Avant Propos

Les travaux de recherche présentés dans cette thèse ont été effectués au sein du laboratoire de Développement Durable (L2D), à la Faculté des Sciences et Techniques de Béni-Mellal - Université Sultan Moulay Slimane, Maroc, sous la direction de M. Benachir EL HADADI et M. Hicham MOUNCIF. Cette thèse a été financée par une bourse d'excellence (N° : J014/012) octroyée par le Centre National de la Recherche Scientifique et Technique (CNRST), et ce dans le cadre du programme des bourses de recherche initié par le ministère de l'Éducation Nationale, de l'Enseignement Supérieur, de la Formation des Cadres et de la Recherche Scientifique.

Je tiens en tout premier lieu à exprimer ma profonde reconnaissance à M. Benachir EL HADADI, doyen de la Faculté Poly-disciplinaire de Béni-Mellal, d'avoir accepté de diriger mes travaux de recherche. Je le remercie vivement pour son intérêt constant, le suivi et l'implication inconditionnels portés à cette thèse, sa direction de cette thèse, sa disponibilité, son soutien continu, et ses encouragements tout au long de ce travail de thèse de doctorat.

Un merci particulier à M. Hicham MOUNCIF professeur d'enseignement supérieur à la Faculté Poly-disciplinaire de Beni-Mellal. Mon Co-encadrent, dont l'expérience et le sérieux n'ont d'égal que sa disponibilité et sa gentillesse. La confiance qu'il a toujours su me témoigner durant ces années ainsi que les précieux conseils qu'il a su me prodiguer aux moments cruciaux ont été pour moi essentiels dans mon travail. Je remercie tout particulièrement les membres de mon jury de thèse, qui ont accepté de juger ce travail et de participer au jury.

Je remercie également ceux qui me sont les plus chers au monde, ma mère, mon père, ma sœur, mon frère et tous les membres de ma famille pour m'avoir soutenu dans les moments les plus difficiles et pour leurs encouragements et soutien infaillibles, et je leur dédie cette thèse.

Mes remerciements s'adressent également à tous ceux qui ont contribué d'une façon ou d'une autre à la réussite de cette thèse de doctorat. Je leur exprime ici toute ma reconnaissance et ma sympathie.

Enfin, aucun mot ne saurait t'exprimer mon profond attachement et ma reconnaissance

à mon époux Mohamed ER-ROUIDI pour l'amour, la tendresse et la gentillesse dont tu m'as toujours entouré. Cher mari j'aimerai bien que tu trouves dans ce travail l'expression de mes sentiments de reconnaissance les plus sincères car grâce à ton aide et à ta patience avec moi que ce travail a pu voir le jour.

Houda.

Résumé

Résumé — Un réseau mobile ad hoc (MANET) est un nouveau domaine de la communication sans fil fonctionnant dans un environnement extrêmement imprévisible et dynamique. Ces réseaux gagnent en popularité ces dernières années en raison de leur facilité de déploiement. Un réseau MANET est constitué d'un ensemble de nœuds mobiles sans fil capables de communiquer entre eux sans l'utilisation d'une infrastructure fixe ou d'une administration centralisée. Par conséquent, en fournissant des communications en l'absence d'une infrastructure fixe ou d'une administration centralisée, les réseaux MANETs constituent une technologie attrayante pour de nombreuses applications. Cependant, cette flexibilité introduit de nouvelles menaces pour la sécurité. De plus, la méthode traditionnelle de protection des réseaux ne s'applique pas directement aux réseaux MANETs.

Parmi les nombreuses attaques et menaces à la sécurité, les réseaux MANET sont particulièrement vulnérables aux attaques par trous noirs car ils peuvent être facilement lancés sur le réseau. Le nœud malveillant qui initie l'attaque du trou noir attire tous les paquets de données vers lui en prétendant faussement un itinéraire le plus court et le plus récent vers n'importe quel nœud de destination du réseau, sans disposer d'aucun itinéraire actif vers la destination spécifiée, puis supprime tous les paquets de données, sans les transférer vers la destination souhaitée.

