REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU
FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire

De Fin d'études

En vue de l'obtention du diplôme de master en informatique

Option : Conduite De projet Informatique

Thème

Etat de l'art sur les systèmes de détection d'intrusion dans les protocoles de routage dans les réseaux Adhoc

Proposé et Dirigé par :

M me Bourkache Ghenima

Réalisé par :

M elle Haddad Souhila

Promotion 2012/2013

Remerciements

C'est avec humilité et gratitude que nous reconnaissons ce que nous devons :

Tous d'abord je remercie le bon Dieu de m'avoir donné le courage et la patience pour mener à bon terme ce travail.

Je tiens aussi à remercier vivement ma promotrice Mme BOURKACHE GHENIMA pour ses précieux conseils et son orientation.

Je remercié chaleureusement les membres du jury pour l'honneur qu'ils ont nous font en acceptant de juger ce mémoire de fin d'études.

Je tiens à remercier tous les enseignants du département de génie informatique.

Enfin, je remercié toutes les personnes ayant contribué de prés ou de loin au bon accomplissement de mon travail.

Dédicaces

J'ai toujours pensé faire où offrir quelque chose à mes parents en signe de reconnaissance pour tout ce qu'ils ont consenti comme efforts, rien que pour me voir réussir, et voilà, l'occasion est venue. Je dédie cet humble mémoire A mon très cher père Ahcéne et ma tendre mére Houria .

Sans oublier tous ceux qui m'ont soutenue et encouragé durant toute cette période.

- *A mon cher mari : KARIM*
- *A ma sœur : HANANE.*
- *A mes frères : MOKRANE, HOUCINE et RABAH.*
- *A mon oncle : BELKACEME et sa femme HOURIA et leur petite fille ALICIA*
- *Toute la famille HADDAD*
- *A ma belle famille MEKAIBECHE*
- *A tous mes amis sans exception, en particulier : Wahiba ,Zitouna ,louiza ,Saida,Nounou.*
- *A toute la promotion Master2 .2013.*

Souhila

Résumé:

Dans ce modeste travail on a présenté les réseaux ad hoc qui sont des réseaux mobiles caractérisés par l'absence d'infrastructure. Les réseaux ad hoc sont très vulnérable et exposé a plusieurs types d'attaques, et pour contrer ces attaques des IDS (Intrusion Detection systemes) sont mis en place, un IDS est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. On a alors exposé trois types d'architectures, la première RIDAN -Real-time Intrusion Detection for Ad hoc Networks-, proposé par stamoli, qui utilise les machines à états finis synchronisées pour définir formellement les attaques contre le protocole de routage. L'architecture proposé par Zhang, W Lee, & Y Huang qui est une architecture distribué et coopératif, et enfin la technique Watchdog pour détecter et atténuer les débordements de routage.

Mots-clés : réseau ad hoc, routage, sécurité, système de détection d'intrusion , AODV,OLSR

Table des matières……..…….1

Listes des figures ……..……..4

Introduction général…….5

Chapitre I : Généralité sur les réseaux sans fil Ad hoc

1. Introduction ……6

2.Définition de réseau sans fil…….……..6

2.1.les types des réseaux sans fil…….6

2.1. 1.les réseaux sans fil avec infrastructure…….....7

2.1.2. les réseaux sans fil sans infrastructure……..7

3. les réseaux Adhoc ……8

3.1.Définition……..8

3.2. modélisation ……...…8

3.3. Les applications des réseaux mobiles Adhoc ……...10

3.4. Les caractéristiques des réseaux Adhoc……....10

3.4. Les avantages des réseaux ad Hoc ……...11

4.Le routage dans les réseaux ad hoc ……...11

4.1. Définition du routage ……11

4.2.Classification des protocoles de routage ……12

4.2.1.Les protocoles de routage proactifs ……...…..13

4.2.2.Les protocoles de routage réactifs ……..14

a. Technique d'apprentissage en arrière ……...14

b.Technique du routage source ……...15

4.2.3.Les protocoles de routage Hybrides ……....18

5. La sécurité dans les réseaux ad hoc …….……18

5.1.La sécurité des réseaux…….…….…18
5.2. La sécurité du routage dans les réseaux ad hoc ……19
5.3. Description des vulnérabilités ……...19
5.4. Description des attaques ……...20
6.Etat de l'art des solutions……...20
6.1. Solutions pour l'authentification ……..….21
6.2.Solution pour l'intégrité Physique des Nœuds ……...22
6.3.Solution pour l'intégrité et l'authentification des messages ……..22
6.4.Solution pour la confidentialité ……..22
6.5. Solution pour la disponibilité ……22
7. Conclusion ……...…23

Chapitre II : les systèmes de détection d'intrusion

1.Intrusion ……..……24
2.La détection d'intrusions ……..……..24
2.1. Définition ……..……24
3.Nécessité et qualités requises des IDS ……..……..24
4.Architecture d'un IDS ……..25
5.Classification des IDS ……26
5.1.Source d'information ……..26
5.2.Réponses des IDS ……...27
5.3.Paradigme de détection ……..28
5.4.Mode de supervision ……..28
5.5.Méthodes de détection d'intrusions ……28
5.5.1.L'approche comportementale ou par anomalie ……28
5.5.2.L'approche par scénarios ……28
6.Détection d'intrusions dans les réseaux Ad Hoc ……..29
6.1.Les IDS Individuels…….29
6.2. Les IDS coopératifs ……...30
6.3.Les IDS hiérarchiques ……31

Chapitre 3 : Les différents systèmes détection d'intrusion dans les réseaux ad hoc

1. Architecture hiérarchique ……..33
2.Présentation de système de détection RIDAN…….…..33
3. Les machines à états finis ……35
3.1.Objectifs ……35

4.Les attaques détecté……..36
4.1.Les attaques liées au protocole de routage AODV ……36
4.1.1.Détection de l'attaque de modification du numéro de séquence ……36
4.1.2.La détection d'attaque de destruction des paquets de routage ……38
5. Architecture de distribution et coopératives ……...41
6. Présentation de l'architecture pour la détection d'intrusion ……42
6.1.Collecte des données(data collection)……43
6.2.Détection locale (Local Detection)……43
6.3. Détection coopérative : Cooperative Detection ……44
6.4.Réponse d'intrusion……44
6.5. Détection Multi-Layer intrusion intégrée et riposte ……..45
7.Détection des anomalies dans les réseaux mobiles Ad Hoc……46
7.1. Construire un modèle de détection des anomalies……46
8. Résultats expérimentaux……...48
9.Architecture Stand-alone……..48
10. Chien de garde et pathrater ……..…49
10.1 .Watchdog ……....49
10.2 .Les nœuds défaillant ……....52
10.3 .Métrique……...53
11. résultat et simulation……...53
12.Discussion ……...…54
Conclusion général.……55

Figure I.1: La décomposition de réseau mobile sans fil ……..……..……..6

Figure I.2 : Les réseaux sans fil avec infrastructure…….……...7

Figure I.3 : Les réseaux sans fil sans infrastructure……...8

Figure I.4 : La modélisation d'un réseau Ad hoc……....9

Figure I. 5 : Le changement de la topologie des réseaux Ad hoc….....9

Figure I.6 : Le chemin utilisé dans le routage entre la source et la destination……..10

Figure I.7 **:** Classification de protocole de routage……13

Figure I.8 : Les deux requêtes RREQ et RREP utilisées dans le protocole AODV……18

Figure II.1 : Architecture d'un IDS Individuel…….29

Figure II.2 :Architecture d'un IDS coopératifs……...….30

Figure II.3 : Architecture d'un IDS coopératifs par un agent mobile……..31

Figure II.4 :Architecture d'un IDS hiérarchique……...32

Figure III.1 : Architecture du système RIDAN…….34

Figure III.2: Première MEF de détection d'attaque de modification de numéro de séquence….……36

Figure III.3 : Deuxième MEF de détection d'attaque de modification de numéro de séquence……. 37

Figure III.4: Troisième MEF de détection d'attaque de modification de numéro de séquence…….. .38

Figure III.5 : L'architecture d'IDS de réseau sans fil ad hoc……42

Figure III.6 : Le modèle conceptuel de IDS Agent ……...…...43

La figure III.7 **:**illustre comment le chien de garde fonctionne……...…….49

Introduction général :

La constante évolution des technologies de l'information et le penchant vers l'utilisation des machines sans fil qui se sont imposées ces dernières années ont fait émerger un nouveau type de réseaux : les réseaux sans-fil ad hoc, ou MANET (Mobile Ad hoc NETwork). Se souciant de pouvoir communiquer et de partager l'information dans n'importe quelle situation, les réseaux ad hoc sont des systèmes autonomes composés par un ensemble d'entités mobiles libres de se déplacer sans contraintes. Ces entités utilisent le médium radio pour communiquer et forment un réseau n'utilisant aucune infrastructure existante. De ces faits, ces réseaux qualités de spontanés présentent une architecture originale qui évolue à tout instant. Un réseau ad hoc est donc un système autonome de nœuds mobiles. Ce système peut fonctionner de manière isolée ou s'interfacer avec des réseaux fixes au travers de passerelles pour devenir un réseau d'extrémité

Il existe plusieurs domaines d'application aux réseaux ad hoc. Le domaine militaire et celui des secours en cas de catastrophes restent des exemples fréquemment cités. Toutefois, plusieurs autres applications des réseaux ad hoc ont vu le jour. Nous citons les réseaux véhiculaires résultant de l'interconnexion de véhicules en mouvement ou les réseaux de capteurs capable de récolter et de transmettre les données environnementales.

En contre partie les réseaux Ad Hoc sont par nature plus vulnérables et plus difficiles à protéger que les réseaux filaires. En effet, comme les réseaux ad hoc sont dynamiques et les nœuds peuvent se déplacer librement, il y a des possibilités qu'un ou plusieurs nœuds soient capturés et deviennent corrompus surtout si le réseau est déployé dans un environnement hostile. Une telle situation montre que la confiance entre les nœuds n'est pas garantie. Des travaux se sont alors intéressés à la définition et à la gestion de la notion de confiance dans les réseaux ad hoc. Le principe fondamental de ces différents travaux est généralement la collaboration entre les nœuds en vue de s'échanger et de gérer des degrés de confiance.

Notre travail entre dans le cadre de l'étude du l'état de l'art sur les systèmes de détection d'intrusion dans les protocoles de routage dans les réseaux mobiles Ad hoc. Notre étude repose principalement sur les travaux de recherche qui ont été fait, et qui se font à l'heure actuelle. Pour cela on a subdivisé le travail en 3 chapitres :

Le premier chapitre : Généralité sur les réseaux Adhoc

Le deuxième chapitre : consiste a déterminé les différents systèmes de détection d'intrusion

Le troisième chapitre : critiquer les travaux de recherche qui ont été faite

1.Introduction :

Les technologies sans fil offrent de nouvelles perspectives en télécommunications. L'évolution récente des moyens de communication sans fil et l'amélioration continue des performances des terminaux mobiles ont permis d'exploiter ces technologies dans les différents et de penser à de nouvelles application.

Dans ce chapitre, nous présenterons l'environnement mobile et les principaux concepts qui lui sont liés. Afin de comprendre ces réseaux sans fils, nous détaillerons quelques principales notions nécessaires de ces systèmes. Et puis, nous étudierons les réseaux ad hoc, qui sont un cas particulier de ces réseaux, le principe de routage et les protocoles et enfin nous finirons sur la sécurité de cette technologie.

2. Définition de réseau sans fil :

Un réseau sans fil (Wireless Network) est un réseau dans lequel les machines (nœuds) participantes ne sont pas raccordées entre elles par un médium physique (de type câble en cuivre ou fibre optique).
Ce type de réseau permet aux utilisateurs de se déplacer dans certain champ de couverture sans perdre le signal et pouvoir bénéficier de toutes les ressources du réseau

2.1. Les type des réseaux sans fil :

Les réseaux sans fil sont regroupés en deux classes selon leur composition : Les réseaux avec infrastructure et les réseaux sans infrastructure.

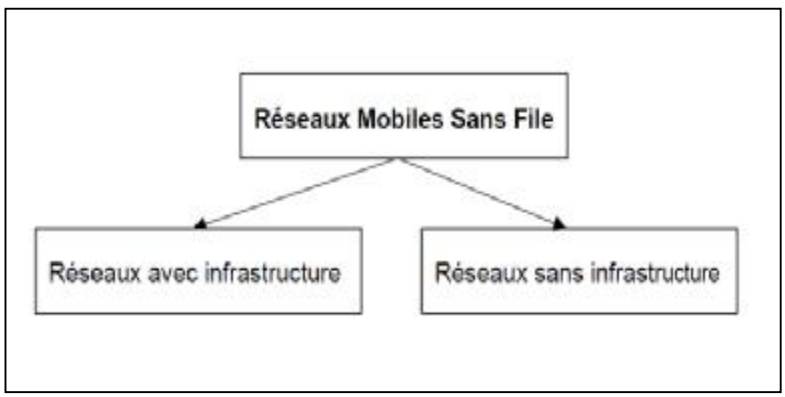


Figure I.1: La décomposition de réseau mobile sans fil

2.1.1. Les réseaux sans fil avec infrastructure : [6]

Dans ce mode de fonctionnement on distingue deux type d'entités : Les « sites fixes » d'un réseau de communication filaire classique (wired network) et les sites mobiles (wireless network)

Certains sites fixes, appelés stations support mobile (Mobile Support Station) ou station de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule.

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages.
Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé.

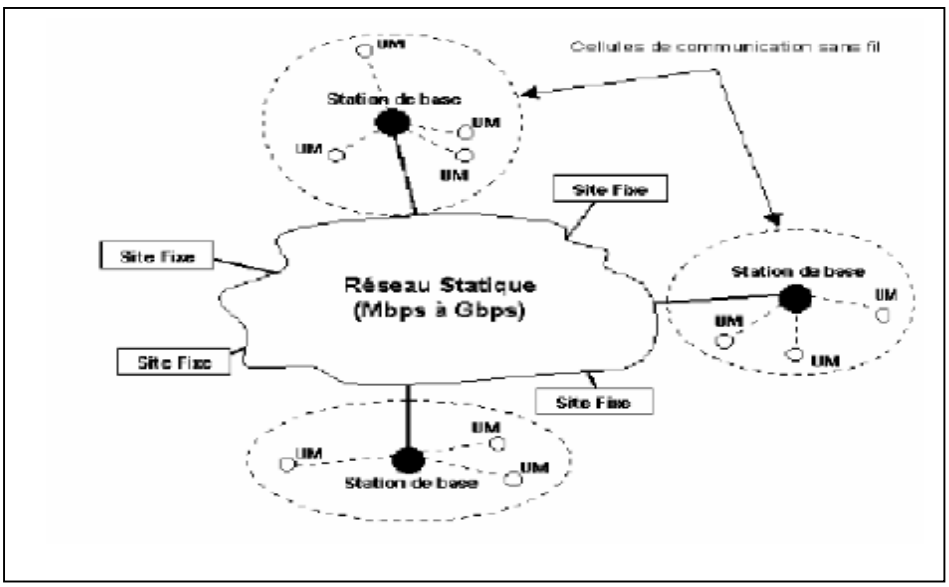


Figure I.2 : Les réseaux sans fil avec infrastructure

2.1.2. Les réseaux sans fil sans infrastructure :

Dans ce mode de fonctionnement le réseau ne sollicite pas une liaison filaire, et ne comporte pas de stations fixes, tous les sites sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil.

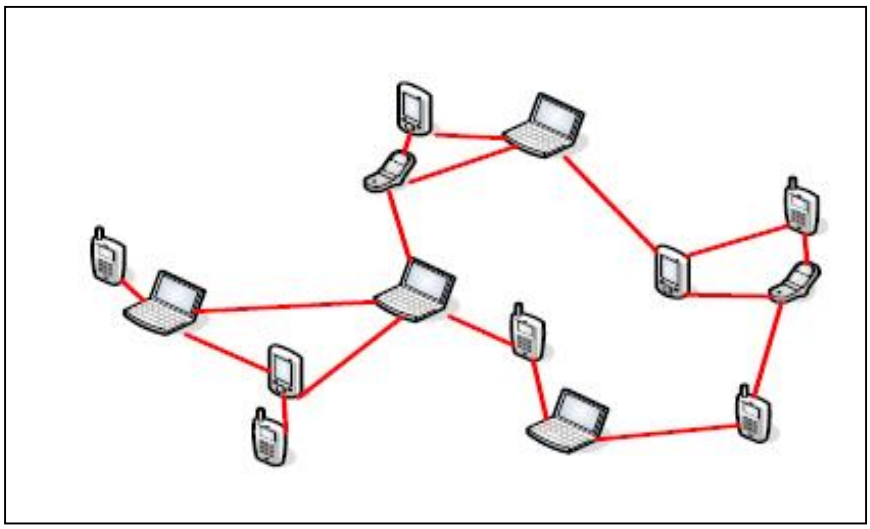


Figure I.3 : Les réseaux sans fil sans infrastructure

3. Les réseaux Ad Hoc :

3.1. Définition : [4]

Un réseau mobile ad hoc est un cas particulier de réseau sans fil, est un environnement mobile sans infrastructure, appelé généralement MANET (Mobile Ad hoc NETWORK), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.

