الجمهورية الجزائرية الديمقراطية الشعبية وزارة
التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــــة

Faculté : Sciences de L'ingéniorat
Département : Electronique
Domaine : Sciences et Techniques
Filière : Télécommunication
Spécialité : Système et télécommunication
Réseaux et télécommunication

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème:

Détection d'intrusions dans les réseaux Ad Hoc

Présenté par : *DELHOUM AICHA & NOUIOUA MAISSOUM*

Encadrant : ***TAIBI Mahmoud*** *Grade Professeur Université : Badji-Mokhtar ANNABA*

Jury de Soutenance :

ZADAM Mohamed	MCB	UniversitéBadji-Mokhtar Annaba	Président
TAIBI Mahmoud	Prof	UniversitéBadji-Mokhtar Annaba	Encadrant
AMARA Fethi	MCB	UniversitéBadji-Mokhtar Annaba	Examinateur

Année Universitaire : 2020/2021

مـلـخص :

يتطلب الافتقار إلى البنية التحتية في الشبكات اللاسلكية المخصصة التكامل ، داخل كل عقدة ، وحدات مختلفة لضمان أمنها الخاص ، وبالتالي المشاركة في الأمن.

نقترح نهجًا لنظام كشف التسلل على مستوى طبقة الشبكة. الهدف هو التعامل مع هجمات الثقب الأسود حيث تدعي العقدة الخبيثة أن لديها أقصر طريق إلى أي عقدة مرغوبة في الشبكة. للقيام بذلك ، قمنا بتنفيذ وحدة تعاون بين العقد المختلفة. يتم تنفيذ خوارزميات الكشف / التفاعل والتحديث بموجب NS2 .

حصلت نتائج التنفيذ والمحاكاة التي تم الحصول عليها على تأثير الهجوم على شبكة Adhoc والأداء الذي يوفره نهجنا.

الكلمات المفتاحية: Ad-hoc، AODV ، الثقب الأسود ، خوارزمية الوقواق ، كشف التسلل ، IDS.

Abstract:

The lack of infrastructure in ad-hoc wireless networks requires the integration within each node, different modules to ensure its own security, and thus participating in the security of the ad-hoc network.

We provide a network layer intrusion detection system approach. The goal is to deal with blackhole attacks where a malicious node claims it has the shortest path to any desired node in the network. To do this, we have implemented a cooperation module between the different nodes. The implementation results and simulations obtained show the impact of the attack on the Ad-hoc network and the performance offered by our approach.

Key words: Ad-hoc, AODV, black hole, cuckoo algorithm, intrusion detection, intrusion detection system.

Résumé :

L’absence d’infrastructure dans les réseaux sans fil ad-hoc nécessite l’intégration, au sein de chaque nœud, différents modules permettant d’assurer sa propre sécurité, et participant ainsi à la sécurité du réseau Ad-hoc.

Nous proposons une approche d’un système de détection d’intrusions au niveau de la couche réseau. L’objectif est de faire face aux attaques par trou noir (blackhole) où un nœud malicieux prétend qu’il a le chemin le plus court vers n’importe quel nœud souhaité dans le réseau. Pour se faire, nous avons mis en œuvre un module de coopération entre les différents nœuds. Les algorithmes de détection /réaction et mise-à-jours sont implémentés sous NS2. Les résultats d’implémentation et des simulations obtenus montrent l’impact de l’attaque sur le réseau Adhoc et les performances qu’offre notre approche.

Mots-clés : Ad-hoc, AODV, trou noir, algorithme de cuckoo, Détection d’intrusions, IDS.

Dédicaces

A l'homme de ma vie, mon exemple éternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, que Dieu te garde toujours avec moi, à toi mon père.

A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ; maman que j'adore.

A celui que j'aime beaucoup et qui m'a soutenue tout au long de ce projet : mon marie CHAWKI et bien sûr à ma sœur RAHMA et mon frère YASER sans oublier ma grand-mère et mes beaux-parents que j'aime.

A toute ma famille, et mes amis, A mon binôme MAISSOUM et sa gentille mère que j'aime, à ma douce amie HANA et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

Tous mes frères et mes sœurs, FATMA, ASMA, BILLEL, je dédie ce travail dont le grand plaisir leurs revient en premier lieu pour leurs conseils, aides, et encouragements.

Aux personnes qui m'ont toujours aidé et encouragé, qui étaient toujours à mes côtés, et qui m'ont accompagné durant mon chemin d'études supérieures, Merci à tout d être dans ma vie.

AICHA DELHOUM

Dédicaces

Je dédie ce mémoire :

A ma mère l'étoile filante qui brille dans mon univers,
A mon papa le père et l'ami,

A mon frère Abdou et ma cousine Rania, sans oublier le sucre de ma vie ma petite sœur Safa
A mes copines Aicha, Tyma et Ranya qui m'a beaucoup inspiré,

Au département d'électronique enseignants et fonctionnaires, toute la promotion de télécommunication.

Pour tous les fonctionnaires d'MSC, en particulier Auaidjia Raouf qui a été très compréhensif,

A tous mes ami(e)s du jardin d'enfant jusqu'à l'université,

A tout ceux que j'aime, je dis merci de tout mon cœur,

Et que dieu vous garde.

Nouioua Maissoum

Remerciements

Tout d'abord, nous remercions Allah le tout puissant, à la sagesse et au savoir infinis,
« ""Gloire à toi ! Nous n'avons de savoir que ce que Tu nous as appris. Certes c'est Toi l'Omniscient, le sage, le tout miséricordieux le très miséricordieux " » (Sourate al-Baqarah, verset 32).

Nous tenons à remercier notre encadreur Mr Taibi Mahmoud pour le grand honneur qu'il nous a fait en nous proposant le sujet de ce mémoire de fin d'étude. Nous avons eu l'honneur et le privilège de travailler sous son assistance et de profiter de ses qualités humaines, professionnelles et de sa grande expérience, il nous a guidé tout au long de ce travail. L'élaboration avec amabilité et dynamisme le caractérisant. Que ce modeste travail puisse satisfaire nos examinateurs, pour qu'ils en témoignent nos gratitudes et reconnaissances pour l'aide et les conseils qu'ils nous ont prodigué, ainsi que pour le savoir qu'ils nous ont inculqué.

Nous remercions tous nos enseignants de l'université d'Annaba.

Nos remerciements vont également aux membres de jury d'avoir accepté de juger notre travail.

Nous remercions vivement nos familles, en particulier nos parents, pour nous avoir toujours soutenu au cours de nos études. Qu'ils trouvent ici le fruit de leur patience et du soutien permanent qu'ils nous ont prodigué pour affronter tous les moments difficiles.

Nous tenons également à remercier nos collègues pour leur aide et leur conseils précieux.

Liste des Tableaux

Liste des Figures

Liste des abréviations

MANET	Mobile Ad Hoc Network
AODV	Ad-hoc On-demand Distance Vector
OLSR	Optimized Link State Routing Protocol
DSR	Dynamic Source Routing
PAN	Personal area network
ISO	International Organization for Standardization
DOS	Denial-of-service attack
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
MAC	Media Access Control
IDS	Intrusion detection system
IDWG	Groupe de détection d'intrusion Worhing
IETF	Internet Engineering Task Force
HIDS	host-based intrusion detection system
NIDS	network-based intrusion detection system
WLAN	Wireless Local Area Network
LAN	Local Area Network
DSR	Dynamic Source Routing
DSRV	Destination Sequence-Distance Vector
PDR	Packet delivery ratio
QoS	La qualité de service

Table des matières

Chapitre III : Contribution à la détection d'intrusions dans les réseaux Ad-hoc

Introduction Générale

La prolifération rapide des appareils mobiles et des technologies de communication au cours des dernières décennies, en particulier les technologies de réseau sans fil qui ont révolutionné notre mode de vie. La disponibilité et la commercialisation des technologies sans fil qui permettent une communication directe entre les appareils des utilisateurs a conduit à l'émergence d'un modèle de réseaux sans fil ad-hoc.

Les réseaux sans fil Ad-hoc sont des réseaux ne disposant d'aucune infrastructure préexistante et formés de nœuds mobiles interconnectés par des liaisons sans fil. Leurs architectures évoluent au gré de l'apparition et du mouvement des nœuds. L'absence d'une gestion centrale des fonctionnalités du réseau rend ces réseaux beaucoup plus vulnérables aux attaques que les réseaux avec infrastructure (WLAN, LAN).

Si les MANET se différencient des réseaux classiques, cellulaires ou filaires, par les caractéristiques de leur topologie, les services demandés au réseau par les utilisateurs restent identiques, notamment en matière de sécurité. Les mécanismes de prévention d'intrusion, tels que le chiffrement et l'authentification, ne sont pas suffisants en matière de sécurité, la détection d'intrusions peut être considérée comme une deuxième ligne de défense. La majorité des techniques de détection d'intrusion proposée sont déployées dans la couche réseau.

Cependant, le service de routage de données dans ces réseaux est vulnérable à diverses attaques. Par conséquent, la motivation de cette mémoire découle de la nécessité de l'intégration au sein de chaque nœud, différents modules permettant d'assurer sa propre sécurité, et participant ainsi à la sécurité du réseau Ad-hoc.

Parmi les moyens de défense du réseau, nous avons le système de détection d'intrusion (IDS). Ces systèmes, qui peuvent être de nature logicielle ou matérielle, sont de plus en plus répandus et peuvent représenter une part importante du budget d'un service informatique.

Malheureusement, ces équipements, bien que très utiles, présentent des défauts non négligeables. Le nombre de faux positifs, étant la fausse alarme, peut rapidement dépasser la capacité des analystes de sécurité à les analyser. Pour répondre à ce problème de performance, plusieurs solutions ont été proposées. Ces dernières années, nous avons vu différentes structures IDS telles que la hiérarchie des agents et par agents mobiles.

Notre contribution à la sécurité traite les vulnérabilités au niveau de la couche réseau en particulier le protocole de routage AODV.

Un nœud malveillant peut exploiter ces vulnérabilités au niveau du protocole de la couche réseau dans le but de créer des attaques de type trou noir afin de supprimer la plupart des paquets en diminuant ses performances.

Notre démarche consiste en premier lieu à détecter le nœud malicieux selon un comportement douteux en fonction des demandes prétendant qu'il a le chemin le plus court vers les nœuds de destination. Une fois localisé, une alerte est diffusée à l'ensemble des nœuds voisins pour l'élimination de ce dernier de toutes les tables de voisinage afin de l'isoler.

Dans le cadre de notre travail de recherche, nous proposons un système de détection d'intrusions ou IDS (Intrusion Detection System) pour les MANETs, afin de contrer les attaques par trou noir.

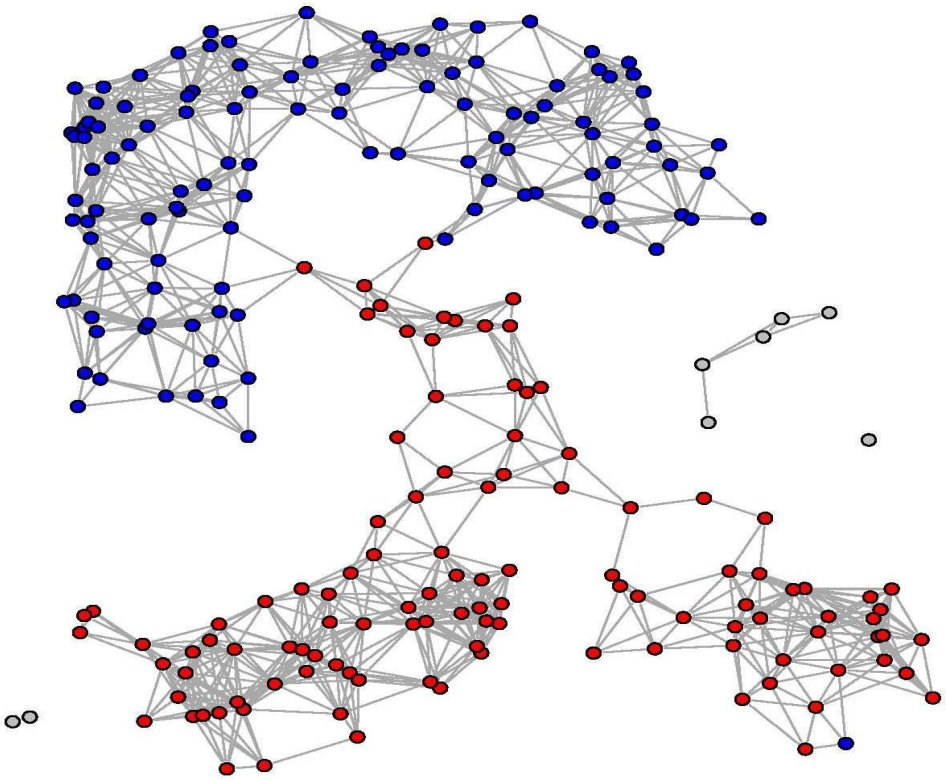
A cet effet, notre présent mémoire est organisé comme suit :

- **Le chapitre I** présente une vue générale détaillé des réseaux sans fil et sans infrastructure (Ad-hoc).
- **Le chapitre II** introduit les IDS, il recense les différentes approches adoptées pour les réseaux Ad-hoc, une étude comparative résume l'ensemble des travaux.
- **Le chapitre III** présente l'approche élaborée « Algorithme de cuckoo en IDS » pour la détection et le traitement d'attaque de types trou noir ainsi que son implémentation, les résultats font l'objet de discussion.

Enfin une conclusion générale clôture ce présent mémoire.

Chapitre I :

Réseaux Ad-hoc



I.1. INTRODUCTION :

Les progrès des performances des réseaux sans fil et la nécessité de créer rapidement des réseaux sans infrastructure préexistante dans les situations d'urgence, et parfois même dans des endroits hostiles, ont favorisé le développement de réseaux mobiles autoorganisés. Les réseaux mobiles autoorganisés (également appelés réseaux autonomes) sont composés de plusieurs entités mobiles et autonomes qui peuvent s'auto organiser et communiquer entre elles sans avoir besoin d'une infrastructure centralisée.

L'élargissement de la gamme des réseaux ad-hoc nécessite une sécurité accrue pour garantir l'intégrité et la confidentialité des données circulant sur le réseau. En fait, les réseaux mobiles ad-hoc sont confrontés à de nombreux problèmes liés à leurs caractéristiques, ce qui fait que les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure ne sont pas adaptées aux contextes ad-hoc. Par conséquent, de nombreux thèmes de recherches ont surgi au cours des dernières années pour remédier à ces vulnérabilités et assurer les services de sécurité dans les réseaux mobiles Ad-hoc.

Ce chapitre est organisé comme suit : dans la section 1.2 ; nous présentons les réseaux mobiles Ad-hoc, leurs caractéristiques, leurs types et leurs domaines d'application, ainsi que leurs avantages et inconvénients, de plus nous avons défini les protocoles de routage dans les MANETs. La section 1.3 est dédiée aux vulnérabilités, la sécurité et classification des différentes attaques dans les réseaux mobiles Ad-hoc. Enfin, la section

1.4 conclut le chapitre.

I.2. Les réseaux sans fil Ad-hoc :

I.2.1. Définition :

Un réseau Ad-hoc [1] est un ensemble d'hôtes équipés par des antennes qui peuvent communiquer entre eux sans aucune administration centralisée, en utilisant une technologie de communication sans fil comme Wifi, Bluetooth, etc. à l'opposé des réseaux filaires où uniquement certains nœuds dits "routeurs" sont responsables de l'acheminement des données, dans un réseau ad-hoc tous les nœuds sont à la fois routeurs et terminaux. Le choix des nœuds qui vont assurer une session de communication dans un réseau ad-hoc se fait dynamiquement selon la connectivité du réseau, d'où l'appellation ''ad-hoc".

Dans un réseau ad-hoc, un nœud peut communiquer directement (mode point-à-point) avec n'importe quel nœud s'il est situé dans sa zone de transmission, tandis que la communication avec un nœud situé en dehors de sa zone de transmission s'effectue via plusieurs nœuds intermédiaires (mode multi-sauts), qui s'approprient le rôle d'un routeur et acheminent les messages à destination. Ce processus se fait grâce au protocole de routage. À cet effet, plusieurs protocoles de routage ont été proposés et standardisés par le groupe MANET.

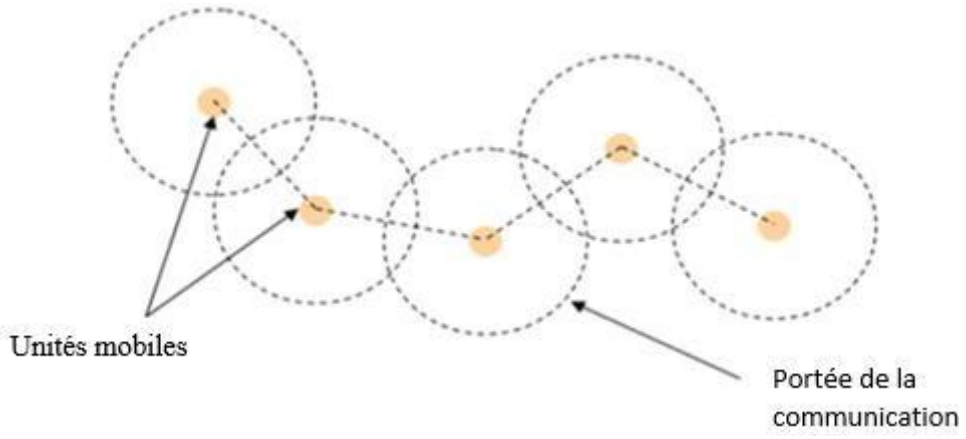


Figure I.1 : Réseau en mode ad-hoc

I.2.2. Caractéristiques des réseaux Ad-hoc :

Les réseaux ad-hoc héritent des mêmes propriétés et problèmes des réseaux sans fil. En plus du fait que le canal radio soit limité en termes de bande passante et sujet à un grand taux d'erreurs, ce qui engendre des liaisons à capacité fluctuante.

