus sont : AODV, DSR, TORA. L'avantage des protocoles réactifs est qu'ils permettent une nette amélioration quant à la surcharge du réseau et à la consommation d'énergie. Les routes ne sont créées et maintenues que lorsqu'elles sont nécessaires et le processus d'inondation est ponctuel. Leurs inconvénient est le délai engendré par l'établissement d'une route avant de pouvoir émettre les paquets de données. On notera également qu'il faudra une inondation du réseau pour s'apercevoir qu'un destinataire n'est pas joignable. Dans ce qui suit nous allons présenté AODV, protocole représentatif des protocoles réactif.

AODV (Ad hoc On Demand Distance Vector)[41] Le protocole AODV a été proposé par Perkin et Royer. Il s'agit d'un protocole à vecteur de distance qui se distingue par une approche réactive pour la découverte des chemins. Il utilise un numéro de séquence afin de maintenir la cohérence des informations de routage en évitant le problème des boucles infinie et des transmissions inutiles de messages sur le réseau. Le protocole est basé sur deux mécanismes : la découverte et la maintenance de route.

- **Découverte de route :**un nœud qui n'a pas de chemin valide dans sa table pour une destination voulue diffuse à ses voisins un paquet RREQ (Route REQuest) pour découvrir une route. Chaque nœud atteint par un RREQ cherche une route dans sa table de routage pour la destination, s'il ne possède pas de route active assez récente alors il diffuse le RREQ à son tour en incrémentant le nombre de sauts. Sinon, il met à jour sa table de routage selon le RREQ reçu et renvoie un paquet de réponse RREP (Route REPlay) vers la source en suivant le chemin inverse du message RREQ. Les nœuds recevant le RREP mettent à jour leur table et font suivre le paquet vers la source, qui commence à émettre ses données. La source changera de route si un RREP reçu par la suite lui apprend une meilleure.
- **Maintenances des routes :**AODV maintient les routes aussi longtemps que celles-ci sont actives, une route est considérée active tant que des paquets des données transitent périodiquement de la source a la destination selon ce chemin. Lorsque la source stoppe d'émettre des paquets des données, le lien expirera et sera effacé des tables de routage des nœuds intermédiaires. Si un lien se rompt lorsqu'une route est active, le lien est considéré défaillant. Les défaillances des liens sont, généralement, dues à la mobilité du réseau ad hoc. La détection des ruptures des liens peut être réalisée à l'aide de messages spécifiques "HELLO" diffusés périodiquement d'un nœud vers ses voisins immédiats ou par la transmission d'un paquet de données sur le lien suivant. Le nœud qui détecte une rupture de lien pour le nœud suivant d'une route active diffuse un message RERR (Route ERRor).

Protocoles hybrides

Les protocoles hybrides permettent de combiner les deux concepts : celui des protocoles proactifs et celui des protocoles réactifs. Généralement, le réseau est divisé en deux zones et le principe est d'utiliser une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum à deux sauts du nœud mobile. Une approche réactive est utilisée au-delà de cette zone prédéfinie afin de chercher des routes. Les protocoles hybrides les plus connus sont : ZRP, CBRP. L'avantage des protocoles hybrides est le fait qu'ils s'adaptent bien aux réseaux de grandes tailles. Cependant, cette approche a comme inconvénient de cumuler les points faibles des

protocoles réactifs et ceux des protocoles proactifs, tels que les messages de contrôle périodique et le coût d'établissement d'une nouvelle route. Dans ce qui suit, nous allons présenté un protocole représentatif de cette classe ZRP.[4]

ZRP (Zone Routing Protocol) Le protocole de routage ZRP utilise les deux approches proactif et réactif, il limite la procédure proactive uniquement aux nœuds voisins (les changements de la topologie doivent avoir un impact local) et, bien que de nature global, offre une recherche rapide et efficace dans le réseau.
ZRP définit deux types de protocoles : l'un fonctionnant localement et le deuxième fonctionnant entre zones. Ces deux protocoles sont :

- **IARP** [41] **(IntrAzone Routing Protocol) :** offrant les routes optimales vers les destinations qui se trouvent à l'intérieur de la zone à une distance déterminée, et tout changement est répercuté uniquement à l'intérieur de la zone.
- **IERP** [22] **(IntErzone Routing Protocol) :** quant à lui s'occupe de rechercher les routes à la demande pour des destinations en dehors d'une zone.

En plus de ces deux protocoles, ZRP utilise le protocole BRP (Bordercast routing protocol). Ce dernier utilise les données de la topologie fournies par le protocole IARP afin de construire sa liste des nœuds de périphérie et la façon de les atteindre. Il est utilisé pour guider la propagation des requêtes de recherche de route de l'IERP dans le réseau. Autrement, une demande d'établissement de route " RREQ " est initiée vers tous les nœuds périphériques, ces derniers vérifient, à leur tour, si la destination spécifiée par la source existe dans leurs zones. Dans le cas positif, la source recevra alors un paquet " RREP " contenant le chemin menant à la destination, sinon, les nœuds périphériques diffusent la requête de demande à leurs propres nœuds périphériques, qui à leurs tours, effectuent le même traitement. Les erreurs de route sont également prévues par l'IERP en utilisant un mécanisme de réponse réactif. Lors d'une propagation d'un paquet, si une erreur survient au niveau du prochain nœud (le nœud devient inaccessible), un message " RERR " est délivré à la source.

1.4 Normes des réseaux ad hoc

Dans cette section, nous allons présenté les différentes normes utilisées dans l'industrie.

1.4.1 Bluetooth (IEEE 802.15)

Les réseaux Bluetooth ont été développés par Ericsson pour permettre la réalisation de réseaux personnels (PAN : Personnal Area Network), dans le but de relier des appareils et périphériques entre eux sans liaison filaire. Ces réseaux doivent permettre des commu-

nications à courte portée, à des débits faibles ou moyens entre toute sorte d'équipements. Ils travaillent dans la bande ISM des 2.4 GHz à des puissances leur permettant d'atteindre des portées allant du mètre à la centaine de mètres environ. Les réseaux Bluetooth sont construits de manière centralisée. Un maître élu peut prendre en charge jusqu'à huit esclaves et forme ainsi un piconet. Dans un piconet, c'est le maître qui contrôle toutes les transmissions. Les esclaves ne peuvent émettre des paquets que s'ils y ont été invités par le maître. Ce dernier doit donc les interroger régulièrement pour savoir s'ils ont des données à envoyer (polling). Plusieurs piconets peuvent être reliés afin de former une structure plus grande appelée scatternet (de l'anglais scatter, dispersé). A cette fin, les mobiles peuvent quitter temporairement leur piconet pour aller s'attacher à un autre [3].

1.4.2 IEEE 802.11

C'est une norme établie par l'IEEE en 1997. Elle décrit les couches physique et MAC d'interfaces réseau radio et infrarouge. Les débits possibles varient entre 1 et 54 Mbit/s suivant les techniques et les éventuelles extensions de la norme employées. Les portées prévues varient entre quelques dizaines et quelques centaines de mètres en fonction de la vitesse choisie et de l'environnement. Cette norme cible deux contextes d'utilisation :

- Les réseaux avec infrastructure où des stations de base reliées entre elles par un réseau filaire assurent la couverture d'une certaine zone et prennent en charge les mobiles dans leur voisinage
- Le mode appelé ad hoc, qui consiste simplement à autoriser les communications entre deux mobiles à portée l'un de l'autre, sans intervention de stations ou d'autres mobiles extérieurs.

Des extensions ont été publiées depuis, qui viennent lui ajouter des améliorations et des modes de fonctionnement plus performants. Les principales extensions sont : 802.11b, 802.11a, 802.11g, 802.11e, 802.11h, 802.11i.

1.4.3 HiperLAN (High Performance Local Area Network)

Il s'agit d'un standard de l'European Technical Standard Institute (ETSI). Il est composé de 2 normes qui sont : HiperLAN1 et HiperLAN2

- **HiperLAN type 1 :** Il décrit le fonctionnement d'équipements travaillant dans la bande des 5.15-5.30 GHz et permettant d'atteindre des débits de 23.5 Mbit/s sur une distance d'environ 50 mètres. L'architecture est totalement décentralisée. Il n'y a pas de notion de point d'accès mais les nœuds HiperLAN 1 peuvent cependant avoir des rôles de passerelles [11].
- **HiperLAN type 2 :** Il est basé sur une centralisation poussée. Les points d'accès sont d'ailleurs indifféremment appelés Access Points (AP) ou Central Controler

(CC). Il a pour but de concurrencer les versions les plus performantes de 802.11 (802.11a et 802.11g) en offrant des débits aussi élevés et un certain nombre de fonctionnalités supplémentaires [11].

1.4.4 Zigbee

Elle est initiée par Motorola et ratifiée en août 2003 sous la norme IEEE 802.15.4. Il Permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie (fonctionnement de six à vingt-quatre mois avec une paire de piles AA). Particulièrement adaptée pour être directement intégré dans de petits appareils électroniques, capables d'opérer plusieurs mois sur batterie et de se relier ensemble en réseau (appareils électroménagers, hi-fi, jouets, ...), il est utilisé pour le repérage des menaces sur un champ de bataille, le relevé de compteurs, la climatisation "intelligente", la détection de risques d'incendie, ... Sa transmission se fait dans la bande des 2.4 GHz globalement mais également 915 MHz en Amérique et 868 MHz en Europe, avec un débits de 250 Kbits/s à 2.4 GHz (10 canaux), 40 Kbits/s à 915 MHz (6 canaux) et 20 Kbits/s à 868 MHz (1 canal), une Portée de 10 à 75 m selon la puissance utilisée, la géographie des lieux et les caractéristiques environnementales et une interconnexion théorique de 255 matériels par réseau [41].

1.4.5 HomeRF

Lancée en 1998 par le HomeRF (Home Radio Frequency) Working Group, formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft. Cette technologie met en avant ses petits prix et sa facilité de mise en œuvre, elle utilise la norme DECT [1] pour réaliser le transfert de la voix (protocole TDMA [2]) et la norme 802.11 pour le transfert de données (CSMA/CA) [3], elle permet de fournir de multiples canaux de voix de bonne qualité. Elle utilise des architectures en modes ad hoc et infrastructure, une transmission dans la bande des 2.4 GHz, un débit de 1,6 Mbits/s pour HomeRF1 ou 10 Mbits/s pour HomeRF2, avec une portée de 50 à 100 m, une modulation FHSS [4] et une sécurité de chiffrement à l'aide d'une clé de 128 bits [7].

1. est une norme de téléphonie sans-fil numérique destinée aux particuliers comme aux entreprises sur la gamme de fréquence 1 880 à 1 900 MHz (micro-ondes).

2. est une technologie basée sur le multiplexage temporel qui consiste à diviser le temps en petits intervalles. Les utilisateurs émettent alors sur des intervalles de temps différents.

3. utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réception réciproque entre l'émetteur et le récepteur, la station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné alors la station peut émettre.

4. est une méthode de transmission de signaux par ondes radio qui utilise plusieurs canaux (sous-porteuses) répartis dans une bande de fréquence selon une séquence pseudo-aléatoire connue de l'émetteur

1.5 Conclusion

Dans ce chapitre, nous avons présenté les réseaux ad hoc, les protocoles de routage ainsi que les normes utilisées dans ce genre de réseau. Un tel réseau est facile, rapide et moins coûteux à déployer. En contre partie, le médium de communication ouvert et partagé utilisé, la mobilité et l'absence d'infrastructure rendent ce réseau vulnérable par plusieurs types d'attaques. En conséquence, la sécurité d'un tel réseau est un sérieux problème qui reste ouvert à la recherche et ceci malgré la diversité des solutions de sécurité proposées dans la littérature. Dans le chapitre suivant, nous allons mettre l'accent sur la sécurité dans ce genre de réseau.

et du récepteur.

Chapitre 2

Sécurité des réseaux ad hoc

2.1 Introduction

La sécurité d'un réseau ad hoc diffère beaucoup de celle des réseaux filaires. En effet, la nature ouverte du lien sans fil utilisé, la mobilité et l'absence d'infrastructure compliquent davantage la conception d'un système fiable du point de vue de la sécurité. Les solutions proposées dans la littérature se basent sur des outils cryptographiques ou non cryptographiques pour sécuriser les communications sans fil. Bien que diversifié, ces solutions restent toujours limitées en termes d'efficacité et de performance. Dans ce chapitre, nous allons mettre l'accent sur la sécurité dans un tel réseau, en particulier, nous présentons les différentes attaques ainsi que les solutions de sécurité correspondantes. Ce chapitre est organisé en six sections. Dans la section deux nous présentons les services ainsi que les vulnérabilités des réseaux ad hoc. Les mécanismes de sécurité utilisés pour la mise en oeuvre de la sécurité sont présentés dans la section trois. La section quatre quant à lui décrit les différentes attaques possibles dans les réseaux ad hoc, suivie par la section cinq ou les solutions de sécurité existantes sont expliqués. Le chapitre se termine par une conclusion concluant la question.

2.2 Services de sécurité et vulnérabilités des réseaux ad hoc

En général, la sécurité informatique est l'ensemble des techniques qui assurent que les ressources (matérielles ou logicielles) d'un système donné sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

A cause des caractéristiques inhérentes des réseaux ad hoc, plusieurs vulnérabilités ont été recensé dans la littérature. Ces vulnérabilités sont :

- **Technologie sans fil :** Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés.
- **vulnérabilité des nœud :** les nœuds sont aussi des points de vulnérabilité du réseau car un attaquant peut compromettre un terminal laissé sans surveillance.
- **Absence d'infrastructure :** A cause de cette vulnérabilité, les solutions de sécurité conçues pour les réseaux filaires ne sont plus utilisables dans les réseaux sans fil.
- **Contrainte d'énergie :** la capacité énergétique modeste des nœuds limite l'utilisation des mécanismes cryptographiques gourmands en calcul et énergie en conséquence.

Sécuriser un réseau sans fil revient principalement à garantir les services suivants :

- **Authentification :**Est le service qui consiste à s'assurer de l'identité des participants dans un réseau. C'est une étape incontournable pour le contrôle de l'accès aux ressources réseau.
- **Confidentialité :**La confidentialité consiste à empêcher les entités non autorisés à consulter les données.
- **Intégrité :**Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission. Pour assurer l'intégrité on utilise souvent les fonctions de hachage.
- **Disponibilité :** La disponibilité permet de s'assurer que les services réseau sont toujours disponibles malgré la présence des attaques.
- **La non répudiation :** C'est un mécanisme destiné à empêcher un nœud de nier l'envoi ou la réception d'un message.
- **Contrôle d'accès :** consiste à empêcher les nœuds étrangers d'utiliser le médium de communication partagé.
- **Anonymat :** L'anonymat est le service qui consiste à cacher l'identité d'un nœud en utilisant un code. Une table est nécessaire pour maintenir la correspondance entre l'identité et le code.

2.3 Mécanismes de sécurité

Plusieurs mécanismes de sécurité ont été utilisés pour la mise en oeuvre de la sécurité. Dans ce qui suit nous allons expliquer les mécanismes les plus répondus.