3.2.Modélisation : [4]

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

La figure suivante représente un réseau ad hoc de 10 unités mobiles sous forme d'un graphe :

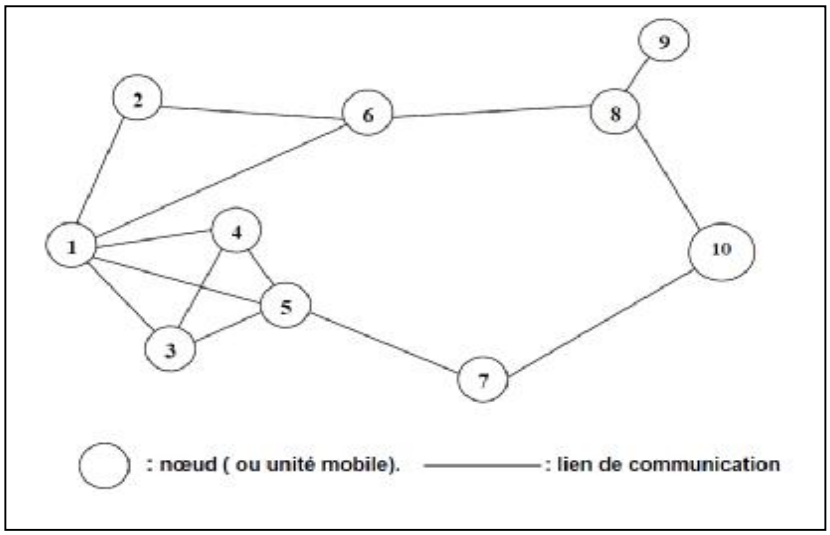


Figure I.4 : La modélisation d'un réseau Ad hoc

La topologie du réseau peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente.

Dans cette figure ce dessous, on présente le changement de la topologie des réseaux Ad Hoc :

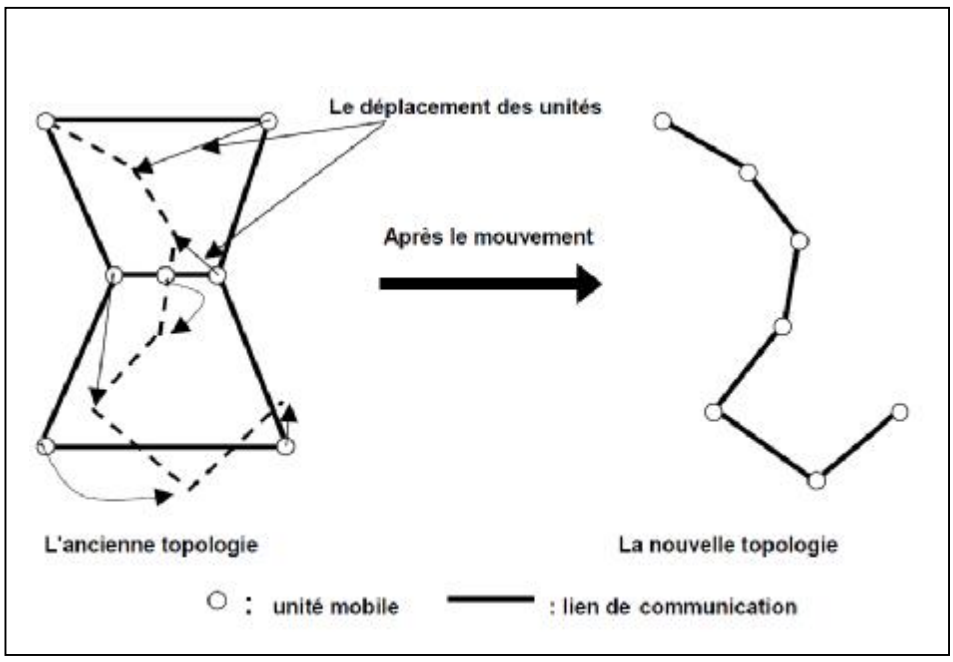


figure I. 5 : Le changement de la topologie des réseaux Ad hoc

3.3.Les applications des réseaux mobiles ad hoc :[6]

La particularité du réseau Ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. On distingue les application suivantes :

- **Les services d'urgence :** opération de recherche et de secours des personnes, tremblement de terre, feux, inondation
- **Le travail collaboratif et les communications dans des entreprises ou bâtiments :** dans le cadre d'une réunion ou d'une conférence par exemple.
- **Home network :** partage d'applications et communications des équipements mobiles.
- **Applications commerciales :** pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.
- **Réseaux de senseurs :** pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, . . . etc.) ou domestiques (contrôle des équipements à distance).
- **Réseaux en mouvement :** informatique embarquée et véhicules communicants.
- **Réseaux Mesh :** c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

3.4. Les caractéristiques des réseaux ad hoc :[6]

Parmi les caractéristiques importantes des réseaux ad Hoc , on citera :

- **Une topologie dynamique :** Les unités mobiles du réseau , se déplacent d'une manière libre et arbitraire**[6]** De plus, le fait qu'une entité quitte un groupe de communication est considéré comme un état normal qui ne doit pas perturber les autres participants[7]
- **Une bande passante limitée :** Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.
- **Des contraintes d'énergie :** Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.
- **Une sécurité physique limitée** : Les réseaux ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

- **L'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.

- **La notion de « multihop »** : un réseau ad hoc est qualifié par « multihop » car plusieurs noeuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires.
- **Sécurité et Vulnérabilité :[11]** Dans les réseaux ad hoc, le principal problème est le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement . Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'intrusions.

3.5.Les avantages des réseaux ad Hoc : [12]

Les réseaux ad-hoc présentent plusieurs avantages, les plus importants sont :

- **Déploiement facile, rapide et économique :** dans les réseaux ad-hoc, la tâche fastidieuse du déploiement des stations de base (câblage, installation, etc.) n'est plus nécessaire. En conséquence, le déploiement est aussi plus rapide et se fait avec un faible coût.

- **Tolérance aux pannes** : un réseau ad-hoc continue à fonctionner même si quelques nœuds tombent en panne, ceci est dû au fait qu'il ne comporte pas de nœuds centraux

4. Le routage dans les réseaux ad hoc :

Dans cette partie nous intéressons aux protocoles de routages dans les réseaux Ad Hoc.

La stratégie de routage dans les réseaux ad hoc est utilisée dans le but de découvrir les chemins qui existent entre les nœuds. Le but principal d'une telle stratégie 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 doit être faite avec un minimum de contrôle et de consommation de la bande passante.

4.1. Définition du routage :[4][22]

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné.
Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance (plus court, plus rapide, absence de boucle de routage …..).

Les caractéristiques d'algorithmes de routage ad Hoc sont les suivantes :

Simplicité : les protocoles doivent engendrer un surcout de données pour la gestion aussi faible que possible et doivent être très simples à développer et déployer.

Auto-organisation : aucun contrôle central ne peut être admis dans un réseau ad hoc et les structures nécessaires à la gestion du routage doivent se créer de façon distribuées et résister autant que possible au changement de topologie.

Extensibilité : les protocoles proposés doivent s'adapter à différentes tailles de réseaux ad hoc et supporter différents modèles de mobilités et de trafic.

Et dans ce qui suit, on illustre une figure qui nous présente le chemin optimal utilisé dans le routage entre la source et la destination

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

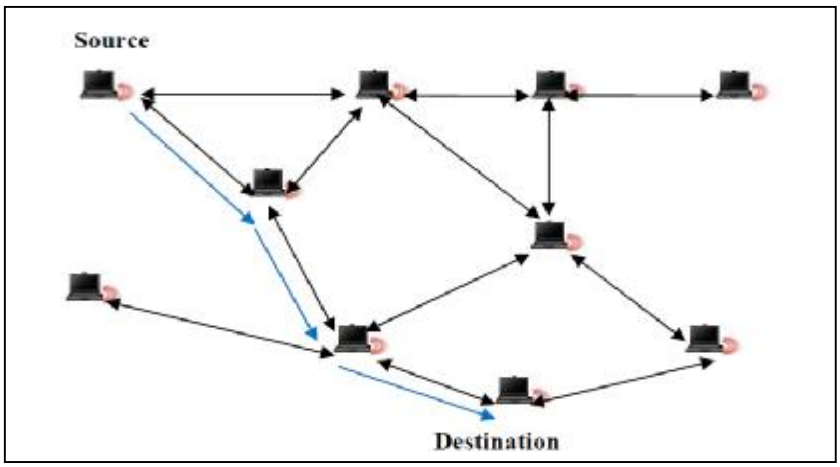


Figure I.6 : Le chemin utilisé dans le routage entre la source et la destination

Actuellement il existe plusieurs types de protocoles de routages pour les réseaux Ad Hoc, chacun ayant des propriétés différentes :

4.2. Classification des protocoles de routage :

Le principal but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui soit robuste et efficace. D'une manière générale, toute stratégie de routage repose sur des méthodes et des mécanismes que l'on peu regrouper en trois grandes classes :

- Les protocoles de routage proactifs
- Les protocoles de routage réactifs
- Les protocoles de routage hybrides

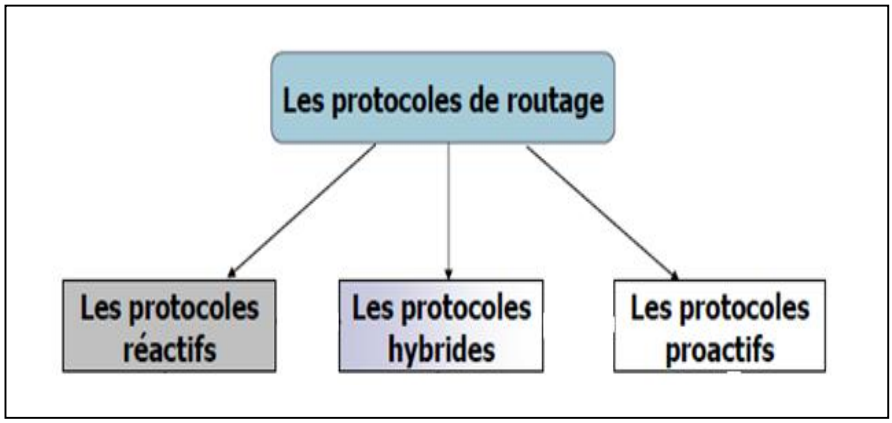


Figure I.7 : Classification de protocole de routage

4.2.1. **Les protocoles de routage proactifs :**

Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les noeuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. **[6]**

Deux principales méthodes sont utilisées dans cette classe de protocoles proactifs : la méthode Link state et la méthode Distance Vector. Qui sont utilisées aussi dans les réseaux filaires.

Un protocole à état de lien est légèrement différent d'un protocole à vecteur de distance dans le sens où les informations échangées entre les routeurs sont de natures différentes**.**

- **Etat de liens (Link state)** ***:***

Dans cette méthode, un protocole à état des liens, les routeurs vont échanger l'état de leur lien avec les autres routeurs. Ce qui correspond à échanger des informations sur le débit, la charge, le retard, le nombre de saut, etc

- **Vecteur de distance (*Distance vector) :***

Dans cette méthode, Un protocole à vecteur de distance permet d'établir une route en fonction du nombre de sauts entre les routeurs. Chaque routeur échange sa table de routage complète.

Il existe plusieurs protocoles de routage proactifs les plus connus , le DSDV, FSR, OLSR.

Et pour cela, on se présente sur le protocole OLSR :

- **Le protocol OLSR (Optimized Link State Routing) [10]**

Est un protocole proactif. Et celui ci est très bien adapté aux réseaux larges et denses. Plus un réseau va être important, plus **OLSR** reprend l'algorithme à état de lien,il se base dessus en y amenant des optimisations.

Dans ce protocole, les différents nœuds qui composent le réseau vont tous être utilisés comme des routeurs et maintient une table de routage complète.

Ainsi chaque nœud a un rôle important, puisque c'est lui qui détermine la route la mieux adaptée en fonction de l'information qu'il a reçue.

OLSR utilise le protocole UDP pour communiquer. Celui-ci modifie juste la table de routage et il fonctionne seulement pour des nœuds appartenant au même sous réseaux IP.
Pour diminuer la charge générée par les messages de contrôle, **OLSR** implémente des MPR .

Chaque nœud choisit ses MPR parmi les voisins qui sont à un saut.
Les MPR doivent permettent d'atteindre toute machine qui se trouve à deux sauts. Ainsi, pour le même nombre de machines, moins on a de MPR sur le réseau et moins il y aura de trafic sur celui-ci.

Chaque nœud calcule une route vers chaque autre nœud en utilisant un algorithme du plus court chemin, ceci avec les informations reçues dans les messages précédents. **OLSR** ne fait que modifier la table de routage, par conséquent il n'agit pas directement dans le routage des paquets.

4.2.1.Les protocoles de routage réactifs :

Ce sont des protocoles dans lesquels la mise à jour ou le contrôle des routes se fait à la demande [9] c'est-à-dire Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information.
Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées[6]
Dans ce cadre plusieurs techniques peuvent être adoptées, les plus importantes sont :

a. **Technique d'apprentissage en arrière :** [9]

Le mécanisme d'apprentissage en arrière ou le **backward learning** est basé sur le fait que lorsqu'un nœud source veut transmettre un message à une destination précise, il procède tout d'abord à l'opération d'inondation de sa requête sur tout le réseau.

Ainsi, chaque nœud intermédiaire dit de transit (appartenant au chemin par lequel va passer le message), indique le chemin au nœud source lors de la réception de la requête.

On dit qu'il apprend le chemin au nœud source, tout en sauvegardant la route dans la table transmise. Enfin, lorsque la requête arrive à bon port, le nœud destinataire, et suivant le même chemin, transmet sa réponse sous forme de requête.

Notons que le chemin établi entre les nœuds est un chemin Full duplex. Signalons aussi que la source garde trace du chemin tant qu'il restera en cours d'utilisation une fois que le chemin sera calculé.

b. Technique du routage source :

Dans cette technique, le nœud source détermine toute la liste des nœuds par lesquels doit transiter le message, ainsi le nœud émetteur inclut dans l'entête du paquet une route source.

En effet, afin de construire la route, le nœud source doit préciser les adresses exactes des nœuds par lesquels le message transitera jusqu'à atteindre le destinataire.

Ainsi, le nœud source transmet le paquet au premier nœud spécifié dans la route. Notons que chaque nœud par lequel le paquet transite, supprime son adresse de l'entête du paquet avant de le retransmettre. Une fois que le paquet arrive à sa destination, il sera délivré à la couche réseau du dernier hôte.

Plusieurs protocoles de routage réactifs existent dont AODV, TORA, DSR, etc.

Et pour cela, on présente le protocole AODV :

Ø Le protocole AODV :

AODV est un protocole réactif, ceci peut être très intéressant lorsqu'un réseau est très grand et composé de nombreux nœuds. **[10]**

v Table de routage et paquets de contrôle [6]

Le protocole AODV, réduit le nombre de diffusions de messages, et cela en créant les routes lors du besoin.

L'AODV est basé sur l'utilisation des deux mécanismes « Découverte de route » et «Maintenance de route ».

L'AODV utilise les principes des numéros de séquence afin de maintenir la consistance des informations de routage.
A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides.

Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraîches (fresh routes).

L'AODV utilise une requête de route dans le but de créer un chemin vers une certaine destination.
Cependant, l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.

Une entrée de la table de routage contient essentiellement :

- L'adresse de la destination.
- Le nœud suivant.
- La distance en nombre de nœud (i.e. le nombre de nœuds nécessaires pour atteindre la destination).
- Le numéro de séquence destination qui garantit qu'aucune boucle ne peut se former.

- Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).
- Le temps d'expiration de l'entrée de la table (temps au bout du quel l'entrée est invalidée).
- Un tampon de requête afin qu'une seule réponse soit envoyée par requête.

A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time).

Si une nouvelle route est nécessaire, ou qu'une route disparaît, la mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds :

- RREQ Route Request, un message de demande de route.
- RREP Route Reply, un message de réponse à un RREQ.
- RERR Route Error, un message qui signale la perte d'une route.

v Format générale d'une RREQ :

@ source	Num.seq.source	Broadcast id	@ destination	Num.seq. destination	Nombre de saut

v Format générale d'une RREP :

@ source	@ destination	Num.seq. Destination	Nombre de Saut	Life time

v Fonctionnalité :

Un nœud diffuse une requête de route (RREQ : Route REQuest), dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible (figure a).

Cela peut arriver si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant (i.e. la métrique qui lui est associée est infinie).

Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage.
Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source.

Comme nous avons déjà dit, après la diffusion du RREQ, la source attend le paquet réponse de route (RREP : Route REPly). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), la source peut rediffuser une nouvelle requête RREQ.

Quand un nœud de transit (intermédiaire) envoie le paquet de la requête à un voisin, il sauvegarde aussi l'identificateur du nœud à partir duquel la première copie de la requête est reçue.

Cette information est utilisée pour construire le chemin inverse (figure), qui sera traversé par le paquet réponse de route de manière unicast (cela veut dire qu'AODV supporte seulement les liens symétriques).

Puisque le paquet réponse de route va être envoyé à la source, les nœuds appartenant au chemin de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse (temps d'expiration, numéro de séquence et prochain saut).

Afin de limiter le coût dans le réseau, AODV propose d'étendre la recherche progressivement. Initialement, la requête est diffusée à un nombre de sauts limité.

Si la source ne reçoit aucune réponse après un délai d'attente déterminé, elle retransmet un autre message de recherche en augmentant le nombre maximum de sauts. En cas de non réponse, cette procédure est répétée un nombre maximum de fois avant de déclarer que cette destination est injoignable.

A chaque nouvelle diffusion, le champ Broadcast ID du paquet RREQ est incrémenté pour identifier une requête de route particulière associée à une adresse source.
Si la requête RREQ est rediffusée un certain nombre de fois (RREQ_RETRIES) sans la réception de réponse, un message d'erreur est délivré à l'application.