D'autres caractéristiques spécifiques aux réseaux ad-hoc conduisent à une complexité et des contraintes supplémentaires, qui doivent être prises en compte alors la conception des algorithmes et des protocoles réseaux [2], à savoir :

- **L'absence d'une infrastructure centralisée :** Les réseaux ad-hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistante et de tout genre d'administration centralisée. Chaque nœud travaille dans un environnement pair à pair distribué et agit en tant que routeur pour relayer des communications, ou pour générer ses propres données.
- **L'auto configuration :** L'auto configuration permet de s'intégrer facilement dans un réseau. Elle facilite la gestion du réseau car l'interconnexion des éléments nécessite qu'un minimum d'intervention technique externe.
- **L'impossibilité de mettre en place un plan d'allocations des fréquences :** Dans les réseaux sans fil cellulaire, caractérisés par les utilisations des stations de base, on cherche à attribuer des fréquences différentes aux stations voisines, de telle façon à éviter les interférences entre les cellules ainsi crées. Pour garantir la connectivité, au sein d'un réseau ad-hoc, comme il n'y a pas d'infrastructures fixes et que tous les nœuds sont susceptible de bouger ou de disparaître, il est plus simple et moins coûteux de travailler avec une seule fréquence et un multiplexage TDD (time division duplex).
- **La mobilité des nœuds et maintenance des routes :** La mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un nœud peut joindre un réseau, changer de position, quitter le réseau. Cette mobilité aura un impact direct sur la morphologie du réseau, elle peut engendrer une modification du comportement du canal de communication et en général provoque des influences significatives sur les performances du réseau. Les algorithmes de routage doivent donc être capable de résoudre ces problèmes, supporté la maintenance des routes et prendre en charge un temps limitée leurs constructions tout en minimisant l'over-Head généré par les messages de contrôle.
- **L'hétérogénéité des nœuds :** Les nœuds dans un réseau ad-hoc peuvent être équipés d'une ou plusieurs interfaces radio ayant des capacités de transmission variées dans des plages de fréquences différentes. Cette hétérogénéité de capacité engendre des liens asymétriques dans le réseau. De plus, ces nœuds peuvent avoir des différences,

en termes de capacité de traitement, de logiciel, de débit (faible, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.

- **La contrainte 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 effectué par le système.
- **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.
- **Les vulnérabilités :** Les vulnérabilités des réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux ad-hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service est plus délicate et l'absence de centralisation rend plus complexe la collecte d'informations pour la détection d'intrusions.

I.2.3. Modes de communications dans les réseaux ad -hoc :

Avant de parler des protocoles de routage proprement dit, nous allons rappeler quels sont les principaux modes de communication [3] dans les réseaux, et particulièrement dans les réseaux ad-hoc :

- **La communication point à point ou unicast :** pour laquelle il y a une source et une seule destination.
- **La communication multipoints ou multicast :** qui permet d'envoyer un message à plusieurs destinations.
- **La diffusion ou broadcast :** envoie un message à tous les nœuds du réseau.

Ces trios modes de communication sont schématisés par la figure suivante :

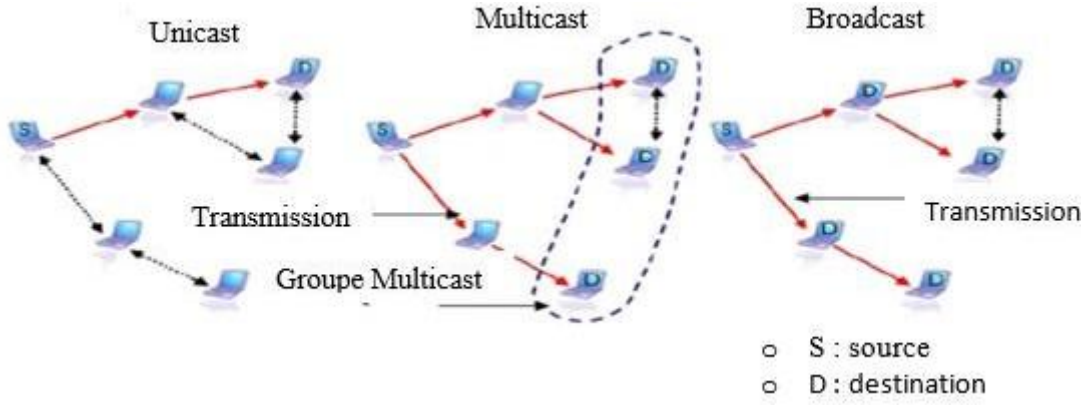


Figure I.2 : Communication dans les réseaux ad-hoc

I.2.4. Types des réseaux ad-hoc :

Les types des réseaux ad-hoc sont divers, nous pouvons en citer quelques uns [3] :

- **Les réseaux personnels PAN (Personal Area Network) :** Désigne un réseau restreint d'équipement informatique habituellement utilisées dans le cadre d'une utilisation personnelle. Parmi les technologies sans fil utilisées par les réseaux PAN, nous pouvons citer le Bluetooth, l'infrarouge (IR), ou le zigbee (la technologie 802.15.4).
- **Les réseaux poste à poste ou Peer to Peer :** sont des réseaux, dont le fonctionnement est décentralisé entre les différents utilisateurs du réseau, dont les machines sont simultanément, client et serveurs (routeur) des autres machines.
- **Les réseaux de capteurs :** sont des réseaux composés de nœuds, intégrant une unité de mesure de capter des grandeurs physiques (chaleur, humidité, vibration) et de le transformer en grandeurs numériques, une unité de traitement informatique de stockage de données et un module de transmission sans fil (Wireless).
- **Les réseaux véhiculaires :** Les voitures de nos jours embarquent de plus en plus de technologie, et ont de plus en plus, besoin de communiquer avec l'extérieur. Les voitures équipées par des capteurs sur les toits et/ou, les pare-chocs sont capables de créer des plateformes des réseaux mobiles ad-hoc et de relier en réseau les automobiles passant à proximité les uns des autres. Des prototypes ont déjà été développés pour les véhicules d'urgence (les ambulances, les voitures des pompiers, etc.).

I.2.5. Les protocoles de routage pour les réseaux Ad-hoc :

Un protocole de routage [4] a pour fonction de déterminer le chemin entre deux nœuds en fonction d'une stratégie prédéfinie. Le routage dans les réseaux Ad-hoc présente des défis plus

complexes en comparaison avec le routage dans les réseaux filaires traditionnels. En effet, une stratégie intelligente de routage est nécessaire pour supporter la nature et les paramètres du réseau (la mobilité, le nombre de nœuds, la densité du trafic, la qualité du service et la superficie du réseau).

Dans un réseau ad-hoc, le protocole de routage, distribué sur l'ensemble des nœuds, vise de plus à minimiser le temps d'établissement de la route, aussi appelé temps de latence, ainsi que l'utilisation des ressources nécessaires à cette opération.

Lorsque deux nœuds échangent directement leurs paquets de données sans passer par des nœuds mobiles intermédiaires, la connexion est dite directe.

Si le chemin entre les nœuds source et destination nécessite la présence de plusieurs nœuds intermédiaires, la connexion est alors qualifiée de multi hop.

Dans un réseau à architecture fixe, les routes vers les différents réseaux sont prédéfinies et maintenues par les équipements d'interconnexion fixes, appelés routeurs. L'architecture dynamique d'un réseau ad-hoc, qui résulte du mouvement, de l'apparition des nœuds ou de l'état de la connexion physique, nécessite une mise à jour régulière des tables de routage situées dans chaque nœud. Pour acheminer un paquet entre deux nœuds mobiles d'un réseau ad-hoc, le mécanisme de base est l'inondation. Celle-ci consiste à transmettre le paquet à l'ensemble des nœuds du réseau. L'inondation est réalisée par diffusions successives à l'ensemble des voisins de chaque nœud.

Des mécanismes complémentaires de contrôle peuvent être utilisés pour éviter les bouclages ou la duplication des paquets. Ce mécanisme d'inondation, très coûteux en ressources réseau, ne peut s'appliquer qu'à de très petits réseaux. Les protocoles de routage viseront, eux, à limiter la propagation des paquets par inondation. Selon le rôle joué par les nœuds dans la diffusion des messages, lorsque tous les nœuds ont des fonctionnalités identiques, le protocole est qualifié d'uniforme, si certains nœuds ont des fonctionnalités particulières dans la diffusion des messages, le protocole est non uniforme.

Comme dans les réseaux à architectures fixes, les deux techniques à état de liens et à vecteur de distance sont utilisées. Les protocoles de routage à vecteur de distance possèdent une table de routage qui à chaque nœud du réseau, associe l'adresse du prochain nœud.

Les protocoles de routage à état de liens utilisent, eux, une base de données qui leur permet de construire la topologie du réseau et de connaître ainsi le chemin vers tous les nœuds du réseau. Une métrique basée généralement sur plusieurs paramètres relatifs aux liaisons est utilisée pour sélectionner la meilleure route.

Si la mise à jour de la table de routage est effectuée de façon périodique, le protocole est alors qualifié de proactif. De cette façon, l'ensemble des routes, mêmes celles inutilisées, sont mises

à jour et demeurent immédiatement disponibles. Cette technique génère de nombreux paquets sur le réseau mais permet de minimiser le temps de découverte d'une route lors de son utilisation.

Pour diminuer la charge réseau due aux paquets de mise à jour, certains protocoles de routage déclenchent la recherche d'une route uniquement quand celle-ci est demandée. Le délai d'obtention d'une route est alors plus long. Les protocoles qui utilisent ce mode de fonctionnement sont dits réactifs.

Pour diminuer le nombre de messages de contrôle nécessaires à la découverte des routes, les protocoles de routage non uniformes sélectionnent certains nœuds pour créer des architectures hiérarchiques et dynamiques. Ainsi, pour les protocoles à sélection de voisins, chaque nœud décharge la fonction de routage à un sous ensemble de voisins directs. Tandis que pour les protocoles à partitionnement, le réseau est découpé en zones dans lesquelles le routage est assuré par un unique nœud maître. Certains de ces protocoles, qualifiés d'hybrides, utilisent conjointement le routage à état de liens et le routage à vecteur de distance.

Dans [27], Les principaux protocoles de routage sont présentés selon leur mode de fonctionnement sur la **figure1.3 :**

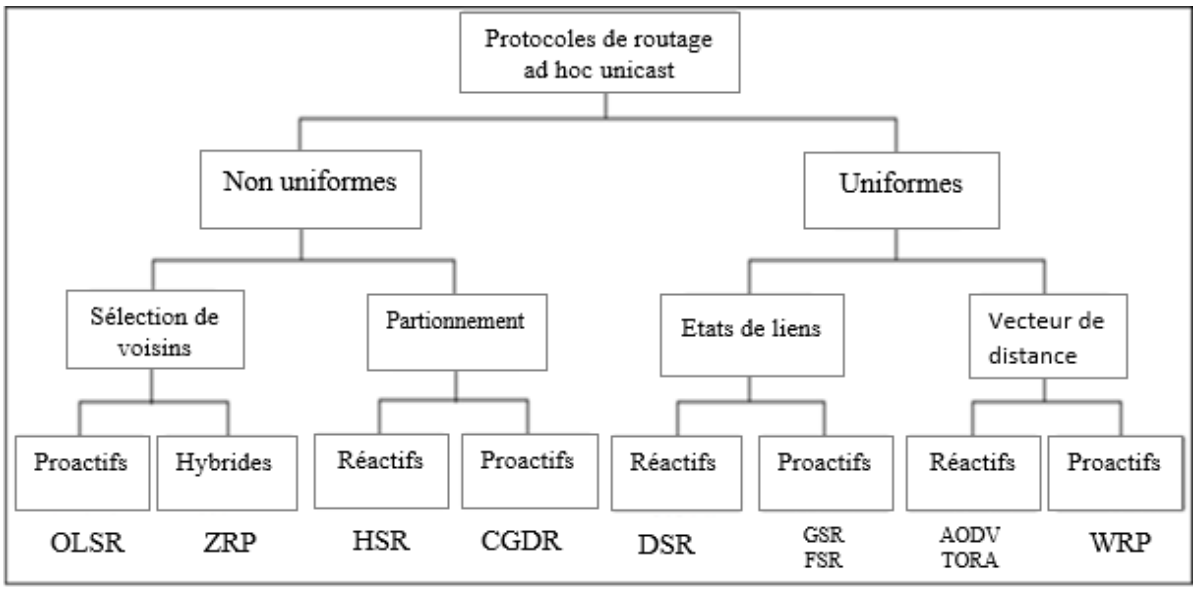


Figure I.3 : Classification des protocoles de routage ad-hoc

Nous prenons les exemples des protocoles AODV [5] et OLSR [6], DSR [7] possédant chacun, des stratégies de routage différentes :

- **AODV (pour Ad-hoc On Demand Distance Vector)** : est un protocole de routage destiné aux réseaux mobiles (réseau ad-hoc). Il est à la fois capable de routage unicast et multicast. Il est libre de boucle, auto-démarrant et s'accommode d'un grand nombre de

nœuds mobiles (ou intermittents). Lorsqu'un nœud source demande une route, il crée les routes à la volée et les maintient tant que la source en a besoin. Ce protocole de routage est peu gourmand en énergie et ne nécessite pas de grande puissance de calcul, il est donc facile à l'installer sur de petits équipements mobiles.

- **OLSR (Optimized Link State Routing Protocol) :** est un protocole de routage destiné aux réseaux maillés, sans fil ou mobiles. Le protocole est une optimisation de l'algorithme d'état de liaison pure. Le concept clé utilisé dans le protocole est l'utilisation des relais multipoints (MPR). L'ensemble MPR est choisi de sorte qu'il couvre tous les nœuds qui sont à deux sauts de suite. Il fonctionne comme un protocole proactif, des informations de topologie avec d'autres nœuds du réseau sont échangées régulièrement.
- **DSR (Dynamic Source Routing)** : est un protocole de routage pour les réseaux maillés sans fils (Wireless mesh networks). Il est similaire à AODV dans le sens où il forme une route à la demande lorsqu'un élément du réseau le sollicite. Cependant, il utilise le routage à la source au lieu de se baser sur la table de routage de chaque routeur intermédiaire.

I.2.6. Domaines d'application d'un réseau ad-hoc :

D'une façon générale, les réseaux Ad-hoc sont utilisés dans toute application [8] où le déploiement d'une infrastructure réseau filaire est trop contraignant, soit parce qu'il est difficile à mettre en place, soit parce que la durée d'installation du réseau est très longue.

- **Militaire :** un réseau ad-hoc donnera accès à l'armée pour maintenir un réseau entre tous les soldats, véhicules et quartiers généraux
- **Réseau personnel (PAN) :** il s'agit d'un réseau local à courte portée où chaque nœud est généralement lié à une plage donnée.
- **Condition de crise :** Parce qu'il est assez facile à créer, il peut être utilisé en temps de crise pour envoyer des signaux d'urgence.
- **Application médicale :** Il peut l'utiliser pour surveiller le patient.
- **Application environnementale :** il peut l'utiliser pour vérifier les conditions météorologiques, les incendies de forêt, les tsunamis, etc…

I.3. Les vulnérabilités et la sécurité des réseaux Ad-hoc :

Les mécanismes de sécurité [9] dans les environnements des réseaux Ad-Hoc présentent de grands défis. Ce type de réseaux a hérité à la fois des problèmes de sécurité des réseaux câblés et aussi ceux des réseaux sans fil. S'ajoute à cela, la nature des réseaux Ad-Hoc qui se

caractérise par une architecture peer-to-peer ouverte, une topologie dynamique et extensible, des ressources limitées et un canal radio accessible par tout le monde.

I.3.1. Classification des attaques :

Une intrusion peut être définie comme tout ensemble d'actions qui essayent d'exploiter une ou plusieurs failles du système à travers une ou plusieurs menaces détectées. La taxonomie des attaques contre les réseaux ad-hoc proposée dans [9] et représentée sur la ***figure1.4*** identifie deux familles d'attaques : les attaques passives et les attaques actives.