- **Cryptographie :** La cryptographie joue un rôle essentiel dans toutes les communications sécurisées en chiffrant un message dit " texte clair " en un deuxième dit " texte crypté " à l'aide d'une clé en utilisant des moyens, matériels ou logiciels conçus à cet effet. Les informations originales sont restituées à partir de celles codées. Cette opération inverse est nommée décryptage[23]. Il existe deux types de cryptographie :

– **Cryptographie symétrique :** Dans la technique de la cryptographie symétrique, chaque entité possède une clé secrète de chiffrement/déchiffrement. Dans le cadre d'échange sur un réseau, une entité émettrice chiffre les données avec la clé et l'entité destinatrice déchiffre les données avec la même clé. La figure 2.1 montre le principe de ce type de cryptographie.

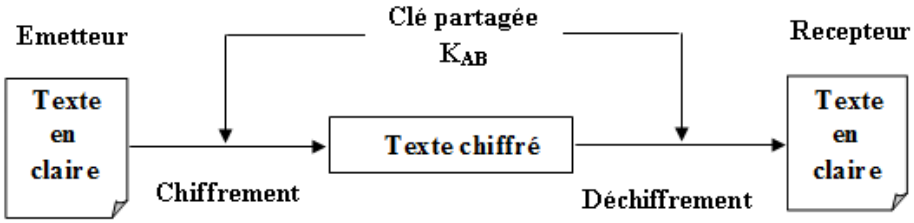

FIGURE 2.1 – Cryptographie symétrique.

– **Cryptographie asymétrique ou à clé publique :** Dans la cryptographie asymétrique, les clés de chiffrement et de déchiffrement sont différentes. Une des clés appelée clé secrète, est mémorisée et utilisée par une entité. L'autre clé appelée clé publique, est distribuée à toutes les autres entités. La clé publique est utilisée lors du chiffrement et la clé privée pour le déchiffrement. Il est mathématiquement impossible de déduire la clé privée de la clé publique. Cette technique garantie la confidentialité ou l'authentification des messages. La figure 2.2montre le principe de la cryptographie asymétrique.

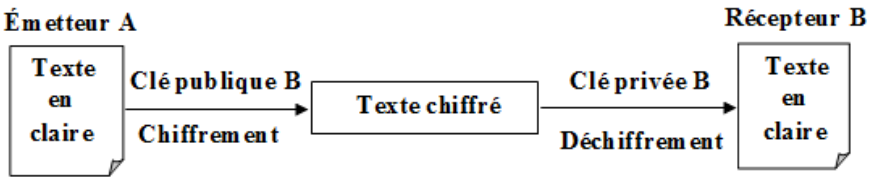

FIGURE 2.2 – Cryptographie asymétrique.

- **Fonctions de hachage :** Une fonction de hachage [16] est une fonction permettant d'obtenir un condensé, appelé aussi empreinte, de longueur fixe à partir d'un texte de longueur arbitraire finie. La fonction de hachage doit être telle qu'elle associe un et un seul condensé à un texte en clair. Cela signifie que la moindre modification du texte entraîne aussi la modification de son condensé. Il s'agit d'une fonction facilement calculable et à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé. En expédiant un message accompagné de son condensé, il est possible de garantir l'intégrité d'un message. La figure 2.3 montre le principe de l'utilisation d'une fonction de hachage.

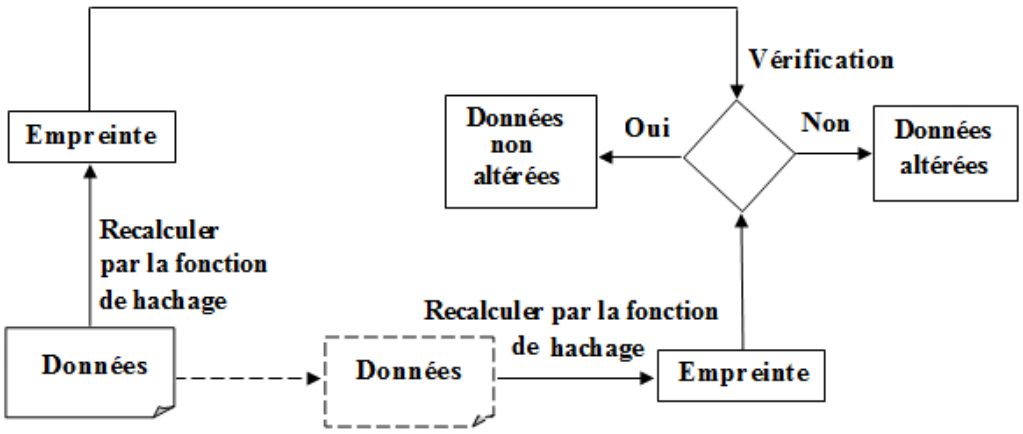

FIGURE 2.3 – Fonction de hachage.

- **Message Authentication Code (MAC) :** Comme une fonction de hachage, l'algorithme MAC produit un condensé de taille fixe. Mais à la différence de celle-ci, il utilise en plus une clé secrète. Le MAC peut être utilisé pour vérifier simultanément l'intégrité de données et l'authenticité de la source des données. L'émetteur calcule le MAC en utilisant la fonction de hachage qui prend en paramètre une clé symétrique k. Ensuite, le message et le MAC sont transmis au destinataire. Celui-ci calcule le MAC du message reçu en appliquant la même fonction de hachage avec la clé symétrique k et compare le résultat obtenu avec le MAC reçu. S'il y a égalité, le message n'a pas été altéré et il provient bien du nœud supposé. En pratique, une méthode de calcul du MAC plus élaborée et plus sûre est utilisée, il s'agit du HMAC (Keyed-Hash Message Authentification Code).
- **Signature numérique :** La signature numérique est définie comme des " données ajoutées à un message ", ou transformation cryptographique d'un message, permettant à un destinataire d'authentifier l'auteur d'un document électronique, garantir son intégrité et protéger contre la contrefaçon (seul l'expéditeur doit être capable de générer la signature), assuré alors la non-répudiation. La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage, et de la cryptographie asymétrique. La figure 2.4 montre le principe de l'utilisation d'une signature numérique.

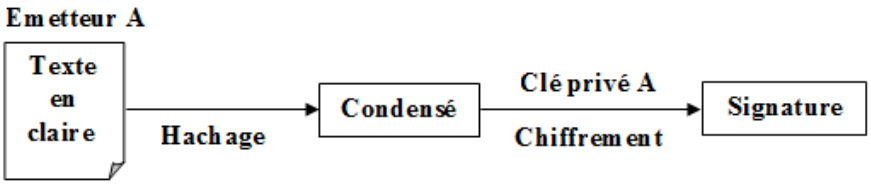

FIGURE 2.4 – Signature d'un message.

- **Certificats numériques :** Un certificat est un élément d'information qui prouve l'identité du propriétaire d'une clé publique. Les certificats sont signés et transmis de façon sécurisée par un tiers de confiance appelé autorité de certification (Certificate Authority, ou CA). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé.

2.4 Attaques de sécurité dans les réseaux ad hoc

Dans cette section, nous allons recenser les différentes attaques possibles menées contre les différentes fonctionnalités dans les réseaux ad hoc.

2.4.1 Classification des attaques

Plusieurs classifications ont été proposé dans la littérature. celle illustrée dans la figure 2.5 se base soit sur l'action malicieuse menée par l'attaque ou selon le type des nœuds.

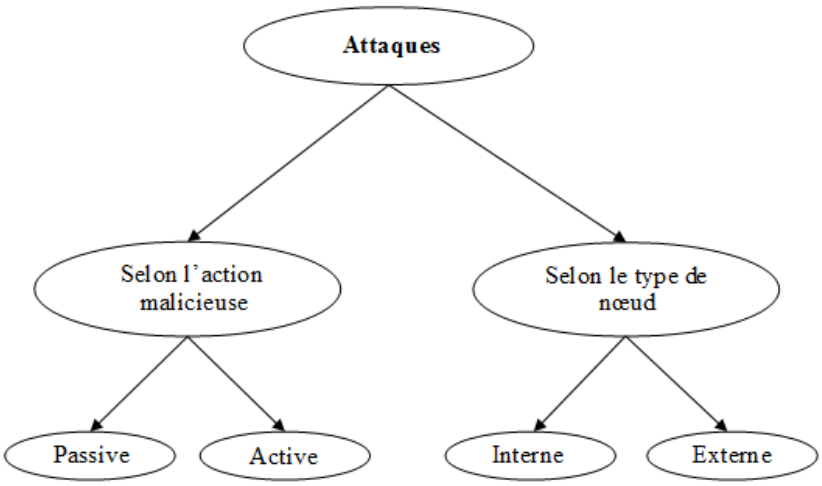

FIGURE 2.5 – Classification des attaques

- **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. 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. Les données analysées aident l'intrus à agir plus tard. Un adversaire passif ne fait que menacer la confidentialité des données.
- **Attaque Active :** Une attaque est active lorsqu'un nœud non autorisé altère des informations par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations dans le fonctionnement du réseau.
- **Attaque interne :** une attaque interne est menée par des nœuds compromis qui sont autorisés à participer au fonctionnement du réseau et disposent donc de l'ensemble de connaissances associées à ce statut tel que les clés secrètes. Étant donné que les attaquants font d'ores et déjà partie du réseau de nœuds autorisés, les attaques internes sont généralement plus difficiles à détecter que les attaques externes.
- **Attaque externe :** l'attaque externe est réalisée par des nœuds qui n'appartiennent pas au réseau, donc ne disposent d'aucune connaissance, ils sont incapables d'effectuer des opérations de cryptographie comme signer, déchiffrer, etc.

Dans ce qui suit, nous allons décrire un certain nombre d'attaques citées dans la littérature.

- **Attaques par personnification :** Dans ces attaques, l'intrus usurpe l'identité (adresse IP ou MAC) et les privilèges d'un autre nœud afin de mener son attaque dans le réseau. Dans cette classe d'attaque, nous citons :
  - **Man-in-the-Middle attack :** L'attaquant peut personnifier le récepteur et l'émetteur en se mettant entre les deux. cette façon, il peut mener son attaque sans qu'aucun des deux ne puisse se rendre compte qu'ils ont été attaqués.
  - **Spoofing attack :** Elle 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.
  - **Sybil attack :** Dans cette attaque, le nœud présente des identités multiples aux autres nœuds du réseau, créant ainsi des inconsistances dans les tables de routage des nœuds voisins. Ce qui permet de créer plusieurs routes passant par le nœud malicieux, qui ne sont en réalité qu'un seul chemin. [26]

- **Attaques par fabrication :** Le nœud malicieux fabrique des messages et il les insère dans le réseau afin de perturber les opérations du réseau ou pour consommer les ressources des nœuds. Dans cette classe on trouve :

  - **Routing Table Poisoning :** Le nœud malicieux envoie de fausses mises à jour de routage, il peut causer des congestions dans le réseau ou un partitionnement du réseau.
  - **Black hole attack :** Dans cette attaque le nœud malveillant essaye d'attirer vers lui le plus de chemins possibles permettant le contrôle de la plus part des données circulant dans le réseau. Pour ce faire, l'attaquant doit apparaître aux autres comme étant très attractif, en présentant des routes optimales. L'attaquant se place généralement à un endroit stratégique et supprime tous les messages qu'il doit retransmettre ou bien permet la mise en œuvre d'une autre attaque. Créant ainsi une sorte de puits ou " trou noir " dans le réseau.[31]
  - **Gray hole attack :** cette attaque est une variante de l'attaque black hole qui consiste à retransmettre sélectivement les paquets. Cette retransmission sélective des messages rend l'attaque plus difficile à détecter que l'attaque du black hole.

- **Attaques par modification :** ces attaques consistent à modifier le contenu des paquets. Les attaques représentatives de cette classe sont :
  - **Misrouting attack :** Le 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 ou par l'expédition du paquet de données au prochain saut faux dans la route à la destination.
  - **Blackmail attack :** L'attaque de blackmail cause une fausse identification en rendant malicieux des nœuds légitimes par l'insertion de ces derniers dans des listes noires utilisées pour garder la trace des nœuds malicieux. En conséquence, un nœud légitime sera vu par les autres nœuds du réseau comme étant un nœud malicieux et il sera évité dans une future communication.

- **Attaques par rejoue :** dans ces attaques un nœud malicieux réinjecte des messages dans le réseau. Des anciens messages continuent à circuler ce qui consomme plus de bande passante. Dans cette classe on trouve :
  - **Trou de ver (Wormhole) :** Dans une attaque wormhole, les paquets captés dans une zone sont acheminés via un tunnel pour être rejouer dans une autre zone. Une telle attaque conduit entre autre à la falsification du voisinage et à la dégradation des performances du réseau en conséquence.

- **Attaques par dénis de service :** Ces attaques qui visent essentiellement la disponibilité du réseau sont faciles à réaliser. Une attaque DoS traditionnelle consiste par exemple à surcharger volontairement les connexions réseau en envoyant une quantité excessive de données jusqu'à la saturation de la bande passante. Dans cette classe

d'attaques, nous trouvons :

– **Brouillage (jamming) :** Vu la sensibilité du médium 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[31].

2.5 Solutions de sécurité dans les réseaux ad hoc

Comme il est illustré dans la figure 2.6 , les solutions de sécurité peuvent être classées en deux classes : protocoles sécurisés pour sécuriser des protocoles existants non sécurisés, ou des protocoles de sécurité conçus au départ en visant la sécurité comme premier objectif.

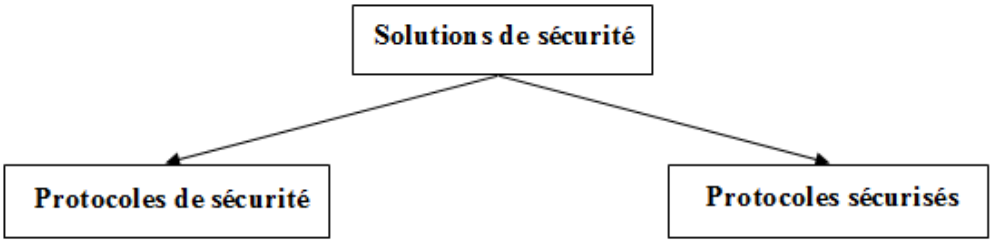

FIGURE 2.6 – Solutions de sécurité.

2.5.1 Protocoles de sécurité

Dans cette classe, on peut citer les protocoles suivant :

- **ARAN (Authenticated Routing protocol for Ad hoc Network) :**Sanzgiri et al. ont proposé le protocole sécurisé ARAN [5] qui prévoit l'utilisation de la cryptographie à clé publique pour sécuriser la construction des chemins des protocoles réactifs. ARAN utilise un serveur de certification. Avant de joindre le réseau chaque nœud demande un certificat de ce serveur. Le certificat contient l'adresse IP et la clef publique du nœud, un " timestamp" t indiquant la date de création du certificat et la date d'expiration du certificat. Toutes ces variables sont concaténées puis signées par la clef privée du serveur. Ensuite la source S diffuse un paquet de découverte de route RDP (Route Discovery Packet) contenant un identifiant du type de paquet, l'adresse IP de destination (IPD), le certificat de S, un nonce N_s et la date courante. Tous ces champs seront concaténés puis signés par la clef privée de S. A chaque fois que le nœud S effectue un RDP il incrémente la valeur de nonce. Cette valeur est associée avec l'adresse IP de la source pour

identifier un RDP. En recevant le paquet RDP, un nœud intermédiaire enregistre le nœud précédent à partir duquel il a reçu le paquet. Ensuite il fait suivre le paquet en signant son contenu. Quand le premier paquet RDP associé à un couple (N_s, IP_s) arrive au destinataire, ce dernier va répondre en envoyant en unicast un paquet REP (REPly) sur le chemin inverse. ARAN s'avère extrêmement coûteux en consommation de ressources à cause du grand nombre des opérations de signature et de vérifications de signature utilisées pour assurer la sécurité.