La destination renvoie un message RREP, ce message peut donc être acheminé vers la source.
Chaque nœud traversé incrémentera le nombre de sauts. Et ajoutera une entrée à sa table pour la destination.

Une réponse adéquate peut aussi être donnée par un nœud situé entre la source et la destination. Dans ce cas l'obtention de routes bidirectionnelles est néanmoins possible grâce au drapeau "Gratuitous RREP".

Le nœud intermédiaire enverra alors en plus un RREP vers la destination. Les nœuds entre le nœud intermédiaire et la destination ajouteront donc à leur table une entrée vers la source du RREQ.

Cette disposition permettra à la destination d'envoyer directement des paquets `à la source sans devoir procéder à la recherche d'une route. C'est utile lors de l'établissement de communications TCP pour l'envoi du premier ACK.

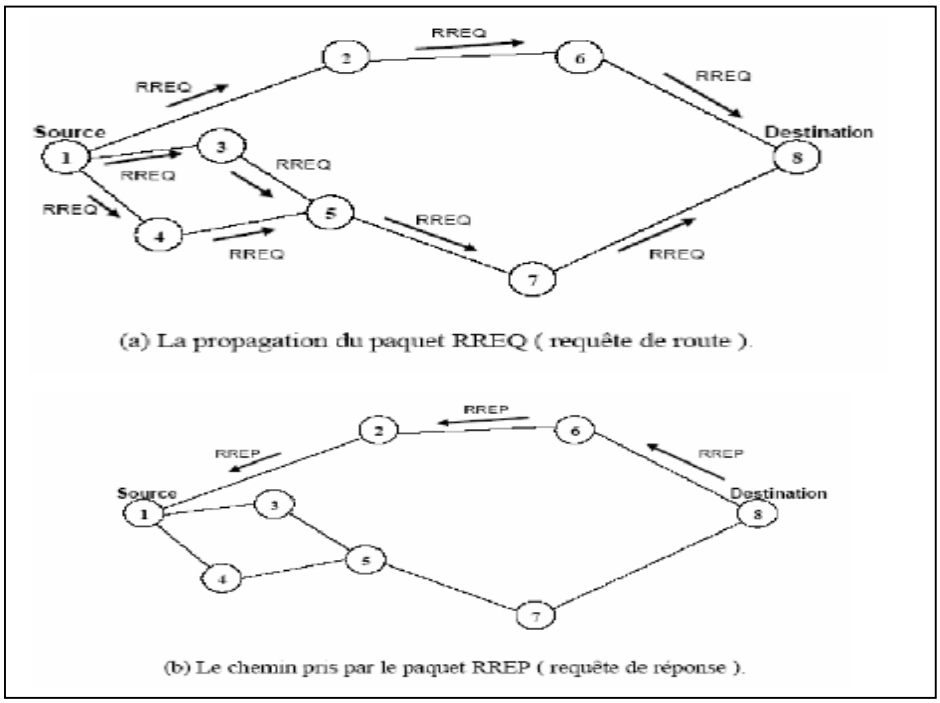


Figure I.8 : Les deux requetes RREQ et RREP utilisées dans le protocole AODV

4.2.3.Les protocoles de routage Hybrides [9]

Les protocoles hybrides combinent les deux idées : celle des protocoles proactifs et celle des protocoles réactifs.

Ils utilisent un protocole proactif pour avoir des informations sur les voisins les plus proches (au maximum les voisins à deux sauts).

Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes.

Ce type de protocole s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs et proactifs en même temps (messages de contrôle périodique, le coût d'ouverture d'une nouvelle route).

Plusieurs protocoles hybrides existent dont le **CBRP** et le **ZRP** (Zone Routing Protocol) .

5. La sécurité dans les réseaux ad hoc :

5.1. La sécurité des réseaux :

La sécurité est une combinaison de techniques et procédures qui assurent la Confidentialité, l'authentification, l'intégrité et la non répudiation :

- **La confidentialité :** assure que seuls les acteurs de la transaction sont en mesure de comprendre les données secrètes échangées.

- **L'authentification :** consiste à vérifier l'identité de l'émetteur auprès du récepteur pour interdire aux intrus d'injecter des messages falsifiés.

- **L'intégrité :** garantit que les données échangées n'ont pas été altérées ou modifiées de manière inattendue.

- **La non-répudiation :** assure qu'un message envoyé ne sera pas nié par son expéditeur.

5.2. La sécurité du routage dans les réseaux ad hoc : [9]

Dans la plupart des travaux sur les protocoles de routage, il est supposé que les entités sont altruistes, c'est-à-dire qu'elles sont pleinement coopératives et qu'elles participent honnêtement aux opérations de routage qui leur incombent. En particulier, les documents de spécification de ces protocoles ne décrivent actuellement aucune mesure de sécurité : il y est seulement fait état des différentes vulnérabilités aux quelles ils sont sujets. Or en raison de leurs caractéristiques, les réseaux ad hoc présentent tout autant de situations adverses que les réseaux filaires.

Dans le contexte des réseaux ad hoc, la décentralisation est poussée à son extrême. Pour aboutir à une auto organisation du réseau, les services gestion du réseau, dont le routage multi-sauts, sont assurés par les entités elles-mêmes. Ces entités, éventuellement indépendantes les unes des autres, font partie inhérente de l'infrastructure de communication, ce qui soulève de nombreux défis de sécurité.

Les solutions basées uniquement sur la mise en place d'un périmètre de sécurité sont insuffisantes, car l'indépendance et le manque de protection physique des entités font que l'exécution correcte des opérations de gestion de réseau n'est plus garantie.

En outre, l'absence d'une entité centrale entraine la remise en question des architectures et des protocoles de sécurité retenus dans le contexte des réseaux filaires. Par ailleurs, l'utilisation de liaison sans fil introduit de nouvelles vulnérabilités puisque les communications sont exposées aux observations par n'importe quelle entité, dans la mesure où elle est munie d'un récepteur radio. Ici, le câblage physique ne représente plus un obstacle pour permettre les écoutes indésirables.

La flexibilité offerte grâce à l'auto organisation et aux communications sans fil rend les réseaux ad hoc particulièrement vulnérables à de nouvelles attaques.

Dans la suite de cette section, nous présentons une description de ces vulnérabilités et attaques.

5.3. Description des vulnérabilités :[3]

La première vulnérabilité de ces réseaux est liée à la technologie sans fil. Quiconque peut potentiellement écouter ou perturber les messages échangés. Et ceci, même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges.

Les nœuds eux-mêmes sont des points de vulnérabilités du réseau car un attaquant peut compromettre un élément laissé sans surveillance.

Les mécanismes de routage sont d'autant plus critiques dans les réseaux ad hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

Contrairement au réseau filaire, il n'est pas nécessaire de pénétrer dans un local physique pour accéder au réseau. Si l'authentification est mal gérée, un attaquant peut s'attacher au réseau sans fil et injecter des messages erronés, l'authentification des parties apparaît donc comme la pierre angulaire d'un réseau sans fil ad hoc sécurisé.

Une fois les parties authentifiées, la confidentialité reste un point important étant donné que les communications transitent via les airs et sont donc potentiellement accessibles à toute personne.

L'intégrité des nœuds est primordiale car les éléments d'un réseau ad hoc sont moins sujets à surveillance. En effet, ils ne sont pas confinés dans un bureau mais transportés par leurs propriétaires et peuvent donc être momentanément égarés.

La disponibilité est une propriété difficile à gérer dans les réseaux ad hoc étant donné les contraintes qui pèsent sur ces réseaux :

• Topologie dynamique.
• Ressources limitées sur certains nœuds de transit.
• Communications sans fil pouvant être facilement brouillées ou perturbées.

5.4. Description des attaques : [7]

Une attaque contre un réseau vise essentiellement à compromettre la confidentialité et l'intégrité des informations en transit, ou de manière plus générale, à perturber son bon fonctionnement.
Dans les réseaux ad hoc, selon le niveau d'intrusion des actions menées par un attaquant, on distingue généralement deux catégories d'attaques : les attaques passives et les attaques actives.
Une attaque est passive lorsqu'un nœud non autorisé obtient un accès à des informations échangées sur le réseau, et ça sans altérer les opérations du réseau.

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

En outre, selon le domaine d'appartenance d'un nœud, les attaques actives peuvent elles mêmes être classées en deux catégories, à savoir les attaques externes et internes. Tandis que les attaques externes sont réalisées par des nœuds qui n'appartiennent pas au domaine du réseau.

6. Etat de l'art des solutions : [3]

6.1. Solutions pour l'authentification :

L'absence d'infrastructures centralisée dans les réseaux ad hoc compromet l'utilisation directe des systèmes d'authentification basés sur la cryptographie à clé publique.

En effet, ces systèmes d'authentification supposent l'utilisation de certificats établis par une autorité centrale.

Le certificat signé par l'autorité centrale, permet de garantir qu'une clé publique appartient bien à son propriétaire et non à un usurpateur. L'opération de vérification de certificat ne se limite pas à contrôler la signature de l'autorité centrale.

Il existe trois grands courants dans le domaine de l'authentification pour les réseaux ad hoc. Deux de ces orientations se basent sur l'établissement d'une clé secrète permettant par la suite l'authentification des participants.

Toute la complexité réside en la manière d'établir cette clé. Les deux modèles basés sur clé secrète sont :

- The Duckling Security Policy Model : Le modèle d'authentification élaboré par Ross Anderson et Frank Stajano.
- The key agreement : Les participants s'entendent sur une clé secrète.
- Le troisième axe de recherche pour l'authentification au sein de réseaux ad hoc , se base sur la cryptographie à clé publique et cherche à s'affranchir du besoin d'une entité centrale de certification.
- Clé Secrète Commune (Key Agreement)

Key agreement : Les recherches en matière de key agreement dans les réseaux ad hoc se focalisent sur la manière d'établir une clé commune entre plusieurs participants qui ne se connaissent pas à priori.

Les participants établissent entre eux une clé secrète leur permettent de s'authentifier afin de communiquer de manière sécurisée.
Dans ce cas, la clé secrète est fournie aux participants du réseau ad hoc via un canal supposé sur.

C'est le cas lorsque des collègues souhaitant établir une communication sure entre eux à l'occasion d'une réunion dans une salle de conférence close, distribue un mot de passe inscrit sur un morceau de papier qui fait le tour de la salle.
La difficulté de ce mode de fonctionnement est de trouver un canal sécurisé pour distribuer la clé. Lorsqu'il n'y a que deux nœuds, le protocole de Diffie-Hellman [1] peut être utilisé.

6.2. **Solution pour l'intégrité Physique des Nœuds** :

L'intégrité des nœuds du réseau dépend fortement de capacités physiques de ce nœud à résisté à des attaques qui permettraient à un attaquant de modifier le fonctionnement du nœud afin de corrompre.

6.3. Solution pour l'intégrité et l'authentification des messages :

Les moyens classiques pour assurer l'intégrité et l'authentification des messages échangés par les nœuds d'un réseau sont l'utilisation de signature numériques ou de MACs.
Les signatures numériques s'appuient sur la cryptographie à clé publique.

Un nœud possède une clé publique qui sert à ses correspondants pour chiffrer des messages lui étant destinés et le nœud déchiffre les messages qu'il reçoit avec sa clé privée.

Dans le cas de la signature, le nœud utilise une clé privée (dédiée à la signature) pour signer un message. Le destinataire du message déchiffre la signature avec la clé publique.

6.4. Solution pour la confidentialité :

La confidentialité dans les réseaux ad hoc est d'abord traitée par l'utilisation de transmission par saut de fréquences (frequency hoping). Les données sont transmises sur une séquence de fréquences définies pseudo aléatoirement.

L'attaquant doit connaître cette séquence pour pouvoir se synchroniser en réception.
Une fois l'authentification des participants clairement établie, les outils cryptographiques permettent de rendre les communications confidentielles.

Toutefois, étant donné qu'une des contraintes des réseaux ad hoc est de devoir être adaptable à des nœuds ayant de faibles capacités de calcul, la cryptographie symétrique sera préférée à la cryptographie à clé publique, cette dernière nécessite beaucoup plus de puissance de calcul.

6.5. Solution pour la disponibilité :

Il n'existe aucun moyen de contrer un déni de service sur le canal radio provoqué par un attaquant puissant ayant les moyens de brouiller efficacement la totalité du spectre radio.

Néanmoins, des techniques comme le saut de fréquence permet de se prémunir contre des attaques ayant des capacités plus réduites.

En effet, ces techniques permettent une transmission des données sur un large spectre de fréquence. Pour être efficace un attaquant doit donc être capable de brouiller l'étendue des fréquences utilisées.

7. Conclusion :

Les réseaux mobiles Ad Hoc se présentent comme une technologie récente des réseaux mobile. Ces réseaux se caractérisent par l'absence de toute infrastructure.
Etant par définition sans infrastructure, ces réseaux ne peuvent pas bénéficier des services de sécurité offerts par des équipements dédiés comme les pare feux et les services d'authentification.

D'où, la nécessité d'avoir des systèmes de détection d'intrusions pour limiter et se prévenir des activités malveillantes en tenant compte des caractéristiques de ces réseaux.

Et pour cela, dans notre prochain chapitre nous intéressant aux systèmes de détection d'intrusion dans les réseaux ad hoc.

1. Intrusion : [9]

C'est un accès interdit avec ou sans intention à un système d'information, qui peut être une activité au sein du système ou/et une activité contre ce système.
Une intrusion peut être aussi toute action visant à compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource.

2. La détection d'intrusions : [23]

2.1. Définition

Détection des intrusions est le processus de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, intégrité, disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau.

L'intrusion est causée par les attaques accédant au système via l'Internet, autorisée l'utilisateur du système qui essayer à gagner les privilèges supplémentaires pour lesquels ils n'ont pas autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés.

Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés.

3. Nécessité et qualités requises des IDS : [9]

Un système de détection d'intrusions doit être mis en place pour capturer des données d'audit et exécuter l'analyse du trafic pour détecter si le réseau ou un nœud spécifique est soumis aux attaques afin de prendre des mesures pouvant réduire au minimum les dommages et informer les autres nœuds légitimes.
Ainsi, pour limiter les attaques exploitant les vulnérabilités des réseaux ad hoc, il est nécessaire que le mécanisme de sécurité choisi puisse accomplir les différentes fonctions principales telles que :

- Surveiller et analyser les activités système et celles des utilisateurs
- Surveiller les configurations système et les vulnérabilités.
- Evaluer l'intégrité des fichiers et données critiques.
- Reconnaître les attaques connues selon leurs signatures.
- Analyser statistiquement les activités anormales.
- Fournir des informations et des documents sur les attaques détectées pour améliorer les diagnostics, la réparation et la correction.

Les systèmes de détection d'intrusions actuels tendent à garantir les cinq propriétés suivantes :

1. **Exactitude de détection :** elle se traduit par une détection parfaite des attaques avec un risque minimal de faux positifs.

2. **Performance :** une détection rapide des intrusions avec une analyse approfondie des événements est indispensable pour mener une détection efficace en temps réel.

3. **Complétude :** une détection exhaustive des attaques connues et inconnues.

4. **Tolérance aux fautes :** les systèmes de détection d'intrusions doivent résister aux attaques ainsi qu'à leurs conséquences.

5. **Rapidité :** une analyse rapide des données permet d'entreprendre instantanément les contre mesures nécessaires pour stopper l'attaque et protéger les ressources du réseau et du système de détection d'intrusions.

Afin d'assurer ces qualités, les systèmes de détection d'intrusions implantent différentes approches de détection.

4. Architecture d'un IDS :

Un système de détection d'intrusions (IDS) est composé de trois fonctions fondamentales :

4.1. Une source d'information :

ou senseur des sources différentes des informations d'événements sont habitués à déterminer si une intrusion est occupée ou non.
Ces sources peuvent être retiré à partir des niveaux différents du système, avec le réseau, centre du serveur, et les applications surveillant la plus commune.

4.2. Module de traitement d'alertes

Ce module est responsable du traitement et de l'analyse des activités collectées par les senseurs. Il est composé par trois éléments : l'analyseur, la base de connaissances et l'organe de réaction.

4.2.1. Analyseur

Ce composant représente le moteur de détection caractérisé par une méthode de détection qui permet d'analyser les données collectées par le senseur suite à la recherche de signes d'intrusions.

Afin de pouvoir prendre une décision, ce composant a recours en général à une base de connaissances.

4.2.2. Base de connaissances :

Les informations identificatrices d'intrusions ou le comportement normal d'un utilisateur sont stockées dans une base de données.

Le module de traitement des alertes peut lui-même stocker, dans une base de données, des informations sur les activités collectées si cette dernière est utile pour détecter d'éventuelles intrusions.

4.2.3. Organe de réaction :

Lorsque l'analyseur considère une activité comme intrusive, une alerte est générée par l'organe de réaction.

Un IDS peut coopérer avec le reste des équipements réseau, ainsi les alertes peuvent être envoyées aux différents autres équipements de sécurité du réseau en vue de prendre la décision nécessaire.

4.3. Module de réponse :

Le module de réponse consiste à répondre à l'attaque en se référant au résultat de traitement. La réponse se présente sous forme d'un rapport généré pour être exploité par un outil automatisé ou par un analyste.

Certains IDS se contentent de déclencher une alarme alors que d'autres prennent des mesures correctives.

5. Classification des IDS :

Les systèmes de détection d'intrusions utilisent diverses techniques de détection et définissent plusieurs modules qui effectuent des tâches distinctes comme la collecte des informations, l'analyse des données, la corrélation des événements et la génération des alarmes.