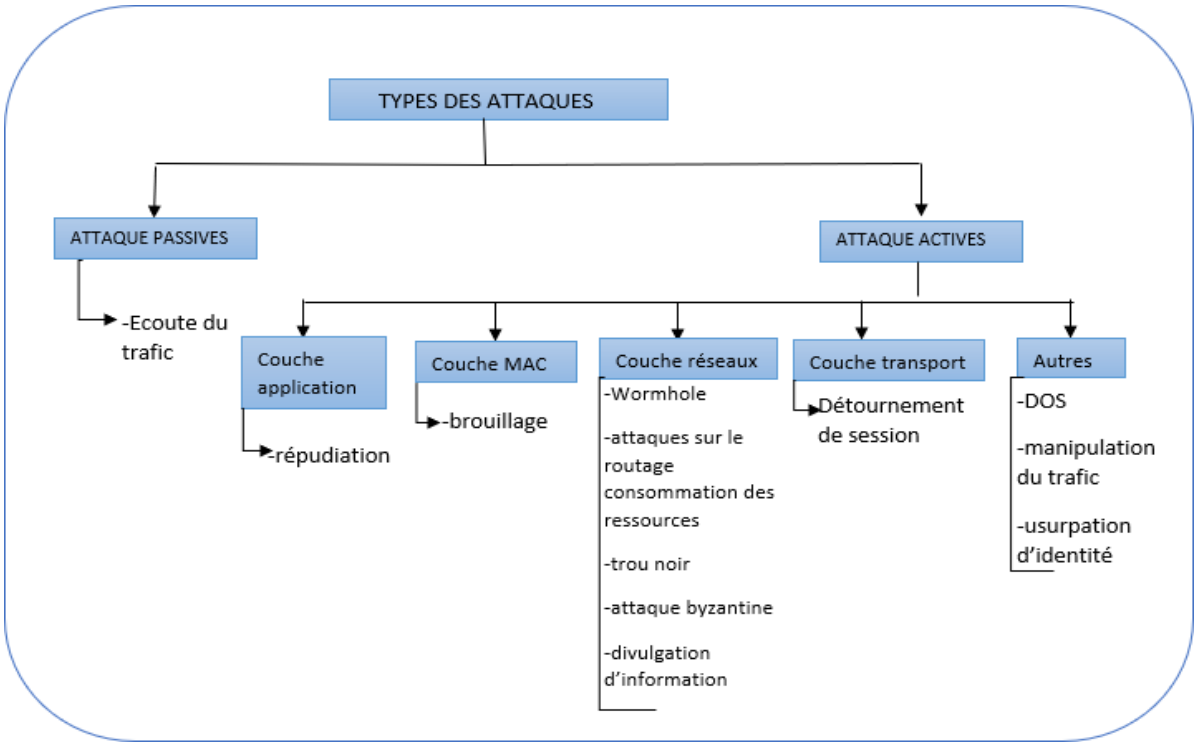


Figure I..4 : Classifications des attaques dans les réseaux Ad-hoc

Les attaques peuvent être conduites pour les raisons suivantes :

- L'obtention d'un accès au système
- Le vol d'informations confidentielles, sensibles, personnelles
- Le vol de données bancaires
- Le trouble du bon fonctionnement d'un service
- L'obtention d'informations sur un tiers
- La corruption du système
- L'exploitation des ressources

- **Attaques passives VS attaques actives :**

Les attaques passives [10] "eavesdropping" se limitent à l'écoute et l'analyse du trafic

échangé. Ce type d'attaque est plus facile à réaliser (il suffit de posséder un récepteur adéquat) et il est difficile de le détecter puisque l'attaquant n'apporte aucune modification sur les informations échangées. L'intention de l'attaquant peut être la connaissance des informations confidentielles ou bien la connaissance des nœuds importants dans le réseau (chef de groupe "cluster head"). En analysant les informations de routage, l'attaquant va se préparer à mener ultérieurement une action précise.

Dans les attaques actives [10], un attaquant tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service.

I.3.2. Objectifs de la sécurité :

Afin de protéger le système représenté par un ou plusieurs périphériques informatiques connectés au réseau, la première étape consiste à établir une politique de sécurité. Cela fournit des règles pour l'application des services de sécurité pour protéger les ressources système. Les ressources système comprennent les données hébergées localement, les applications accessibles par l'utilisateur et toutes les ressources matérielles locales, telles que l'espace disque ou les processeurs.

L'ISO a défini les services de sécurité suivants [11] :

- **Authentification :** L'authentification des entités apparait donc comme la pierre angulaire d'un réseau sans fil ad-hoc sécurisé. Elle permet d'identifier et contrôler d'identité des participants afin d'interdire aux intrus d'injecter des messages falsifiés ou erronés.
- **Disponibilité :** Est une propriété difficile à gérer dans les réseaux sans fil ad-hoc vu les contraintes qui pèsent sur ce type de réseau :
  - Topologie dynamique.
  - Limitation des ressources énergétiques sur quelques nœuds.
  - Communications sans fil pouvant être facilement brouillées ou perturbées.

Plusieurs attaques ont pour but de remettre en cause cette propriété, pour cela le protocole de routage doit surmonter toute tentative d'attaque de type dénis de service (DoS).

- **Intégrité :** elle permet de garantir que les messages échangés n'ont pas été altérés ou modifiés de manière inattendue.

L'intégrité des données peut être remise en cause par plusieurs événements dont on note :

- Les attaques visant à modifier le contenu des messages.
- La faible fiabilité des liaisons filaires.

- **Non répudiation :** assure qu'une entité ne puisse nier avoir effectué une activité (i.e. un message envoyé ne sera pas nié par son expéditeur).
- **La confidentialité des données :** qui garantit que l'information ne doit être ni rendue accessible, ni divulguée à un utilisateur, une entité ou un processus non autorisé. Dans le contexte des réseaux Ad-hoc, la confidentialité consiste à refuser l'accès aux informations échangées entre deux nœuds dans le réseau par tout nœud malveillant ou non désiré. Or, les réseaux Ad-hoc sont caractérisés par la diffusion générale des informations, ce qui constitue un vrai challenge pour la confidentialité.

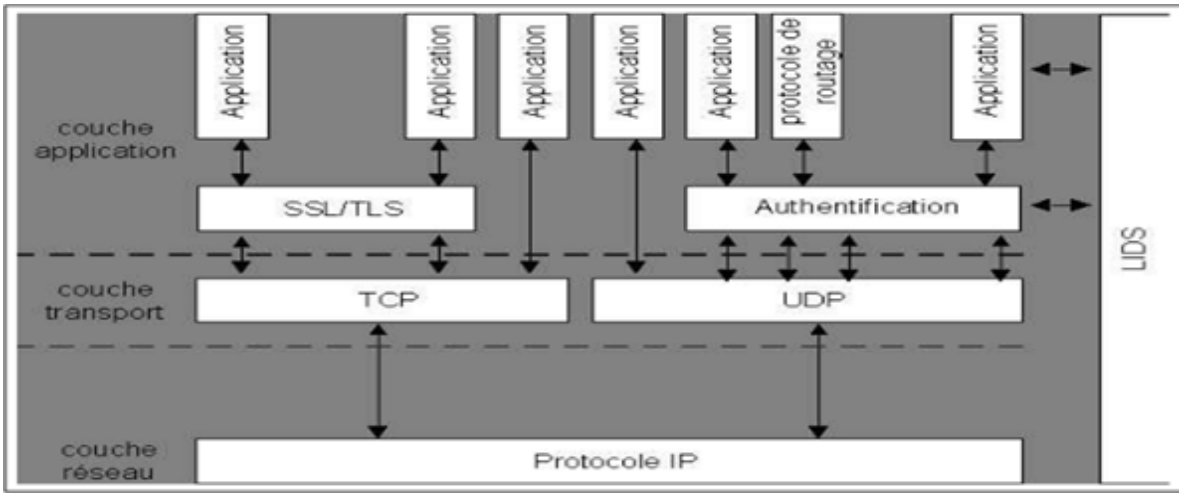


Figure I.5 : Modèle de sécurité pour les réseaux ad-hoc

I.3.3. Défense contre les attaques dans les réseaux Ad-hoc :

Plusieurs solutions ont été proposées pour pallier les problèmes de sécurité dans les réseaux Ad-Hoc. Le tableau I.1 présente des exemples de solutions proposées [9] pour la sécurité des réseaux Ad-Hoc :

Tableau I.1 présentation des différentes attaques avec leur solution

Attaques	Définition	Solutions proposées
Wormhole	Un attaquant pourrait rediriger le trafic entre deux zones géographiquement éloignées pour créer un vertex dans la topologie et ainsi avoir une bonne position géographique pour contrôler le trafic qui passe par lui.	Packet Leashes (Hu, Perrig et Johnson, 2003)
Attaque de routage	Un nœud malicieux pourrait perturber le fonctionnement d'un protocole de routage en modifiant les informations de routage, fabriquer les fausses informations de routage ou usurper l'identité d'un autre nœud.	SEAD (Perkins et Bhagwat, 1994),ARAN (Sanzgiri et al., 2002),ARIADNE (Hu, Perrig et Johnson, 2002), SAODV (Zapata, 2002).
Brouillage (Jamming)	C'est une attaque classique sur la disponibilité du canal de communication grâce à la génération massive d'une grande quantité d'interférence radio.	FHSS, DSSS (Wang et al., 2006)
Brouillage virtuel (Virtual jamming)	Un attaquant pourrait exploiter les vulnérabilités au niveau de la couche MAC et former de faux paquets de contrôle avec une fausse adresse de destination, afin que les nœuds récepteurs de ces paquets bloquent leurs transmissions inutilement, dans le but de créer une attaque de type déni de service dans le réseau.	DATA-Send (DS) RTS validation
Attaque trou noir (Backhole attack)	Le but de cette attaque est la falsification des informations de routage ou le détournement du trafic	(Ramaswamy et al., 2003).
Attaque sur les Ressources	Les réseaux MANET sont caractérisés par des ressources limitées (batterie et bande passante). Une attaque sur les ressources pourrait avoir des conséquences sur la disponibilité	SEAD (Perkins et Bhagwat, 1994).
Attaque Byzantine	Grâce à cette attaque, un nœud malicieux altère les messages et pourrait créer des problèmes de boucle de routage, routage de paquets vers des chemins non optimaux, sélectionné les paquets à rejeter... Ce type d'attaque est difficile à détecter carle réseau semble fonctionner correctement	OSRP (Awerbuch et al., 2002), (Awerbuch et al., 2004).
DoS	Ce type d'attaque consiste à envoyer délibérément des messages pour causer une saturation de la bande passante et paralyser le réseau.	SEAD (Perkins et Bhagwat, 1994), ARIADNE (Hu, Perrig et Johnson,2002),SAODV (Zapata, 2002).
Divulgation d'information	L'échange des informations confidentielles doit être protégé contre l'écoute ou l'accès non autorisé.	SMT(Papadimitratoset Haas, 2003),SRP (Papadimitratos et Haas, 2002).
Répudiation	Ce type d'attaque a une conséquence sur l'intégrité des communications entre les nœuds dans le réseau.	ARAN (Sanzgiri et al., 2002).
Usurpation d'identité	L'usurpation d'identité a pour but la falsification des informations relatives aux identités. Ce qui pourrait conduire à l'isolement de nœuds, l'échange de fausses informations de routage et l'atteinte à la confidentialité et l'intégrité	ARAN (Sanzgiri et al., 2002), SAODV (Zapata, 2002)..

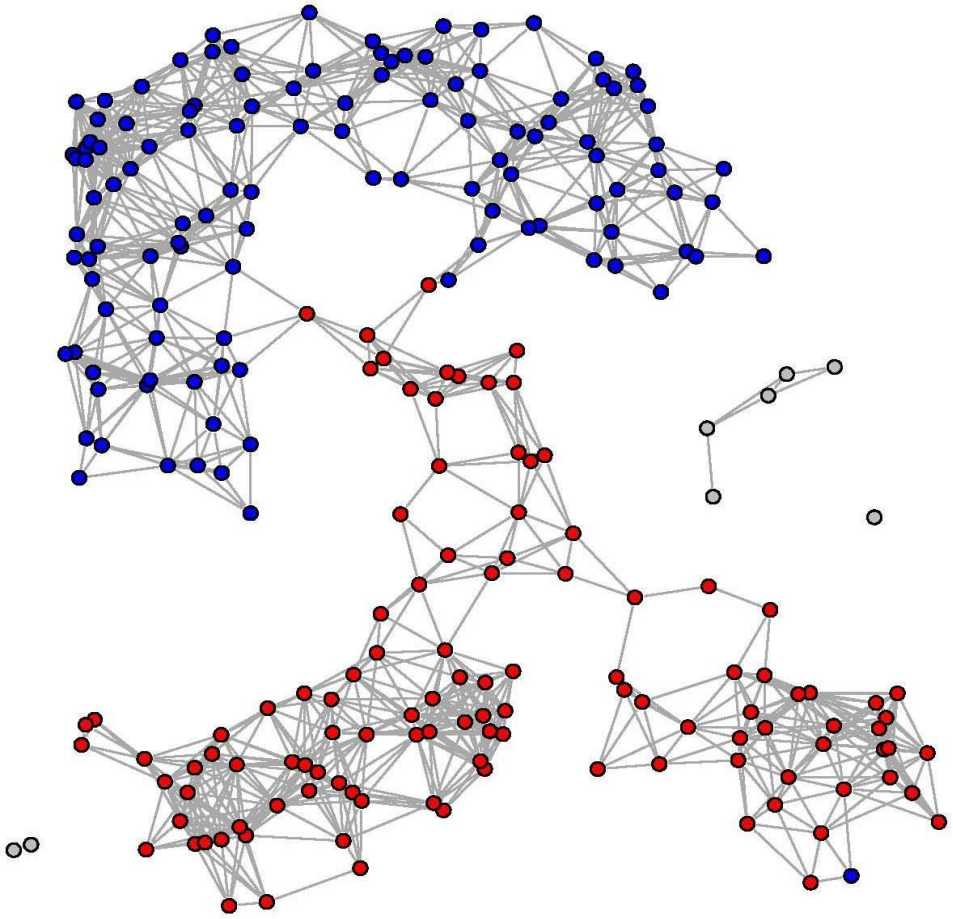
I.4. Conclusion :

Après avoir l'environnement mobile ad-hoc et décrit ses principales caractéristiques, les avantages et les inconvénients qu'il présente et les différents domaines d'applications qui ont recours à ce type de réseaux sans fil, ainsi que les protocoles de routages.

Nous avons présenté dans ce chapitre les besoins en sécurité dans ces réseaux. En outre, nous avons discuté des différents domaines de recherche liés à la sécurité dans les réseaux mobiles Ad-hoc. Les mécanismes de sécurité préventifs forment la première ligne de défense du système contre les différentes menaces. On ne peut toutefois considérer cette protection comme absolue, permanente et incontournable. Une surveillance permanente du système protégé peut permettre de renforcer l'action des mécanismes de sécurité. D'où, la nécessité d'avoir des systèmes de détection d'intrusions pour limiter les activités malveillantes en tenant compte des caractéristiques de ces réseaux.

Chapitre II :

Les Systèmes de Détection d'Intrusions



II.1. INTRODUCTION :

La sécurité de l'information est plus que jamais importante pour nos sociétés. En effet, Internet s'est développé pour démocratiser les outils utilisés pour pénétrer les systèmes informatiques, les rendant accessibles aux enfants de script de ce monde. En outre, un besoin toujours croissant d'échange d'informations a conduit à une intégration et à un inter connectivité accrues des systèmes, les rendant ainsi plus complexes et donc plus susceptibles de contenir des vulnérabilités de sécurité.

Les grandes organisations de ce monde ont investi massivement dans celui du système de détection d'intrusion (IDS). Ces systèmes visent à reconnaître différentes attaques en analysant différentes sources de données, principalement le trafic réseau et les journaux d'événements du système. Malheureusement, leur efficacité reste mitigée compte tenu du nombre généralement élevé de fausses alarmes obtenues.

Dans le bureau de résolution de ce problème, la communauté scientifique doit développer des architectures innovantes de systèmes de détection d'intrus et doit avoir les moyens de les évaluer pour sa réponse au problème sauvegardé. Ce chapitre va se penchera sur l'évaluation des performances de différentes architectures IDS. Nous concentrons nos efforts sur l'élaboration d'un mécanisme pour évaluer la performance des systèmes.

Dans ce chapitre nous présentons les différentes étapes des processus de détection d'intrusion ainsi que les caractéristiques des IDS. Ensuite nous représentons les différentes architectures d'IDS pour les réseaux ad-hoc et les travaux IDS –ad-hoc existants.

II.2. Système de détection d'intrusion :

Un système de détection d'intrusion (IDS) [12] est une application qui alerte un administrateur d'une faille de sécurité, d'une violation de stratégie ou de tout autre problème susceptible de compromettre son réseau informatique.

Les systèmes de détection d'intrusion surveillent et analysent l'activité du réseau, analysent les configurations et les vulnérabilités du réseau et vérifient l'intégrité des fichiers. Ils peuvent reconnaître les schémas d'attaque classiques. Pour ce faire, ils analysent les comportements

anormaux et suivent les violations de règles par les utilisateurs. Certains systèmes de détection d'intrusions industriels peuvent également répondre aux menaces détectées.

Un système IDS est généralement à double déclenchement. La première étape, que l'on peut qualifier de passive, se déroule sur la machine. Cela implique l'inspection des fichiers de configuration réseau, notamment pour détecter les paramètres obsolètes et les violations de stratégie. La deuxième étape, que l'on peut qualifier d'actif, se déroule sur le réseau. Ici, les mécanismes réutilisent les méthodes d'attaque identifiées et enregistrent les réactions.

Un système de détection d'intrusions efficace doit mettre en évidence plusieurs mesures comme [13] :

- **Précision :** Un système de détection d'intrusions imprécis signale un taux important des actions anormales ou intrusives pour les actions légitimes dans l'environnement.
- **Performance :** La détection d'intrusions en temps réel et un faible temps de réponse pour traiter les évènements.
- **Complétude :** Un système de détection d'intrusions qui ne parvient pas à détecter une attaque est un système incomplet, cette mesure est relative du fait que c'est impossible d'avoir une connaissance globale sur les anomalies.
- **Tolérance aux fautes :** Avec le développement des attaques, un système de détection d'intrusions peut être attaqué directement, pour cela il faut qu'il soit conçu pour résister contre les attaques, la plupart des IDSs fonctionnent sur des systèmes d'exploitation et de matériel commercialisé, donc ils sont connus par leur défaillances et vulnérabilités aux types d'attaques particulièrement le déni de service.
- **Rapidité :** Cette mesure englobe la vitesse de traitement et le temps nécessaire pour propager l'information et réagir contre les alertes, cela va permettre à l'agent de sécurité de réagir avant que les dégâts se produisent pour empêcher l'attaquant de subvertir la source d'audit ou le système de détection d'intrusions lui-même.

II.2.1. Architecture d'un IDS :

Le groupe de détection d'intrusion Worthing (IDWG) de l'IETF a proposé un modèle fonctionnel d'IDS composé de trois composants de base [4]. La ***figure 2.1*** illustre les interactions entre ces trois composants. Un capteur (ou Senseur) est chargé de collecter des informations sur l'évolution de l'état du système et de fournir une séquence d'événements

reflétant l'évolution de l'état du système. Une analyse détermine si un sous-ensemble des événements produits par le capteur est caractéristique d'une activité malveillante. Un gestionnaire de collecte des données générées par le capteur, les formate et les présente pour utilisation.