- **Ariadne :** Hu et Johnson ont proposés Ariadne [20], un protocole de routage réactif sécurisé basé sur le protocole DSR. Pour authentifier les messages de routage Ariadne peut utiliser l'un des mécanismes suivants : partage de clefs secrètes entre chaque paire de nœuds du réseau, signature numérique ou partage de clef secrète entre la source et la destination seulement avec authentification des nœuds intermédiaires par l'utilisation du protocole TESLA. Ce dernier permet de vérifier l'intégrité et authentifie la source en attachant au message un MAC dépendant d'une clef secrète K qui n'est divulguée par l'émetteur qu'après un délai d. La valeur de d est calculée de manière à être sûr que tous les récepteurs ont bien reçu le paquet avant la divulgation de la clef, ce qui assure l'intégrité et l'authenticité du paquet. Un paquet ne sera accepté par le récepteur que si sa clef n'est pas encore divulguée. La clef secrète utilisée pour générer le MAC est issue d'une chaîne de clefs. Au début l'émetteur choisit un nombre aléatoire K_n. Ensuite les autres éléments de la chaîne sont calculés récursivement de la manière suivante : $K_i = F(K_i + 1)$ où F est une fonction de hachage non réversible. L'émetteur va utiliser ces clefs dans l'ordre inverse de leur génération c'est à dire dans l'ordre $K_0, K_1, \ldots, K_n$. A la réception d'un nouveau paquet le destinataire vérifie la relation $K_{i-1} = F(K_i)$ où K_i est la clef dernièrement reçue et K_{i-1} la clef précédente. Cette condition permet de vérifier que la clef K_i fait bien partie de la chaîne de clefs de l'émetteur, ce qui assure la propriété d'authentification de la source. Le récepteur peut calculer toute clef intermédiaire K_i à partir de la dernière clef reçue K_n à partir de la relation $K_i = F(n-1)(K_n)$, ce qui lui permet de vérifier des paquets dont les clefs sont perdues. Il est à noter la nécessité d'authentifier la première clef (K_0) en utilisant le procédé de signature numérique.

- **SAR (Security Aware Routing) :** 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 clef. En recevant un message RREQ, le nœud va essayer de le déchiffrer. Dans le cas où le nœud ne possède pas la clef, il sera obligé de supprimer le paquet et par la suite de s'exclure de la route. Ce protocole garantit un niveau de sécurité minimal mais il peut augmenter la longueur de la route en excluant certains nœuds. De plus ce protocole n'est pas extensible en particulier si on a plusieurs niveaux de confiance. En effet, il faut associer à chaque niveau de confiance une clef. Un nœud doit tester à chaque réception d'un message RREQ toutes les clefs qu'il possède puisqu'il ne connaît pas le niveau de confiance du message. Si aucune de ces clefs ne parvient à déchiffrer le message le nœud va le supprimer. Et donc on aura une consommation inutile de ressources. Une solution pour palier cet inconvénient est d'attacher un texte en clair au message RREQ indiquant son niveau de confiance. Un nœud va donc vérifier dès le début s'il possède ou non la clef. Il faut aussi noter la nécessité d'avoir un mécanisme de gestion et distribution de clefs. A chaque fois que les membres du réseau changent, des nœuds peuvent quitter et d'autres peuvent joindre le réseau, les clefs doivent être renouvelées.

- **SLSP (Secure Link State Protocol) :** Papadimitratos et Haas proposent SLSP [40], un protocole à état de lien dont ils ont modifié les messages de contrôle afin d'en sécuriser le contenu. Ce protocole utilise les signatures numériques ainsi que les chaînes de hachage à sens unique pour garantir l'intégrité des mises à jour de l'état des liens. L'authentification du message se fait par vérification de la signature avec la clé publique de l'émetteur. Alors que les chaînes de hachage permettent juste de limiter le diamètre de diffusion des messages de mise à jour topologique.

- **Watchdog and Pathrater :** Le chien de garde (Watchdog) et l'évaluateur de chemins (Pathrater). Le Watchdog, utilisé localement par chaque nœud, a pour rôle de contrôler que le nœud suivant sur le chemin procède bien à l'opération de retransmission des paquets de données. Lorsqu'une action observée ne correspond pas à un résultat attendu, le nœud observateur comptabilise un échec de

retransmission. A partir du moment où le compteur pour un nœud dépasse un seuil fixé, l'information est reportée au Pathrater. Le Pathrater est ensuite utilisé pour sélectionner les chemins les plus fiables entre une source et une destination, en évitant les nœuds qui ont été détectés comme non coopératifs. La faiblesse de cette approche est qu'elle ne permet ni de sanctionner ni d'isoler les nœuds qualifiés de non coopératifs. Ces derniers, bien qu'exclus de la construction des chemins, sont toujours en mesure d'utiliser les ressources des autres nœuds dans le réseau pour leurs propres communications. Ces mécanismes sont également vulnérables, car ils peuvent être détournés par un attaquant. Un nœud malicieux peut facilement faire en sorte qu'un nœud valide soit ajouté à la liste noire, ce dernier sera en conséquence isolé du réseau [35].

- **TIK (Tesla with Instant Key disclosure) :** TIK est un protocole dérivé de TESLA qui est une solution pour l'attaque de type wormhole. Il utilise un paquet leash, c'est-à-dire une trame d'information qui restreint la distance de transmission maximale d'un message ou sa durée de vie. Tous les nœuds du réseau doivent avoir des horloges fortement synchronisées. L'authentification des clés est accomplie grâce à des arbres de hachage qui sont une optimisation des chaînes de hachage. Le nœud d'émetteur génère un MAC de la forme $H(M, K_i)$ à l'aide d'un paquet M et une clé K_i. La clé K_i a un temps de vie t_i et peut être authentifiée par la valeur hi dans l'arbre de hachage. Le MAC est inclus dans la fenêtre du message. Avant d'envoyer le paquet, le nœud estime une limite au temps d'arrivée du paquet et ajoute la clé K_i. Le nœud qui reçoit le paquet vérifie que la clé n'a pas été divulguée en se basant sur le temps t_i. Si la vérification a réussi, le nœud destinataire authentifie la clé K_i en utilisant h_i et peut vérifier l'intégrité du message en comparant le MAC reçu avec celui calculé.

- **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 est qu'il s'adapte à tous les protocoles de routage qu'il soit proactifs ou réactif.

2.5.2 Protocoles sécurisés

Cette classe inclut les protocoles qui ont été développés pour sécuriser les protocoles de routages déjà existants. Parmi ces protocoles :

- **SAODV (Secure Ad hoc On demand Distance Vector) :** Zapata et Asokan ont proposé une extension de sécurité pour le protocole AODV nommée Secure AODV [48]. Contrairement à l'extension ARAN pour laquelle les données des messages de contrôle sont retirées, l'idée principale de SAODV consiste à faire usage d'une signature numérique pour protéger les données statiques des messages de contrôle, puis de recourir à des chaînes de hachage pour protéger l'intégrité de la partie non statique qu'est le compteur de sauts. En particulier, étant donné une fonction de hachage H, lorsqu'un nœud initie une demande de recherche de chemin, il choisit aléatoirement un nombre seed et inclut, en plus du compteur de sauts $nbs = 0$, le nombre maximal de sauts que doit parcourir le message $max - nbs = TTL$, la valeur $H_{max-nbs}(seed)$ et la valeur $s = seed$. Avant de retransmettre un tel message, un nœud intermédiaire vérifie la signature numérique et si elle est valide, augmente la valeur du nombre de sauts nbs de un et remplace la valeur précédente de s par $H(s)$. Ensuite, pour vérifier l'authenticité du compteur de sauts courant $nbs = k$, un nœud vérifie que la valeur $H_{max-nbs}(seed)$ est égale à $H_{max-nbs-k}(s)$. Ce procédé assure qu'à la réception d'un message de contrôle, la valeur du compteur de sauts est exacte, dans le sens ou elle n'a pas été faussement décrémentée par un attaquant sur le chemin.

- **SRP (Secure Routing Protocol) :** Papadimitratos et Haas ont proposés SRP [40], une extension de sécurité pour les protocoles de routage réactif à la source, dont en particulier DSR. Cette extension se fonde sur l'ajout d'un en-tête de sécurité aux messages de recherche d'un chemin entre une source et une destination (laquelle contient un numéro de séquence de façon à garantir leur fraîcheur), et sur l'existence d'un RREQ et de RREP à un chemin au moyen d'un code d'authentification de message (MAC). Ainsi, la destination est capable de détecter toute modification sur les données statiques d'un message de demande de chemin. Du point de vue de la source, le MAC lui permet de vérifier l'intégrité du chemin découvert inclus dans le message sur lequel il porte, et d'en authentifier son origine. L'authentification mutuelle de bout en bout fait de SRP une approche relativement légère, puisqu'il requiert au total seulement quatre opérations cryptographiques pour sécuriser la phase de découverte de chemin, et ce, indépendamment de la longueur du chemin entre les nœuds communicants. En revanche, il présente certains défauts qui limitent son utilisation. Premièrement, SRP ne sécurise pas la phase de maintenance des

chemins et délègue cette tache à un autre protocole complémentaire. Ensuite, SRP ne permet pas de contrer les attaques par modification portant sur les informations de routage habituellement soumises à modification lors du routage.

- **SOSLR :** Le protocole OSLR a aussi été l'objet de recherches visant à le sécuriser. Parmi celles-ci on peut noter les travaux qui ont proposés approche d'authentification de saut en saut dans laquelle chaque nœud signe les paquets OLSR au fur et à mesure de leur retransmission. Ainsi, à la réception d'un paquet OLSR (un tel paquet pouvant contenir plusieurs messages OLSR de type HELLO et TC), un nœud intermédiaire vérifie la signature du nœud précédent, la retire, puis appose sa propre signature. Cette approche permet d'inclure dans le calcul de la signature numérique les champs devant être modifiés en transit, tels que le TTL (Time To Live) et le nombre de sauts. De manière similaire à Secure OLSR, une approche de sécurité pour le protocole OLSR basée sur l'utilisation de signatures numériques. Une première différence se situe au niveau du type des données protégées. Dans cette approche, une signature numériques est associée à chaque message de contrôle OLSR (i.e. HELLO ou TC) et non plus à chaque paquet OLSR. Ensuite, une approche d'authentification de bout en bout selon laquelle un nœud récepteur d'un message de contrôle authentifie le nœud d'origine plutôt qu'un nœud intermédiaire dans son cheminement. Ici, les champs TTL et nombre de sauts ne sont pas protégés par la signature, car ces derniers doivent être modifiés en transit par chaque nœud intermédiaire. En remplacement au TTL et pour déterminer si un paquet est trop ancien et s'il doit être rejeté.

- **AdvSig :** Dans le but d'empêcher l'injection d'informations d'état de liens non valides par des nœuds attaquants internes,Raffo et al. Ont proposés un schéma de signatures nommée Advanced Signature [1]. Le schéma proposée s'appuie sur le fait que la topologie du réseau évolue selon une séquence chronologique précise et en particulier, que l'état de lien entre deux nœuds au temps $(t+1)$ dépend directement de l'état de ce même lien au temps (t). L'idée est que pour tout message reçu d'un voisin, un nœud stocke les informations relatives à ses liens, puis les réutilise en tant que preuve de validité de son ensemble d'état de liens dans les messages qu'il émet ultérieurement. Pour éviter toute fabrication de faux messages, ces informations sont signées et encapsulées dans un message spécifique nommé AdvSig.

- **SEAD (Secure Efficient Ad hoc Distance vector routing protocol) :** SEAD [21] est un protocole proactif de routage ad hoc sécurisé, basé sur DSDV et permet d'authentifier l'émetteur d'une information de routage. En utilisant les chaînes de

hachage à sens unique, SEAD permet d'empêcher l'altération des champs mutables, à savoir le champ métrique, nombre de saut et le champ numéro de séquence. En appliquant d'une manière répétitive une fonction de hachage à sens unique, on obtient une chaîne. Les éléments de cette chaîne seront utilisés par les nœuds dans la procédure d'authentification et cela sans utiliser le cryptage à clé publique. Ainsi, il évite les opérations coûteuses dues aux signatures.

- **CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad hoc NeTworks) :** L'objectif de CONFIDANT est d'exclure les nœuds qui ne jouent pas leur rôle dans les opérations de routage, que ce soit au niveau du processus d'acheminement des données ou au niveau du processus de découverte des voisins. Il a été conçu comme étant une extension de sécurité des protocoles de routage réactifs à la source tels que DSR. Le système, maintenu par chaque nœud du réseau, définit quatre composants :
  - **Un moniteur :** Le rôle du moniteur consiste à vérifier, sur la base d'observations directes, le comportement des nœuds à l'égard des opérations de routage. Dès lors que le moniteur détecte un événement suspicieux ou une incohérence, il en informe le système de réputation.
  - **Un système de réputation :** a pour rôle de maintenir à jour les valeurs de réputation pour chaque nœud observée. Dans le but de limiter les effets négatifs dus aux imprécisions du mécanisme de détection d'une part, et pour accélérer le mécanisme d'apprentissage des informations servant à évaluer les nœuds d'autre part, les valeurs de réputation sont éventuellement échangées entre les nœuds. Ainsi, en plus de ses observations directes, un nœud intègre les valeurs de réputation des voisins dans le calcul de réputation des autres nœuds. Dans CONFIDANT, seules les valeurs de réputation négatives sont diffusées à travers des messages d'alarme.
  - **Un gestionnaire de confiance :** il a pour rôle de prendre la décision d'envoyer ce type de messages, puis de déterminer dans quelle mesure les informations reçues doivent être prises en considération pour le calcul de la valeur de réputation d'un nœud.
  - **Un gestionnaire de chemins :** évalue les chemins à partir de la topologie du réseau et des informations des autres composants. Il calcule les chemins les plus sûrs en utilisant comme métrique les valeurs de réputation des nœuds, et peut décider de rejeter les demandes de retransmission de paquets pour les nœuds affichant une faible réputation.

- **BISS (Building Secure routing out of an incomplete Set of security Associations) :** Le protocole BISS est un ensemble d'optimisation aux protocoles de routages existants, qui ont été conçus avec l'exigence que les nœuds participants ont établi un ensemble inachevé d'associations de sécurité entre eux-mêmes. L'authentification des nœuds intermédiaires le long d'un chemin de découverte de route n'est pas effectuée seulement la base des associations préétablies, mais également en échangeant les certificats à clés publiques avec ces nœuds. BISS suppose que le nœud cible d'un procédé de découverte de route à une association existante de sécurité avec les nœuds intermédiaires et qu'une autorité de confiance offline a certifié les clés publiques de tous les nœuds participants. Bien que les idées générales présentées par BISS puissent être appliquées aux protocoles réactifs. Les nœuds intermédiaires qui reçoivent des paquets de demande de route vérifiant la signature de l'initiateur et authentifient la destination par une association préétablie de sécurité. Le message est annoncé plus loin si l'initiateur et la destination sont authentifiés correctement et le nœud intermédiaire reçoit le paquet de demande de route pour la première fois. Quand la demande atteint le nœud cible l'authenticité des routes incluses sont vérifiées en utilisant les associations de sécurité et une route est choisie. L'approche suivie de BISS a pour effet d'augmenter le nombre d'associations de sécurité dans un réseau ad hoc. Les clés et les certificats des nœuds précédemment inconnus sont distribués dans le réseau pendant la découverte de route en permettant à des nœuds d'établir des secrets symétriques partagés.
  Le tableau 2.1 recapitule les différentes solutions citées auparavant.