Selon Debar les cinq critères pour classer les systèmes de détection d'intrusion sont : **[9]**

5.1. Source d'information :

Les données analysées partagent les systèmes de détection d'intrusions en deux catégories :

5.1.1. Les systèmes de détection d'intrusions réseaux : filtre le trafic réseau et se déploie généralement dans des endroits précis du réseau.

Et pour cela on citera quelques avantages et inconvénients de N-IDS :

Avantage de N-IDS :

- Le N-IDS peut surveiller un grand réseau.
- L'déploiement de N-IDS a peu d'impact sur un réseau existant. L'N-IDS sont habituellement des dispositifs passifs qui écoutent sur un fil de réseau sans interférer l'opération normale d'un réseau. Ainsi, il est habituellement facile de monter en rattrapage un réseau pour inclure IDS avec l'effort minimal.

- N-IDS peut être très sûr contre l'attaque et être même se cache à beaucoup d'attaquants

Inconvénients

- Il est difficile à traiter tous les paquets circulant sur un grand réseau. De plus il ne peut pas reconnaître des attaques pendant le temps de haut trafic.
- N-IDS ne peut pas analyse des informations chiffrées (cryptées). Ce problème a lieu dans les organisations utilisant le VPN.
- La plupart de N-IDS ne peuvent pas indiquer si un attaque réussi ou non. Il reconnaît seulement que une attaque est initialisée. C'est-à-dire qu'après le N-IDS détecte une attaque, l'administrateur doit examiner manuellement chaque host s'il a été en effet pénétré.

5.1.2. les systèmes de détection d'intrusions hôtes : analyse les données des journaux de sécurité établis par les systèmes d'exploitation et les applications qui tournent sur les machines. Ces IDS sont déployés directement sur les hôtes du réseau.

Et pour cela on citera quelques avantages et inconvénients de H-IDS :

Avantages

- Pouvoir surveiller des événements local jusqu'au host, détecter des attaques qui ne sont pas vues par N-IDS
- H-IDS n'est pas atteint par le réseau commuté.
- Lors que H-IDS marche sur la traîné de l'audit de SE, ils peuvent détecter le Cheval de Troie ou les autres attaques concernant à la brèche intégrité de logiciel.

Inconvénients

- H-IDS est difficile à gérer, et des informations doivent configurées et gérées pour chaque host surveillé.
- Puisque au moins des sources de l'information pour H-IDS se résident sur l'host de la destination par les attaques, le IDS peut être attaqué et neutralisé comme une partie de l'attaque.
- H-IDS n'est pas bon pour le balayage de réseau de la détection ou l'autre tel que la surveillance qui s'adresse au réseau entier parce que le H-IDS ne voit que les paquets du réseau reçus par ses hosts.
- H-IDS peut être neutralisé par certaine attaque de DoS.

5.2. Réponses des IDS :

Les systèmes de détection d'intrusions émettent des réponses actives qui influent directement la source d'attaque, comme ils peuvent se restreindre à des réponses passives qui inscrivent l'événement suspect.

Une liste de réponses actives et passives est présentée dans le tableau suivant :

Réponse passive	Réponse active
➔ Émettre un rapport ➔ Générer une alarme ➔ Activer un archivage plus détaillé ➔ Activer un archivage à distance ➔ Créer des fichiers de sauvegarde	➔ Bloquer le compte d'un utilisateur ➔ Suspendre des processus malveillants ➔ Terminer une session ➔ Bloquer une adresse IP ➔ Arrêter la machine ➔ Déconnecter la machine du réseau ➔ Mettre hors service les ports et les services attaqués ➔ Avertir l'utilisateur ➔ Tracer l'origine de la connexion ➔ Forcer une nouvelle authentification ➔ Restreindre les activités d'un utilisateur

Tableau : réponse aux attaques des systèmes de détection d'intrusions

5.3. Paradigme de détection :

La détection d'intrusions s'effectue en analysant l'état courant du système ou en supervisant les transitions des états normaux aux états dangereux. Durant ces deux types d'inspection, l'IDS récupère les informations en interrogeant directement le système ou en écoutant passivement les événements.

5.4. Mode de supervision :

L'analyse assurée par un système de détection d'intrusions peut être continue ou périodique dans le temps.

5.5 Méthodes de détection d'intrusions

La méthode d'analyse est le principal critère pour sélectionner un IDS.

Deux approches existent sont : l'approche comportementale et l'approche par scénarios.

5.5.1. L'approche comportementale ou par anomalie : se base sur l'observation du comportementale de l'utilisateur et sur la détection d'un comportement déviant par rapport à ses habitudes. Cette modification du comportement peut traduire une tentative d'intrusion, due soit à une usurpation de l'identité de l'utilisateur, soit à l'exécution par celui-ci de commandes non autorisées. Et permet de détecter des attaques inconnues.

5.5.2. L'approche par scénarios : Contrairement à la détection d'intrusions par anomalie qui apprend le comportement normal, elle consiste à identifier chaque attaque par une signature propre et ensuite à rechercher dans les fichiers d'audits du système les traces de ces signatures.

On peut noter que cette approches par scénario nécessite de connaitre la signature d'une attaque avant de pouvoir la détecter.

6. Détection d'intrusions dans les réseaux Ad Hoc :

Pour répondre aux problèmes liés aux réseaux Ad Hoc, plusieurs approches ont été conçues pour ces réseaux.

Alors dans cette partie, nous allons présenter les modèles les plus importants des systèmes de détection d'intrusion pour les réseaux Ad Hoc :

6.1. Les IDS Individuels :

Les IDS Individuels est la première approche adoptée pour les réseaux Ad Hoc. Cette approche se base sur le fait que chaque nœud n'a confiance qu'en soi même.

En effet, l'ouverture du médium du réseau Ad Hoc et la facilité de s'introduire dans un tel réseau ainsi que la difficulté de protéger les terminaux mobiles d'être captés par des utilisateurs malveillants influe sur le niveau de confiance entre les différents nœuds.

Puisque les informations circulant entre les différents nœuds peuvent être transformés et captées par tout nœud situé dans la zone de transmission de l'un des nœuds communicants, le travail coopératif est écarté pour ce type d'IDS et le processus de détection d'intrusions se déroule localement sans aucun échange d'informations entre les nœuds du réseau (voir Figure II.1).

Ces IDS sont caractérisés par une indépendance entre les différents nœuds dans le processus de détection. En effet, chaque nœud ne s'occupe que de sa protection.

Ils peuvent utiliser les techniques comportementales ou par signatures. Le problème pour ces systèmes est leur faiblesse contre les attaques distribuées.

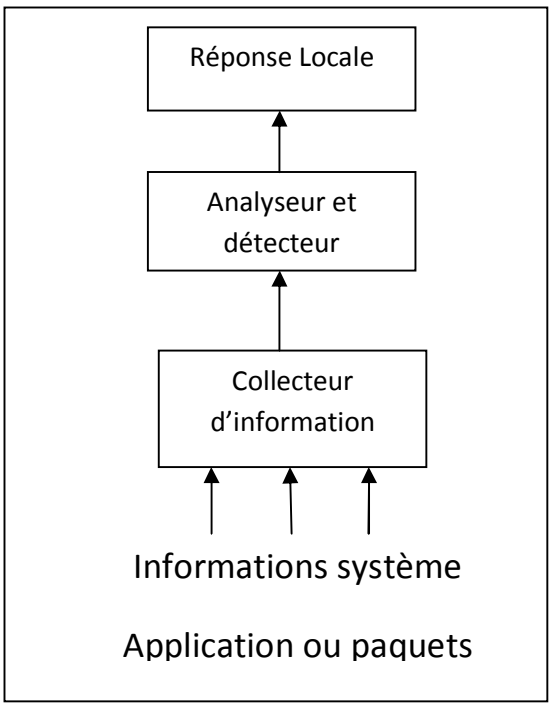


Figure II.1 : Architecture d'un IDS Individuel

6.2. Les IDS coopératifs :

Avec la méthode de détection, les IDS trouvent des insuffisances. Comme exemple, un H-IDS est incapable de détecter les attaques réseaux, et le N-IDS est incapable de déterminer les violations au niveau des machines.
Donc, aucun type ne peut tout seul assurer la sécurité. D'où, la nécessité d'avoir une coopération entre ces IDS pour remédier à ces insuffisances et pour avoir une vision globale sur les intrusions.

Les IDS coopératifs sont caractérisés par une coopération entre les nœuds voisins si la détection est inaccomplie individuellement. Cette coopération est réalisée par l'échange des informations ou encore des alertes.
Si un nœud détecte une intrusion avec une forte évidence, il peut indépendamment déterminer l'attaque. Sinon s'il détecte une intrusion avec une faible évidence, il peut lancer un procédé global coopératif de détection d'intrusion.

L'architecture des IDS coopératifs présente 6 modules (voir figure II.2).

Dans la base de gestion des alertes, les alertes des différents nœuds sont regroupées ensemble, transformées en un seul format et enregistrées dans une base de données d'alertes.

Dans le deuxième module, il y a un accès sur la base de données pour la génération des groupes d'alertes. Ces groupes sont des ensembles d'alertes qui ont une même occurrence d'attaque.

Le module de fusion consiste à créer, à partir de chaque groupe, une alerte globale qui représente les informations contenues dans les différentes alertes.

Le module de corrélation d'alertes, a pour but de déterminer, à partir de ces alertes globales, le scénario d'attaque réalisé par l'intrus.

De cette façon, nous avons une vue globale sur l'intrusion et nous pouvons par la suite réagir contre cette attaque.

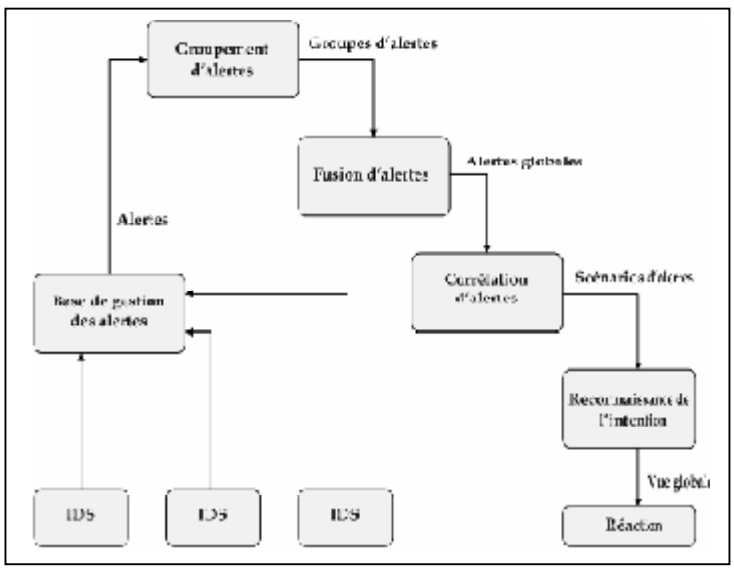


Figure II.2. Architecture d'un IDS coopératifs

En effet, le problème pour ces IDS est qu'ils causent la dégradation des performances du réseau par le trafic échangé entre les différents agents IDS en plus du gaspillage de la bande passante.

La coopération entre les IDS repose sur des techniques différentes comme les agents mobiles (Voir Figure II.3).

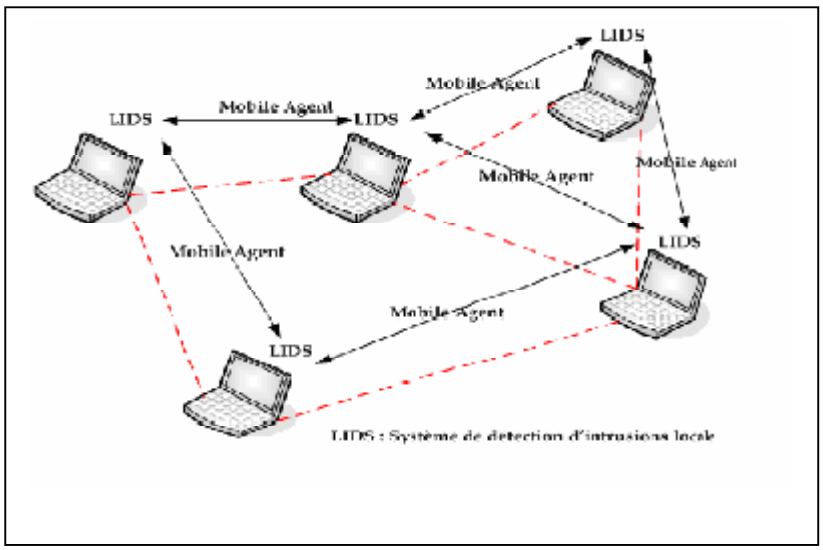


Figure II.3 Architecture d'un IDS coopératifs par un agent mobile

6.3. Les IDS hiérarchiques :

Pour remédier à l'absence de coopération entre les différents IDS proposés pour les réseaux Ad Hoc, une autre méthode a été proposée pour la détection d'intrusions dans les réseaux Ad Hoc.
Cette approche se base sur la division du réseau Ad Hoc en un ensemble de groupes (clusters) ayant chacun un seul chef de groupe déterminé par un algorithme coopératif entre les différents nœuds. Ceci est en fait intéressant pour minimiser l'utilisation des ressources du réseau.

Les systèmes de détection d'intrusions hiérarchiques essayent alors de réduire la coopération entre les nœuds et ceci par la division du réseau en groupes (voir Figure).

Dans ce cas, la coopération est effectuée entre le chef de groupe élu et chacun des membres du même groupe et ceci dans les réseaux Ad Hoc multicouches.
Ainsi une alerte est reportée au chef du groupe si un nœud membre de ce groupe n'arrive pas à détecter seul une attaque, soit qu'il manque d'autres informations, soit que la certitude de détection est inférieure à un certain seuil.

Cette approche minimise ainsi la surcharge du réseau puisque la coopération est réduite entre les chefs de groupes et leurs membres. Cependant, elle ne permet pas d'avoir une vision globale du réseau à cause de l'absence de coopération entre les différentes cellules et reste par la suite inefficace contre certaines attaques distribuées.

Le chef de groupe dans ce type d'IDS joue le rôle de l'administrateur de son groupe et permet de surveiller ce qui se passe au sein de sa cellule. D'autre part, l'agent de détection est

distribué dans tous les nœuds du réseau alors que la réponse aux alertes se fait d'une manière hiérarchique suivant le niveau de certitude de détection.

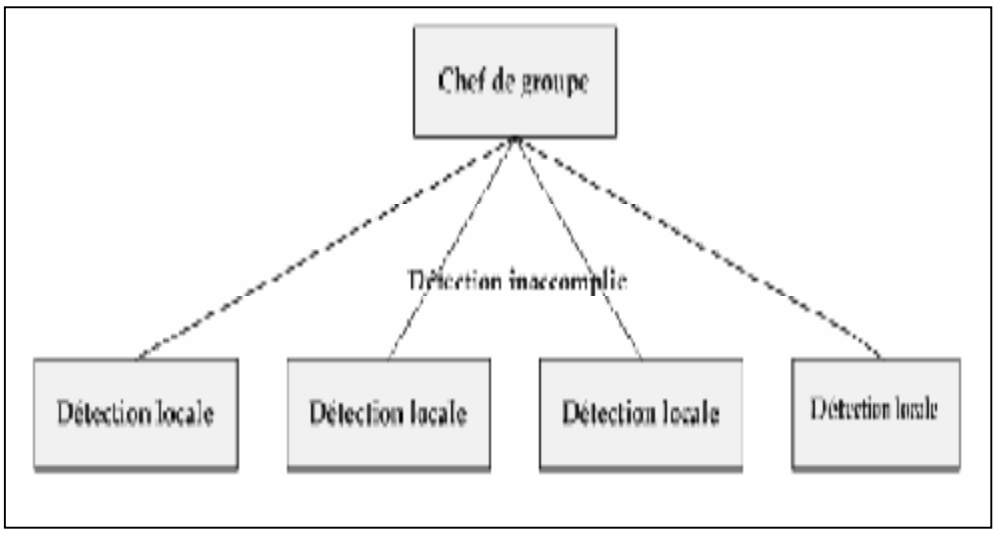


Figure II.4 . Architecture d'un IDS hiérarchique

Les techniques de détection d'intrusions qui ont été proposées pour les réseaux ad hoc ne sont pas très fiables mais les IDS continuent d'évoluer pour répondre aux exigences technologiques et offrent un éventail de fonctionnalités capables de satisfaire les besoins de tous les types d'utilisateurs. Pour représenter le comportement normal attendu par un protocole, des techniques basées sur la spécification ont été proposées.

1. **Architecture hiérarchiqque** :

Stamouli [14] a proposé un système de détection RIDAN « Real-time Intrusion détection ad hoc network" qui base sur une architecture hiérarchique :

Il propose une modélisation du protocole AODV sous la forme d'une machine à états finis . Dans leur approche, il distingue deux types de nœuds, les nœuds ordinaires et les nœuds moniteurs. Ce sont ces derniers qui ont pour responsabilité de détecter les anomalies dans les traces observées sur le réseau, en utilisant la machine à états finis d'AODV comme référence. Certaines hypothèses fortes telles que l'unicité des adresses MAC (servant à identifier un nœud à l'origine d'une anomalie) font que cette approche n'est pas viable dans le contexte des réseaux ad hoc.

2. Présentation de système de détection RIDAN:

Le système RIDAN est basé sur la recherche présentée dans « l'analyse en temps réel pour détecter des attaques du protocole de routage d'état de liens, alors que son exécution vise spécifiquement le protocole de routage AODV. La raison pour laquelle il peut être classifié comme modèle d'architecture et il n'affecte aucun changement au protocole de routage fondamental mais concerne simplement le trafic de routage et d'application. Ainsi, le système de sécurité fonctionne dans une couche différente sans interférer l'opération normale du protocole de routage AODV. Sachant que le système RIDAN n'utilise aucun mécanisme cryptographique pour assurer la protection contre des activités malveillantes, il ne présente aucun frais additionnel de calcul au processus de routage. En outre, il n'exige pas l'envoi de paquets additionnels, ainsi il ne consomme pas la largeur de bande disponible.