Finalement. Le manager est responsable de la réaction à adopter. Nous détaillerons chacun de ces trois éléments ci-dessous.

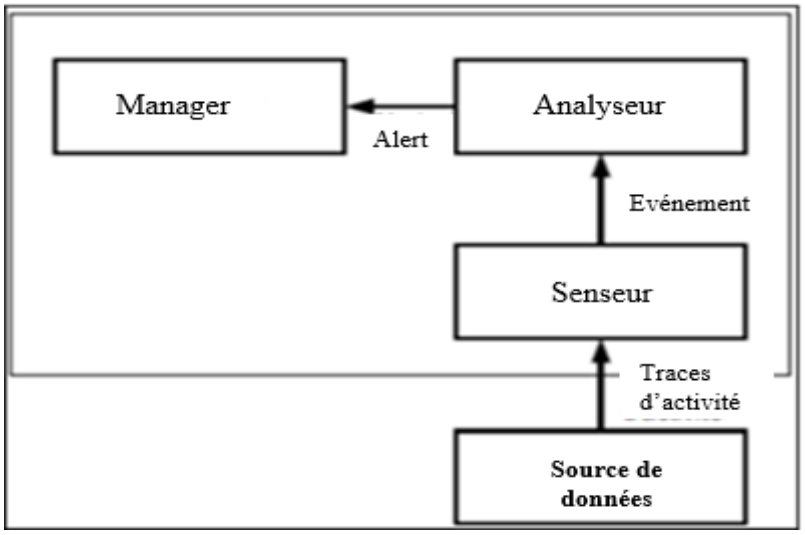


Figure II.1 : Modèle d'architecture IDS de IDWG

II.2.1.1. Le capteur :

Le capteur [14] observe l'activité du système par le biais d'une source de données et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système. Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. On distingue classiquement trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs.

II.2.1.2. L'analyseur :

L'objectif de l'analyseur [14] est de déterminer si le flux d'événements fourni par le capteur contient des éléments caractéristiques d'une activité malveillante.

Nous pouvons distinguer trois principales méthodes de détection à savoir :

- **L'approche par scénarios (misuse detection identifie) [13]** : Ils ont été conçus pour chercher des modèles déjà connus comme des intrusions, ce sont des IDSs basés sur des signatures ou des connaissances. Les fonctionnalités intéressantes de ces systèmes de détection d'intrusions où les caractéristiques des attaques et le mode d'attaque peuvent être facilement connus dans des règles ou un système expert.
- **L'approche comportementale [13] :** Ce sont les IDSs basés sur le comportement, nous cherchons à créer le modèle qui représente le comportement normal de notre réseau informatique, chaque déviation par rapport à ce comportement sera considérée comme intrusion, ce qui va déclencher une alerte.
- **L'approche hybride** : qui combine entre les deux techniques précédentes. Quelle que soit l'approche choisie comportementale, par scénarios ou hybride, tous les IDS se trouvent confrontés au problème de la détection de nouvelles attaques, plus précisément à la détection d'attaques inconnues suite à la complexité croissante des réseaux et des attaques auxquels ils sont sujets [4].

II.2.1.3. Le manager :

Le manager [14] collecte les alertes produites par le capteur, les met en forme et les présente à l'opérateur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être :

- Confinement de l'attaque, qui a pour but de limiter les effets de l'attaque
- Eradication de l'attaque, qui tente d'arrêter l'attaque.
- Recouvrement, qui est l'étape de restauration du système dans un état sain.
- Diagnostic, qui est la phase d'identification du problème.

II.2.2. Fréquence d'utilisation d'un système de détection d'intrusion :

Un système de détection d'intrusion peut effectuer la surveillance des évènements selon deux cas [13] :

- **Surveillance périodique (offline) :** On parle ici du temps consumé entre l'évènement et son analyse, elle se fait périodiquement, le flux des données n'est pas transmis de manière continue vers le détecteur, la plupart des IDS hôte utilisent cette technique avec une période constante pour examiner le trafic et les logs de système.

- **Surveillance en temps réel (online) :** Les IDSs réseaux utilisent l'approche de traitement des informations en continu "en temps réel", cette manière de traiter les informations de trafic réseau facilite la prise des contre-mesures afin de freiner la progression des attaques au bon moment.

II.2.3. Action de détection :

Après la détection d'intrusions, le système lance certaines actions pour prendre l'initiative avec l'action adéquate aux actions typiques ne rentrant pas fréquemment dans le domaine de la détection d'intrusions, c'est une post-détection qui peut être classée en deux grandes catégories [13] :

- **Réponse Active :** Ce type des IDSs entreprend une action pour isoler ou empêcher l'attaquant de reproduire l'attaque et mettre fin à cette intrusion. Il est connu aussi par IPS (Intrusion Prevention System) qui répond avec une action de prévention active afin de garantir la sécurité des éléments ciblés. En général, les IPSs utilisent les routeurs à cause de leurs emplacements qui simplifient l'intervention d'isolement.
- **Réponse passive :** Ce type d'IDS envoie les alertes détectées vers un mécanisme de gestions expertes, les actions de ce type de réponse peuvent déclencher la génération et la sauvegarde d'alerte dans une base de données ou de générer l'alerte et la transmettre par un email comme SNMP (Simple Network Management Protocol) alertes, un message, à travers une page web, un mobile ou une interaction avec un autre outil de sécurité comme le pare-feu.

II.2.4. Familles de systèmes de détection d'intrusion :

- Les systèmes de détection d'intrusion réseaux (NIDS : Network Intrusion Detection System) [15] : sont les IDS les plus répandus. Ce sont des outils très utiles pour l'administrateur réseaux qui va pouvoir, en temps réel, comprendre ce qui se passe sur son réseau et prendre des décisions en ayant toutes les informations.
- Les systèmes de détection d'intrusion hôte (HIDS : Host-based Intrusion Detection System) [15]: sont des IDS mis en place directement sur les hôtes à surveiller. Ils vont directement analyser les fichiers de l'hôte, les différents appels système et aussi les événements réseaux. Par conséquent ces analyses sont strictement limitées à l'hôte sur laquelle l'HIDS est installé et n'ont aucune vue sur le réseau.

- Les systèmes de détection d'intrusion collaboratif (CIDS : Collaborative Intrusion Detection System) [15]: sont des systèmes reposant sur d'autres IDS, de ce fait le CIDS peut opérer sur des systèmes hétérogènes.

II.3. Les nouveaux défis de l'IDS dans les MANETs :

Les solutions IDS [4] pour les réseaux traditionnels déploient généralement des capteurs de réseaux, tels que des commutateurs, des routeurs et des pares-feux, aux points clés où le trafic est concentré. Ces IDS (NIDS) basés sur des capteurs de réseau sont physiquement sécurisés et utilisent des techniques de détection basées sur des signatures pour détecter les attaques. De plus, ces solutions ne peuvent pas être utilisées dans des réseaux autoorganisés. En effet, les réseaux ad-hoc n'ont pas de point de contact capable de contrôler le trafic réseau. Cela limite l'efficacité de l'IDS basé sur des capteurs de réseau, car il ne peut surveiller le trafic généré que dans la portée de transmission radio. De plus, dans un réseau autoorganisé caractérisé par une topologie dynamique et des changements imprévisibles, il peut être difficile de s'appuyer sur l'existence de nœuds centralisés pour effectuer l'analyse et la découverte.

Par conséquent, l'IDS ad-hoc a besoin d'une architecture pratique et évolutive pour recueillir suffisamment de preuves en temps réel afin de détecter les attaques de manière efficace. En outre, les liaisons sans fil entre les nœuds mobiles sont beaucoup plus fiables que les liaisons dans les réseaux filaires. Par conséquent, le mécanisme de détection doit être capable de tolérer la perte de message afin d'avoir suffisamment de données pour analyser et maintenir la précision de la détection.

II.3.1. Les limites de l'IDS :

Comme tout système informatique, les IDS ont des limites. On peut en citer [14] :

- **Pollution/surcharge :**

  Les IDS peuvent être pollués ou surchargés, par exemple par la génération d'un trafic important (le plus difficile et lourd possible à analyser). Une quantité importante d'attaques peut également être envoyée afin de surcharger les alertes de l'IDS. Des conséquences possibles de cette surcharge peuvent être la saturation de ressources (disque, CPU, mémoire), la perte de paquets, le déni de service partiel ou total.

- **Consommation de ressources :**

  Outre la taille des fichiers de logs (de l'ordre du Go), la détection d'intrusion est excessivement gourmande en ressources. En effet un système NIDS doit générer des

journaux de comptes-rendus d'activité anormale ou douteuse sur le réseau.

- **Perte de paquets (limitation des performances) :**

Les vitesses de transmission sont parfois telles qu'elles dépassent largement la vitesse d'écriture des disques durs, ou même la vitesse de traitement des processeurs. Il n'est donc pas rare que des paquets ne soient pas traités par l'IDS, et que certains d'entre eux soient néanmoins reçus par la machine destinataire.

- **Vulnérabilité aux dénis de service :**

Un attaquant peut essayer de provoquer un déni de service au niveau du système de détection d'intrusion, ou pire au niveau du système d'exploitation de la machine supportant l'IDS.

Une fois que l'IDS est désactivé (« hors service »), l'attaquant peut tenter tout ce qui lui convient.

II.3.2. Caractéristiques d'un IDS pour MANET :

Dans un MANET, la mobilité des nœuds, la distribution des fonctions et des données et les caractéristiques des connexions sans fil imposent des contraintes spécifiques pour la détection d'intrusions. A partir des caractéristiques générales des IDS, et des contraintes imposées par les réseaux ad-hoc, nous établissons dans cette section les spécifications d'un IDS pour MANET [17] :

- **Les principes de détection :** deux approches principales sont couramment utilisées. L'approche comportementale consiste à identifier la déviation d'un comportement par rapport à un modèle de référence. L'approche par scénarios s'appuie sur la recherche, dans les données collectées, de traces d'attaques préalablement spécifiées.
- **Les sources de données :** les données peuvent être collectées au niveau du système, dans les fichiers de log des applications ou du système d'exploitation, ou au niveau du réseau, par l'intermédiaire d'un « sniffer ». On qualifie alors respectivement les IDS de « Host Based » et de « Network Based ». Quelques travaux (Cabrera et al., 2001) proposent également l'utilisation des données stockées dans les MIB (Management Information Base)
- **La fréquence d'utilisation :** la détection des tentatives d'intrusions doit être réalisée en temps réel pour permettre aux utilisateurs de réagir immédiatement.
- **Le comportement après détection :** la réaction à la détection d'une intrusion est généralement informative, dans certains cas particuliers elle peut aussi être corrective.

Dans un objectif de portabilité et de performances, nous proposons que l'architecture de l'IDS soit indépendante de la source des données et de la méthode de détection. Les tests de détection, basés notamment sur l'évolution des faux positifs, nous permettront ensuite de sélectionner la méthode de détection la plus performante face aux différents types d'intrusions. Les données locales utilisées pour la détection des intrusions sont collectées dans la MIB. Cette source d'information est préférée ici car elle contribue à rendre l'IDS indépendant des plates-formes matérielles et logicielles utilisées. La réponse à la détection d'une intrusion doit toujours se faire sous le contrôle de l'utilisateur du nœud attaqué. Celle-ci doit pouvoir être réactive localement, par exemple en coupant la liaison avec un nœud jugé suspect, afin de renforcer le niveau de sécurité, et informative vers les autres nœuds de la communauté.

De plus, cette architecture doit aussi être adaptée aux caractéristiques des nœuds et du réseau [17] :

- **La distribution des nœuds :** l'architecture de l'IDS doit prendre en compte le caractère spontané des réseaux ad-hoc ainsi que l'absence de nœud central permanent.
- **Les débits limités des liens inter-nœuds : l**es technologies WLAN offrent encore aujourd'hui des débits inférieurs à ceux des LAN. L'IDS doit s'appuyer sur les technologies les moins consommatrices de ressources réseaux.
- **La mobilité des nœuds :** l'IDS doit utiliser des technologies adaptées à la mobilité des nœuds.
- **Normalisation :** l'architecture de l'IDS doit adopter les normes actuelles notamment pour pouvoir coopérer avec d'autres IDS.

II.4. Détection d'intrusions dans les réseaux Ad-hoc :

L'absence des nœuds pour une surveillance centralisée et le manque de confiance entre les nœuds d'un réseau mobile ad-hoc, rendent un système de détection d'intrusions centralisé irréalisable. Pour remédier aux limites des IDS classique inapproprié aux réseaux ad-hoc, plusieurs travaux de recherche ont été réalisés dans ce domaine. Dans cette partie, nous allons illustrer les modèles les plus importants des systèmes de détection d'intrusions proposés pour les réseaux Ad-hoc [4]

II.4.1. Les IDS autonomes :

Dans cette architecture, chaque nœud exécute un IDS qui détecte les attaques de façon indépendante. L'IDS autonome n'a confiance qu'en soi même, donc, il n'existe aucune coopération, ni de partage d'informations avec les autres nœuds du réseau (voir Figure). Ainsi, toute décision de détection d'intrusion est basée sur des informations disponibles au niveau du nœud.

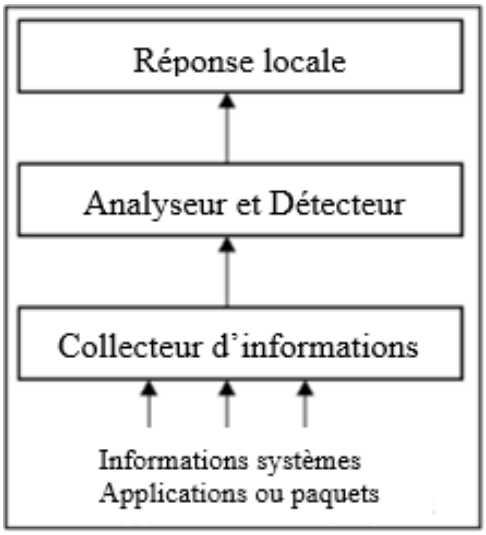


Figure II.2 : Architecture générale d'un IDS individuel

Bien que l'efficacité de cette solution soit limitée, cette architecture est mieux adaptée dans un environnement où tous les nœuds ne sont pas capables d'exécuter des IDS [4].

II.4.2. Les IDS distribués et coopératifs :

L'approche utilisé pour les IDS distribués et coopératifs [4] repose sur le principe de base des réseaux ad-hoc, la détection des intrusions, comme tous les autres services du réseau ad-hoc, doit aussi être distribuée sur l'ensemble des nœuds du réseau. Chaque nœud est autonome, et de ce fait, il ne peut s'appuyer que sur ses ressources propres pour détecter les intrusions dont il est la cible. La détection de certains types d'intrusions peut nécessiter la collecte d'informations complémentaires disponibles uniquement sur d'autres nœuds. Dans ce cas, les nœuds sont amenés à coopérer pour s'échanger des données ou encore des alertes. Zhang et Lee ont proposé la première architecture d'IDS distribuée et coopérative pour les réseaux ad-hoc présenté dans la figure 2.3.

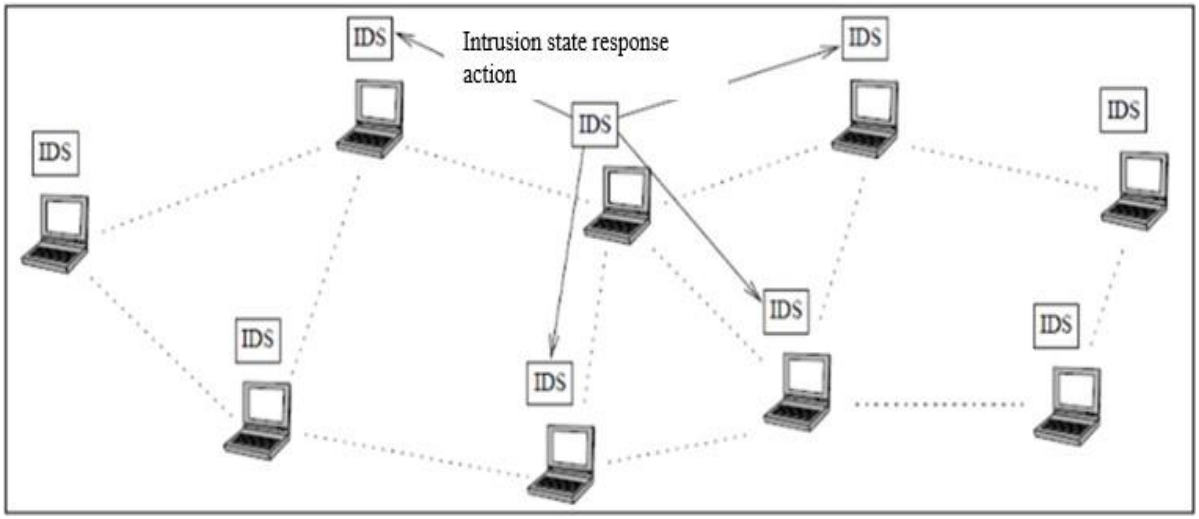


Figure II.3 : Architecture d'IDS distribué et coopératif

II.4.3. Les IDS réparties en groupes :

Les IDS réparties en groupe (Cluster-based IDS) [4] ont été proposés afin de minimiser la surcharge du réseau et d'économiser l'énergie. Dans cette architecture, le réseau Ad-hoc est divisé en un ensemble de groupes (clusters) ayant chacun un seul chef de groupe (Cluster-head) qui agit comme une petite station de base. Ainsi, la coopération est limitée entre le chef de groupe élu et chacun des membres du même groupe. Les activités malveillantes sont reportées au chef de groupe pour les analysés et détecté les intrusions. Parallèlement, tous les chefs de groupe peuvent coopérer pour former un IDS globale.