Protocole	**Routage**	**Mécanisme cryptographique**	**Caractéristiques**
ARAN	Réactif	Signature à clé publique	Assure l'authentification ,l'intégrité et la non-répudiation
SODV	Réactif	Signature à clé publique,chaîne de hachage	Assure l'authentification d'un message
SRP	Réactif	MAC	Les MACs contre l'attaque IP spoofing

ARIADNE	Réactif	Signature à clé publique ou MAC ou MAC couplé avec TESLA	Assure l'authentification et l'intégrité.
SOSLR (paquet)	Proactif	MAC	Contre l'attaque de rejoue
SOSLR (message)	Proactif	Signature à clé publique ou MAC	Contre l'attaque de rejoue
Advig	Proactif	Signature à clé publique	Contre l'attaque de rejoue
SAR	Proactif	Niveau de confiance	Contre l'attaque du trou noir
SEAD	Proactif	Chaîne de hachage	Détecte les attaques qui modifient le numéro de séquence
SLSP	Proactif	Signature à clé publique et chaîne de hachage	Assure l'intégrité et l'authentification.
CONFIDANT	Réactif	Un moniteur, Un système de réputation, Un gestionnaire de confiance, Un gestionnaire de chemins.	Contre les attaques qui perturbent le procédé de découverte de route
TIK	Réactif	Paket leash, utilisant des MAC	Contre l'attaque wormhole
MAE	Proactif et réactif	Certification et cryptographie à seuil	Assure l'authentification et l'adaptation à tous les protocoles de routage
BISS	Réactif	Signature à clé publique	Assure l'authentification

TABLE 2.1 – Tableau récapitulatif des solutions de sécurité

2.6 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur la sécurité dans les réseaux ad hoc. Nous avons présenté en premier lieu les différentes vulnérabilités et les services de sécurité. Ensuite les différentes attaques possibles ainsi que les solutions proposées dans la littérature ont été recensés. L'objectif tracé dans notre travail est l'étude des attaques liées aux identités. Dans le chapitre suivant, nous allons mettre l'accent sur cette classe d'attaques ainsi que sur les solutions de sécurité proposées pour y remédier.

Chapitre 3

État de l'art sur les attaques liées aux identités

3.1 Introduction

En raison de la nature ouverte du support de communication sans fil utilisé dans les réseaux ad hoc, ces derniers sont vulnérables par plusieurs types d'attaques. Les attaques liées aux identités constituent une classe particulière d'attaques qui exploitent l'identité d'un nœud pour mener une action malicieuse. Deux types d'attaques d'identité sont distinguables : Le spoofing (ou l'usurpation) d'identité et le Sybil. Le spoofing consiste à voler l'identité d'un nœud et l'utiliser pour mener l'action malicieuse, tandis que le Sybil est l'utilisation de plusieurs identités différentes dans le réseau. L'impact de ces attaques sur le réseau est certainement négatif car leur objectif est la dégradation de la performance du réseau.

Dans ce chapitre, nous allons présenter la spécification des attaques liées aux identités, ensuite, nous allons résumer les différentes approches de sécurité proposées dans la littérature pour remédier à ces attaques.

3.2 Spécification des attaques liées aux identités

Dans ce qui suit, nous allons présenter la spécification des attaques du spoofing et du Sybil, et expliquer comment ces attaques sont menées.

3.2.1 Spécification de l'attaque spoofing

Les attaquants peuvent recueillir des informations d'identité utiles des appareils sans fil et les utiliser pour lancer des attaques de type spoofing identitaires dans les réseaux sans

fil. Par exemple, dans un réseau 802.11, il est facile pour un appareil sans fil d'acquérir une adresse MAC valide et passer pour un autre appareil. La suite de protocole 802.11 fournit une vérification d'identité insuffisante pendant l'échange de messages, y compris la plupart des cadres de contrôle et de gestion. Par conséquent, l'adversaire peut utiliser cette faiblesse et recevoir divers services comme s'il s'agissait d'un autre utilisateur. Une attaque par usurpation basée sur l'identité peut devenir une menace sérieuse dans le réseau car elle représente une forme de compromis d'identité et peut faciliter une série d'attaques d'injection de trafic, y compris par déni de service (DoS) d'attaques spoofing. Par exemple, un adversaire peut lancer une attaque d'authentification ; après qu'un client aie choisit un point dans la communication, il doit s'authentifier auprès du point d'accès avant que la session de communication commence. Le client et le point d'accès sont autorisés à demander explicitement d'annuler la relation d'authentification existant avec l'autre. Malheureusement, ce message dés-authentification n'est pas authentifié. Par conséquent, un attaquant peut usurper de ce message d'authentification soit pour le compte du client ou au nom du point d'accès [2]. L'adversaire peut répéter continuellement cette attaque et empêcher complètement le client de transmettre ou de recevoir. En outre, un attaquant peut utiliser l'usurpation d'identité et lancer une attaque de point d'accès voyous (AP) contre le réseau sans fil. Dans l'attaque du AP voyous, l'adversaire définit d'abord un point d'accès non autorisé avec la même adresse MAC et SSID le point d'accès légitime, mais avec un signal plus fort. Quand une station entre dans la couverture de l'AP voyous, la configuration par défaut du réseau associera automatiquement avec le point d'accès non autorisé qui a un signal plus fort ; puis l'adversaire peut prendre des mesures pour influer sur la communication. Par exemple, il peut diriger de faux trafic à la station associée ou déposer les demandes formulées par la station. Outre les attaques de base par inondation de paquet, l'adversaire peut faire usage de l'usurpation d'identité pour effectuer des attaques d'inondation plus sophistiqués sur des points d'accès, tels que la demande de la sonde, la demande d'authentification et les attaques demande d'association d'inondation [13].

Types d'attaques spoofing

Une attaque Spoofing peut nuire au fonctionnement du réseau. On cite les différents types d'attaque spoofing :

- **IP spoofing :** IP spoofing est l'acte de manipuler les en-têtes dans un message transmis afin que le message apparaisse comme s'il est d'une source fiable. Le pirate manipule le paquet en utilisant des outils pour modifier le champ "adresse source". L'adresse source est l'adresse IP de l'expéditeur du message donc une fois un intrus forge cette adresse et le serveur de destination ouvre une connexion, à ce moment de nombreuses attaques peuvent avoir lieu.

- **ARP spoofing :** ARP (Address Resolution Protocol) est un protocole qui est utilisé pour résoudre les adresses IP aux adresses MAC pour transmettre des données. Dans une attaque par usurpation ARP, un tiers malveillant envoie des messages ARP usurpés à travers un réseau local afin de relier l'adresse MAC de l'attaquent avec l'adresse IP d'un membre légitime du réseau. Le résultat de ce type d'attaque est que les données qui sont destinées à l'adresse IP de l'hôte seront envoyées à l'attaquant à la place. Les personnes malveillantes utilisent couramment ARP spoofing pour voler les informations, modifier des données en transit ou arrêter la circulation sur un réseau local. Les attaques ARP spoofing peuvent également être utilisées pour faciliter d'autres types d'attaques, y compris le déni de service, le détournement de session et les attaques man-in-the-middle.
- **Web Spoofing :** Comme pour les autres formes d'usurpation, l'usurpation Web ou de lien hypertexte fournit aux victimes de faux renseignements. Web Spoofing est une attaque qui permet à quelqu'un de voir et modifier toutes les pages Web envoyées à la machine de la victime. Elle est capable d'observer toute information qui est entrée par la victime ; il peut s'agir notamment de danger dû à la nature des informations saisies dans les formulaires,comme les adresses, numéros de cartes de crédit, numéros de comptes bancaires et les mots de passe qui accèdent à ces comptes.
- **DNS spoofing :** DNS (Domain Name System) est un système qui associe les noms de domaine avec des adresses IP. Les appareils qui se connectent à internet ou d'autres réseaux privés s'appuient sur le DNS pour la résolution des URL, les adresses électroniques et d'autres noms de domaine lisibles dans leurs adresses IP correspondantes. Dans une attaque par usurpation de serveur DNS, un tiers malveillant modifie le serveur DNS afin de rediriger un nom de domaine à une adresse IP différente. Dans de nombreux cas, la nouvelle adresse IP sera pour un serveur qui est effectivement contrôlée par l'attaquant et contient des fichiers infectés par des logiciels malveillants. les attaques DNS spoofing sont souvent utilisées pour propager des vers informatiques et les virus.

3.2.2 Spécification de l'attaque Sybil

Le terme Sybil attack a été introduit pour la première fois dans [8] pour désigner une attaque où l'attaquant, un nœud Sybil, tente de forger des identités multiples. Les attaques Sybil sont particulièrement faciles à lancer dans les réseaux sans fil où le moyen de communication est ouvert. En outre, en utilisant un nœud unique pour présenter des identités multiples dans le réseau, l'attaque Sybil peut réduire de manière significative l'efficacité des systèmes à tolérance de pannes telles que des mécanismes de redondance,

le stockage distribué, multi routage, et le maintien de la topologie. Une attaque Sybil est également utilisé par des sociétés pour augmenter l'indice des pages de leurs clients, et a été utilisé pour relier certains termes de recherche à des résultats inattendus pour des raisons politiques. Les spammeurs peuvent utiliser cette attaque pour accéder à plusieurs comptes sur libre systèmes de messagerie. L'attaque Sybil peut vaincre les mécanismes de redondance, des partitions de stockage et des algorithmes de routage.

Types d'attaques Sybil

Les attaques Sybil peuvent être classées en trois catégories selon le type de communication, d'identité et leur participation dans le réseau. Ces catégories sont brièvement discutées dans les paragraphes suivants :

- **Communication :** Quand un nœud honnête envoie un message à un nœud Sybil, le nœud malveillant écoute le message. De la même manière, les messages envoyés à partir des nœuds Sybil sont en fait envoyés par l'un des nœuds malveillants.
- **Identité :** Lors d'une attaque Sybil, un attaquant crée une nouvelle identité Sybil. Un attaquant peut fabriquer cette identité ou il peut usurper l'identité légitime d'un de ses voisins.
- **Participation :** De multiples identités Sybil créées par des nœuds malveillants peuvent participer simultanément à l'attaque ou l'attaquant peut utiliser ces identités une par une. Une identité particulière peut quitter ou rejoindre le réseau à plusieurs reprises.

  Une attaque Sybil peut nuire au fonctionnement de tout le réseau. On peut citer différents cas :

  - **Routage** Les attaques Sybil peuvent perturber les protocoles de routage dans les réseaux ad hoc, en particulier le mécanisme de routage multicast. Les chemins séparés qui semblent initialement disjoints peuvent passer à travers les nœuds de Sybil d'un seul attaquant. Un autre concept de vulnérabilité du routage c'est le cas où les nœuds malveillants peuvent apparaître à plus d'un endroit à un moment [26].
  - **Falsifications de vote et la réputation Système** En cas de n'importe quel environnement où il existe un système de vote en place à des fins telles que le signalement et l'identification des nœud dans le système, la mise à jour des scores de réputation et ainsi de suite, une attaque Sybil peut être particulièrement dangereuse. A titre d'exemple, un attaquant peut créer suffisamment d'identités malveillantes à signaler à plusieurs reprises, puis supprimer des nœuds légitimes du réseau. Alternativement, ces nœuds malveillants peuvent se protéger et ne jamais être supprimés car ils sont en collision.

- **Salon des ressources** Les attaques Sybil peuvent également être utilisées pour permettre à l'attaquant d'obtenir une part injuste et disproportionnée des ressources qui ont été destinés à être répartis entre tous les nœuds sur le réseau de manière égale. Cette attaque nie les nœuds légitimes de leur part méritée des ressources et les fournit également aux nœuds malveillants avec plus de possibilités pour d'autres attaques.
- **Mémorisation distribuée** Systèmes de stockage de fichiers en Peer-to-Peer et les réseaux de capteurs sans fil peuvent être compromis par l'attaque Sybil. Ce résultat est obtenu en battant les processus de fragmentation et de réplication dans le système de fichiers. Un système peut être amené à stocker des données dans les identités multiples de Sybil au même temps sur le réseau.
- **Agrégation de données** Les lectures des réseaux de capteurs sont calculées par des protocoles de requête [33] dans un réseau plutôt que de retourner la lecture de chaque capteur individuel. Ceci est fait pour économiser l'énergie. Une identité Sybil peut être en mesure de rapporter les lectures du capteur incorrectes influençant ainsi le total calculé globale. Un utilisateur malveillant peut être en mesure de modifier sensiblement l'ensemble avec suffisamment d'identités.

3.3 Approches de sécurité contre les attaques liées aux identités

Dans cette section, nous allons présenter les différentes approches de sécurité proposées dans la littérature pour se protéger contre les attaques de spoofing et de Sybil. La figure 3.1 schématise ces approches.

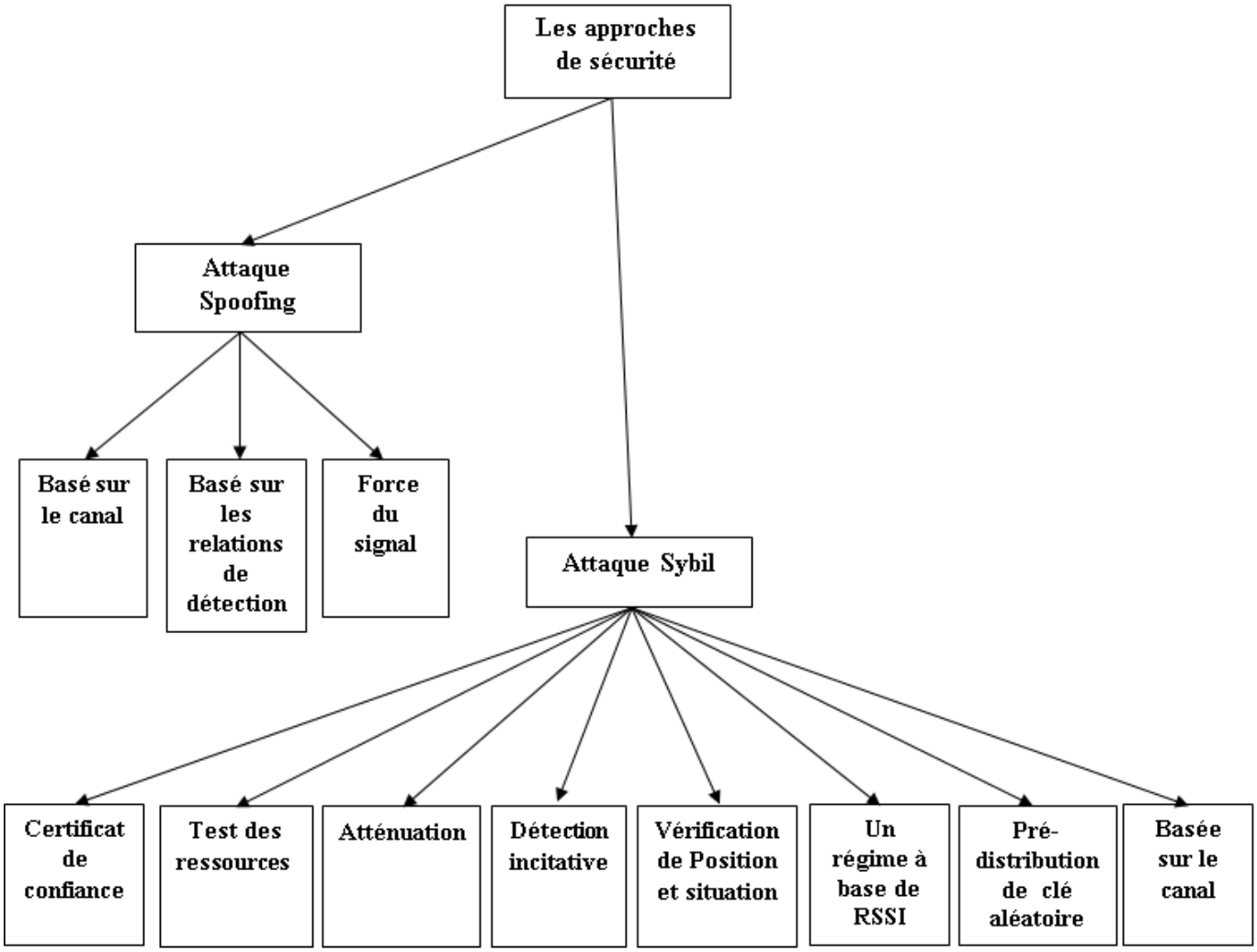

FIGURE 3.1 – Approches de sécurité contre les attaques liées aux identités.