Le système RIDAN utilise les machines à états finis synchronisées pour définir formellement les attaques contre le protocole de routage AODV.

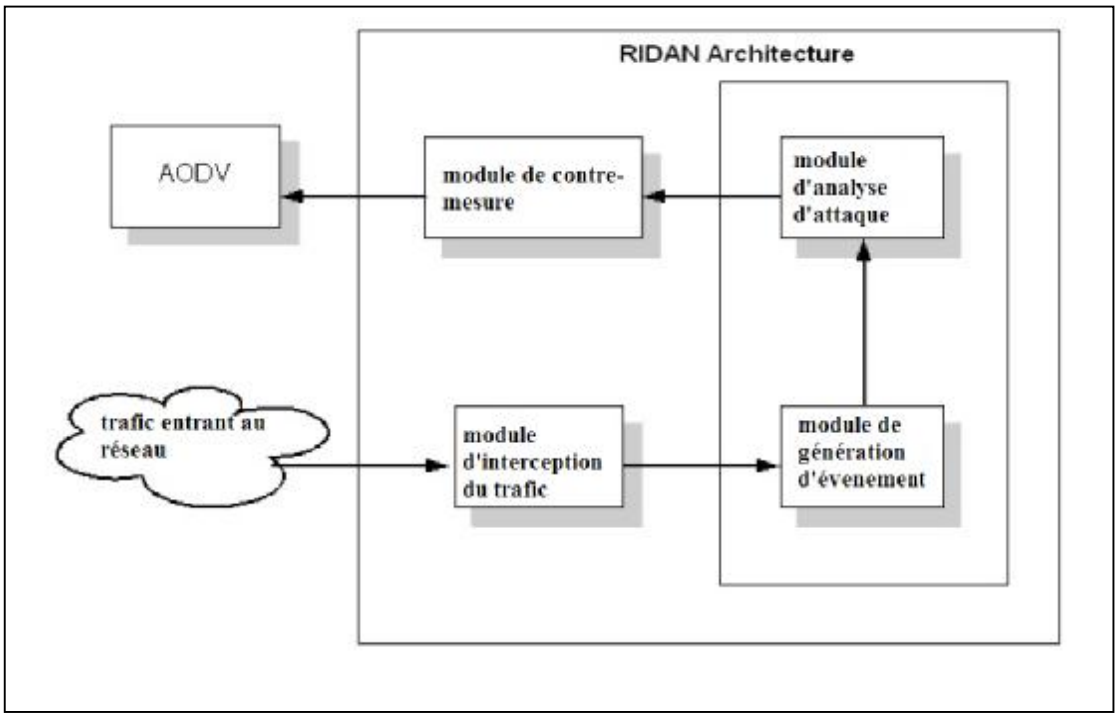


Figure III.1. Architecture du système RIDAN

La figure illustre les composants de l'architecture du système RIDAN et montre l'action logique du système entre le module d'interception du trafic et le module de contre-mesures via la machine à états finis.

Le module d'interception du trafic (trafic Interception Module) capture ou intercepte le trafic entrant au réseau et sélectionne ou choisit les paquets qui doivent être traités.

Le module de génération d'événements (Event Genaration Module) est responsable de soustraire l'information essentielle exigée par le module d'analyse d'attaque (attack Analysis Modul) pour déterminer s'il y a une activité malveillante dans le réseau.

Le module de génération d'événements et le module d'analyse d'attaque sont réalisés par l'utilisation de machines à états finis synchronisées. Le composant final de l'architecture de RIDAN est le module de contre-mesures (Counter measure Module).

Ce module se charge de prendre les mesures ou actions appropriées afin d'assurer l'exécution du réseau avec un minimum de performance acceptable. Ainsi, les composants du système de détection d'intrusions RIDAN fonctionnent entre le trafic du réseau et le protocole de routage et ceci n'exigeant aucune modification sur le protocole de routage qui est utilisé dans le réseau.

Le système de détection d'intrusions RIDAN fonctionne localement dans chaque nœud participant et analyse exclusivement le trafic qu'il observe. Ainsi, le système RIDAN est un système de détection d'intrusions basé sur l'hôte (H-IDS). L'opération du système est terminée

quand un nœud malveillant est détecté, toutefois pour fournir une solution plus complète, les nœuds sur alarme prennent des contre-mesures pour s'occuper de l'isolement du nœud se conduisant malveillant et garder l'exécution du réseau dans des limites acceptables.

Comme il est présenté dans ce chapitre, le système de détection d'intrusions RIDAN a des taux d'exactitude élevés en détectant les nœuds malveillants et les contre-mesures prises par les nœuds individuellement pour permettre au réseau de résister aux attaques agressives et d'assurer le bon fonctionnement du réseau mobile ad hoc.

3. Les machines à états finis

Les machines à états finis sont employées pour spécifier le comportement dynamique de certains systèmes utilisés pour décrire certaines parties des interfaces utilisateurs. Les automates à états finis sont représentés graphiquement par des diagrammes de transition d'états, graphes orientés dont les nœuds sont des états et les arcs de transitions. Un état est un ensemble de valeurs qui caractérise le système à un moment donné dans le temps. Une transition d'état est une relation entre deux états indiquant un changement d'état possible, et qui est annotée pour indiquer les conditions et les sources de déclenchement (événements) et les opérations qui en résultent (sorties).

Les états de la machine correspondent aux états du système en voie de compromission et ils contiennent des assertions qui doivent être vérifiées pour pouvoir transiter d'un état à un autre. Les arcs sont étiquetés par des événements qui forment le scénario d'attaque. Le système de détection d'intrusions RIDAN implante cette approche pour détecter les attaques sur le réseau. Leur modélisation transforme l'infrastructure réseau en un hypergraphe dont les nœuds sont des interfaces réseaux et les arcs sont des hôtes et des liens réseau.

3.1. Objectifs :

Une énumération des objectifs du système peut nous aider dans le processus d'évaluation du système de détection d'intrusions RIDAN . D'où les objectifs du système de RIDAN peuvent être résumés dans les points suivants :

. Créer un modèle de détection d'intrusion pour les réseaux ad hoc sans fil pouvant fonctionner avec les protocoles de routage soient réactifs ou proactifs.
. Choisir certaines des attaques actives qu'un noeud malveillant pourrait exécuter sur le protocole de routage AODV et les mettre en application.
. Décrire formellement la détection des attaques avec l'utilisation des machines à états finis synchronisées et les ajuster pour obtenir le maximum d'exactitude.

. Selon le trafic de routage observé plus d'une machine à états finis peut être déclenchée simultanément, toutefois le système dans son ensemble ne doit pas prendre des décisions contradictoires.
. Lors de détection d'activité malveillante, le noeud détecteur doit pouvoir prendre des contre-mesures pour assurer la continuité du fonctionnement du réseau.

. Les noeuds malveillants détectés seront pénalisés pendant une période finie et peuvent même être isolés pour toujours afin d'éviter l'impact les possibles fausses alarmes positives.

Pour tester le système de détection d'intrusion RIDAN , il a choisit trois types d'attaques qui ont un impact significatif sur les performances du réseau quand elles sont activement exécutées. Seulement une de ces attaques est spécifique au protocole de routage AODV, alors que les deux autres peuvent être appliquées sur n'importe quel protocole de routage.

4. Les attaques détectées

4.1. Les attaques liées au protocole de routage AODV :

4.1.1. Détection de l'attaque de modification du numéro de séquence :

Pour que le système de détection d'intrusion RIDAN puisse identifier correctement l'attaque de modification du numéro de séquence,

trois différentes machines à états finis synchronisées sont indispensables.

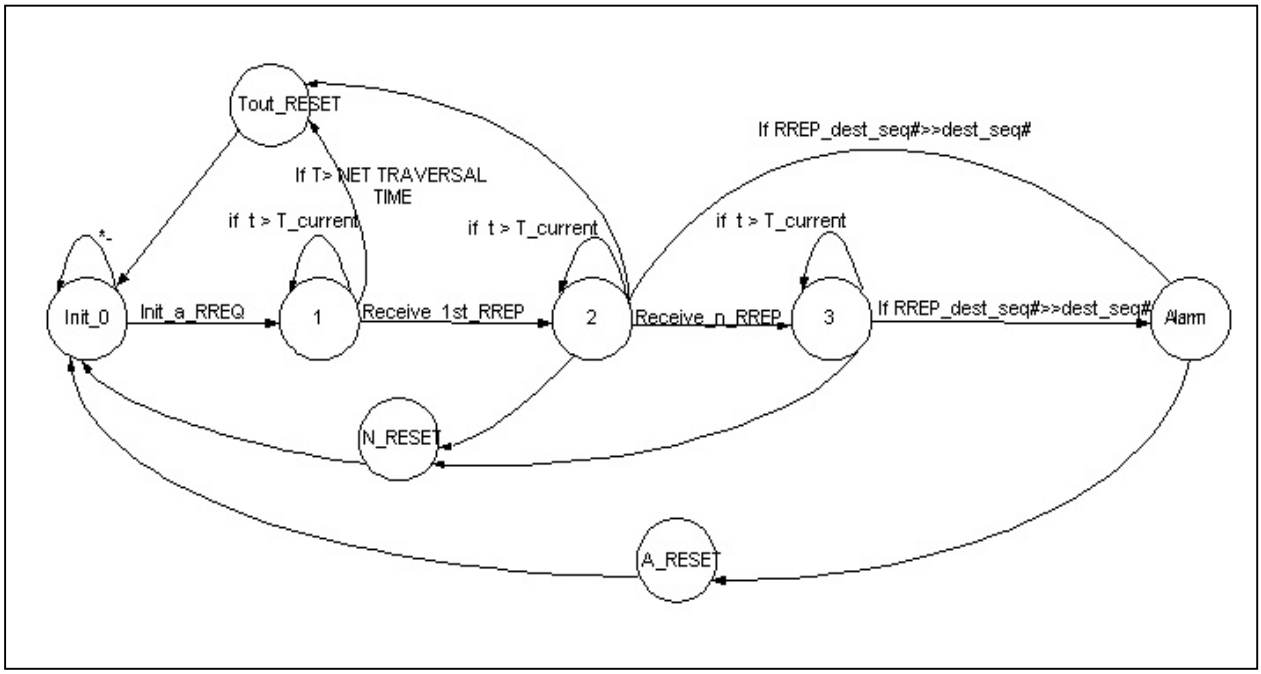


Figure III.2. : Première MEF de détection d'attaque de modification de numéro de séquence.

Dans la figure III.2 : la première MEF est graphiquement illustrée. Cette MEF est déclenchée à chaque fois qu'un noeud lance un procédé de découverte d'itinéraire (étape 1). Si un message RREP n'arrive pas au cours de la période de temps NET_TRAVERSAL_TIME définie intérieurement dans l'exécution du protocole AODV, la MEF (étape 2) passe à l'état de réinitialisation (Tout_RESET) et puis à son état initial (init_0). Sur la réception du premier paquet RREP (étape 3) il vérifie si le RREP_destination_sequence_number (RREP_dest_seq#) est supérieur à

l'original_sequence_number (orig_dest_seq #) inclus dans le RREQ. S'il est largement supérieur (étape 4), alors il entre directement dans son état d'alarme (Alarme). Et si tel n'est pas le cas, il attend dans le même état pendant un temps t (étape 5). Si le temporisateur expire sans recevoir un autre RREP (étape 6), il se déplace à son état de réinitialisation normale (N_RESET). Si avant expiration du temporisateur il reçoit un autre RREP, il vérifie la validité du numéro de séquence de destination et décide pareillement s'il doit se déplacer à l'état d'alarme. Quand une alarme se produit le noeud source sait que l'information contenue dans le RREP est fausse et qu'elle ne doit pas mettre à jour sa table de routage avec de fausses informations de routage. De l'état de l'alarme la MEF va reprendre son état initial (init_0) via l'état de remise de l'alarme (A_RESET).

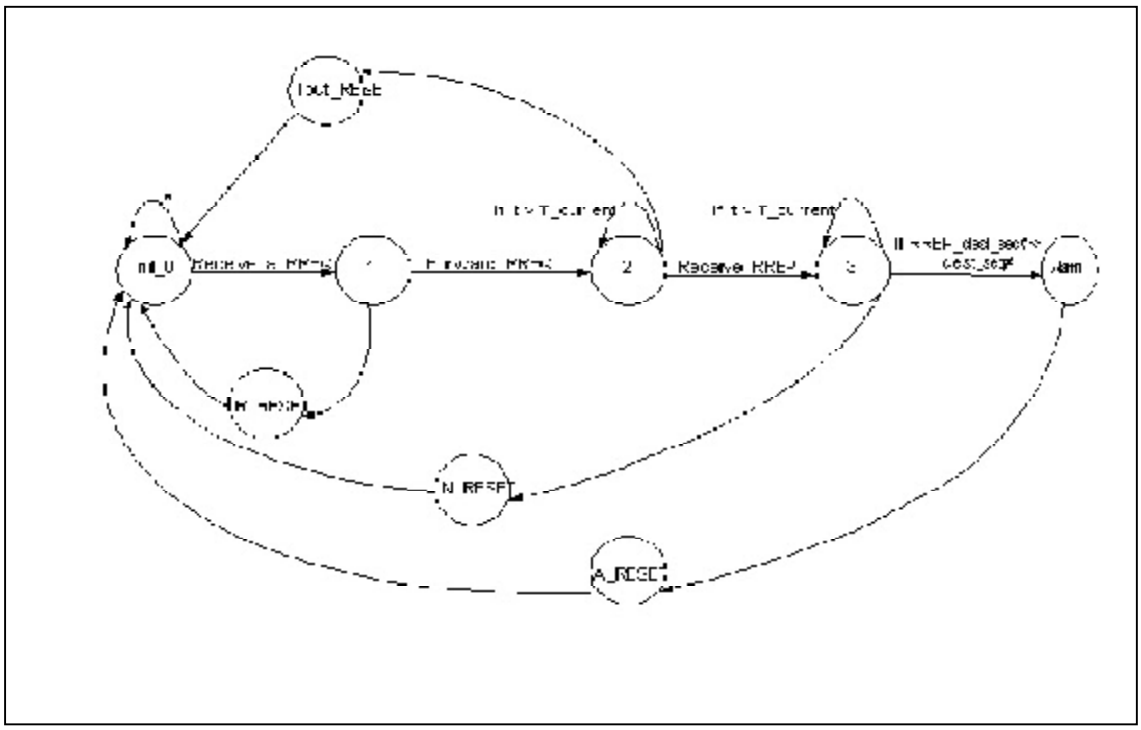


Figure III.3. : Deuxième MEF de détection d'attaque de modification de numéro de séquence.

La deuxième MEF (la figureIII.3) protège les nœuds intermédiaires qui reçoivent le RREQ lancé par le nœud source (étape 1). Ainsi, quand un nœud intermédiaire reçoit un message RREQ et ayant un itinéraire assez frais vers la destination il répond (étape 2) et la FSM se déplace à l'état REPLY_RESET (R_RESET). Au cas où le nœud intermédiaire n'aurait pas l'information nécessaire pour répondre à ce message RREQ, il expédie le paquet et se positionne à l'état 2 et la FSM reste à cet état pendant le temps ***t*** (étape 3). Si le temporisateur expire, il se déplace à l'état Tout_RESET (étape 4) et de nouveau à l'état initial init_0. Si dans les délais il reçoit un RREP (étape 5), il se déplace à l'état 3 et vérifie la validité du numéro de séquence de destination comme dans la MEF précédente. Si le numéro

de séquence est dans les délais acceptables, il passe à l'état N_RESET pour se mettre à l'état initial init_0 (étape 6). Au cas contraire, il passe à l'état Alarme (étape 7) et il n'ajoute pas le faux itinéraire dans sa table de routage. De l'état d'alarme la MEF est remise à l'état A_RESET (étape 8). Il est à noter que le nœud intermédiaire ne doit pas détruire le paquet RREP même contenant de fausses informations. Alternativement, il diffuse le paquet RREP de nouveau au nœud source qui déterminera lui-même si le paquet contient une information suspecte.