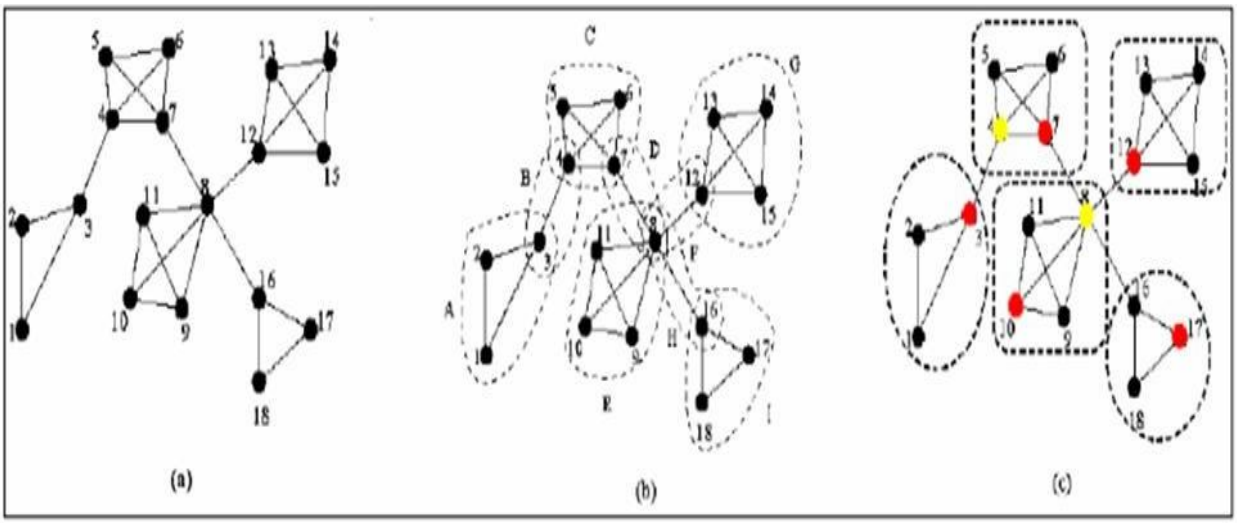


Figure II.4 : Formation des clusters dans l'IDS en groupe

II.4.4.Les IDS hiérarchique :

Une architecture hiérarchique distribuée [18] représentée à la Figure II.5 peut être décrite comme étant structurée à la manière d'un arbre avec un système de gestion et de contrôle à son sommet, des unités d'agrégation d'information comme nœuds internes et des unités d'opérations comme nœud a ses extrémités. Les unités d'opérations peuvent être des senseurs de réseaux, des IDS locaux, des détecteurs de virus ou tout systèmes de réponses aux attaques

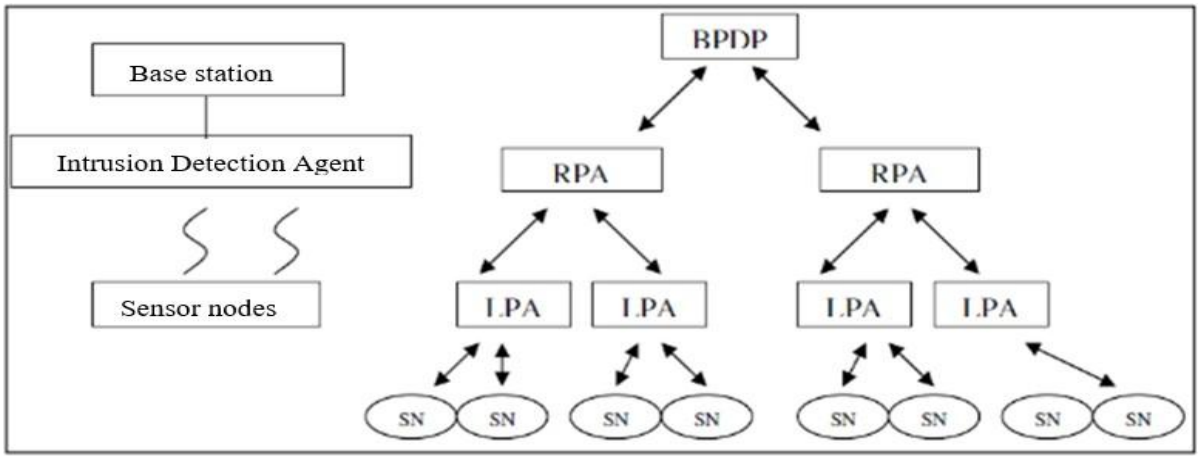


Figure II.5 : Architecture d'IDS Hiérarchique

II.1. Travaux antérieurs sur les IDS Ad hoc :

La détection d'intrusion dans les réseaux Ad hoc est devenue l'objet de nombreuses études. Recherche ces dernières années. En fait, même avec des mesures de sécurité préventives, il y a toujours Certains nœuds peuvent être endommagés. Dans ce cas, la détection d'intrusion peut Utiliser comme une autre couche de défense et un élément de base des réseaux publicitaires Hoc hautement sécurisé.

Plusieurs solutions ont été proposées pour la détection d'intrusions dans les réseaux Ad hoc que nous résumerons dans Le ***Tableau II.1*** [19]**.**

Tableau II.1 Solutions proposées pour la détection d'intrusions dans les réseaux Ad hoc

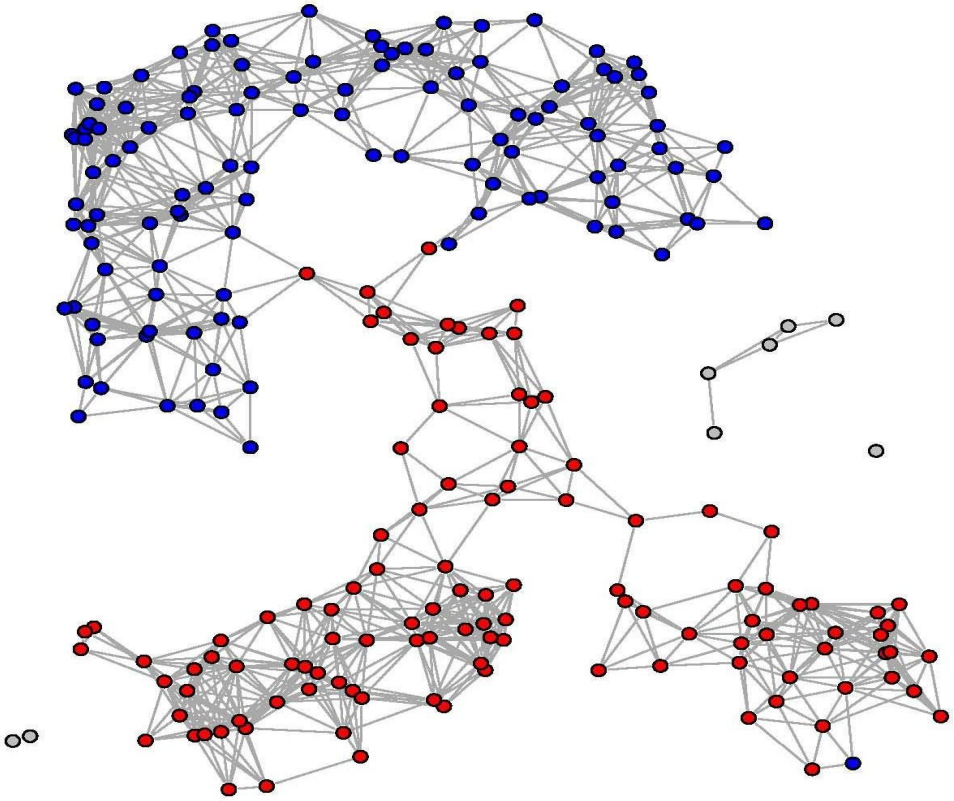
Nom de l'IDS	Origines des données	Type de détection	Prétraitement des donnés	Attaque	Type de réponse	Année
A Cooperative Intrusion Detection System for Ad hoc Networks	Couche Routage	Comportementale	Répartie en groupes	Blackhole, Routing Loop, Selfishness, Sleep Deprivation, Denial-of-Service	Passive	2003
Effective Intrusion Detection Using Multiple Sensors in Wireless Ad hoc Networks	Système	Comportementale	Répartie en Groupes	Denial-of-Service	Passive	2003
A Specification-based Intrusion Detection System for AODV	Couche Routage /AODV	Scénarios	Distribué	Forged Sequence number, Forged Hop count, Tunnelling attack	Passive	2003
IA General Cooperative Intrusion Detection Architecture for MANETs	Couche Routage /AODV	Scénarios	Hiérarchique Ré	Packet Dropping Attacks	Active	2005
nntrusion Detection of Packet Droppig Attacks in Mobile Ad hoc Networks	Couche MAC	Comportementale	Distribué	Packet Dropping Attacks	Passive	2006
Detecting Intrusion attacks in Ad hoc Networks	Couche Routage /AODV	Scénarios	Distribué	Resource Consumption, Packet dropping, Fabrication attack	Active	2007
Power-Aware Hybrid Intrusion Detection System (PHIDS) using Cellular Automata in Wireless Ad hoc Networks	Hybride/ HIDS+NIDS	Comportementale	Répartie en Groupes	Denial-of-Service	Passive	2008
Hierarchical Design based Intrusion Detection System for Wireless Ad hoc Sensor Network	Couche Routage/AO DV	Scénarios	Hiérarchique	Denial-of-Service	Active	2010

II.6 Conclusion :

Dans ce chapitre, nous avons présenté et introduit les composants nécessaires à la mise en œuvre Détection d'intrusion dans les réseaux mobiles ad hoc. Après avoir posé le contexte Spécifique à la détection des intrusions dans MANET et Les principaux IDS de ces réseaux. Nous avons conclu que le choix de l'architecture L'IDS des réseaux mobiles ad hoc dépend de la source et du type de données d'audit Nous voulons analyser l'invasion. Le prochain chapitre a pour but de présenter Nous utilisons un modèle IDS collaboratif distribué pour les réseaux sans fil autoorganisés. Analyse Le modèle IDS distribué le plus avancé nous permettra de localiser les éléments suivants Notre travail.

Chapitre III :

Contribution à la Détection d'Intrusions dans les Réseaux Ad-hoc



III.1. Introduction :

Dans un réseau Ad-hoc toutes les entités peuvent participer au routage, donc il n'y a pas de barrières pour un nœud malicieux de causer des perturbations dans le trafic circulant. L'intérêt de l'attaquant vise essentiellement à compromettre la confidentialité et l'intégrité des informations en transit.

Les MANETs sont vulnérables à diverses attaques. Les types d'attaque généraux sont les menaces au niveau de la couche MAC et la couche réseau qui est la couche la plus importante qui fonctionnent pour le mécanisme de routage du réseau ad-hoc. D'abord, la majorité des techniques de détection d'intrusion proposée dans les réseaux mobiles ad-hoc sont déployées dans la couche réseau. Les problèmes de sécurité de la couche réseau sont vitaux pour le réseau ad-hoc qui protège la fonctionnalité du réseau pour transférer les paquets entre les nœuds mobiles via le transfert de paquets à plusieurs sauts. Ensuite, dans ce chapitre, nous nous concentrons sur la détection d'intrusions d'une attaque de type « trou noir » (blackhole) qui consiste pour un nœud compromis à n'effectuer aucune retransmission des paquets qui lui ont été envoyés. De plus, nous présentons un aperçu du protocole de routage AODV et de sa relation avec l'attaque par trou noir. Enfin, dans ce chapitre nous proposons de renforcer la sécurité par un système de détection d'intrusion pour contrer l'attaque de trou noir et nous décrivons l'évaluation des performances.

III.2. Positionnement bibliographique :

Dans cette section, nous présentons le protocole AODV et le problème d'attaque en trou noir.

III.2.1. Le protocole AODV (Ad-hoc On-demand Distance Vector) :

Dans cette recherche, nous avons choisi le protocole de routage à vecteur de distance à la demande ad-hoc (AODV) [20][21] car il présente de meilleures caractéristiques de performances que les autres protocoles de routage réactifs sous différentes métriques de performances. la raison pour laquelle AODV est meilleure que les autres protocoles de routage réactifs est qu'il combine les techniques du protocole de routage DSR et DSDV et obtient les avantages des deux.

La création de lien entre deux nœuds utilisant AODV nécessite deux types de paquets de contrôle appelés **Route Request** (**RREQ**) (demande de routage) et **Route Reply** (**RREP**) (réponse de routage).

RREQ est diffusé aux nœuds adjacents pour leur demander un itinéraire vers le nœud souhaité, les nœuds continuent de transmettre RREQ jusqu'à ce qu'il atteigne le nœud de destination, ou un nœud qui a un chemin vers celui-ci.

RREP est envoyé au nœud source depuis le nœud de destination ou depuis un nœud intermédiaire qui a un chemin vers le nœud de destination. Après avoir reçu un RREP, le nœud source commence à envoyer des paquets au nœud de destination, puis met à jour ultérieurement ses informations de routage du meilleur itinéraire vers le nœud de destination. Chaque entrée de table de routage contient les informations suivantes :

- Nœud de destination
- Saut suivant
- Nombre de sauts
- Numéro de séquence de destination
- Voisins actifs pour l'itinéraire
- Minuteur d'expiration pour l'entrée de la table de routage

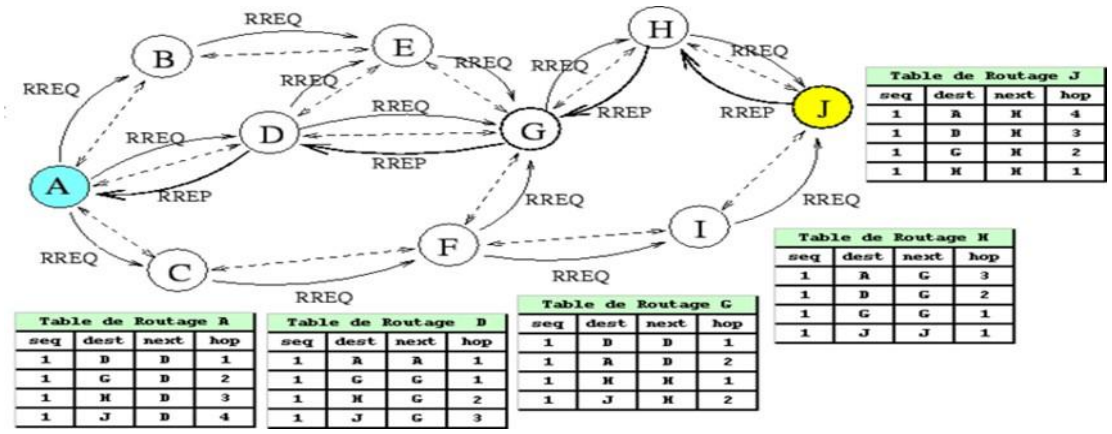


Figure III.1 : Fonctionnement de protocole AODV

Le processus de découverte de route est réinitialisé pour établir une nouvelle route vers le nœud de destination, si le nœud source se déplace dans une session active. Lorsque le lien est rompu et que le nœud reçoit une notification, et que le paquet de contrôle d'erreur de routage (RERR) est envoyé à tous les nœuds qui utilisent ce lien corrompu pour une communication ultérieure. Ensuite, le nœud source redémarre le processus de découverte.

III.2.2 Attaque en trou noir (Black-Hole Attack) :

Il s'agit d'un type d'attaque active [22][23] où le nœud attaquant prétend qu'il a le chemin le plus court vers n'importe quel nœud souhaité dans le réseau même s'il n'en a aucun ; par conséquent, tous les paquets le traverseront, ce qui permet au nœud de trou noir de transmettre ou de rejeter des paquets pendant la transmission de données. Les nœuds normaux commencent la phase de découverte afin de trouver un chemin vers le nœud de destination. Le nœud source diffuse une requête vers le nœud destination, tout nœud recevant cette requête vérifie s'il a un nouveau chemin vers le nœud destination. Lorsque le nœud trou noir reçoit cette demande, il envoie immédiatement une réponse au diffuseur affirmant qu'il a le chemin le plus récent et le plus court vers le nœud de destination.

Le nœud source croit cette réponse car il n'y a pas de mécanisme pour vérifier que la demande provient d'un nœud normal ou d'un nœud trou noir. Le nœud source commence à transférer des paquets au nœud de trou noir dans l'espoir de livrer ces paquets au nœud de destination, puis le nœud de trou noir commence à abandonner ces paquets transférés.

Les figures ci-dessous montrent un exemple d'attaque de trou noir MANET. Les attaques de trous noirs peuvent être classées en deux types : les attaques de trous noirs simples et coopératives où la classification est basée sur le nombre de nœuds attaquants. Dans une attaque par trou noir unique, un seul nœud attaquant est actif tandis que dans une attaque par trou noir coopérative, il existe un groupe de nœuds attaquants qui travaillent ensemble afin de dégrader la fiabilité du réseau.

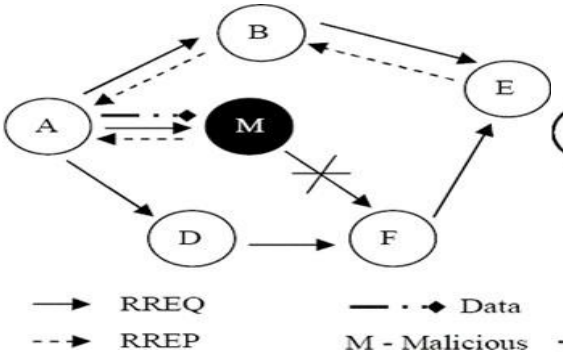


Figure III.2 : Attaque de trou noir simple

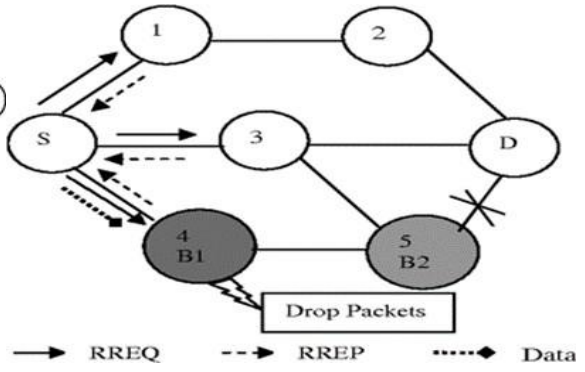


Figure III.3 : Attaque de trou noir coopérative

Comme le montre la ***figure III.2***, lorsque le nœud source demande une route vers le nœud de destination, le nœud trou noir prétend avoir le chemin le plus court vers ce nœud souhaité. Le nœud source commence à transmettre des paquets au nœud de trou noir dans l'espoir de livrer ces paquets au nœud de destination ; Le nœud trou noir supprime tous les paquets transférés pour empêcher la communication entre la source et le nœud de destination.