3.3.1 Approches de sécurité contre le spoofing

Plusieurs solutions de sécurité ont été proposées pour se protéger contre l'attaque de spoofing d'identité, dans ce qui suit, nous allons résumer les approches les plus répondues.

Approches basées sur le canal

Basé sur le fait que la réponse du canal sans fil decorréle assez rapidement dans l'espace, un système d'authentification basé sur les canaux a été proposé pour distinguer entre les émetteurs à différents endroits, et donc de détecter les attaques de type spoofing dans les réseaux sans fil [47]. Un attaquant qui est à un endroit différent du véritable utilisateur encourra différents profils de réponse du canal autre que celui de véritables utilisateurs.

Techniques d'authentification basées sur un canal exploitent directement les propriétés uniques du domaine sans fil pour faire face aux menaces de sécurité. Les propriétés phy-

siques du support sans fil sont une puissante source d'information spécifique à un domaine qui peut être utilisé pour améliorer les mécanismes de sécurité traditionnels. Par conséquent, la nature du support sans fil peut être tournée à l'avantage du réseau pour sécuriser les communications sans fil ; en particulier dans les riches trajets multiples environnements sans fil, la réponse du milieu le long d'une voie d'émission-réception est sélectif en fréquence (ou dans le domaine temporel, dispersion) d'une manière qui est spécifique à la localisation. Cela signifie que : (1) Le canal peut être défini par un certain nombre d'échantillons complexes, soit dans le domaine fréquentiel (un ensemble de gains complexes à un ensemble de fréquences) ou le domaine temporel (une série d'échantillons de réponse impulsionnelle à une série de temps retards). (2) Ces ensembles de nombres décorrélent à partir d'une voie d'émission-réception à une autre si les trajets sont séparés par l'ordre d'une longueur d'onde de RF ou plus.

- **Solution 1 :** Considérons trois partis différents : A, B et E situés dans des positions séparées dans l'espace. A est considéré comme l'émetteur qui initie la communication, alors que B sera le destinataire prévu. L'adversaire E servira comme un nœud indésirable qui s'injecte a la communication dans l'espoir d'usurper l'identité de A. L'objectif de sécurité est de fournir une authentification entre A et B, malgré la présence du nœud spoofing E. Par conséquent, il est souhaitable pour B d'avoir la capacité de différencier entre les signaux légitimes de A et signaux illégitimes de E. Dans un environnement de trajets multiples, la propriété de la décorrélation spatiale rapide peut être utilisée pour authentifier un émetteur. Supposons qu'A sonde le canal à une fréquence suffisante pour assurer la cohérence temporelle entre les estimations du canal et que, avant l'arrivée de E, B a estimé le canal A-B. Maintenant, l'adversaire E transmet un signal à B et souhaite le convaincre qu'il est A. B utilise la version reçue du signal d'authentification pour estimer la réponse du canal et de comparer avec un précédent record pour le canal A-B. Si les signaux des deux canaux sont des estimations proches les uns des autres alors B conclura que la source du message est la même que la source du message précédent. Si les estimations de canal ne sont pas similaires, B devrait conclure que la source n'est probablement pas A par conséquent, le signal transmis à partir du nœud usurper E est détectée.

Approches basées sur les relations de détection

Cette approche implique l'utilisation de relation de forge résistant à la commande d'accès au support (MAC) pour détecter l'usurpation potentiel. La stratégie utilise des relations associées à un flux de paquets provenant d'une identité de réseau individuel. Chaque fois que l'adversaire tente d'usurper une identité particulière, l'existence de multiples sources provoque ces relations pour être difficile pour un adversaire, ce qui augmente

considérablement les chances que l'adversaire se révèle. Plus précisément, la monotonie du champ de numéro de séquence et la distribution des temps inter entre les paquets sont proposées pour détecter les attaques spoofing.

- **Solution 1 :** Guo et Chiueh [18] proposent pour détecter les attaques de type spoofing sur la base de l'écart du numéro de séquence : si un grand nombre de lacunes supérieure à la valeur de seuil sont visibles dans le numéro de séquence provenant d'un nœud dans un certain laps de temps, une alarme sera soulevée pour spoofing. Pour effectuer la détection des attaques de type spoofing, la différence entre le numéro de séquence cadres consécutive modulo 4096 est calculé. Et ensuite, l'écart calculé est comparé au seuil prédéfini. Si l'écart est supérieur au seuil, une alarme sera relevée sur les attaques spoofing. C'est l'approche la plus simple et nécessite une surcharge minimale sur le dispositif sans fil. Toutefois, en raison de la perte naturelle de paquets, ce procédé entraîne de fausses alarmes élevées.
- **Solution 2 :** Dans [29], plutôt que d'opérer strictement sur deux paquets consécutifs, Li et Trappe proposées pour détecter les attaques de type spoofing basé sur une fenêtre de paquets provenant d'une identité spécifique. Compte tenu de la fenêtre $W(k) = [S(k), S(k-1), ..., S(k-N-1)]$, constitué de N numéro de séquence de paquets consécutifs, le détecteur d'attaque calcule le $N-1$ Numéro de séquence de différences ,$d_1, d_2, ..., d_N - 1$ où $d_i = [S(k-i-1) - s(k-i)] mod 4096$. En utilisant une fenêtre de points de données, une attaque de spoofing peut être déclarée si max (d_i)¿ seuil ou la différence commutative dans la fenêtre ci-dessus est un certain seuil. En raison de l'utilisation d'une fenêtre de paquets, cette approche présente l'avantage de faibles alarmes faussement négatives ; cependant, il a un coût de calcul élevé par rapport à l'approche ci-dessus.
- **Solution 3 :** Li et Trappe proposent d'utiliser le trafic inter-arrival du temps observés par un dispositif de surveillance pour détecter les attaques de type spoofing [29]. Supposons qu'il y a deux nœuds A et B qui utilisent la même identité réseau, et un dispositif de surveillance X qui enregistre les délais dans lesquels elle observe des paquets provenant de cette identité du réseau. Supposons que le dispositif A est le dispositif initial de cette identité du réseau. Dans la vérification de la cohérence de l'arrivée de la circulation, le dispositif A envoie les paquets tels que le temps entre les paquets transmis suit une distribution fixe. Avant la deuxième source de communication, le moniteur X observera que les temps inter-τ suivent une distribution $f_T(\tau)$. Cette distribution peut être mesurée pendant un temps de fonctionnement ininterrompu entre A et X. Lorsque la deuxième source B commence à communiquer, une nouvelle distribution sera observée $f_E(\tau)$. En effectuant des tests de distribution, tels que X^2 l'essai et test de Kolmogorov-Smirnov, nous pouvons comparer si la distribution observée $f_E(\tau)$ correspond à $f_T(\tau)$ ou non. Si la distribution observée

est significativement différente de $f_T(\tau)$, l'attaque d'usurpation est déclarée. Cette méthode est adaptée pour les réseaux de capteurs où les nœuds de capteurs suivent un schéma d'échantillonnage fixe et donc produisent un motif de trafic fixe. Cependant, cette méthode est facile d'être compromise aussi longtemps que l'adversaire apprend le circuit de circulation dans des conditions normales.

Approches basées sur la force du signal

La force du signal reçu (RSS) est la force d'un signal reçu mesurée à l'antenne du récepteur. RSS est déterminée par la puissance d'émission, la distance entre l'émetteur et le récepteur, et l'environnement radio. La force du signal reçu est une mesure qui est difficile à établir de manière arbitraire et il est fortement corrélé à l'emplacement de l'émetteur. En supposant que l'attaquant et la victime sont séparés par une distance raisonnable, RSS peut être utilisé pour les différencier pour détecter les attaques de spoofing. Dans la méthode de détection des attaques de spoofing basée RSS, il y aura plusieurs points d'accès (AP) à des endroits fixes servant de RSS capteurs qui mesurent les lectures RSS du trafic sans fil transmis à partir des nœuds sans fil dans la zone intéressée.

- **Solution 1 :** Faria et Cheriton ont proposés pour détecter les attaques de type spoofing utilisant un signalprint, qui est le vecteur de RSS à plusieurs points d'accès [12]. L'idée de base derrière la méthode de signalprint est que les nœuds à différents endroits produisent des signalprints distincts qui peuvent être utilisés pour distinguer les appareils sans fil situés géographiquement en dehors. Pour construire des singalprints, AP observe le trafic et recueillent le niveau de puissance du signal reçu pour chaque paquet reçu avec succès. Les lectures de flux sont ensuite utilisées pour créer un signalprint pour chaque paquet. Chaque signalprint est représenté comme un vecteur de mesures d'intensité du signal, avec une entrée pour chaque point d'accès servant de capteur. Les valeurs entre signalprints apparaissent toujours dans le même ordre, ce poste i contient toujours le niveau de puissance du signal (en dBm) déclarés par le i ème point d'accès. Pour faire face à l'adversaire avancée qui a l'intention de changer sa puissance d'émission pour suivre le système de détection, Faria et Cheriton ont proposés d'utiliser la force du signal différentiel au lieu de la force du signal absolu. L'intensité du signal différentiel est la différence entre les valeurs d'intensité de signal et la valeur maximale trouvée du signalprint. Compte tenu des deux signalprints, deux règles d'appariement de signaux, max-matchs et min-matchs, sont précisées afin de déterminer si ces deux signalprints sont produites par le même émetteur. Supposons deux signalprints $S_1[i]$ et $S_2[i]$, où i représente le ième AP, un max-match de εdB se trouve lorsque les valeurs différentes par la plupart εdB,(C-à dire) $|S_1[i] - S_2[i]| \leq \varepsilon$).Max-matchs sont utiles pour déterminer si deux signalprints sont produits par le même émetteur, l'émetteur à une position

produira des singalprints similaires. D'autre part, les min-matchs sont utilisés pour classer deux singalprints provenant de différents dispositifs. Un min-match de εdB se trouve lorsque les valeurs diffèrent du εdB,(c'est-à-dire $|S_1[i] - S_2[i] \geq |$).

- **Solution 2 :** Sheng et al. [45] a proposé de construire un RSS profilage pour l'émetteur à chaque emplacement en utilisant les échantillons de RSS observées à plusieurs points d'accès. Plus précisément, ils ont observés les lectures RSS suivies d'un mélange de plusieurs distributions gaussiennes lorsque l'émetteur et les récepteurs sont équipés de deux antennes. Motivé par cette observation, les lectures RSS pour n'importe quel émetteur paire AP donnée sont représentés comme un modèle de mélange gaussien (GMM)[43]. Ils ont développé un algorithme de RSS profilage fondé sur l'espérance-maximisation (EM) algorithme d'apprentissage pour MGM. Dans les conditions normales, sans attaques, le profil de RSS est établi pour un émetteur à chaque emplacement possible ; aucune différence significative dans les modèles de flux n'est considérée comme une attaque par usurpation potentiel pendant la phase de détection en ligne. En outre, en utilisant la coordination entre plusieurs points d'accès augmente la précision de détection.

3.3.2 Approches de sécurité contre le Sybil

Bien qu'il n'y ait pas de solution générale, universellement acceptée à l'attaque Sybil, un certain nombre d'approches pour diverses combinaisons d'environnements et les attaques ont été proposées ; pour contrer les attaques Sybil qui sont comme suit :

Solutions utilisant un certificat de confiance

La certification est de loin la solution la plus fréquemment citée pour vaincre les attaques Sybil [28]. Il implique la présence d'une autorité de certification de confiance (CA) qui valide une correspondance entre une entité sur le réseau et son identité associée. Cette CA centralisée élimine ainsi le problème d'établir une relation de confiance entre les deux nœuds de communication. Douceur a prouvé que ce type de certification est la seule méthode qui peut potentiellement éliminer les attaques Sybil complètement [8]. Bien que cette approche semble intuitivement comme la méthode idéale pour lutter contre ces attaques, il y a un certain nombre de questions de mise en œuvre spécifiquement sur la façon dont l'AC doit établir la cartographie entité-identité. Dans les applications du monde réel ce qui peut entraîner un coût de performance appréciable notamment si elle est effectuée manuellement sur systèmes à grande échelle.

- **Solution 1 :** Zhang et el [49] ont proposés d'utiliser l'identité de certificats pour se défendre contre les attaques Sybil. Leur modèle de réseau suppose un ensemble puissant jusqu'à un serveur pour nœuds de capteurs préconfiguré. Le serveur d'installa-

tion, avant le déploiement, attribue à chaque nœud certaines informations uniques. Le serveur crée alors un certificat d'identité de liaison de l'information unique assigné, et le téléchargement de ces informations dans le nœud. Un nœud démontre son identité en toute sécurité, en présentant d'abord son certificat d'identité, puis prouve qu'il possède ou correspond à l'information unique associée. Ils ont utilisé l'arbre de hachage de Merkle [36] comme moyen de base de certificats d'identité informatique. Leur technique nécessite l'échange de plusieurs messages et est donc consommatrice de ressource.

- **Solution 2 :** Un paradigme peut être pris en charge par le choix d'un (t, n), technique de seuil pour un système de certification. Un seuil $A(t, n)$ signifie que, dans un réseau comportant n nœuds, un seuil t est établi où t est un nombre de nœuds inférieur à n. Dans ce seuil paradigme (t, n), la fonctionnalité d'une autorité de certification est uniformément distribuée à chaque nœud dans le réseau de sorte que n'importe quel T de n nœuds dans le réseau en même temps peut effectuer la fonctionnalité d'une autorité de certification de confiance et peut fournir un certificat vérifiables individuellement pour chaque identité honnête dans le réseau. Le réseau continue à fonctionner correctement, aussi longtemps que le nombre de nœuds est inférieure à t.

Solutions reposant sur le test des ressources

Pour contrer les attaques Sybil, une approche consiste à valider directement chaque identité du nœud est la seule identité présentée par le dispositif physique correspondant. Douceur a proposé des tests de ressource en tant que méthode de validation [8]. Dans les essais de ressources radio, il assume que chaque périphérique physique est limité dans certaines ressources, telles que le calcul, le stockage et la communication. Le but des tests de ressources est de déterminer si un nombre d'identités possèdent moins de ressources que prévu, s'ils correspondent à des dispositifs physiques différents. Toutefois, dans les réseaux sans fil à ressources limitées, le calcul et les essais de stockage ne conviennent pas car l'attaquant utilise peut-être un dispositif physique avec plusieurs ordres de grandeur plus de calculs et de stockage d'une capacité de ressources affamés.