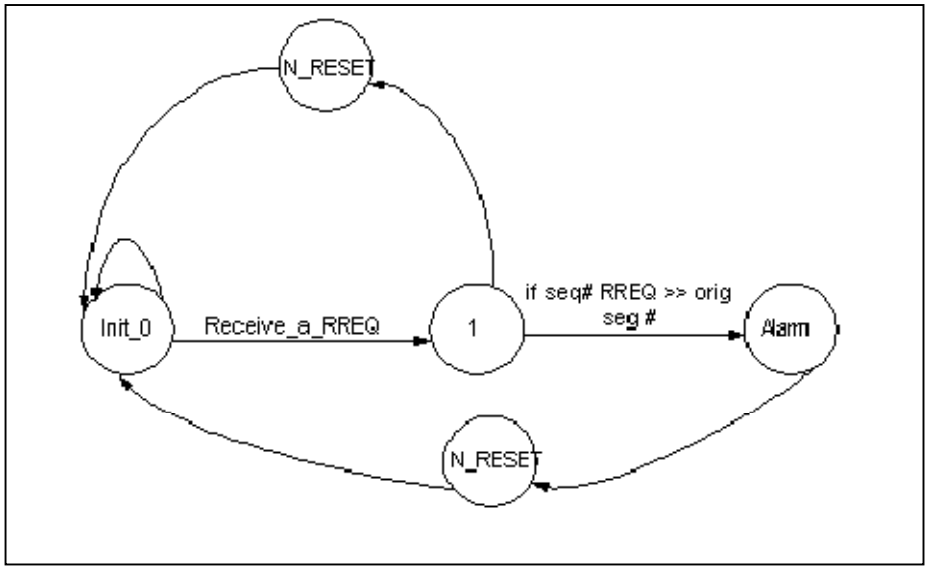


Figure III.4.: Troisième MEF de détection d'attaque de modification de numéro de séquence

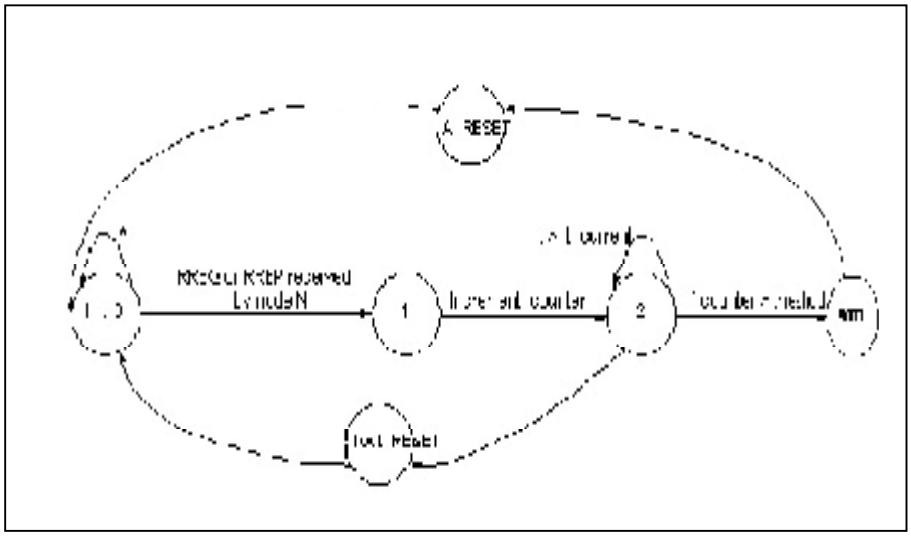
La troisième MEF représentée à la figure 3.5 est utilisée afin d'avoir un système complet pour la détection de cette attaque. Elle est déclenchée à chaque fois que le nœud destination reçoit un paquet RREQ (étape 1) pour une route qui lui est adressée. Si le numéro de séquence de destination contenu dans le message RREQ est égal à son propre numéro de séquence alors la MEF est réinitialisée normalement à l'état initial init_0 via l'état N_RESET (étape 2). Cependant, si le RREP_dets_seq# est beaucoup plus grand que celui (orig_dest_seq #) inclus dans le RREQ elle se met à l'état Alarme (étape 3) et il ne met pas à jour son numéro de séquence. Si cette MEF est déclenchée cela signifie que le nœud qui a lancé le procédé de découverte de route avait de fausses informations dans sa table de routage et il provient d'un nœud malveillant.

4.1.2. La détection d'attaque de destruction des paquets de routage :

Sachant que tous les nœuds participants au réseau opèrent en mode ‘’promiscuous’’, les nœuds voisins peuvent détecter si un nœud malveillant a expédié le paquet de routage ou pas.

Cependant, le nœud en question peut ne pas expédier le paquet de routage suite à la surcharge du trafic. Le système de détection d'intrusion pour empêcher les fausses alarmes provoquées

par la surcharge du trafic, le MEF se déplace d'abord à un état de pré alarme et dans cet état il diffuse le paquet de routage au nœud responsable encore.



La MEF incrémente le compteur à chaque fois qu'un nouveau paquet de routage est reçu du nœud spécifique. Il reste dans l'état 2 pendant le temps ***t*** (étape 2). Si le compteur atteint la valeur seuil alors cela signifie qu'il a détecté une génération de trafic anormale et il se déplace à l'état d'Alarme (étape 3). Dans cet état d'alarme, le nœud laisse tomber tout le trafic de routage entrant au nœud observateur pour un intervalle de temps fini de sorte qu'il ne consomme pas les ressources du réseau et du nœud .

Stamouli a implémenté et interpréter les résultats des différentes simulations faites sur le protocole de routage AODV normal, AODV sous attaque et AODV-RIDAN sous attaque. Effectuer avec le simulateur de réseau NS-2, AODV sous attaque de point de vue performance et réponse aux attaques actives.

Paramètres de simulation

Dans cette simulations, l'environnement est un réseau de taille 1000 x 1000 m, dans lequel se trouvent 31 noeuds. Ceux-ci sont soit 30 noeuds mobiles légitimes et un noeud malveillant responsable des attaques actives.
Il a effectuer des simulations d'une durée de 1000 secondes. Ces paramètres peuvent être trouvés dans le tableau

Paramètre	Valeur
Nombre de nœuds	31
Temps de simulation	1000sec
Topologie	1000*1000m

Mobilité des nœuds

Dans son simulations, il a fixé la vitesse maximale à 20m/s. Le temps de pause est, quant à lui, sauf mention explicite, de 10s. Ces paramètres sont repris au tableau

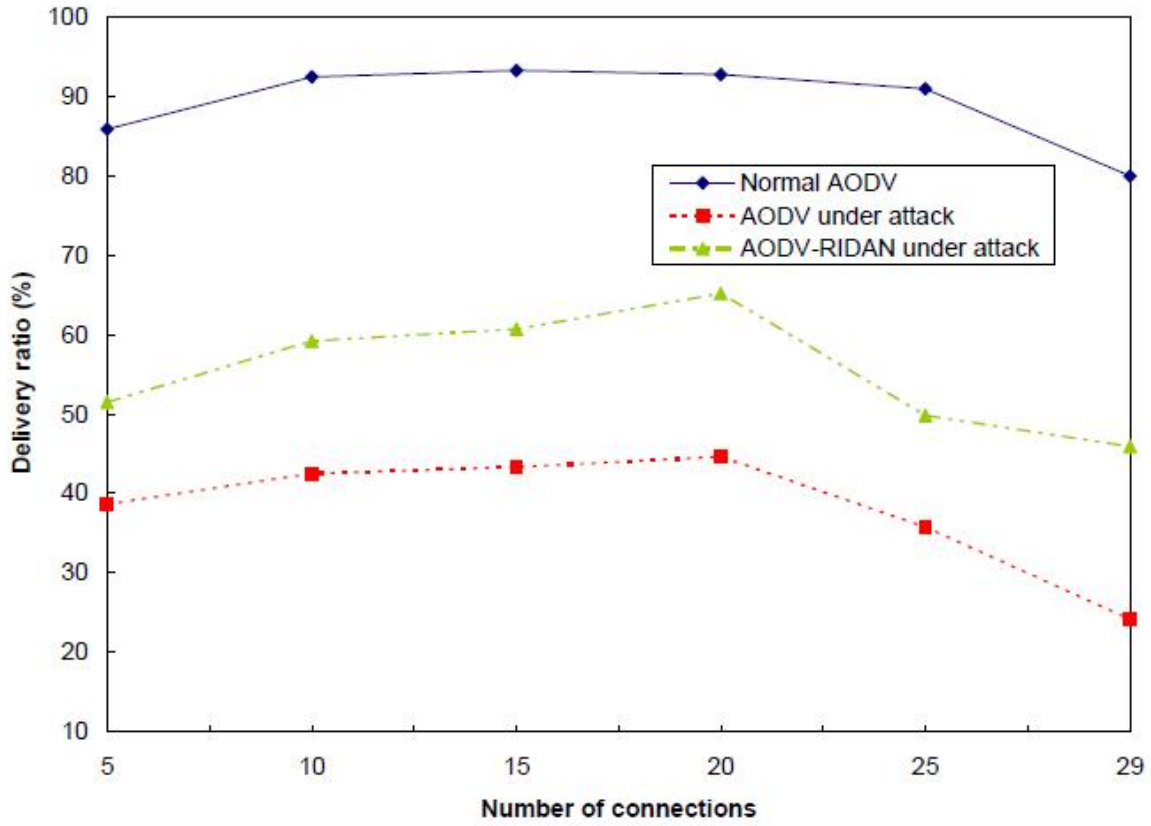
Paramètre	Valeur
Nombre de nœuds	31
Temps de pause	10 secondes
Vitesse maximale	20 m/sec

Trafic entre les noeuds

Le paramètre suivant à définir est l'établissement des différents trafics entre les noeuds du réseau. Dans NS-2, il existe un générateur de trafic permettant de créer deux types de trafic différents : TCP (Transport Control Protocol) ou CBR (Constant Bit Rate).

Résultat :

Cet exemple montre l'attaque de modification de numéro de séquence



Sur cette figure nous observons que le taux de paquets livrés avec succès du protocole de routage AODV normal diminue légèrement en fonction du nombre de connexions. Nous remarquons également sur la même figure que l'attaque de modification de numéro de séquence dégrade considérablement le taux de paquets livrés avec succès. Cette dégradation du PDR est prévisible dans la mesure où le nombre de paquets émis est largement supérieur au nombre de paquets reçus. Le nombre de paquets émis est important parce que le nœud malveillant après réception de paquet RREQ génère un paquet RREP pour faire croire au nœud source que l'itinéraire passant par lui est de meilleur coût. Et tous les paquets de données reçus par le nœud malveillant sont généralement ignorés. Nous constatons que le système de détection d'intrusions RIDAN améliore le PDR de 25% par rapport au protocole AODV sous attaque.

5. Architecture de distribution et coopératives:

Zhang, W Lee, & Y Huang ont proposés l'architecture « distribution et coopératives IDS »

Ils ont proposés [13] l'architecture pour une meilleure détection d'intrusions dans un environnement informatique mobile devrait être distribué et coopératif. La détection d'anomalies est une composante critique de la détection d'intrusion globale et mécanisme de réponse. Analyse de traces et la détection d'anomalie doivent être effectuées localement dans chaque nœud et, éventuellement, par la coopération avec l'ensemble des nœuds dans le réseau. De loin, la détection d'intrusion devrait avoir lieu dans toutes les couches réseau et travailler

de manière transversale comme couche intégrée. Nous avons concentré notre recherche sur routage ad hoc protocoles parce qu'ils sont à la base d'un réseau mobile ad-hoc. Ils ont proposé d'utiliser des modèles de détection d'anomalies construits à l'aide des informations disponibles à partir d'un protocole de routage pour une détection d'intrusion.

6. Présentation de l'architecture pour la détection d'intrusion :

Dans l'architecture proposée (figureIII.5) chaque nœud du réseau mobile ad-hoc participe à la détection d'intrusion et de réponse. Chaque nœud est chargé de détecter des signes d'intrusion localement et de manière indépendante, mais les nœuds voisins peuvent collaborer et enquêter dans une gamme plus large.

Dans l'aspect des systèmes, des agents IDS individuels sont placés sur chaque nœud. Chaque agent IDS fonctionne indépendamment et surveille les activités locales (y compris les activités de communication, activités systèmes et utilisateur, et dans l'intervalle de radio). Il détecte l'intrusion à partir des traces locales et initie les réponses. Si une anomalie est détectée dans les données locales, ou si la preuve est peu concluante alors une recherche plus large est nécessaire, les voisins agents IDS participeront en collaboration dans les actions de détection d'intrusion globale. Ces agents IDS individuelles forment collectivement le système IDS pour défendre le réseau mobile ad-hoc.

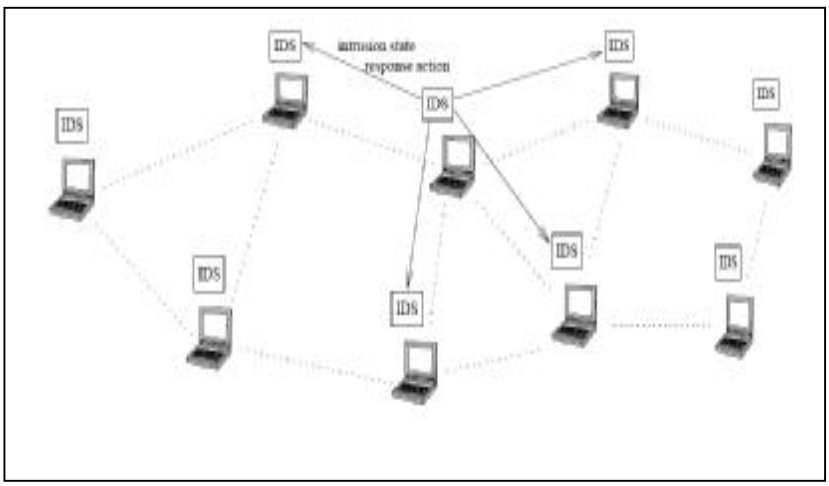


Figure III.5. L'architecture de IDS de réseau sans fil ad hoc

L'intérieur d'un agent IDS peut être assez complexe, mais conceptuellement, il peut être structuré en six morceaux (Figure). Le module de collecte de données est responsable de la collecte des traces d'audit locales et les journaux d'activité. Ensuite, le moteur de détection locale va utiliser ces données afin de détecter une anomalie locale. Les méthodes de détection qui ont besoin d'ensembles de données plus larges ou qui nécessitent la collaboration entre les agents IDS vont utiliser le moteur de détection coopérative. Les mesures d'intervention d'intrusion sont fournies par les deux modules de réponse globale et de réponse locale. Le module de réponse locale déclenche des actions locales pour ce nœud mobile, par exemple un

agent IDS alerte l'utilisateur local, tandis que celle qui est globale coordonne les actions entre les nœuds voisins, comme les agents IDS dans le réseau élient une action de réparation. Enfin, un module de communication sécurisé fournit un canal de communication de haute confiance des agents IDS.

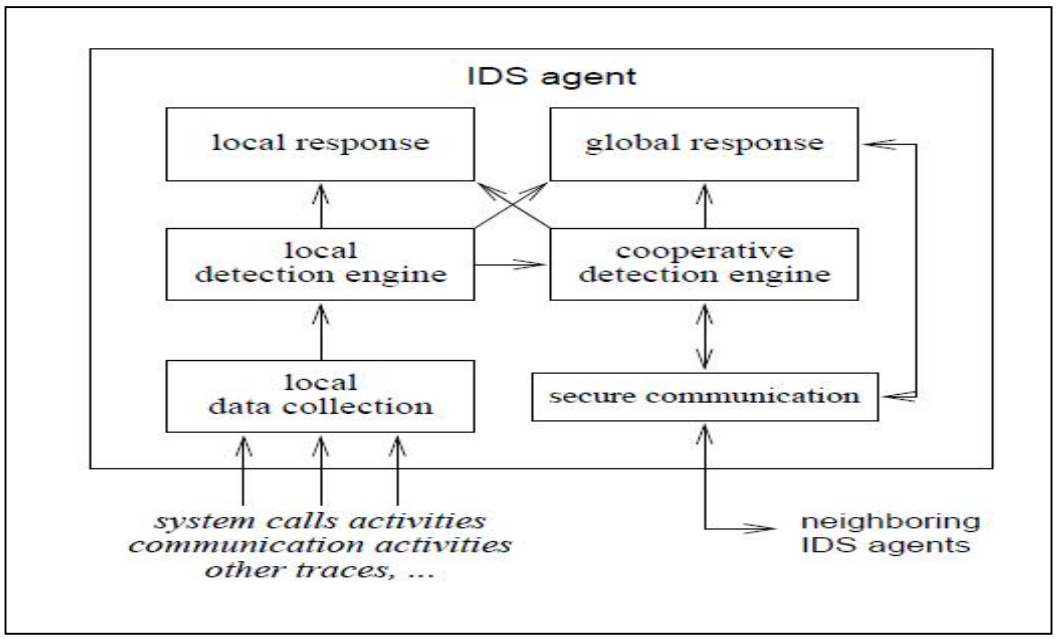


Figure III.6. le modèle conceptuel de IDS Agent

6.1. Collecte des données(data collection)

Le premier module, la collecte de données locale, rassemble des flux de données d'audit en temps réel provenant de diverses sources. Selon les algorithmes de détection d'intrusion, ces flux de données utiles peuvent inclure les activités système et utilisateur dans le nœud mobile, les activités de communication par ce nœud, ainsi que des activités de communication dans l'environnement radio observables par ce nœud.

6.2. Détection locale (Local Detection)

Le moteur de détection locale analyse les traces de données locales collectées par le module local de collecte de données pour l'évidence des anomalies. Il peut inclure à la fois l'utilisation abusive de protections ou la détection d'anomalie . Parce qu'il est concevable que le nombre de type d'attaque récemment crées montés sur l'environnement informatique mobile va augmenter rapidement de plus en plus les appareils réseau deviennent mobiles et sans fil, les techniques de détection des anomalies joueront un rôle plus important.