III.3. Méthodologie proposée :

Nous proposons un nouvel IDS d'architecture distribué et coopérative qui sera présenté en adaptant dans chaque nœud de réseau un Cuckoo Algorithme qui sera responsable de la détection d'intrusions. Cette méthode utilisée pour informer les autres nœuds d'une attaque détectée localement et, si nécessaire, pour collecter des informations complémentaires disponibles uniquement sur les autres nœuds du réseau.

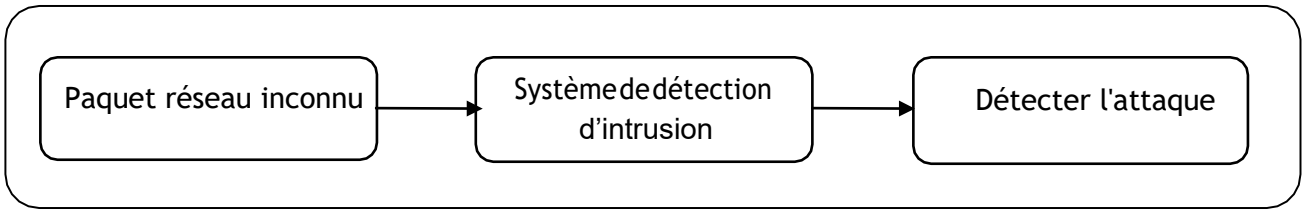


Figure III.4 : Système de détection d'intrusion

III.3.1. Algorithme de Cuckoo :

L'algorithme de Cuckoo est développé comme une approche métaheuristique avec une inspiration de coucou d'oiseau. Cet oiseau ne fait jamais son nid et pond généralement ses œufs dans le nid d'un autre oiseau. Peu d'oiseaux hôtes peuvent s'engager directement avec le coucou intrus [24][25]. Si l'oiseau hôte trouve les œufs, qui ne sont même pas les siens, alors il jette les œufs du nid ou soulage son nid ou fait un nouveau nid. Dans le nid, chaque œuf montre une solution et l'œuf de cuckoo représente une nouvelle et meilleure solution. La solution obtenue est une nouvelle solution basée sur une solution existante avec quelques modifications dans les caractéristiques. L'algorithme de cuckoo est utilisé pour résoudre les problèmes de planification et pour résoudre les problèmes d'optimisation de la conception en ingénierie structurelle.

La recherche de coucou admire le comportement de reproduction et peut être développée pour différents problèmes d'optimisation comme mentionné ci-dessous [24] :

- Chaque coucou pond un seul œuf à la fois et le dépose dans un nid choisi arbitrairement.
- Les meilleurs nids ayant une qualité d'œufs élevée porterait à la génération suivante.
- Il y a un nombre fixe de nids hôtes accessibles et si un oiseau hôte trouve l'œuf de coucou ayant une probabilité de page [0,1] alors l'oiseau peut les jeter ou les abandonner et générer un nouveau nid.

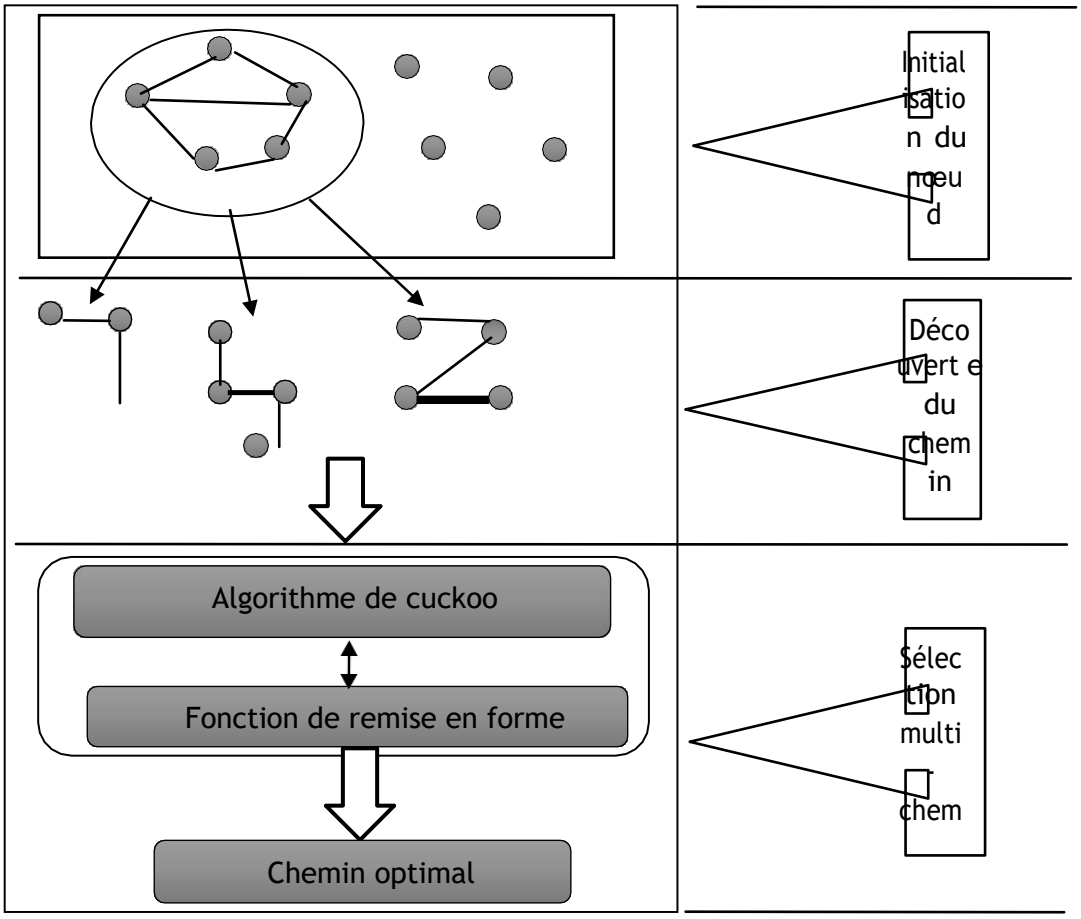


Figure III.5 : Fonctionnement de l'algorithme de cuckoo

III.3.2. Aperçu sur NS2 :

Plusieurs simulateurs pour réseaux informatique sans fil ont été proposés ces dernières années, parmi lesquels NS-2, GloMoSim, JiST/SWANS, GTSNetS, OMNet++, Opnet, ...etc. Ces simulateurs offrent tous un environne avarice de programmation pour l'implémentation et l'évaluation des performances des protocoles de communication.

Network Simulator (NS-2) est un simulateur à événements discrets orienté objet, écrit en C++ avec une interface qui utilise le langage OTcl (Object Tool Command Langage). A travers ces deux langages il est possible de modéliser tout type de réseau et de décrire les conditions de simulation : La topologie réseau, le type du trafic qui circule, les protocoles

utilisés, les communications qui ont lieu ...etc. Le langage C++ sert à décrire le fonctionnement interne des composants de la simulation. Pour reprendre la terminologie objet, il sert à définir les classes. Quant au langage OTcl, il fournit un moyen flexible et puissant de contrôle de la simulation comme le déclenchement d'événements, la configuration du réseau, la collecte de statistiques, ...etc. [26]

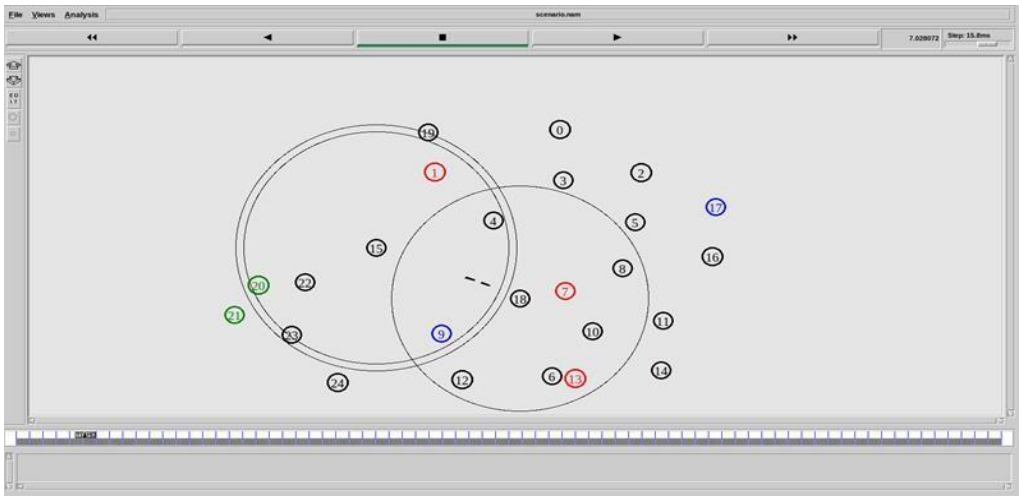


Figure III.6 : Simulateur NS2

III.4. Simulation :

III.4.1. Objectifs :

L'objectif principal de cette simulation consiste à implémenter un réseau ad-hoc avec le protocole de routage AODV et augmenter le nombre de nœuds à chaque foi. Ensuite, arriver à comparer et évaluer les performances d'un réseau Ad-hoc par rapport à la qualité de service dans les cas d'une intrusion et sa solution proposé (IDS), en mesurant le débit, le taux de livraison des paquets, le délai de bout en bout et les pertes des paquets. Dès lors, nous devons à travers notre simulation se rapprocher le plus possible de la réalité en choisissant des modèles réalistes.

III.4.2. Implémentation de l'IDS dans le noyon de NS2 :

Dans notre proposition de détection d'intrusion l'algorithme de Cuckoo est intégré au protocole AODV pour une meilleure découverte du routage après avoir détecté l'intrus. La méthode proposée est simulée dans NS2 et les résultats sont calculés pour un nombre variable de nœuds. Pour l'expérience, des modifications mineures sont apportées à la recherche de base du coucou à des fins d'intégration et pour un meilleur fonctionnement. Comme NS2 est compilé en C++, la recherche de coucou est écrite en C++ et elle est intégrée dans la partie découverte de route.

En général AODV, les nœuds avec un numéro de séquence plus élevé et moins de nombre de sauts sont sélectionnés. En utilisant l'algorithme de cuckoo, ces nœuds sont sélectionnés après plusieurs itérations assurant l'efficacité du chemin. Si l'efficacité est réduite, un nouveau chemin est trouvé à l'itération suivante. Lors d'une attaque de trou noir, lorsque les paquets ne sont pas reçus par destination, l'algorithme de cuckoo supprime le chemin actuel et trouve un nouveau chemin et marque les nœuds malveillants et les restreint de les sélectionner plus loin dans la découverte d'itinéraire. L'algorithme utilisé dans l'expérience est illustré ci-dessous :

Algorithme de cuckoo :

```
Begin
Objective function Gi
Produce initial population for n number of host nest equal to nodes
While (m<Max Generation) or (halt criteria)
        Obtain a cuckoo arbitrarily
        Execute its fitness Gi
        Decide a nest between n arbitrarily
            If (Gi<Gj)
            Change j with novel solution
            End if
A fraction of inferior nest is discarded and novel ones are developed
Keep the better solutions
Rank the solution and evaluate the solution and existing best
End while
    Post process results
End begin
```

L'organigramme de base qui sera suivi est présenté ci-dessous :

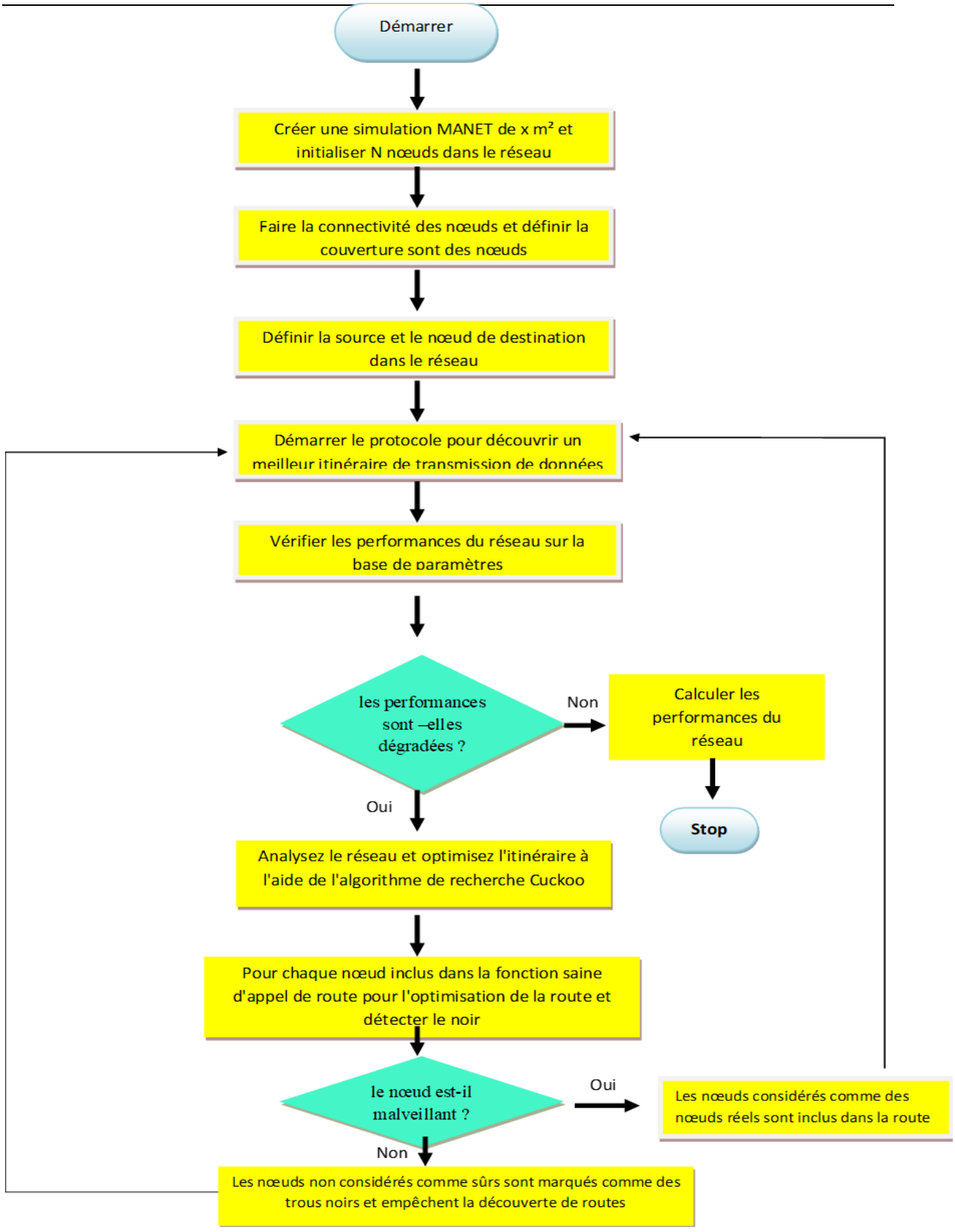


Figure III.7 ***: Organigramme***

III.5. Résultats de la simulation :

Dans cette partie, la mise en œuvre de l'algorithme proposé est faite. L'algorithme a été exécuté plusieurs fois avec différents nombres de nœuds. L'expérience a été faite plusieurs fois pour obtenir des meilleurs résultats.

III.5.1. Paramètres d'entrée :

Pour des résultats efficaces, le nombre de nœuds est varié séquentiellement de 20 nœuds à 30 nœuds. Dans chaque cas, le nombre de trous noirs est également augmenté pour maintenir le nœud de trou noir. Pour conserver un semblable environnement, un nombre fixe de paquets est envoyé sur chaque cas, c'est-à-dire 490 paquets et chaque simulation est exécutée pendant une période fixe de 40 secondes. Les nœuds sont tous placés dans le plan XY.

Tableau III.1 : Nœuds et trous noirs

Nœuds	Trous noirs
20	2
25	2
30	3

Ces paramètres de QoS sont utilisés pour calculer performances du réseau :

- **Taux de livraison des paquets (*PDR : packet delivery ratio)*** : Il est défini comme un nombre de paquets de données délivrés à celui généré par les sources.

PDR = Paquet de données délivré à toutes les sources / Paquet de données envoyé par toutes les sources

- **Délai de bout en bout *(End to end delay) :*** Le délai de bout en bout ou délai unidirectionnel (OWD) fait référence au temps nécessaire pour qu'un paquet soit transmis sur un réseau de la source à la destination. Il s'agit d'un terme courant dans la surveillance des réseaux IP et diffère du temps aller-retour (RTT) en ce que seul le chemin dans une seule direction de la source à la destination est mesuré.
- **Débit *(Throughput) :*** le débit est le taux avec lesquels les paquets sont réussis transmis sur le réseau. Il est généralement représenté comme une moyenne et calculé en paquets de données par seconde ou en bits par seconde (bps). Il est considéré comme un indicateur nécessaire de la qualité et les performances d'un réseau. Une

grande quantité d'échec la livraison des paquets entraînera une baisse débit et des performances réduites. Le débit du réseau est affecté par de nombreux facteurs. Il s'agit de fonctionnalités comme le traitement du matériel physique Puissance. Le débit peut être affecté par congestion du réseau et perte de paquets.