- **Solution 1 :** Dans [39], Newsome et al. proposent aussi l'utilisation du test de ressources. Dans cette approche, ils supposent que tout capteur physique possède seulement une seule radio et que cette radio est incapable d'envoyer et de recevoir simultanément sur plus d'un canal. Dans ce papier, les auteurs considèrent que chaque vérifieur attribue un canal différent à chacun de ses n voisins afin d'y broadcaster un message. Ensuite, il choisit aléatoirement un canal sur lequel il décide d'écouter. Si le vérifieur arrive à attendre le message sur ce canal, cela signifie que le voisin à qui était attribué ce canal est légitime. Dans le cas échéant, cela signifie que ce voisin

est un nœud Sybil. La difficulté de cette approche est que nous n'avons pas toujours autant de canaux que de voisins. Dans ce cas, si nous n'avons pas suffisamment de canaux à attribuer, cela peut prendre beaucoup de temps pour détecter une attaque Sybil. Elle peut même demeurer indétectée s'il y a autant ou plus de nœuds Sybil que de canaux.

- **Solution 2 :** cette solution est basée sur l'hypothèse que chaque nœud dans un réseau général est incapable de transmettre sur plus d'un canal radio en même temps. Chaque fois qu'un nœud souhaite vérifier si elle est victime d'une attaque Sybil, il affecte chacun de ses voisins un canal unique et leur demande de diffuser un message d'accusé de réception (ACK) sur leur canal alloué à une heure spécifiée. Le nœud accorde au hasard à son récepteur sur un canal particulier et attend de recevoir un message ACK. Si aucun message d'accusé de réception n'est reçu, le nœud déduit que le nœud attribué sur ce canal particulier est un nœud Sybil puisque le nœud malveillant est incapable de diffuser le message d'accusé de réception de l'ensemble de ses fausses identités sur plusieurs canaux simultanément.

Solutions basée sur l'atténuation

Dans [14], Fong considère un autre type de Sybil attaque tout à fait celui qui est distinct des autres qui affligent Peer-to-Peer et les systèmes de réputation. Cette attaque vise à créer des identités pseudonymes ou fausses dans un système de réseau social (SNS) et les amener à s'entendre pour modifier favorablement les relations de confiance existantes dans le réseau. Ces relations sont représentées par un modèle de relation théorie des graphes qui existe entre le propriétaire d'une ressource et un accesseur prospective de la même ressource et est appelé un graphe social. Ces modèles sont communs dans un certain nombre populaires des Systèmes réseaux sociaux tels que Facebook. Les politiques de contrôle d'accès sont telles que définis par les SNSes respectifs eux-mêmes. Cette notion de contrôle basée sur les relations accès (ReBARC) [17] est à la base des décisions d'autorisation dans le système. Lorsque les identités contrefaites ou fausses dans le SNS s'entendent, ils peuvent acquérir la capacité d'accéder aux informations personnelles des utilisateurs. Pour contrer cette menace, Fong a proposé une version particulière du Principle Of Privilege Attenuation POPA qui est à la fois une condition nécessaire et suffisante pour contrecarrer ces attaques, avec une analyse de la politique statique pour vérifier le respect POPA [14].

Solutions de détection incitative

Margolin et Levine proposent un protocole [34] appelé Informant qui est basée sur une politique d'incitation économique et est une solution générale qui n'est pas spécifique à

un domaine d'application particulier. Une entité (appelée le détective) récompense Sibyl pour se révéler eux-mêmes. Une identité donne le nom de l'homologue de cible et un dépôt de garantie pour le détective tandis que le nœud cible reçoit le dépôt et une certaine récompense. Une adjudication au hollandais est utilisée pour établir la récompense minimale qui va révéler un nœud Sybil. Pas de jetons physiques ne sont nécessaires tels que les radios et l'horloge biaise contrairement à d'autres approches de détection Sybil.

Solution reposant sur la vérification de la position et de la situation

Cette solution est spécifique aux réseaux sans fil ad hoc. Procédés d'emploi de cette technique font usage du fait que toutes les identités qui sont projetées par tout dispositif physique unique doivent être dans le même emplacement. Les emplacements sont vérifiés à l'aide des méthodes spécifiques telles que la triangulation [46]. Donc, pour un attaquant avec un dispositif physique unique, toutes les identités Sybil seront dans le même lieu ou apparaîtront à se déplacer ensemble.

- **Solution 1 :** Dans [32], Lv et al. Proposent une méthode pour détecter les attaques Sybils dans des réseaux sans fil. Dans cet article, ils n'ont pas donné davantage de précisions sur le modèle d'attaque. Dans leur méthode, chacun des nœuds non-alignés A, B et C mesure la distance qui le sépare du nœud D en utilisant la puissance du signal reçu (RSS). Par conséquent, la position du nœud D est déterminée en effectuant la construction des trois cercles CA (de centre A et de rayon AD), CB (de centre B et de rayon BD) and CC (de centre C et de rayon CD). Ainsi, en utilisant les informations RSS à partir de plusieurs nœuds voisins coopérant, il peut être possible de déterminer les positions relatives des différentes identités du réseau. Dans cette configuration, une attaque Sybil est détectée lorsque deux ou plusieurs identités différentes ont quasiment la même position. Malheureusement, cette méthode souffre d'un taux élevé de faux négatifs.
- **Solution 2 :** Dans [38], Saha et Mukhopadhyay proposent un mécanisme pour vérifier si la position physique d'un nœud est située dans une région donnée. Dans leurs hypothèses du réseau, il y a un serveur de configuration qui configure le réseau, ainsi, il est conscient de l'emplacement de tous les nœuds déployés. Dans leur conception, de nouveaux nœuds sont autorisés à rejoindre le réseau que s'ils sont dans l'enveloppe convexe de l'ensemble initial des nœuds déployés. Leur protocole vise à vérifier en toute sécurité la position de tout nouveau nœud qui rejoint le réseau. Un agent logiciel est conscient de l'emplacement de tous les nœuds de capteurs déployés. Lorsque le nouveau nœud X rejoint le réseau, l'agent identifie le triangle T (formé par les nœuds V_1, V_2 et V_3) dans lequel est situé la position demandée de X. Puis, chacun des nœuds V_i génère un nombre aléatoire R_i, y greffe sa propre identité et envoie au nouveau nœud X le message $M_i = R_i V_i$ via le canal de trans-

mission radio. Ainsi, X reçoit trois messages M_i, un de chaque V_i, et construit les messages$M_i' = R_iX$ qu'il renvoie à chacun des nœuds V_i par le canal de transmission sonore. Chaque nœud V_i mesure le temps écoulé t_{ii} et le retourne à l'agent logiciel. Ce dernier détermine ensuite si l'emplacement revendiqué est déjà enregistré. S'il en est ainsi, l'agent rejette le nouveau nœud. Pour ce faire, il compare t_{ii} avec t_{ij} où t_{ij} est le temps total nécessaire pour qu'un message atteigne V_i à partir de V_j et en revienne. Par conséquent, il vérifie que $t_{ii} < t_{ij}$ pour $i = 1; 2; 3$. Même si elle semble être très simple à mettre en œuvre et nécessite peu de communication et peu de calcul, cette solution ne fonctionne pas bien quand un ou plusieurs sommets du triangle T ne sont pas des nœuds honnêtes.

Solutions basées sur la mesure RSSI

Dans [9], Demirbas et Song introduisent une méthode de détection Sybil fondé sur l'indicateur Received Signal Strength (RSSI) de messages. La coopération d'un nœud supplémentaire (et donc une communication de message) est nécessaire pour le bon fonctionnement de ce protocole. Un algorithme de localisation est utilisé dans ce schéma d'attaque Sybil et peuvent être détectés avec un caractère complet de 100 avec peu de fausses alertes. Malgré le fait que RSSI est pas fiable et que les transmissions par radio sont non-isotrope, l'utilisation de rapports de RSSI à partir de plusieurs récepteurs résout ce problème.

- **Solution 1 :**Demirbas et Song ont proposé l'utilisation d'un indicateur de force du signal reçu (RSSI) pour détecter les attaques Sybil [6]. Chaque fois que la réception de n'importe quel message d'un nouvel expéditeur, le nœud calcule le RSSI du message. Le nœud se lie avec le RSSI et stocke l'ID de l'expéditeur dans une table de consultation. Si le nœud à tout moment dans l'avenir reçoit un autre message avec le même RSSI, mais un identifiant de l'expéditeur différente, elle se perçoit immédiatement être victime d'une attaque Sybil. Pour chaque occurrence RSSI, quatre indicateurs simultanées différentes étaient nécessaires pour tenir compte du caractère variable et peu fiable de la puissance du signal reçu.
- **Solution 2 :** Xiao et al. [47] ont proposé un système distribué pour détecter les attaques Sybil dans un réseau véhiculaire ad hoc (VANET) en vérifiant la position de chaque nœud. Le processus de détection utilise une analyse statistique de la distribution de puissance du signal et permet de connaître les emplacements actuels des nœuds authentiques. la distribution de puissance du signal sera observée sur une période de temps pour un nœud sans fil suspect. Pour vérifier la position d'un nœud sans fil (c'est-à-dire, claimer), le vérificateur permettra de recueillir la position du claimer plus le RSSI de son voisin et calculer localement la position estimée d'un claimer. Si la position estimée d'un claimer est loin de ce prétendu, le claimer sera

considérée comme un nœud Sybil. Une fois un nœud Sybil est détecté, l'algorithme de classification Sybil est effectué pour vérifier pour d'autres ID Sybil généré par le même agresseur. Comme le régime utilise la distribution d'intensité du signal, il est difficile pour un nœud malveillant de modifier sa distribution de puissance du signal. La précision du système est augmentée du nombre de témoins et majoration de la période d'observation.

Solutions basées sur la pré-distribution aléatoire des clés

Cette technique permet à un nœud d'un réseau de capteurs sans fil d'établir des liaisons sécurisées pour communiquer avec un autre nœud [14]. Dans la pré-distribution des clés aléatoires, un ensemble de touches sont affectés au hasard à un nœud permettant de découvrir ou de calculer les clés communes qu'il partage avec ses nœuds voisins. Le secret de nœud à nœud est assuré par l'aide des touches communes comme une clé secrète partagée de session. Les idées principales sont l'association de l'identité avec la touche affectée à un nœud et la validation de la clé. La validation consiste à s'assurer que le réseau est en mesure de valider les clés qu'une identité pourrait avoir.

- **Solution 1 :**[30]La pré-distribution des clés aléatoires existe quand une séquence de clefs symétriques sera choisie aléatoirement parmi un grand nombre de clefs. Chaque séquence de clefs symétriques sera sauvegardée dans un nœud. Chaque paire de capteurs voulant communiquer vont chercher, chacun dans sa propre séquence, une clef commune. S'ils en trouvent une, ils vont l'utiliser pour chiffrer les messages. Cela n'est pas toujours le cas, mais avec une probabilité d'établissement de clefs suffisante, les nœuds peuvent partager des clefs symétriques avec plusieurs nœuds afin d'obtenir un réseau connecté. L'avantage de ce protocole est que la station de base ne sera pas un point unique de défaillance (point dont le reste du réseau est dépendant et dont une panne entraîne l'arrêt complet du système) et que chaque nœud aura besoin de sauvegarder une séquence de clefs symétriques et non pas des clefs pour un réseau formé de n capteurs. Par contre, la communication entre une paire de nœuds de capteurs n'est pas garantie, et si un adversaire réussit à compromettre un nombre de capteurs suffisant, il sera capable de découvrir toutes les clefs du réseau.
- **Solution 2 :**SPINS [42] " Security Protocols for Sensor Networks " profite de la station de base pour la distribution des clefs. Cette approche propose d'avoir une seule clef partagée entre chaque nœud et la station de base. Si deux nœuds veulent communiquer entre eux, ils doivent établir leurs clefs de sessions à travers la station de base. Cette méthode n'exige pas beaucoup de mémoire pour sauvegarder une clef mais rend la station de base un point défaillance et augmente le coût de transmission.

Solutions basées sur le canal

Dans les scénarios sans fil typiques avec diffuseurs riches, comme dans les environnements intérieurs et urbains, la réponse du canal decorréle rapidement dans l'espace [25]. Deux dispositifs sans fil ayant des réponses de canal similaires sont susceptibles d'être dans le même emplacement. En examinant les réponses du canal de deux identités sans fil, si ces deux réponses des canaux sont similaires, ces deux identités sans fil sont très probablement du même dispositif sans fil (et donc du nœud Sybil). La technique de détection Sybil basée sur le canal repose sur des mécanismes d'estimation des canaux existants dans les systèmes sans fil.

3.4 Conclusion

Dans ce chapitre, nous avons spécifié les attaques liées aux identités et expliquer comment un attaquant arrive à mener ces attaques. Nous avons aussi récapitulé les différentes approches de sécurité proposées dans la littérature pour se protéger contre ces attaques. A noter que malgré la diversité de ces approches, les attaques liées aux identités ne sont pas entièrement éliminées. Dans le but de renforcer davantage la sécurité contre ces attaques, nous avons proposé dans le chapitre suivant une solution de sécurité contre l'attaque Sybil.

Chapitre 4

Schéma de détection de l'attaque Sybil

4.1 Introduction

A cause des caractéristiques inhérentes des réseaux sans fil ad hoc, plusieurs attaques peuvent être facilement menées dans un tel type de réseau. Les attaques liées à l'identité d'un nœud représentent une classe plus ou moins sévère d'attaques. Parmi ces attaques figure l'attaque sybil, dans laquelle un nœud malhonnête se présente dans le réseau en utilisant plusieurs identités, en vue de falsifier les opérations du routage et d'acheminement des données, il peut mener aussi d'autres actions malicieuses telles que la consommation des ressources ou gagner faussement un consensus.

Pour se protéger contre l'attaque sybil, la littérature propose plusieurs solutions qui se basent essentiellement sur le test des ressources, les certificats de confiance et l'utilisation de la mesure RSSI. Bien que efficace dans pas mal de cas, ces solutions restent toujours limitées dans le sens où elles ne peuvent pas éliminer complètement l'impact de l'attaque et elles sont généralement coûteuses en termes d'overhead de communication, de calcul et de stockage. Ces limitations nous ont motivé de proposer une solution de sécurité contre l'attaque sybil. Notre solution se base sur l'utilisation de la distance qui sépare les nœuds et la direction à partir de laquelle sont reçus les paquets pour détecter les nœuds qui utilisent plusieurs identités à la fois. La solution proposée présente l'avantage d'être légère au moment où aucun overhead (de calcul, de communication et de stockage) n'est généré lors de sa mise en œuvre. Par simulation, nous allons prouver son efficacité en termes de taux détection, et mettre en avant ses avantages et ses inconvénients.

Le reste de ce chapitre est organisé comme suit : La deuxième section décrit le modèle de réseau suivie par la section trois qui présente en détail notre solution de sécurité. Dans la section suivante, nous analysons et interprétons les résultats de simulation et nous

terminons par une conclusion dans la dernière section.