6.3. Détection coopérative : Cooperative Detection

Tout nœud qui détecte localement une intrusion ou anomalie connue avec des preuves solides (à savoir, la règle de détection déclenché a un taux de précision très élevé, historiquement), peut déterminer de manière indépendante que le réseau est sous attaque et peut initier une réponse. Toutefois, si un nœud détecte une anomalie ou d'intrusion avec une faible investigation, ou l'investigation n'est pas concluante, mais garantit une investigation plus large, il peut engager une procédure de détection d'intrusion coopérative mondiale. Cette procédure fonctionne par la multiplication des informations d'état de détection d'intrusion entre les nœuds voisins (ou plus bas si nécessaire). Les informations d'état de détection d'intrusion peut varier d'une valeur de niveau de confiance simple comme :

• «Avec p % de confiance, le nœud A conclut de ses données local qu'il ya une intrusion"

• «Avec p % de confiance, le nœud A conclut de ses données local et des Etats voisins qu'il ya une intrusion"

• «Avec p% de confiance, le nœud A, B, C, ... concluent collectivement qu'il ya une intrusion"

À un état plus précis qui répertorie les suspects, comme :

• «Avec p% de confiance, le nœud A conclut de ses données local ce nœud X a été compromise"

Ou à un dossier compliqué, y compris les preuves complète. Comme prochaine étape, nous pouvons déduire un algorithme consensus distribué pour calculer un nouvel état de détection d'intrusion pour ce nœud, en utilisant les informations d'état d'autres nœuds reçu récemment. L'algorithme peut inclure un calcul pondéré dans l'hypothèse où les nœuds proches ont des effets plus importants que les nœuds loin, c'est à dire, en donnant les voisins immédiats les valeurs les plus élevées dans l'évaluation des états de détection d'intrusion. Par exemple, une procédure de détection d'intrusion majoritaire, répartie et basée peut comprendre les étapes suivantes:

• le nœud envoie à un nœud voisin "une requête d'état d'intrusion (ou anomalie)»;

• chaque nœud (y compris le nœud d'initialisation) peut envoyer les informations d'état, indiquant la probabilité d'une intrusion ou d'anomalie, à son voisins immédiate;

• chaque nœud détermine ensuite si la majorité des rapports reçus indiquent une intrusion ou anomalie, si oui, alors il conclut que le réseau est sous attaque;

6.4. Réponse d'intrusion

Le type de réponse d'intrusion pour les réseaux mobiles ad-hoc dépend du type d'intrusion, le type de protocoles et des applications réseau, et la confiance (ou la certitude) dans la preuve. Par exemple, voici une réponse:

• Réinitialisation des canaux de communication entre les nœuds (par exemple, la force re-key).

• Identifier les nœuds compromis et de réorganiser le réseau pour exclure les nœuds compromis.

Par exemple, l'agent IDS peut avertir l'utilisateur final, qui peut à son tour faire sa propre enquête et prendre les mesures appropriées. Il peut également envoyer une demande de «réauthentification" à tous les nœuds du réseau à inciter les utilisateurs finaux de s'authentifier (et donc leurs nœuds mobiles), en utilisant out-of-reliés mécanismes (comme, par exemple, les contacts visuels). Seuls les nœuds ré-authentifié, qui peuvent négocier collectivement un nouveau canal de communication, se reconnaissent comme légitime. Autrement dit, les nœuds malveillants ou compromis peuvent être exclus.

6.5. Détection Multi-Layer intrusion intégrée et riposte : (détection d'intrusion multi-couche intégrée et riposte)

Les IDS utilisent les données uniquement de la partie inférieure des couches:

Les IDS basés sur le réseau analysent les paquets de données TCP/ IP et les IDS basées sur l'hôte analysent les données des appels système. C'est parce que dans les réseaux filaires, les pare-feu de couche application peuvent prévenir efficacement les attaques, et des modules spécifiques à l'application, par exemple : les systèmes de détection de fraude de Carte de crédit, ont également été développés pour protéger les services essentiels à la mission. Dans les réseaux sans fil, il n'y a pas de pare-feu pour protéger les services de l'attaque. Cependant, la détection intrusion dans la couche d'application est non seulement faisable, comme discuté dans la section précédente, mais aussi nécessaire. Certains Attaques, par exemple, une attaque qui tente de créer un accès «back-door » non autorisé à un service, peuvent sembler tout à fait légitimes pour les couches inférieures, par exemple, les protocoles MAC. Nous croyons aussi que certaines attaques peuvent être détectées plus tôt dans la couche d'application, comme causes des informations sémantiques plus riches disponibles que dans les couches inférieures. Par exemple, pour une attaque DoS, la couche d'application peut détecter très rapidement qu'un grand nombre de connexions de service entrantes n'ont pas les opérations réelles ou les opérations n'ont pas de sens (et peut être considéré comme des erreurs), tandis que les couches inférieures, ce qui repose uniquement sur des informations sur la quantité de trafic réseau (ou le nombre de demandes de canal), peut prendre un peu plus longtemps pour reconnaître le volume inhabituellement élevé. Étant donné qu'il ya des vulnérabilités dans de multiples couches de réseaux sans fil et mobiles qu'un module de détection d'intrusion doit être placé au niveau de chaque couche sur chaque nœud d'un réseau, nous devons coordonner alors la détection d'intrusion et les efforts d'intervention. Nous utilisons le système d'intégration suivant:

• Si un nœud détecte une intrusion qui affecte l'ensemble du réseau, par exemple, lorsqu'il détecte une attaque contre le protocole de routage ad hoc, il initie la réauthentification traiter d'exclure les nœuds / malveillants compromis du réseau;

• Si un nœud détecte une intrusion locale à une couche supérieure, par exemple, quand il détecte les attaques de l'un de ses services, les couches inférieures sont avertis. Le modules de détection peut ensuite approfondir, par exemple, en initiant le processus de détection d'attaques possibles sur les protocoles de routage ad hoc, et peut répondre à l'attaque en bloquant l'accès à partir du nœud fautif (s) et avertir les autres nœuds dans le réseau de l'incident.

Dans cette approche, le module de détection d'intrusion au niveau de chaque couche doit encore fonctionner correctement, mais la détection sur une couche peut être lancé ou aidé par des preuves

7. **Détection des anomalies dans les réseaux mobiles Ad Hoc**

Dans cette section, ils ont discutons de la façon de construire des modèles de détection d'anomalie pour les réseaux sans fil mobiles. La détection en fonction des activités dans les différentes couches du réseau peut être différente selon le format et la quantité de données de vérification disponibles ainsi que les algorithmes de modélisation. Cependant, ils croient que le principe derrière les approches sera le même.

Pour illustrer leur approche, ils ont basé leur discussions sur les protocoles de routage ad hoc.

7.1. **Construire un modèle de détection des anomalies**

Framework La prémisse de base pour la détection d'anomalie est qu'il n'y a pas de caractéristique intrinsèque et observables du comportement normal qui est distinct de celui du comportement anormal. Ils ont utilisé des mesures d'informations théoriques , à savoir, l'entropie et l'entropie conditionnel, pour décrire les caractéristiques des flux d'information habituels et d'utiliser des algorithmes de classification pour construire des modèles de détection d'anomalies. Par exemple, nous pouvons utiliser un classificateur, formant des données normales, de prédire ce qui est normalement le prochain événement. Dans le suivi, lorsque l'événement réel n'est pas ce que le classificateur a prédit, il ya une anomalie. Lors de la construction d'un classificateur, les caractéristiques avec gain d'information élevée (ou la réduction des en-entropie) sont nécessaires. Autrement dit, un classificateur doit tester des valeurs de fonction de partition du jeu de données d'origine (mixte et haute en-entropie) en sous-ensembles purs (et à faible entropie), idéalement avec une (bonne) Classe de données.

Dans ce cadre, ils ont utilisés la procédure suivante pour la détection d'anomalies:

a) Sélectionnez (ou partition) des données d'audit de sorte que l'ensemble de données normale est faible (conditionnel) d'entropie;

b) effectuer les transformations appropriées des données selon l'entropie de mesures (par exemple, construction définies de nouvelles fonctionnalités avec un gain d'information élevé);

c) calcul et classification à l'aide des données de formation,

d) appliquer le classificateur pour tester les données

e) les alarmes post-traitement pour produire des rapports d'intrusion.

Modèles d'attaque dans cette étude, on ne considère que les attaques sur les protocoles de routage. En général, ces attaques sont dans les formes suivantes:

1. compromis de la logique de l'itinéraire Ce type d'attaques arrive en manipulant des informations de routage, soit en externe par l'analyse de faux messages d'itinéraire ou en interne en modifiant le routage cache malicieusement information. En particulier, nous considérons plusieurs cas particuliers:

(a) l'erreur d'acheminement: envoi d'un paquet à un nœud incorrect

(b) faux propagation du message: distribuer une mise à jour de fausse voie.

2. Trafic modèle distorsion Ce type d'attaques changements default / comportement normal de la circulation:

(a) chute de paquets;

(b) génération de paquets avec une adresse source falsifiée;

(c) la corruption sur le contenu des paquets,

(d) déni de service.

Notez que ces deux types d'attaques peuvent être combinés en une seule intrusion.

Dans leur étude, ils ont mis les attaques suivantes de la simulation:

(1) la falsification des chemins de routage / entrée de route dans son propre cache d'un nœud ,et (2) paquet aléatoire tomber. La première est une abstraction de routage attaques car ils ont recours à la modification des informations de routage pour malveillants pur-poses. Le second est tout simplement une distorsion de modèle de trafic. Chaque séance d'intrusion nous avons simulé comprend un seul de ces types d'attaques. Cependant, chaque trace d'exécution peut contenir plusieurs sessions d'intrusion avec différents types d'attaque.

Les données de vérification , ils ont proposé ces deux sources de données locales sont utilisés pour la détection de l'anomalie:

(1) locale de routage en formation, y compris les entrées de cache et les statistiques de trafic,
(2) de localisation de la position, ou GPS, que nous supposons ne seront pas compromises et peuvent donc prévoir de manière fiable position et de la vitesse de nœuds dans l'ensemble du quartier. Nous n'utilisons que des informations locales provoquées par des nœuds distants pouvant être compromises et leurs données ne sont pas fiables .

Sélection caractéristique, la sélection d'entité est une étape cruciale dans la construction d'un modèle de détection. Plus précisément, puisque nous utilisons les classificateurs comme des détecteurs, ils ont besoin de sélectionner les caractéristiques, à partir des données de vérification disponibles, qui ont un gain d'information élevé. Le critère de gain d'information n'est pas a priori. Ils ont utilisé une méthode non supervisée pour construire l'ensemble des fonctionnalités. Tout d'abord, ils ont construit un grand ensembles de fonctionnalités pour couvrir un large éventail de comportements. Il n'est pas efficace de faire fonctionner toutes les expériences avec toutes ces fonctionnalités. Un petit nombre de descentes d'entraînement peut être effectué avec l'ensemble des fonctionnalités de petites traces de données de vérification de façon aléatoire choisi parmi un des journaux d'audit préalablement stockées. Pour chaque cycle de formation, un modèle correspondant est construit. Les fonctions qui apparaissent dans les modèles ont des poids non inférieure à un seuil minimum sont choisis dans l'ensemble des fonctionnalités essentielles. Pour les différents protocoles de routage et de différents scénarios, l'ensemble des caractéristiques essentielles est différente. Dans la pratique, ils ont attendé que l'ensemble de la fonction soit mis à jour après une certaine période, comme les caractéristiques de comportement de routage peuvent changer avec le temps.

8 . Résultats expérimentaux

Pour étudier la faisabilité de leur architecture de sécurité, ils ont mis en œuvre la détection d'anomalies dans un simulateur de réseau et ont effectué une série d'expériences pour évaluer son efficacité. Ils ont choisi trois protocoles sans fil ad-hoc spécifiques que les sujets de leur étude. Ils sont protocole DSR , Ad-hoc On-Demand Distance Vector Routing (AODV) protocole , et Destination-Sequenced Distance-Vector Routing (DSDV Protocol) , ils ont choisis parce qu'ils représentent différents types de protocoles ad-hoc sans fil de déroutement, proactive et à la demande. Ils ont utilisé le logiciel de simulation de réseaux sans fil, à partir de simulateur de réseau ns 2^{1} .

9. Architecture stand_alone :

Sergio Marti , T,G Giuli , kevin lai et Mary Backer ont proposé un systéme est Wathdog et pathrate basé sur l'architecture Stand_alone
Sergio Marti , T,G Giuli , kevin lai et Mary Backer [15] ont aborder le problème de non-coopération sont ceux de Marti . Dans leurs travaux, les auteurs traitent le cas du protocole de routage DSR en proposant un système fondé sur deux composants :
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. Cette surveillance est possible car, s'agissant d'un protocole de routage par la source, chaque nœud intermédiaire connaitre le prochain nœud vers la destination grâce du descriptif du chemin inclus dans l'entête du paquet. Lorsqu'une action observée ne correspond pas à un résultat attendu, le, nœud observateur comptabilise un échec de retransmission. A partir du moment ou 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.

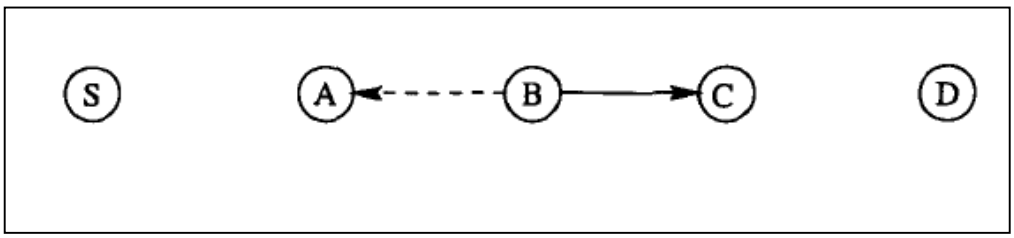
Ils ont supposé les interfaces sans fil prennent en charge le fonctionnement en mode espion. Mode espion signifie que si un nœud A est à portée d'un nœud B, il peut entendre les communications de et vers B, même si ces communications n'impliquent pas directement les interfaces WaveLAN de A. Lucent Technologies ont cette capacité. Alors que le mode espion n'est pas approprié pour tous les scénarios de réseau ad hoc (en particulier certains scénarios militaires), il est utile dans d'autres scénarios pour améliorer les performances du protocole de routage .

10 . Chien de garde et PATHRATER

Dans cette section, nous présentons le chien de garde et le pathrater - outils pour détecter et atténuer les débordements de routage. Nous décrivons également les limites de ces méthodes. Bien que nous mettions en œuvre ces outils au-dessus de DSR, certains de nos concepts peuvent être généralisés à d'autres sources de protocoles de routage. Nous notons ces concepts qui peuvent être généralisés au cours de nos descriptions des techniques.

10.1 Watchdog :

La méthode de surveillance détecte les nœuds qui se comportent mal.



La figure III.7 : illustre comment le chien de garde fonctionne. Supposons qu'il existe un chemin de nœud S de D à travers des nœuds intermédiaires A, B et C. Un nœud ne peut pas transmettre tout le chemin vers le nœud C, mais il peut écouter le trafic du nœud B. Ainsi, lorsque A transmet un paquet pour B pour le transmettre à C, A peut souvent dire si B transmet le paquet. Si le cryptage n'est pas effectuée séparément pour chaque lien, qui peut être coûteux, alors A peut également dire si B a altéré la charge ou la tête.

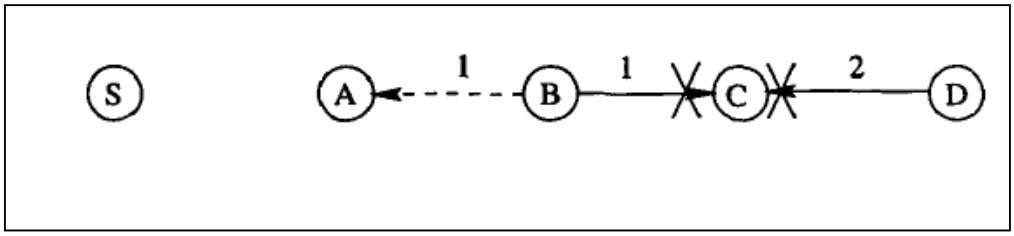


Figure III.8: le nœud A n'entend pas B transmettre le paquet 1 à C, parce que la transmission est heurter à A par le paquet 2 de la source S.

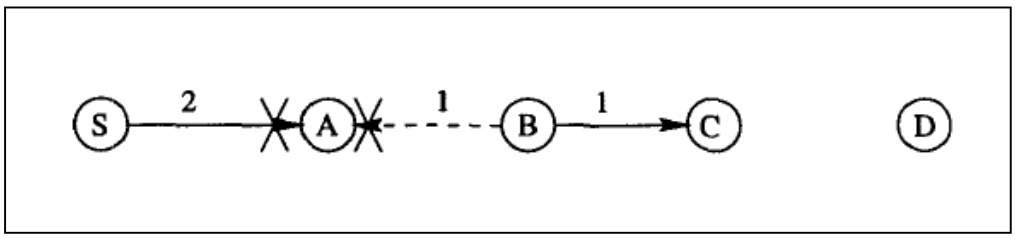


Figure III.9: le nœud A croit que B a transmis paquet 1 à C, mais C n'a jamais reçu le paquet dû à une collision avec le paquet 2.

Ils ont mettons en œuvre la surveillance par le maintien d'une zone tampon des paquets récemment envoyés et en comparant chaque paquet entendu avec le paquet dans la mémoire tampon pour voir s'il ya une ressemblance. Si c'est le cas, le paquet dans la mémoire tampon est retiré et oublié par le chien de garde, dés la transmission. Si un paquet est resté dans le tampon pendant plus d'un certain délai d'attente, les incréments de surveillance de comptage d'un défaut pour le nœud chargé de transmettre le paquet. Si le décompte dépasse un certain seuil de bande passante, elle estime que le nœud est malveillant et envoie un message à la source lui notifiant que le nœud a une mauvaise conduite.

Le problème de collision ambigu empêche de surprendre transmissions de B. Comme la (figure III.8) illustre, une collision de paquets peut se produire au moment ou il est à l'écoute de B. A ne sait pas si la collision a été causée par le paquet envoyé par B comme il se doit ou la collision a été causée par les autres nœuds voisins de A. En raison de cette incertitude, A ne devrait pas accuser immédiatement B de mauvaise conduite, mais devrait plutôt continuer à regarder B sur une période de temps. Si A échoue de façon répétée pour détecter le renvoi B sur les paquets, alors A peut supposer que B se conduit mal.