- **Perte de paquets *(Packet loss) :*** La perte de paquets est le nombre du nombre de paquets qui ont perdu la trace du chemin et ne parvient pas à atteindre leur destination. Les erreurs de transmission de données, comme la congestion du réseau, ou sur les réseaux sans fil sont les principales raisons de la perte de paquets. Dans notre projet, principale raison de la perte de paquets est l'existence de trous noirs dans le réseau. La perte de paquets est calculée pour montrer combien le trou noir affectera les performances du réseau. La perte de paquets est calculée en plus car le taux de livraison des paquets peut ne pas.

Tableau III.2 : Paramètres de simulation

Paramètres	Définition
Protocole	AODV
Nombre des nœuds	20.25.30
Nombre de nœud de trou noir	2
La durée de simulation	10s
Type de trafic	CBR (constant bit rate)
La taille du paquet	512 Octets
Simulateur	NS2 version 2.34

III.5.2. Evaluation de l'impact des attaques :

Les résultats de la simulation sont donnés dans les figures. La performance du réseau est analysée en fonction de quatre des mesures telles que le taux de livraison des paquets, le débit, perte de paquets et le délai de bout en bout.

Comme le montre la ***figure 3.8***, le résultat de débit en AODV lorsqu'il y a un nœud de trou noir dans le réseau qui était le plus bas en raison de la perte de paquets causé par le nœud de trou noir.

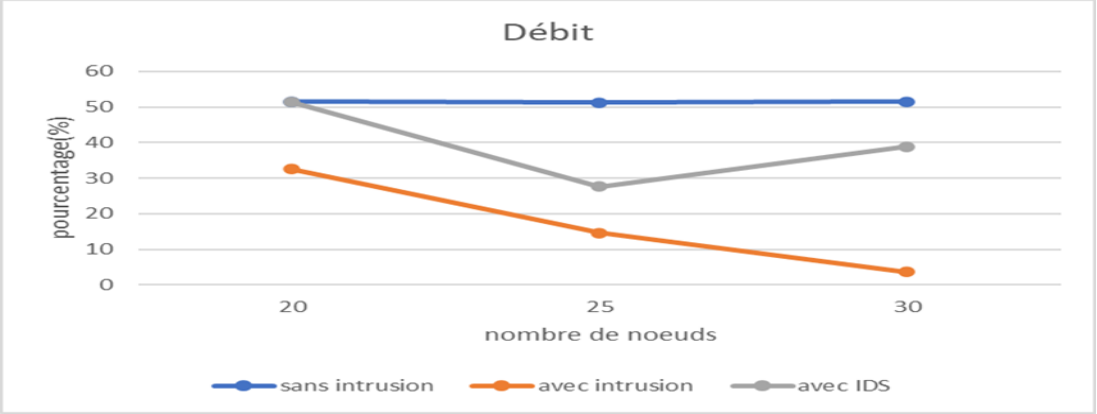


Figure III.8 : Débit

Dans la ***figure 3.9,*** le résultat de PDR dans AODV quand il y a un nœud de trou noir dans le réseau. Le résultat de la PDR dans l'AODV lorsqu'il n'y a pas de nœud de trou noir dans le réseau était le plus élevé. En regardant les résultats du IDS ont montré un PDR plus élevé que l'AODV quand il y a un nœud de trou noir, mais inférieur à l'AODV lorsqu'il n'y a pas de nœud de trou noir dans le réseau. L'amélioration de l'IDS suggéré est due à la baisse de toute réponse provenant d'un nœud inconnu, ce qui diminue PDR. De plus, la position du nœud de trou noir joue une règle importante, car il peut être situé dans le chemin le plus court entre la source et la destination.

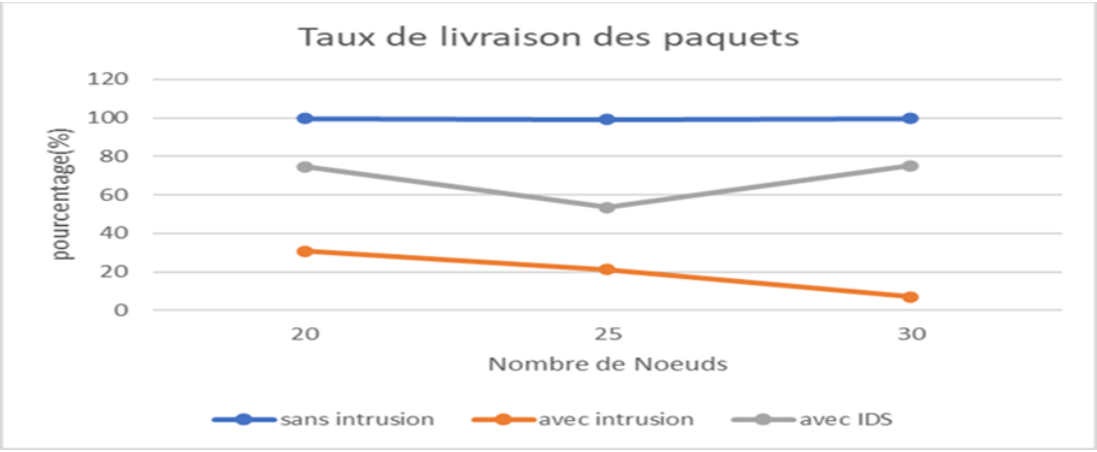


Figure III.9 : Taux de livraison des paquets

Comme le montre la ***figure 3.10***, le résultat du délai de bout en bout dans AODV avec intrusion dans le réseau était le plus élevé. Les résultats montrent une légère différence dans le délai de bout en bout par rapport à l'AODV natif quand il n'y a pas de nœud de trou noir et c'est à cause du mécanisme de sélection de chemin dans IDS qui reste le même comme pour le cas dans AODV sans intrusion.

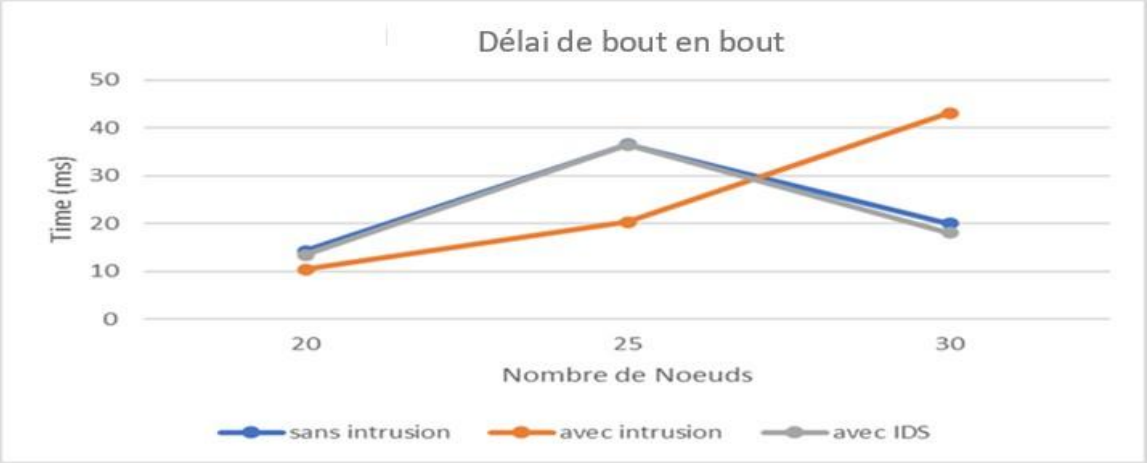


Figure III.10 : Délai de bout en bout

On peut supposer qu'avec plus de nœuds, le rapport de livraison de paquets est égal à celui de l'AODV simple sans trou noir.

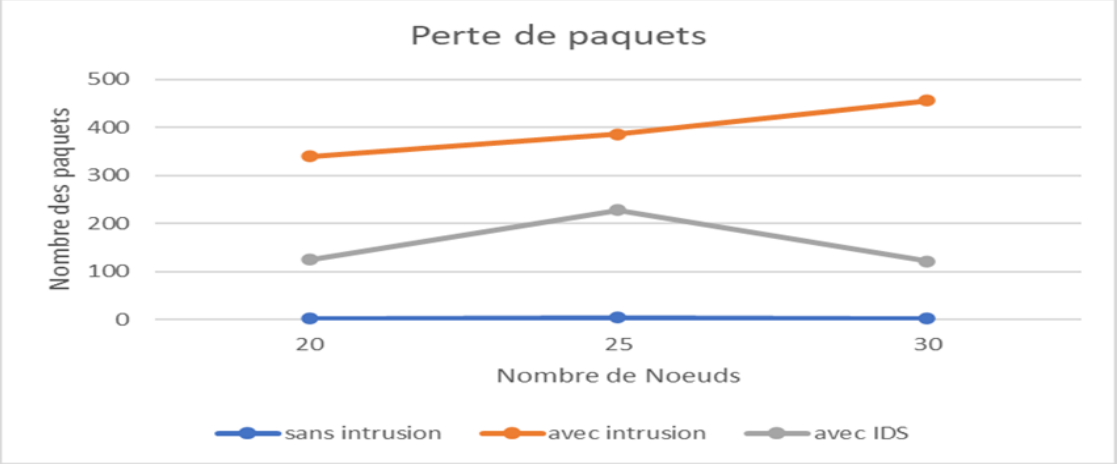


Figure III.11 : Perte de paquets

III.5.3. Etude comparative

Nous avons choisi de comparer notre solution avec la solution de Sandeep Kumar Arora, Shivani Vijan et Gurjot Singh Gaba nommé « Detection and Analysis of Black Hole Attack using IDS » [27].

Les auteurs ont mis en place sous NS2 les paramètres d'entrée suivants :

Paramètres de simulation	Spécification
Zone de simulation	900×900
Temps de simulation	20s

Tableau III.3 : paramètres de simulation de S. Kumar

Type de canal	Sans fil
Modèle d'antenne	Omnidirectionnelle
Propagation radio	Terre à deux voies
Nombre de nœuds	20 et 25
Nombre de nœuds de trous noirs	1
Taille du paquet	512 octets
Type de trafic	Débit binaire constant (CBR)
Mobilité	Point de cheminement aléatoire (RWP)

Comparaison des résultats pour 20 nœuds :

Tableau III.4 : résultats de S. Kumar pour 20 nœuds

Paramètres (Pour 20 nœuds)	Cas Idéal	Attaque par trou noir	Après le retrait de l'attaque de trou noir par IDS
Débit (Kbit/s)	446.11	102.16	778.63
PDR (taux de livraison des paquets) %	0.9992	0.2271	0.9762

Tableau III.5 : notre résultat pour 20 nœuds

Paramètres (Pour 20 nœuds)	Cas Idéal	Attaque par trou noir	Après le retrait de l'attaque de trou noir par IDS
Débit (Kbit/s)	51.44	32.51	51.32
PDR (taux de livraison des paquet) %	99.59	30.75	74.54

D'après les tableaux ; lorsque nous avons mis en œuvre l'IDS pour 20 nœuds, on supprime les nœuds faibles.

Le débit de notre simulation est faible en raison du délai applicable dans ce scenario, en effet, la raison est notre PC non performant, nous ne pouvons pas utiliser le même temps de simulation que dans [27], et le PDR est relativement proche les uns des autres

- Comparaison des résultats pour 25 nœuds :

Tableau III.6 : résultats de S. Kumar pour 25 nœuds

Paramètres (Pour 25 nœuds)	Cas Idéal	Attaque par trou noir	Après le retrait de l'attaque du trou noir par IDS
Débit (Kbit/s)	446.47	138.89	786.21
PDR (taux de livraison des paquets) %	0.9935	0.3089	0.053

Tableau III.7 : notre résultat pour 25 nœuds

Paramètres (Pour 25 nœuds)	Idéal Cas	Attaque par trou noir	Après le retrait de l'attaque du trou noir par IDS
Débit (Kbit/s)	51.21	14.65	27.66
PDR (taux de livraison des paquets) %	99.19	21.18	53.53

La même observation pour touts les paramètres sauf le PDR dans le cas d'attaque par trou noir. Le PDR est légèrement supérieur à notre résultat parce qu'ils utilisent un seul nœud de trou noir.

D'après les tableaux, lorsque nous avons mis en œuvre l'algorithme IDS pour 20 et 25 nœuds, ce dernier supprime les nœuds vulnérables du réseau et améliore la Qualité de service (QoS). Il est également décrit que le PDR dans le cas de l'IDS est amélioré de 76,2 % et d'autres paramètres sont également améliorés.

Les deux résultats montrent clairement que le débit et le PDR est diminué lorsque l'attaque du trou noir est simulée et après la suppression du nœud de trou noir, la valeur du débit et PDR est améliorée par IDS et approximativement atteint la même valeur qu'elle était présente pour le cas idéal.

III.5.4. Evaluation de performance dans le cas général :

Dans le but d'étudier l'impact de ces attaques dans le cas général, nous avons simulé un réseau de 60 nœuds dans une topologie en deux Grid superposé, le premier de type 6x6, la distance entre les nœuds est fixée à 225 mètres, le deuxième Grid de type 5 x 5 pour contenir uniquement les nœuds malicieux, la même distance entre les nœuds est respectée. Chaque nœud malicieux se trouve exactement au milieu de quatre nœuds du premier Grid. Le rayon de la portée de transmission est fixé à 250 mètres. Pour le trafic réseau nous utilisons cinq connexions de type CBR (0→35, 30→5, 11→6, 12→17, et 23→18) avec des paquets de taille égale à 512 bytes pendant une durée de simulation de 10 secondes.

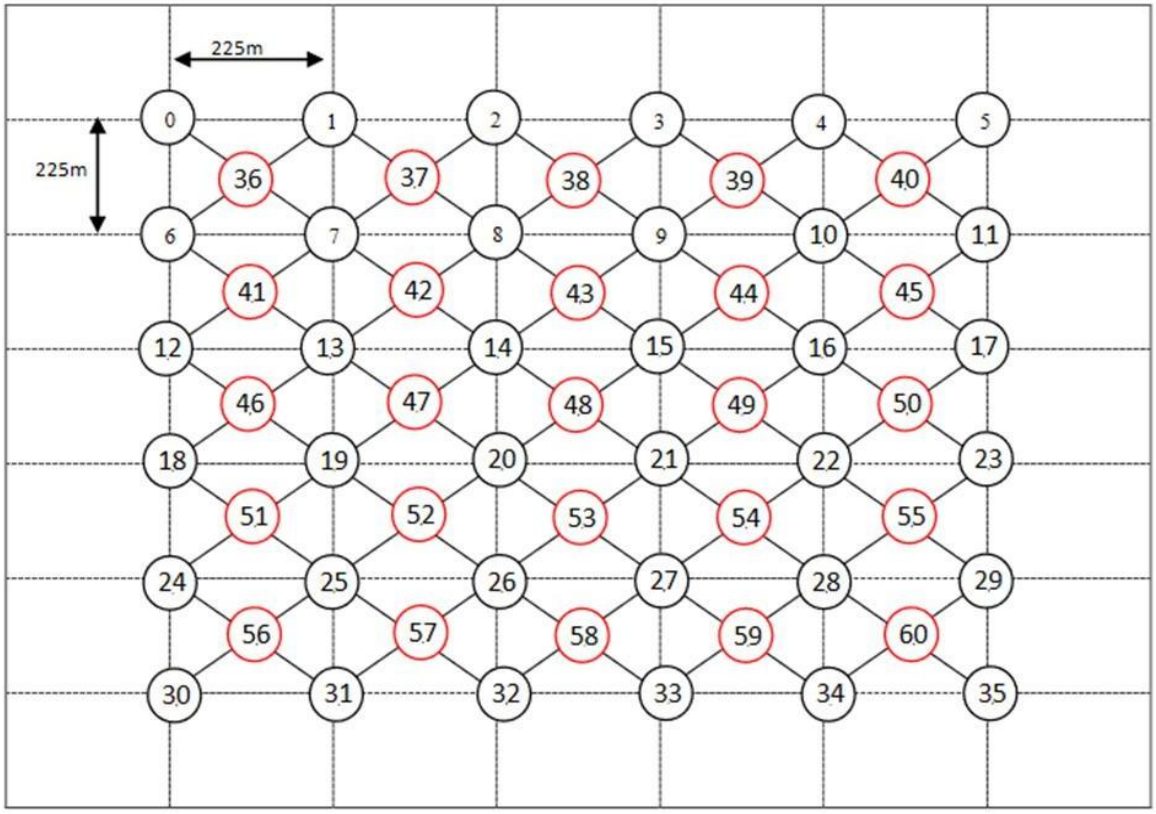


Figure III.12 : Topologie de type Grid

Pour évaluer les performances de nos solutions, nous intéressons aux métriques suivantes :

- Le débit moyen.
- Le nombre de collisions des paquets.

La ***figure3.13*** illustre l'impact du nombre des nœuds attaquants dans le réseau (de 0 à 25) avec 10 secondes comme durée de simulation.