4.2 Modèle de réseau

Un réseau ad hoc est modélisé comme étant un ensemble d'identités qui utilisent des liaisons sans fil pour communiquer. Chaque identité est censée être utilisée par un seul nœud dans le réseau. L'ensemble des nœuds composant le réseau peut être subdivisé en deux sous ensembles, le sous ensemble des nœuds corrects et le sous ensemble des nœuds sybil. Chaque nœud correct est associé à une identité unique, tandis qu'un nœud sybil peut utiliser plusieurs identités (fabriquées ou volées). Au niveau du réseau, une identité peut être l'adresse IP, l'adresse MAC ou tout autre identifiant représentant les nœuds dans le réseau. A noter que l'attaque sybil peut être mené d'une manière simultanée ou non simultanée. Dans notre simulation l'attaque sybil est menée de la façon où un nœud envoi plusieurs paquets et à chaque envoi une identité différente est utilisée. Ces paquets peuvent être les fameux paquets HELLO utilisés dans les protocoles de routage pour détecter le voisinage. En d'autres termes, un nœud sybil peut envoyer des paquets HELLO en utilisant à chaque fois une identité différente. De cette façon, le nœud sybil parviendra à perturber l'opération de routage et obtenir des faux chemins conduisant ainsi à paralyser entièrement le réseau.

4.3 Solution de sécurité proposée

Dans cette section, nous allons décrire en détail notre solution de détection de l'attaque sybil. Pour cela nous énumérons d'abord les hypothèses sous lesquelles notre solution est fonctionnelle, ensuite nous détaillons la solution proposée.

4.3.1 Hypothèses

Dans le réseau dans lequel notre solution est implémentée, nous supposons que l'attaque sybil est menée d'une manière non simultanée et que chaque nœud utilise une et une seule interface de communication, l'objectif de cette hypothèse est d'exclure le cas ou un nœud donné possède plusieurs interfaces de communication représentant des identités légitimes.

On suppose aussi que les nœuds dans le réseau sont homogènes et que les antennes utilisés dans la communication sans fil sont directionnelles.

4.3.2 Détails de la solution

Pour détecter une attaque sybil, un nœud honnête a besoin de connaître la distance entre lui et le nœud sybil, et aussi la direction à partir de laquelle il reçoit les paquets de la part de nœuds sybil, ces deux informations sont facilement calculables sans l'aide des autres nœuds. Ceci représente un avantage par rapport aux solutions qui se basent sur la localisation pour détecter l'attaque sybil, en effet, dans ces dernières plusieurs nœuds doivent coopérer pour calculer la position d'un nœud dans le réseau. L'idée derrière la connaissance de la distance et la direction est de pouvoir localiser plusieurs identités représentants éventuellement un seul nœud physique. En d'autres termes, un nœud honnête, quand il reçoit plusieurs paquets avec des identités différentes venus de la même direction, de la part de plusieurs nœuds dont les distances entre eux et le nœud honnête sont égales, détecte facilement la présence d'une attaque sybil.

Comme il est illustré dans la figure 4.1, le nœud sybil S utilise plusieurs identités id_i avec $i = 1, 2, 3\ldots$, pour envoyer des paquets en utilisant à chaque envoi une identité différente. Le nœud honnête D, à chaque fois qu'il reçoit un paquet, il calcule la distance entre lui et le voisin émetteur du paquet et il détermine en parallèle la direction à partir de laquelle le paquet a été reçu. Si plusieurs paquets sont reçus avec la même distance et direction, dans ce cas là, une attaque sybil est susceptible d'être présente dans le réseau.

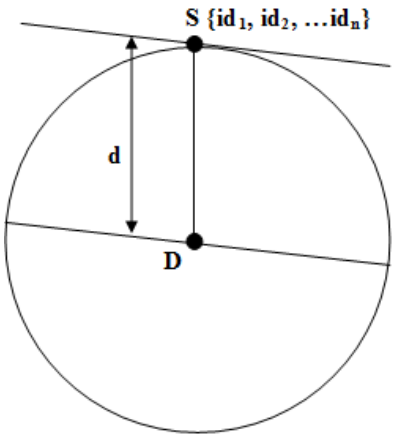

FIGURE 4.1 – Attaque sybil

A noter que la connaissance de la direction à partir de la quelle les paquets sont reçus est indispensable, cela pour distinguer le cas où plusieurs nœuds se retrouvent sur le même périmètre par rapport au nœud honnête D. Comme il est illustré dans la figure 4.2.b, bien que les nœuds représentés par les identités $id_1, id_2, id_3\ldots$ se retrouvent à distances égales du nœud D, mais elles ne représentent pas le même nœud physique, i.e., ces identités ne sont pas des identités sybil. Par contre dans la figure 4.2.a, le nœud sybil S est bien

représenté par les identités sybil id_i avec $i = 1, 2, 3...$. En conclusion, la connaissance de la direction est indispensable pour distinguer les deux cas de figure illustrés dans la figure 4.2.

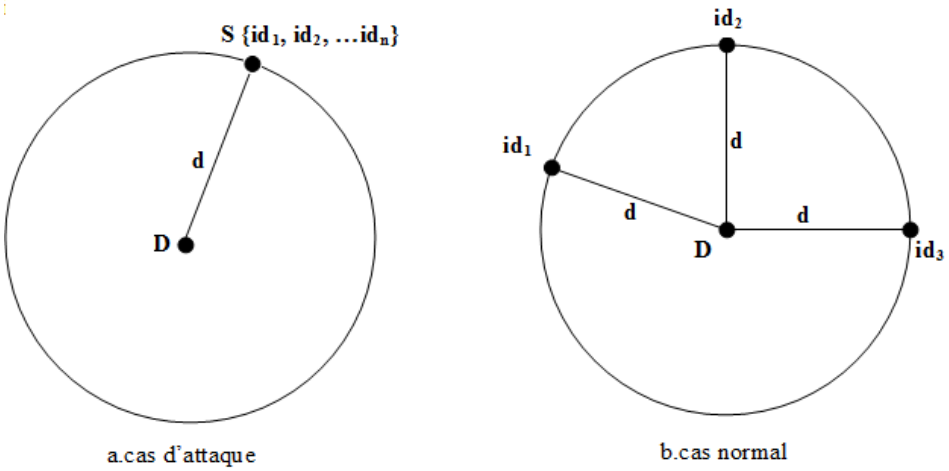

FIGURE 4.2 – Schéma de la solution proposée

Le pseudo algorithme suivant résume le principe de notre solution Soit D un nœud honnête

1. A chaque fois que D reçoit un paquet de la part de l'un de ses voisins n_i avec $i = 1, 2, \ldots m$, il calcule la distance d_i et détermine la direction α_i correspondante au paquet reçu et il enregistre le triplet (n_i, d_i, α_i) dans un ensemble S.
2. Dans l'ensemble S, on ne sélectionne que les triplets dont les couples (d_i, α_i) sont identiques. En conséquence, plusieurs sous ensembles F_k sont construits.
3. Les identités de chaque sous ensemble F_k sont des identités sybil représentant le même nœud physique.

Notre schéma repose sur la connaissance de la distance entre un nœud et son voisin. Cette distance est facilement calculable en utilisant la formule $P_r = P_t.k/d^{\alpha}$ avec P_r est la puissance du signal reçu, P_t la puissance de transmission, k est une constante $d$est la distance qui sépare les deux nœuds et α le gradient de la puissance. Aussi, notre schéma qu'on propose exploite la direction des paquets reçus pour localiser les identités sybil. On note que la direction à partir de laquelle le paquet est reçu peut être déterminer en utilisant des antennes directionnelles.

Comparativement avec les solutions proposées dans la littérature telles que celles qui se basent sur la cryptographie à clé publique et celles qui se basent sur le test des ressources, notre solution présente l'avantage d'être légère et scalable. En effet, pour calculer la distance et déterminer la direction, un nœud honnête n'a pas besoin de l'aide des autres

nœuds, ce qui rend le schéma proposé plus performant. A la différence des autres solutions, la gestion des clés dans les solutions basées sur la cryptographie, et la mise en œuvre du test des ressources, sont déjà un goulot d'étranglement qui affecte considérablement les performances du réseau, et rendent moins scalables les solutions de sécurités existantes.

4.4 Résultats de simulation

Pour prouver l'efficacité de notre solution dans la détection de l'attaque sybil et évaluer sa performance, nous avons effectués une série de simulation en utilisant les paramètres de simulation listés dans le tableau 4.1 :

Paramètre	**Signification**
Le nombre de nœuds	20
Taille du réseau	$100 * 100m^2$
portée de communication	$20m$
Taille du paquet	1024 bits
Protocole de routage	AODV
Temps de simulation	$500s$
Modèle de mobilité	WLAN power

TABLE 4.1 – Paramètres de simulation

Dans une surface de $100 * 100m^2$, les 20 nœuds sont dispersés d'une manière aléatoire. Parmi ces 20 nœuds on choisit un nœud malicieux S qui va jouer l'attaque. L'action malicieuse consiste à générer plusieurs paquets HELLO en utilisant à chaque fois une identité différente. Comme il est illustré dans la figure 4.3, nous choisissons aussi un nœud honnête qui va jouer le rôle du détecteur de l'attaque. Ce dernier va recevoir donc les paquets HELLO générés par le nœud sybil S.

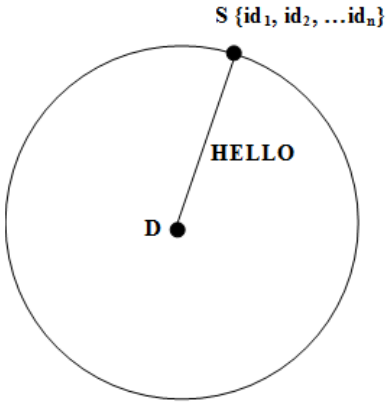

FIGURE 4.3 – Principe de l'attaque

4.4.1 Métriques de simulation :

Les métriques qui ont été mesurées sont

- **Taux de détection :** désigne le rapport entre le nombre de message HELLO considéré légitime par le nœud détecteur D et le nombre total de paquets HELLO reçus. Cette métrique a été envisagée parce que les paquets HELLO portant des identités sybil vont être ignorés par le nœud détecteur dés que détectés. Ceci va nous permettre d'évaluer l'efficacité de notre solution dans la détection de l'attaque.
- **Faux négatif :** C'est une mesure utilisée pour montrer le cas où notre solution se retrouve dans l'incapacité de détecter l'attaque sybil. Ce taux peut être calculé comme étant le rapport entre le nombre d'identités sybil détecté et le nombre total des identités sybil utilisés par le nœud sybil S.
- **Faux positif :** C'est une mesure utilisée pour montrer le cas où la solution proposée détecte faussement des identités sybil qui sont réellement des identités légitimes. Ce taux peut être calculé comme étant le rapport entre le nombre d'identités légitime considérés sybil et le nombre total des identités légitime.

4.4.2 Analyse et interprétation des résultats

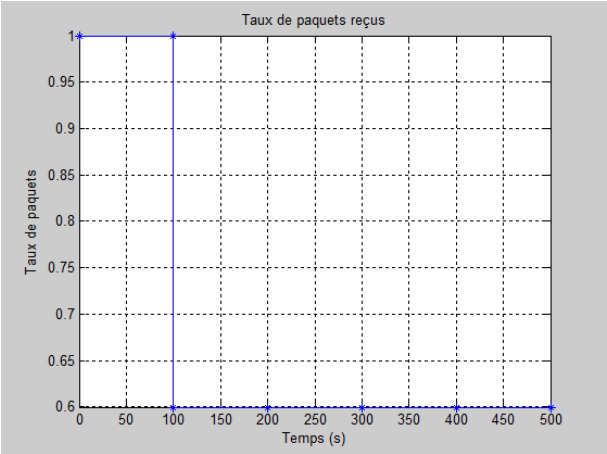

FIGURE 4.4 – Taux de paquets HELLO reçus

La figure 4.4 illustre le taux de paquets HELLO reçus par le détecteur en fonction du temps de simulation. Nous constatons que ce taux égal à 1 jusqu'à l'instant 100, ensuite ce taux chute à la valeur 0.6 à partir de l'instant 100. Ceci est justifié par le fait que l'attaque sybil à été détecter à partir de l'instant 100 et le nœud détecteur a ignoré l'ensemble des paquets HELLO envoyés par le nœud sybil S. Ceci montre que notre solution détecte bien les identités sybil et elle est en conséquence efficace dans la détection de l'attaque sybil.

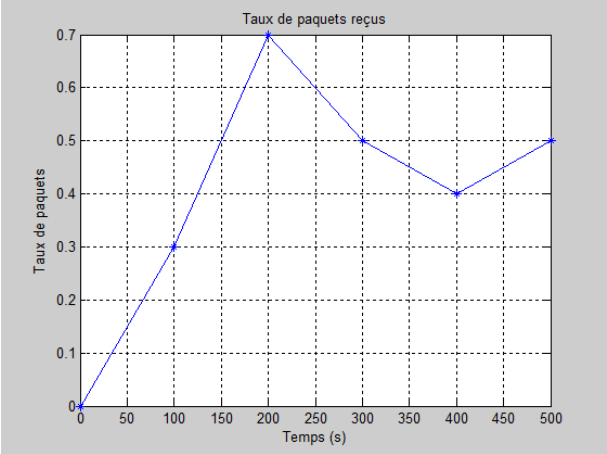

FIGURE 4.5 – Taux de faux négatif

La figure 4.5 illustre la mesure de faux négatif en fonction du temps. Nous remarquons que l'allure du graphe n'est plus uniforme c'est-à-dire le taux de faux négatif des fois il augmente et des fois il diminue. En d'autres termes le cas où une attaque sybil mené dans

le réseau n'est pas détectée est bien présent et ceci malgré l'utilisation de la solution de sécurité proposée. En point de vue pratique, ce scénario peut se produire à cause de la mobilité des nœuds. Par exemple un nœud sybil qui bouge continuellement autour du nœud détecteur est difficile à détecter par ce dernier car la direction à partir de laquelle les paquets ont été reçus change avec la mobilité de nœud émetteur qui est dans notre cas le nœud sybil.

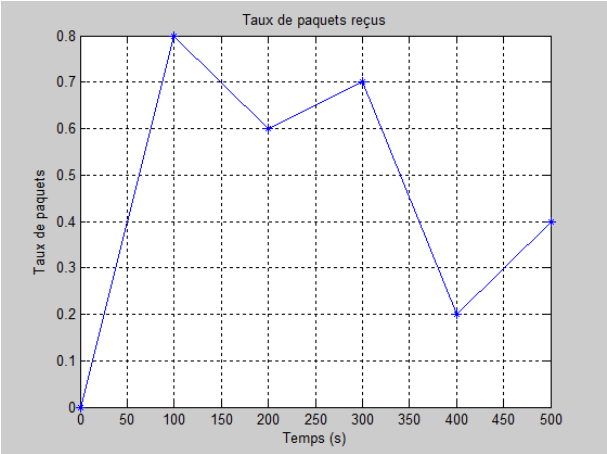

FIGURE 4.6 – Taux de faux positif

La figure 4.6 illustre le taux de faux positif tel qu'il est mesuré en fonction du temps. Idem à la figure 4.5, nous constatons que l'allure du graphe n'est plus uniforme c'est-à-dire le taux de faux positif des fois il augmente et des fois il diminue. Ce comportement montre que le scénario où des identités légitimes sont considérées comme étant des identités sybil peut se produire. Ceci est dû toujours à la mobilité. En effet, plusieurs nœuds légitimes qui sont très proches les un des autres peuvent être considérés par notre solution comme étant des identités sybil car ces nœuds légitimes possèdent approximativement la même position et la même direction par rapport au nœud détecteur D. Aussi, le scénario ou un nœud légitime qui se trouve dans une position donnée à un instant donné et qui est remplacé par un autre nœud légitime suite à la mobilité des deux nœuds est considéré comme étant une attaque et considéré par notre solution comme une attaque, car deux nœuds légitimes se sont retrouvés dans la même position et direction par rapport au nœud détecteur durant une période donnée.