Dans le récepteur collision problème, le nœud A peut dire si B envoie le paquet à C, mais il ne peut pas dire si C reçoit (Figure III.9). Si une collision se produit à C lorsque B en premier transmet le paquet, A ne voit pas B transférer le paquet et A suppose qu'il s'agit de C qui reçoit avec succès. Ainsi, B pourrait se passer de retransmettre le paquet. B pourrait aussi provoquer délibérément la collision en transmettant un paquet à C en attendant que C émette un autre et ensuite le transmette le paquet. Dans le premier cas, un nœud peut être égoïste et

ne pas vouloir perdre le pouvoir avec retransmissions. Dans ce dernier cas, la seule raison pour laquelle B agirai ainsi est qu'il soit malveillant. B gaspille la puissance de la batterie et le temps du CPU, de sorte à ne pas être égoïste. Un nœud surchargé ne serait pas s'engager dans ce comportement soit, car cela gaspille du temps CPU peu nécessaire et la bande passante. Ainsi, ce second cas devrait être rare.

Un autre problème peut se produire lorsque les nœuds sont déclarés t faussement aux autres nœuds comme des nœuds malveillant. Un nœud malveillant pourrait tenter de diviser le réseau en prétendant que certains nœuds suivants dans le chemin se comportent mal. Par exemple, le nœud A pourrait indiquer que le nœud B n'est pas en état de transfère de paquets, alors qu'en fait il l'est. Cela entraînera S à marquer B comme ayant une mauvaise conduite alors que A est le coupable. Ce comportement, cependant, sera détecté. Puisque A est passé des messages sur la B (tel que vérifié par S), puis les remerciements de D à S passeront par A à S et S se demandera pourquoi il reçoit des réponses de D lorsque soi-disant B paquets sont perdus dans la direction vers l'avant. En outre, si A a des remerciements essaye de les cacher à S, alors le nœud B détecte cet écart de conduite et fera rapport à D.

Un autre problème est qu'un nœud malveillant qui peut commander sa puissance d'émission peut contourner le chien de garde. Un nœud pourrait limiter sa puissance d'émission de telle sorte que le signal est suffisamment fort pour être entendu par le nœud précédent, mais trop faible pour être reçu par le destinataire réel. Il faudrait pour cela que le nœud se conduise mal et connaisse la puissance de transmission requise pour atteindre chacun de ses nœuds voisins. Seul un nœud avec une intention malveillante pourrait se comporter de cette manière – les nœuds égoïstes n'ont rien à gagner puisque la puissance de la batterie est gaspillée et surchargé les nœuds pour ne pas relâcher pas la congestion en faisant cela.

Enfin, un nœud peut contourner le chien de garde en éliminant des paquets à un taux inférieur à celui configuré seuil de mauvaise conduite minimum de chien de garde. Bien que la surveillance ne détecte pas ce nœud comme mauvaise conduite, ce nœud est obligé de transmettre à la bande passante le seuil. De cette façon, le chien de garde sert à appliquer cette bande passante minimale.

Le mécanisme de surveillance pourrait être utilisé dans une certaine mesure de détecter les attaques par rejoue mais nécessiterait le maintien d'un grand nombre d'informations d'état à chaque nœud comme il surveille ses voisins afin de s'assurer qu'ils ne sont pas des retransmetteurs de paquet qu'ils ont déjà transmis. En outre, si une collision a eu lieu au niveau du nœud de réception, il serait nécessaire et correct pour un nœud de retransmettre un paquet, ce qui peut apparaître comme une attaque au nœud qui agit comme chien de garde. Par conséquent, la détection des attaques par rejoue ne serait ni efficace ni une utilisation efficace du mécanisme de surveillance.

Pour le chien de garde qui fonctionne correctement, il doit savoir où un paquet devrait être en deux sauts. Dans leur implémentation, le chien de garde a cette information parce que DSR est une source de déroutement de protocole. Si le chien de garde n'a pas cette information (par exemple, si elle était mise en œuvre au-dessus d'un protocole de routage par-hop-hop), puis un nœud malveillant ou cassé pourrait diffuser le paquet à un nœud inexistant

et le chien de garde n'aurait aucun moyen de le savoir. En raison de cette limitation, le chien de garde fonctionne le mieux sur le dessus d'une source de protocole de routage.

Ils ont utilisé la version du simulateur de réseau de Berkeley (ns) qui comprend wireless extensions apportées par le projet CMU Monarch. Ils ont utilisés également un outil de visualisation de la CMU appelé ad-Hockey pour voir les résultats de leur simulations et détecter les tendances globales du réseau. Pour exécuter les simulations, ils ont utilisés PC (450 ou 500 MHz Pentium III avec au moins 128 Mo de RAM) fonctionnant sous Linux 6.1.

leur simulations ont lieu dans un 670 par 670 mètres espace plat rempli d'une diffusion de 50 nœuds sans fil. La couche physique et la couche MAC 802.11 qu'ils ont utilisés sont incluses dans les extensions sans fil CMU pour ns.

10.2. Les nœuds défaillant :

De 50 nœuds dans le réseau simulé, une variable de pourcentage des nœuds malveillant. Dans leur simulations, un nœud a un mauvais comporter si celui ci accepte de participer à la retransmission des paquets (il ajoute son adresse dans Route Request paquets-ETS), mais ça diminue ensuite indistinctement tous les paquets de données qui sont acheminés à travers elle.

Ils ont varier le pourcentage du réseau composé de misbe-ayant nœuds de 0% à 40% en incréments de 5%. Même si un réseau avec 40% des nœuds mauvaise conduite peut sembler irréaliste, il est intéressant d'étudier le comportement des algorithmes dans un environnement plus hostile qu'il ont espéré rencontrer dans la vraie vie. Ils ont utulisé Tcl intégrée dans nombre pseudo-aléatoire générateur de désigner mauvaise conduite nœuds au hasard. Ils ont utilisé la même graine à travers le 0% à 40% de variation du paramètre nœuds mis-comportement, ce qui signifie que le groupe de nœuds a mauvaise conduite dans le cas de 10% est un sur-ensemble du groupe de nœuds mauvaise conduite dans le cas de 5%. Cela garantit que les obstacles présents dans plus faible pourcentage mauvaise conduite pistes de nœuds sont également présents en plus grand pourcentage mauvaise conduite pistes de nœuds.

10.3. Métrique :

Ils ont évalué leur extensions en utilisant les trois critères suivants:

Débit: C'est le pourcentage de données envoyées qui sont effectivement reçus par les destinataires prévus.

Overhead : C'est le rapport de transmissions de routage connexes (requête de route, réponse d'itinéraire, itinéraire ER-ROR et chien de garde) pour les transmissions de données dans une simulation. Une transmission est l'envoie ou la transmission d'un paquet par un nœud. Par exemple, un paquet étant transmis à travers 10 nœuds compterait que 10 transmissions. Ils ont compté transmissions au lieu de paquets parce que nous voulons comparer routage liés aux transmissions de données et au données transmise, mais certains paquets de routage sont plus

important au réseau que les autres paquets: les paquets DEMANDEUR DE ROUTE sont diffusés à tous les voisins qui à leur tour diffuse à l'ensemble de leurs voisins, qui entraînerait un arbre de transmission de paquets. Unicast ROUTE RE-PLI, ERREUR DE ROUTE, chien de garde, et les paquets de données ne se déplacent que le long d'un chemin unique.

Effets de wathdog et les faux positifs sur travers réseau. Les faux positifs se produisent lorsque le chien de garde rapporte qu'un nœud se conduit mal, alors qu'en fait il ne s'agit pas, pour les raisons mentionnées à la section 3. Ils ont étudié l'impact de cette situation sur le débit.

11. résultat des simulations :

Dans cette section, ils ont présenté les résultats de leurs simulations. Ils ont concentrés sur les trois critères d'évaluation:

Le débit du réseau, les frais généraux de routage, et les effets de faux positifs sur le rendement. Ils ont montré que l'augmentation des faux positifs se traduisent par plus de chemins, y compris un nœud mauvais présumée. Le pathrater enverra alors plus de route demandées vers la destination. Cela augmente la surcharge dans le réseau, mais il fournit également au nœud de destination une liste plus fraîche de routes pour son cache d'itinéraire.

Discussion :

Dans la première partie, ils ont étudié les performances du système de détection d'intrusions RIDAN proposé par la simulation et son impact sur le protocole de routage AODV sous les attaques actives précédemment décrites. Et d'après stamouli nous remarquons que le système de détection d'intrusions permet la détection de ces trois attaques actives et prend des contre-mesures pour réagir contre les actions malveillantes afin d'assurer la disponibilité et le bon fonctionnement du réseau dans des limites acceptables.

Les résultats de l'expérience du deuxième système de détection d'intrusion montrent qu'une approche dans la détection d'anomalie peut bien fonctionner sur différents réseaux sans fil ad-hoc. C'est le comportement normal d'un protocole de routage qui peut être établi et utilisé pour détecter les anomalies. . Les erreurs sont inévitables dans les traces normales, les troubles «multiples» sont généralement enregistrés au cours d'intrusion délibérée. En choisissant une bonne taille de la fenêtre, nous pouvons éviter le taux élevé de faux positifs qui ont un taux de détection élevé.

Par exemple, en utilisant les données de connexion réseau, la détection d'anomalie peut être très efficace contre un scan de ports de connexion basée sur plusieurs attaques DDoS, mais pas pour une connexion unique basé sur une attaque buffer-overflow. Cela montre qu'il ya des limites naturelles sur les capacités de détection, en fonction de quelle couche les données sont collectées. En cette expérience, nous trouvons aussi quelques-uns des paramètres systèmes qui peuvent changer le comportement normal lourdement. L'un d'eux est le niveau de la mobilité - si le modèle est classé à l'aide des valeurs d'un autre niveau de la mobilité, le taux d'alarme peut être beaucoup plus élevé. Ceci peut être résolu par hasard de niveau de mobilité dans l'expérience . on a tendance a conclure d'après cette expérience que le type de protocole le plus adapté serait AODV et DSR. On remarque alors que le modèle topologique, qui est sensiblement plus dynamique dans l'environnement ad hoc, doit être a plus grande valeur si il est utilisé par un protocole qui prend des décisions de routage. Par exemple, de nouveaux protocoles de routage tels que le protocole de routage Location-Aided [25] ce qui tentent d'utiliser l'information topologique peut être plus avantageux.

La technique de surveillance Watchdog a ses avantages et ses inconvénients. DSR avec le chien de garde peut détecter les disfonctionnement au niveau de la transmission, et pas seulement au niveau de la liaison. Les faiblesses de l'équipement sont qu'il pourrait ne pas détecter un nœud à mauvaise conduite en présence de

1) collisions ambiguës,

2) les collisions de réception,

3) la puissance de transmission limitée,

4) Faux débordements,

5) la collusion et abandon partiel.

la technique du Wacthdog n'est pas adaptée à l'identification des nœuds non coopératifs dans la phase de signalisation. Le problème est qu'il n'est fait aucune distinction entre les situations de suppression conformes aux règles dernies par le protocole et les situations de suppression malveillantes. En général, les protocoles de routage réactifs possèdent un mécanisme d'optimisation qui consiste en la suppression des messages de contrôle dupliqués. Lorsqu'un message de recherche de chemin est inondé, chaque nœud reçoit de multiples copies de ce message, même si les valeurs de certains champs tels que par exemple, le nombre de sauts et la séquence de nœuds du chemin vers la source, varient. Suivant ce mécanisme d'optimisation, chaque nœud ne transmet qu'une seule fois un même message (identifie par son numéro de séquence), les autres étant supprimés, réduisant ainsi considérablement les couts de l'inondation. or de telles suppressions sont identifiées à tort comme étant des comportements de non-coopération.

Conclusion :

Ces techniques présentent l'avantage de détecter des intrusions sans recourir à une base de connaissances sur les signatures d'attaques, tout en produisant peu de fausses alarmes (détection de faux). En comparaison avec les solutions basées sur la cryptographie, elles affichent des couts plus légers en termes de puissance de calcul.
Néanmoins, un défi réside dans la définition des contraintes qui décrivent les opérations Correctes du protocole : si le modèle n'est pas décrit assez finement (complexité), alors les attaques ne seront pas détectées efficacement. Entre autres, des attaques éventuellement plus complexes, et ou les spécifications du protocole ne sont pas directement transgressées, peuvent passer inaperçues.

Conclusion général:

Les réseaux ad hoc constituent, de par leur nature, un formidable challenge pour la sécurité informatique. En effet, les réseaux ad hoc sont stimulés par l'évolution rapide des technologies informatiques vers la miniaturisation et l'intégration. L'authentification des nœuds et des messages échangés, constitue le point de départ incontournable pour la sécurité des réseaux ad hoc. les réseaux ad hoc sont connus pour être des réseaux dynamiques sans infrastructure et sans autorité centrale. D'où, la nécessité d'avoir des systèmes de détection d'intrusions pour limiter et se prévenir des activités malveillantes en tenant compte des caractéristiques de ces réseaux. Des techniques développées pour contrer les différents types d'attaques. Ces techniques présentent l'avantage de détecter des intrusions sans recourir à une base de connaissances sur les signatures d'attaques, tout en produisant peu de fausses alarmes (détection de faux). Cependant, un défi réside dans la définition des contraintes qui décrivent les opérations correctes du protocole : si le modèle n'est pas décrit assez finement (complexité), alors les attaques ne seront pas détectées efficacement. Entre autres, des attaques éventuellement plus complexes, et ou les spécifications du protocole ne sont pas directement transgressées, peuvent passer inaperçues. Enfin, il apparaît clairement que les mécanismes de routage constituent un point sensible pour la sécurité des réseaux ad hoc. Les deux axes de recherche que sont l'authentification des nœuds et messages d'un côté, les mécanismes de routage sécurisés de l'autre, apparaissent comme des directions de travail primordiales. La prise en compte de ces deux problématiques doit se faire rapidement afin d'assurer un déploiement des réseaux ad hoc fiables et sécurisés.

[1]Soraya AIT CHELLOUCHE « Délivrance de services média suivant le contexte au sein d'environnements hétérogènes pour les réseaux média du futur » THESE UNIVERSITE BOURDEAUX 1 , Année 2012

[2]Sofiane HAMRIOUI « Amélioration de la Performance des Protocoles Routage et MAC pour une Meilleure QoS dans un MANET » Département d'Informatique, Université des Sciences et de la Technologie Houari Boumediene, Alger, E-NGN, Algérie

[3] M.Mehdi, A.Anou, S.Zair, M.Bensebti et M.Djebari « La Sécurité dans les Réseaux Ad Hoc » Département électronique, Université de BLIDA, ALGERIE ; March 25-29, 2007

[4] Nadjib BADACHE et Tayeb LEMLOUMA « Le Routage dans les Réseaux Mobiles Ad Hoc »

[5] K.AHMED. Titre : «Adaptation de la méthode CTH* aux réseaux mobiles Ad Hoc» Université O.SMAR Alger (I.N.I) 2007/2008

[6] M.DAWOUD. Titre : «Analyse du protocole AODV» Université Paul Sabatier (Liban) 2005/2006

[7] C.BURGOD titre: Contribution à la sécurisation du routage dans les réseaux Ad Hoc. Université de LIMOGES

[8] R.N.Guibadj, S.Mehar SRS_AODV (Secure Routing Scheme for AODV).

[9] AW Issa Konaté ; PFE, ANNEE 2005/2006

[10] Stephane LOHIER « Étude de protocoles de routage Ad-Hoc principes de base des protocoles AODV et OLSR », Année 2007 – 2008

[11] F.AMEZA. Titre : «Les technologies sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV)» Université de Bejaia, juin 2007

[12] Saloua CHETTIBI «protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobiles ad-hoc », 2008

[13] Y. Zhang, W. Lee , Y.Huang « Intrusion Detection Techniques for Mobile Wireless Networks » Année 2003

[14] Ioanna Stamouli « Real-time Intrusion Detection for Ad hoc Networks »

[15] S.Marti,T.J. Giuli , k. Lai « Mitigating Routing Misbehavior in Mobile Adhoc Networks »

[16] K.Dhamecha , R.padhyay , B.Trivedi « IDSs based on Stand-alone Architecture for MANET A Survey » Année 2012

[17] Jean-Marc Percher, Ricardo Puttini Ludovic Mé , Olivier Camp ,Bernard Jouga,Patrick Albers « Un système de détection d'intrusions distribué pour réseaux ad hoc »

[18] Yi-an Huang et Wenke Lee « Attack Analysis and Detection for Ad Hoc Routing Protocol »

[19] Alexandre POCQUET « Les attaques sur le routage dans les Réseaux Ad hoc »

[20] Guibadj Rym Nesrine , Mehar Sara « SRS_AODV (Secure Routing Scheme for AODV) »

[21]Jimmi Grönkvist, Anders Hansson, and Mattias Sköld « Evaluation of a Specification-Based Intrusion Detection System for AODV»

[22] Houda labiod « multicast routing in mobil ad hoc networks »

[23] M.dominguez Hugo « les Systèmes de détection des intrusions et les systèmes d'empéchement des intrusion » Montréal , février 2005

[24] www.commentcamarche.com Encyclopédie informatique libre

[25]Young-Bae Ko and Nitin H. Vaidya ". Location-aided routing (LAR) in mobile ad hoc networks." ACM/Baltzer Wireless Networks (WINET) journal, Vol 6-4 - Extended version of the Mobicom'98 paper., 2000.