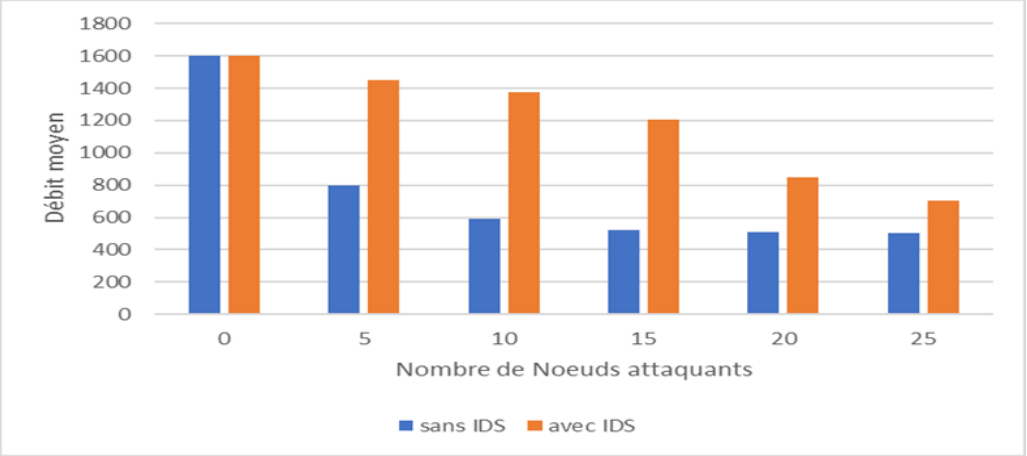


Figure III.13 : Impact du nombre d'attaquants sur le débit du réseau

Nous remarquons que lorsque le nombre de nœuds malicieux augmente, le débit du réseau diminue rapidement. Par ailleurs, en absences de nœuds malicieux, le débit sans et avec notre solution reste inchangé, cela implique que notre solution n'est pas coûteuse en termes de débit. De plus, le débit avec l'implémentation de l'IDS est toujours supérieur comparé au débit sans notre solution en cas d'attaque.

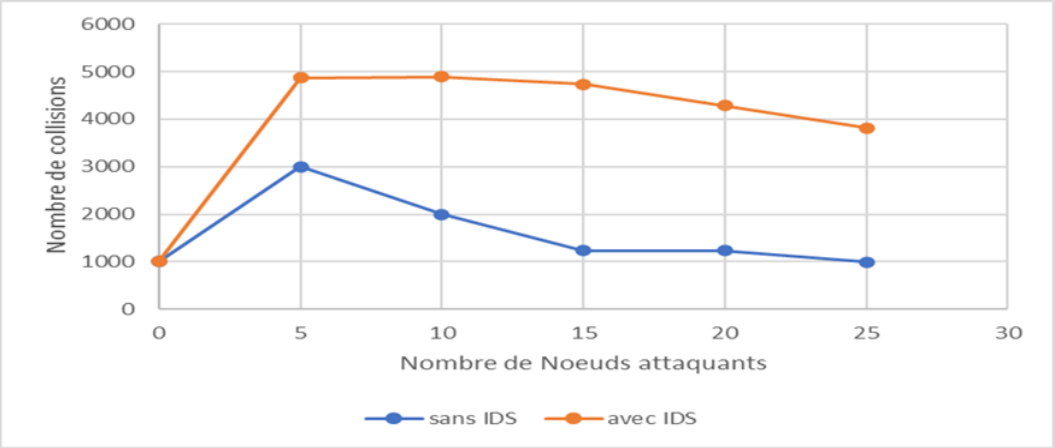


Figure III.14 : Nombre de collisions générées

La figure montre le nombre de collisions dans le réseau avec le protocole AODV (sans implémentation de l'IDS), et le nombre de collisions obtenue en intégrant l'IDS.

Nous remarquons que le nombre de collisions augmente dans le cas de 5 attaquants sans IDS, ensuite il commence à diminuer avec l'augmentation des nœuds attaquants. Cela est causé par l'envoi répétitif des demandes prétendant qu'il a le chemin le plus court de la part des attaquants.

Dans le cas où on implémente l'IDS, les nœuds ignorent toute demande de réservation du canal de communication par les attaquants en continuant d'échanger des paquets.
Parallèlement, les attaquants envoient indéfiniment les demandes, ce qui engendre un nombre important de collisions.

III.6. Conclusion :

Dans ce chapitre, nous avons montré les vulnérabilités au niveau de la couche réseaux et particulièrement dans le protocole de routage AODV et les attaques susceptibles d'exploiter ces faiblesses. Nous avons illustré l'impact négatif de cette attaque via des simulations. Un attaquant peut facilement réduire la réputation ou le niveau de confiance d'un nœud qui se comporte bien. De plus, l'opération de routage peut être affectée par cette attaque. Pour contrer ces attaques, nous avons proposé un système de détection d'intrusion distribué et coopératif avec un algorithme de cuckoo, pour le traitement de l'attaque de type trou noir, la détection et l'isolement de l'attaquant afin d'éviter le piège d'un nœud corrompu est supprimé. Tous les paquets en réclamant un nouveau chemin vers le nœud de destination et après cela, supprimer tous les paquets au lieu de les transmettre au nœud qui est défini comme destination.

Conclusion Générale

Notre mémoire a pour objectif d'apporter des solutions de détection d'intrusions dans les réseaux mobiles Ad-hoc. Les caractéristiques de ces réseaux ne permettent pas l'utilisation des solutions de détection déjà existantes.

Dans un premier temps, nous nous sommes intéressés au problème lié à la couche réseau, nous avons montré les vulnérabilités basées sur le protocole de routage AODV. Notre étude s'est focalisée sur les attaques ciblant le processus de création de table de routage en raison de son importance mais surtout de son impact sur le surmenage du protocole. Après avoir étudié l'architecture IDS et ses caractéristiques, on peut détecter les nœuds malveillants, nous avons conçu un système de détection d'intrusion basé sur la spécification du protocole AODV. Chaque nœud IDS peut détecter un nœud malveillant en analysant les paquets qu'il envoie et en les comparant avec des caractéristiques. En fonction de chaque type de paquet et du rôle du nœud malveillant (trou noir) dans le cluster, le nœud de surveillance effectue l'analyse appropriée pour extraire les informations nécessaires à la découverte du paquet.

Nous avons examiné l'impact de ces attaques sur les topologies de réseau ad-hoc à l'aide de différents scénarios. Après simulation, les résultats montrent l'efficacité de notre approche en matière de détection. De plus, le temps de réponse de la solution proposée est étudié en comparaison avec l'impact négatif des attaques, ce temps est insignifiant.

Cependant, dans la continuité du travail présenté, nous pouvons étendre notre architecture pour faire face à diverses attaques basées sur les trous noirs au niveau de la couche réseau. A cet effet, nous avons l'intention d'augmenter notre solution pour supporter la détection des attaques de routage.

Enfin, l'approche de détection d'intrusions proposée dans ce présent mémoire peut être étendue et adaptée aux réseaux de capteurs.

Annexes

Annexe A : Installation NS2 sous Ubuntu18.04 :

- Installer les logiciels complémentaires avec la commande suivante :

Sudoapt-getinstallbuild-essential autoconfautomakelibxt-dev libx11-dev libxmu-dev

- Installer le compilateur C++ avec la commande suivante :

  sudoapt-getinstall g++-4.3

- Copier le package d'installation « ns-allinone-2.34.tar .gz » dans votre dossier personnel (/home/Aicha).
- Extraire le fichier dans le même répertoire personnel.
- Entrer dans le répertoire de ns-allinone-2.34/otcl-1.13 et modifier les fichiers suivants :
- Le fichier Makefile.in : remplacer

  CC = @CC@ Par CC = gcc-4.3
- Le fichier Configue.in : remplacer

  CC = @CC@ Par CC = gcc-4.3
- Lancer l'installation de NS2 :

  - cd ns-allinone2.34
  - ./install
  - ./validate
- Editer quelque chemine dans le fichier "~/.bashrc"

  - sudogedit .bashrc
- Sauvegarder.
- Redémarrer l'ordinateur.
- Taper dans un terminal « ns », il doit s'afficher le symbole « % », dans ce cas le NS2 a été bien installé.
- Installer xgraph avec la commande : sudoapt-getinstallxgraphygraph.

Annexe B : Implémentation de IDS SOUS NS2 :

- Configuration des paramètres de simulation :

```
#     Simulation parameters setup
#=====================================
set val(chan)   Channel/WirelessChannel     ;# channel type
set val(prop)   Propagation/TwoRayGround    ;# radio-propagation model
set val(netif)  Phy/WirelessPhy             ;# network interface type
set val(mac)    Mac/802_11                  ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue     ;# interface queue type
set val(ll)     LL                          ;# link layer type
set val(ant)    Antenna/OmniAntenna         ;# antenna model
set opt(x)      1186                            ;# X dimension of the topography
set opt(y)      584                             ;# Y dimension of the topography
set val(ifqlen) 50                        ;# max packet in ifq
set val(nn)     25                          ;# number of mobilenodes
set val(seed)   1.0                         ;
set val(rp)     AODV                        ;# routing protocol
set val(stop)   100.0                       ;# time of simulation end
set val(t1)     0.0                         ;
set val(t2)     0.0                         ;
```

- Décommenter pour tester AODV-blackhole :

```
set val(dir)        "25node/blackhole/"                         ;# directory name
# Uncomment to test AODV-ori
# set val(dir)        "25node/normal/"                          ;# directory name
set val(cp)         "$val(dir)cbr.txt"          ;# traffic filename
set val(sc)                     "$val(dir)scenario.txt" ;# mobility filename
set val(out_tr)     "$val(dir)scenario.tr"   ;# output filename of tracefd
set val(out_nam)        "$val(dir)scenario.nam" ;# output filename of nametrace

#=====================================
#        Initialization
#=====================================
# Create a ns simulator
set ns [new Simulator]

# Setup topography object
set topo       [new Topography]
$topo load_flatgrid $opt(x) $opt(y)

# Create god
create-god $val(nn)

# Open the NS trace file
set tracefile [open $val(out_tr) w]
$ns trace-all $tracefile

# Open the NAM trace file
set namfile [open $val(out_nam) w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $opt(x) $opt(y)
```

- Créer un canal sans fil :

```
set chan [new $val(chan)];

#===================================
#     Mobile node parameter setup
#===================================
$ns node-config -adhocRouting  $val(rp) \
                -llType        $val(ll) \
                -macType       $val(mac) \
                -ifqType       $val(ifq) \
                -ifqLen        $val(ifqlen) \
                -antType       $val(ant) \
                -propType      $val(prop) \
                -phyType       $val(netif) \
                -channel       $chan \
                -topoInstance  $topo \
                -agentTrace    ON \
                -routerTrace   ON \
                -macTrace      ON \
                -movementTrace ON
```

- Créer des nœuds de trous noirs :

- Implémenter IDS pour détecter les nœuds de trous noirs :

```
#===================================
#         Agents Definition
#===================================
#Setup a UDP connection
set udp0 [new Agent/UDP]
$ns attach-agent $n21 $udp0
set null1 [new Agent/Null]
$ns attach-agent $n17 $null1
$ns connect $udp0 $null1
$udp0 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 1000
$cbr0 set rate_ 0.1Mb
$cbr0 set random_ null
$ns at 1.0 "$cbr0 start"
$ns at 20.0 "$cbr0 stop"
#Setup a UDP connection
set udp1 [new Agent/UDP]
$ns attach-agent $n20 $udp1
set null2 [new Agent/Null]
$ns attach-agent $n9 $null2
$ns connect $udp1 $null1
$udp1 set packetSize_ 1500
```

```
#Setup a CBR Application over UDP connection
set cbr1 [new Application/Traffic/CBR]
$cbr1 attach-agent $udp1
$cbr1 set packetSize_ 1000
$cbr1 set rate_ 0.1Mb
$cbr1 set random_ null
$ns at 20.0 "$cbr1 start"
$ns at 40.0 "$cbr1 stop"
#Setup a UDP connection
set udp3 [new Agent/UDP]
$ns attach-agent $n11 $udp3
set null3 [new Agent/Null]
$ns attach-agent $n18 $null3
$ns connect $udp3 $null1
$udp3 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr2 [new Application/Traffic/CBR]
$cbr2 attach-agent $udp3
$cbr2 set packetSize_ 1000
$cbr2 set rate_ 0.1Mb
$cbr2 set random_ null
$ns at 40.0 "$cbr2 start"
$ns at 60.0 "$cbr2 stop"
set udp4 [new Agent/UDP]
$ns attach-agent $n17 $udp4
set null4 [new Agent/Null]
$ns attach-agent $n18 $null4
$ns connect $udp4 $null4
$udp4 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr4 [new Application/Traffic/CBR]
$cbr4 attach-agent $udp4
$cbr4 set packetSize_ 1000
$cbr4 set rate_ 0.1Mb
$cbr4 set random_ null
$ns at 60.0 "$cbr4 start"
$ns at 100.0 "$cbr4 stop"

#
```

- Exécuter la simulation :

```
#Setup a CBR Application over UDP connection
set cbr4 [new Application/Traffic/CBR]
$cbr4 attach-agent $udp4
$cbr4 set packetSize_ 1000
$cbr4 set rate_ 0.1Mb
$cbr4 set random_ null
$ns at 60.0 "$cbr4 start"
$ns at 100.0 "$cbr4 stop"

#====================================
#        Applications Definition
#====================================

#====================================
#        Termination
#====================================
#Define a 'finish' procedure
proc finish {} {
    global ns tracefile namfile
    $ns flush-trace
    close $tracefile
    close $namfile
    # exec nam 25node/scenario.nam &
    exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

Bibliographies

[1]	M. Ilyas;" The Handbook of Ad Hoc Wireless Networks"; USA, CRC Press LLC, ISBN 0-8493- 1332-5, 2003.
[2]	S.Carson and j.Macker,«RFC 2501 : Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration » January 1999.
[3]	Melle.BESSAIH et Mme BOUCHAKEL «Routage et simulation dans les réseaux mobiles ad hoc». Mémoire de Fin de cycle . Béjaia 2017.
[4]	Benyettou lahouari ;" DETECTION D'INTRUSIONS DANS LES RESEAUX AD HOC", mémoire de magister en informatique, Oran 2011.
[5]	C. Perkins, E. Belding-Royer, S. Das, AODV Ad hoc On-Demand Distance Vector Routing , IETF: The Internet Engineering Task Force, July 2003, RFC 3561, work in progress.
[6]	T. Plesse, J. Lecomte, C. Adjih, M. Badel, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler et A. Plakoo, « OLSR performance measurement in a military mobile ad-hoc network », 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings, IEEE, vol. 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings, 23 mars 2004.
[7]	D. Johnson, D. Maltz, Y-C. Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) IETF: The Internet Engineering Task Force, April 2003, draft-ietf-manet-dsr-09.txt, work in progress.
[8]	FARHI LOUIZA & NAIT IGHIL Atika ; « Etude de performances de protocole de routage dans les réseaux ad hoc ».Mémoire de fin d'étude en informatique. Bejaïa 2020.
[9]	R. Abdellaoui, "SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR". Maîtrise en génie concentration réseaux de télécommunications à l'école de technologie supérieure, Montréal, 05-05-2009.
[10]	Mme LABRAOUI Nabila ; « LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL AD HOC », thèse de doctorat en informatique. TLEMCEN 2012.
[11]	Omar Cheikhrouhou « La sécurité des réseaux Ad hoc », mémoire d'ingénieur d'état en informatique, Ecole Sfax tunisien, 2005.

[12]	La Rédaction TechTarget.« Système de détection d'intrusions», le Magit (novembre 2016). Récupéré de : https://www.lemagit.fr/definition/Systeme-de-detection-dintrusions.
[13]	Mr. KEZIH Mouaad; "Détection d'attaques dans les protocoles de routage pour des réseaux informatiques." , thèse de doctorat 3 ème cycle en Electronique. ANNABA 2016.
[14]	Melle BEN BRAHIM EMBARKA & Melle AMICHE SELYNA ; « Mise en place d'une solution de détection d'intrusion ». Mémoire de Fin d'Etude de Master Académique en Réseaux & Télécommunications. TIZI-OUZOU 2017.
[15]	Sailesh Kumar, « Survey of Current Network Intrusion Detection Techniques », CSE571S: Network Security, 2007, p. 102-107.
[16]	Niva Das et Tanmoy Sarkar, « Survey on Host and Network Based Intrusion Detection System », Int. J. Advanced Networking and Applications Volume: 6 Issue: 2, 2014, p. 2266-2269
[17]	Jean-Marc Percher « un systeme de détection dintrusions distribué pour réseaux ad hoc », article dans Researchgate, mars 2004.
[18]	TRUDEAU SIMON « DETECTION D'INTRUS DANS LES RESEAUX A L'AIDE D'AGENTS MOBILES », MEMOIRE DE MAITRISEES SCIENCES APPLIQUE (GENIE INFORMATIQUE). Université de MONTREAL AOUT 2006.
[19]	Abdelaziz Amara Korba "Détection d'Intrusion et Sécurisation du Routage dans les Réseaux Ad hoc", thèse de doctorat 3ème cycle en informatique. ANNABA 2016.
[20]	Melle Hanane BOUKHALFA. Mme Nadjette MOUICI « L'impact des attaques sur la fiabilité du routage dans les réseaux Ad Hoc», MEMOIRE DE MASTER EN INFORMATIQUE. Tébessa 2016.
[21]	R.Ranjana & M.Rajaram ; "Detecting Intrusion Attacks in ADHOC Network". Asian journal of information technology 6 (7): 758-761 , India 2007. ISSN: 1682-3915.
[22]	Monika Roopak , Dr. Bvr Reddy "Performance Analysis of Aodv Protocol under Black Hole Attack", in International Journal of Scientific & Engineering Research Volume 2, Issue 8,August-2011, ISSN 2229-5518
[23]	Vimal Kumar , Rakesh Kumar "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network". Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology. Gorakhpur, 273010, U.P. , India 2015.

[24]	J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.
[25]	N. Schweitzer, A. Stulman, A. Shabtaiand R. D. Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes," in IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163- 172, Jan. 1 2016.
[26]	UC Berkeley and USC ISI, "The network simulator ns-2", Part of the VINT project. Available from http://www.isi.edu/nsnam/ns, 1998.
[27]	Sandeep Kumar Arora, Shivani Vijan and Gurjot Singh Gaba "Detection and Analysis of Black Hole Attack using IDS". Indian Journal of Science and Technology, Vol 9(20), DOI: 10.17485/ijst/2016/v9i20/85588, May 2016.