4.5 Conclusion

Dans ce chapitre, nous nous sommes focalisées sur l'attaque sybil dans les réseaux ad hoc. Il s'agit d'une attaque dans la quelle un nœud malicieux se présente dans le

réseau en utilisant plusieurs identités. Son impact sur les différentes fonctionnalités du réseau et certainement négatifs. Pour se protéger contre une telle attaque, nous avons proposé un schéma de sécurité exploitant la distance et la direction pour détecter les identités sybil. L'idée est qu'à chaque fois plusieurs identités se trouvent dans la même position et direction par rapport au nœud détecteur sont identifiés comme étant des identités sybil. Les résultats de simulation montrent que notre solution détecte efficacement l'attaque sybil, néanmoins elle présente des limitations dans le sens ou des scénarios de présence ou d'absence d'attaques peuvent se produire sans être identifiés dans notre solution. Dans un travail futur, nous envisageons à améliorer notre solution pour qu'elle prenne en considération les scénarios cités auparavant.

Conclusion générale & Perspectives

Un réseau sans fil ad hoc est une collection de nœuds qui communiquent via des liaisons sans fil sans recourir à une infrastructure préexistante ou une administration centralisée. A cause de l'ouverture et le partage de médium de communication, la mobilité et l'absence d'infrastructure, ce genre de réseau est facilement vulnérable à plusieurs attaques possibles. Les solutions proposées dans la littérature restent toujours limitées, moins efficaces et moins performantes pour faire face à ces attaques. Dans ce travail, nous nous sommes intéressés à l'attaque Sybil qui appartient à la classe des attaques liées aux identités. Il s'agit d'une attaque dans laquelle un nœud malicieux se présente dans le réseau tout en utilisant plusieurs identités. La conséquence d'une telle attaque est le gain de plus de ressources réseau que les autres nœuds légitimes. Pour faire face, la littérature propose plusieurs solutions qui se basent essentiellement sur le test des ressources et la cryptographie à clé publique pour s'assurer de l'unicité de l'identité. Bien que multiples, ces solutions n'arrivent pas à se débarrasser entièrement de cette attaque. Ce qui nous a motivés de travailler sur le sujet et proposer une solution de sécurité contre cette attaque.

Notre solution se base sur le calcul de la distance qui sépare deux nœuds et exploite la direction à partir de laquelle les paquets sont reçus pour s'assurer de l'unicité de l'identité des nœuds voisins émetteurs. Plusieurs identités avec la même distance et direction peuvent représenter un nœud physique unique et elles sont identifiées comme des identités Sybil en conséquence. Le nœud détecteur maintient bien évidemment une liste noire qui contient les identités Sybil pour les éviter dans une communication future. Par simulation, nous avons prouvé l'efficacité de notre solution et nous avons évalué sa performance. Dans notre solution, aucun matériel n'est nécessaire et aucune coopération entre nœud n'est exigée pour sa mise en œuvre. La distance et la direction sont facilement et localement calculables ce qui rend notre solution légère et scalable. En contrepartie, des scénarios où plusieurs nœuds d'identités différentes, qui sont très proches les uns des autres peuvent être accusés à tort par notre solution. Aussi, la mobilité des nœuds peut conduire à des scénarios où l'attaque Sybil ne peut pas être détectée par notre solution. La liste noire

utilisée pour maintenir les identités Sybil peut accroître exponentiellement ce qui pose éventuellement un problème de stockage au niveau des nœuds.

En perspectives, nous allons comparer notre solution avec des solutions de références pour évaluer davantage l'efficacité, la robustesse et la performance de notre solution. Aussi, nous envisageons d'améliorer notre solution pour tenir en compte toute les limites citées auparavant.

Bibliographie

[1] Adjih C, Clausen T, Jacquet P, Laouiti A, Mühlethaler P, and Raffo D,*Securing the olsr protocol. In Proceedings of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop, Mahdia, Tunisia, June 25-27 2003.*

[2] Arbaugh W, Shankar N, Wan Y, Zhang K,*Your 80211 wireless network has no clothes, IEEE Wirel.Commun. Volume 9, numéro 6. Décembre 2002. pp 44-51.*

[3] *Bluetooth IN http : //www.bluetooth.com.*

[4] Brahma M,*Etude de la QoS dans les réseaux ad hoc : intégration du concept de l'ingénierie du trafic. Thèse de doctorat, spécialité informatique. Université de Haute Alsace. 13 Décembre 2006. 176p.*

[5] Burgod C,*Contribution à la sécurisation du routage dans les réseaux ad hoc. Thèse de doctorat, Spécialité informatique, Université de LIMOGES, le 12 octobre 2009.*

[6] Demirbas M, Song Y,*An RSSI-based scheme for Sybil attack detection in wireless sensor networks, in : Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks, June 2006, pp. 564-570.*

[7] Dioum B,*Effets de la mobilité sur les protocoles de routage dans les réseaux ad hoc. Mémoire d'ingénieur d'état en système d'information. Université Mouloud Mammeri de Tizi-Ouzou. 2007.*

[8] Douceur JR,*The Sybil Attack, in First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7-8, 2002. pp 251-260.*

[9] Du W, Deng J, Han Y. S, and Varshney P. K,*A pairwise key predistribution scheme for wireless sensor networks. In ACM CCS 2003. Oct. 2003. pp 42-51.*

[10] Estrin D, Govindan R, Heidemann J.S, and Kumar S,*Next century challenges : Scalable coordination in sensor networks. In MOBICOM, pp 263-270, 1999.*

[11] *ETSI : High Performance Radio Local Area Network.*

[12] Faria D, Cheriton D,*Detecting identity-based attacks in wireless networks using signalprints, in : WiSe '06 Proceedings of the 5th ACM workshop on Wireless security. Septembre, 2006. pp 43-52.*

[13] Ferreri F, Bernaschi M, Valcamonici L,*Access points vulnerabilities to DoS attacks in 802.11 networks, in : IEEE Wirel.Commun. Volume 14, numéro 2. Avril 2008. pp159-169.*

[14] Fong P,*Preventing Sybil Attacks by Privilege Attenuation : A Design Principle for Social Network Systems. In IEEE Symposium on Security and Privacy, 2011. pp. 263-278.*

[15] Gada D, Gogri R, Rathod P, Dedhia Z, Mody N, Sanyal S, Abraham A,*A Distributed Security Scheme for Ad Hoc Networks. ACM Crossroads, Special Issue on Computer Security. Volume 11, No. 1, September 2004, pp. 1-10.*

[16] Galice S. ,*Modèle de sécurité dynamique pour les réseaux spontanés Thèse de doctorat. Institut National des Sciences Appliquées de Lyon. 2007.*

[17] Gates C. E,*Access control requirements for Web 2.0 security and privacy, in Proc. of Workshop on Web 2.0 Security & Privacy (W2SP), Oakland, California, USA, May 2007.*

[18] Guo F, Chiueh T,*Sequence Number-Based MAC Address Spoof Detection, in : Recent Advances In Intrusion Detection, Springer, Seattle, WA, 2006, pp 309-329.*

[19] http ://www.ietf.org/rfc/rfc2501.txt.

[20] Hu Y, Perrig A, and Johnson D.B,*Ariadne : a secure on demand routing protocol for ad hoc networks. in Wireless Networks Volume 11 Issue 1-2, janvier 2005. pp 21-38.*

[21] Hu Y, Johnson D.B, Perrig A,*SEAD : Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. WMCSA '02 Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems & Applications.2002.pp3-13.*

[22] ISO,*Intermediate system system Intradomain routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service. In(ISO 8473).ISO DP 10589, February 1990.*

[23] Jacques A, Sainson V, Benjada M,*Le grand livre de la sécurité. Edition sécurité informatique. pp. 75-90. 2004. IN http ://www.securiteinfi.com.*

[24] Jacquet P, Laouiti A, Minet P, and Viennot L,*Performance of multipoint relaying In ad hoc mobile routing protocols. Editors NETWORKING, volume 2345 of Lecture Notes in Computer Science. Springer, 2002. pp 387-398.*

[25] Jakes W, Cox D,*Micro-ondes Mobile Communications. Wiley-IEEE Press, New York, 1994.*

[26] Karlof C, Wagner D,*Secure routing In wireless sensor networks : attacks and countermeasures. Ad Hoc Networks volume 1, issues 2-3.Septembre 2003.pp 293-315.*

[27] Laouiti A,*Unicast et multicast dans les réseaux ad hoc. Thèse de doctorat, spécialité informatique. Université de Versailles, Saint-Quentin-en-Yvelines. 9 juillet 2002. 183p.*

[28] Levine B.N, Shields C et Margolin N.B,*A survey of solutions to the Sybil attack. University of Massachusetts Amherst, MA, 2006.*

[29] Li Q, Trappe W,*Relationship -based Detection of Spoofing-related Anomalous Traffic In Ad Hoc Networks. In Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on vol.1,2006. pp 50-59.*

[30] Liu D. and Ning P,*Establishing pairwise keys in distributed sensor networks. In Proc. of 10th ACM Conference on Computer and Communications Security (CCS"03). 2003. pp. 52-61.*

[31] Li Y, Thai T, Wu W,*Wireless Sensor Networks and Applications, Springer Science and Business Media LLC, 2008.*

[32] Lv S, Wang X, Zhao X, and Zhou X,*Detecting the Sybil attack cooperatively in wireless sensor networks. In International Conference on Computational Intelligence and Security, CIS 2008. 13-17 December 2008. Suzhou, China, Volume 1 - Conference Papers, pp 442-446, Washington, DC, USA, 2008. IEEE Computer Society.*

[33] Madden S, Franklin M. J, Hellerstein J. M, and Hong W,*TAG : a tiny aggregation service for ad hoc sensor networks. ACM SIGOPS Operating Systems Review-OSDI '02 : Proceedings of the 5th symposium on Operating systems design and implementation Volume 36. 2002. pp 131-146.*

[34] Margolin, N.B, and Levine B.N,*Informant : Detecting Sybils using incentives, In Proceedings of Financial Cryptography. February 2007. pp 192-207.*

[35] Marti S, Giuli T.J, Lai K, and Baker M,*Mitigating Routing Misbehaviour In Mobile Ad Hoc Networks. In International Conference on Mobile Computing and Networking. Proceedings of the 6th annual international conference on Mobile computing and networking. Boston, Massachusetts, USA. ACM , 2000. pp 255- 265.*

[36] Merkle R.C,*Protocols for public key cryptosystems. In Proceedings of the 1980 IEEE Symposium on Security and Privacy, 1980.*

[37] Morris R, Jannotti J, Kaashoek M, Li J, and Decouto D,*Carnet : a scalable ad hoc wireless network system. In ACM SIGOPS European Workshop. 2000. pp 61-65.*

[38] Mukhopadhyay D. and Saha I,*Location verification based defense against sybil attack in sensor networks. In Distributed Computing and Networking, 8th International Conference, ICDCN 2006, Guwahati, India. December 2006. pp 27-30.*

[39] Newsome J, Shi E, Xiaodong D, and Perrig A,*The Sybil attack in sensor networks : analysis and defenses. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, Berkeley, California, USA. April 26-27, 2004, pp 259-268.*

[40] Papadimitratos P, and Haas Z.J,*Secure link state routing for mobile ad hoc networks. In SAINT Workshops. IEEE Computer Society, 2003. pp 379-383.*

[41] Perkins C.E, Belding-Royer E.M, and Das S.R,*IETF RFC3561 :ad hoc on-demand distance vector (AODV) routing. July 2003.*

[42] Perrig A, Szewczyk R, Wen V, Culler D and Tygard,*SPINS : security protocols for sensor networks. In Proc of ACM MobiCom, 2001. pp. 189-199.*

[43] Redner R, Walker H,*Mixture Densities, Maximum Likelihood and the EM Algorithm. SIAM Rev. vol.26 numéro 2. 1984. pp 195-239.*

[44] Sadqi Y, Zaoui M,*Les protocoles de routage mis en place dans le cadre des réseaux ad hoc. Mémoire de master informatique des systèmes repartis.2010/2011.*

[45] Sheng Y, Tan K, Chen G, Kotz D, Campbell A,*Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength , In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.13-18 Avril 2008, Phoenix, AZ.*

[46] Tangpong A,*Managing Sybil Identities in Distributed Systems. Thesis at Doctor of Philosophy. The Pennsylvania State University, May 2010.*

[47] Xiao L, Greenstein LJ, Mandayam NB, Trappe W,*Empreintes digitales dans l'éther : en utilisant la couche physique pour l'authentification sans fil, In : Actes de la Conférence internationale IEEE sur les communications. CCI, 2007, IEEE, pp 4646-4651.*

[48] Zapata MG, and Asokan N,*Securing ad hoc routing protocols. Editors Workshop on Wireless Security. ACM, 2002. pp 1-10.*

[49] Zhang Q, Wang P, Reeves D.S, Ning P,*Defending against Sybil Attacks in Sensor Networks.In Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on 6-10 Juin 2005. pp 185-191.*

Résumé

Le Sybil est une attaque sévère, dans laquelle un nœud malicieux se présente dans le réseau en utilisant plusieurs identités. L'objectif est de gagner plus de ressources réseau que les autres nœuds légitimes. La littérature propose des solutions qui se basent essentiellement sur le test des ressources ou la cryptographie à clé publique. Ces solutions n'arrivent pas à lutter efficacement contre une telle attaque et elles sont généralement coûteuses en termes d'overhead de communication, de calcul et de stockage. Notre solution se base sur le calcul de la distance qui sépare deux nœuds et exploite la direction à partir de laquelle les paquets sont reçus pour détecter les identités Sybil. Ces dernières sont ensuite maintenues dans une liste noire pour les éviter dans une communication future. Notre solution est à la fois légère et scalable car aucun matériel supplémentaire n'est nécessaire et aucune coopération entre nœuds n'est exigée pour sa mise en œuvre. Les résultats de simulation montrent que la solution proposée est efficace dans la détection de l'attaque Sybil, il reste à la comparer avec d'autres travaux de référence pour prouver davantage son efficacité et évaluer sa performance.

Mots clés : réseaux ad hoc, sécurité des réseaux ad hoc, attaques liées aux identités, sybil

Abstract

The Sybil is a severe attack in which a malicious node is present in the network using multiple identities. The objective is to gain more network resources than other legitimate nodes. The literature provides solutions that are based mainly on testing resources or public key cryptography. These solutions are not able to fight effectively against such an attack, and they are generally expensive in terms of communication, computing and storage overheads. Our solution is based on the computing of the distance between two nodes and exploits the direction from which packets are received to detect the Sybil identities. Thereafter, these identities are blacklisted in order to avoid them in a future communication. Our solution is both lightweight and scalable because no additional hardware is needed and no cooperation among nodes is required for its implementation. Simulation results show that the proposed solution is effective to detect the Sybil attack, it remains to compare it with other reference works to further prove its effectiveness and evaluate its performance.

keywords : ad hoc networks, security ad hoc networks, identities related attacks, Sybil