Dans cette thèse, nous proposons quelques mécanismes de sécurité pour les réseaux mobiles ad hoc, en premier lieu, un protocole de routage AODV (Ad hoc On Demand Distance Vector) modifié est conçu avec des contre-mesures pour éliminer une ou plusieurs attaques de trou noir. Deuxièmement, un mécanisme de sécurité cryptographique a été proposé pour sécuriser le protocole OLSR (Optimized Link-State Routing). Enfin, nous proposons un système de détection d'intrusion bénéficiant de la combinaison du système ANFIS (Adaptive Neuro Fuzzy Inference System) et de l'optimisation d'essaims de particules (PSO) afin de détecter et de prévenir l'attaque des trous noirs.

Mots clés : Réseaux mobiles ad hoc, routage sécurisé, système de détection d'intrusion, attaque par trou noir, Ad hoc On demand Distance Vector (AODV), Optimized Link-State Routing protocol (OLSR), simulateur NS-2.

Abstract

Abstract — Mobile Ad hoc NETwork (MANET) is a new field of wireless communication operating in an extremely unpredictable and dynamic environment. These networks are gaining an increasing popularity in recent years due to their ease of deployment. A MANET consists of a set of wireless mobile nodes that are capable of communicating with each other without the use of any fixed infrastructure or any centralized administration. Therefore, by providing communications in the absence of a fixed infrastructure or centralized administration, MANETs are an attractive technology for many applications. However, this flexibility introduces new security threats. Furthermore, the traditional way of protecting networks is not directly applicable to MANETs.

Among the numerous security attacks and threats, MANETs are particularly susceptible to black hole attack because it can be easily launched on the network. The malicious node that initiates the black hole attack attracts all the data packets towards it by falsely claiming a shortest and recent route to any destination node in the network, without having any active route to the specified destination, and then drops all the data packets, without forwarding it to the desired destination.

In this thesis, we propose some security mechanisms for mobile ad hoc networks, first, a modified Ad hoc On demand Distance Vector (AODV) routing protocol is designed with countermeasures to eliminate one or multiple black hole attack. Secondly, a cryptographic security mechanism has been proposed to secure the Optimized Link-State Routing protocol (OLSR). Finally, we propose an intrusion detection system benefitting from the combination of Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) in order to detect and prevent the black hole attack.

Keywords : Mobile Ad hoc NeETworks (MANETs), secure routing, Intrusion Detection System, Black Hole Attack, Ad hoc On demand Distance Vector (AODV), Optimized Link-State Routing protocol (OLSR), Network Simulator (NS-2).

Table des matières

Table des figures

Liste des tableaux

Table des sigles et acronymes

ADSN	*Average Destination Sequence Number*
ANFIS	*Adaptive Neuro Fuzzy Inference System*
ANN	*Artificial Neural Network*
ANSN	*Advertised Neighbor Sequence Number*
ARAN	*Authenticated Routing for Ad hoc Networks*
ARIADNE	*A Secure On-Demand Routing Protocol for Ad Hoc Networks*
AODV	*Ad hoc On demand Distance Vector*
CBR	*Constant Bit Rate*
DSR	*Dynamic Source Routing*
FIS	*Fuzzy Inference System*
FPR	*Forward Packet Ratio*
GA	*Genetic Algorithm*
GPS	*Global Positioning System*
IDS	*Intrusion detection system*
MANET	*Mobile Ad hoc NETworks*
MF	*Membership Function*
MPR	*Multi-Point Relays set*
MSE	*Mean Squared Error*
MSN	*Message Sequence Number*
NS-2	*Network Simulator version 2*
OLSR	*Optimized Link State Routing*
OTCL	*Oriented Tool command Language*
PAN	*Personal Area Network*
PDA	*Personal Digital Assistant*
PDR	*Packet Delivery Ratio*
PSO	*Particle Swarm Optimization*

RERR	*Route ERRor*
RREP	*Route REPly*
RREQ	*Route REQuest*
SAODV	*Secure Ad hoc On demand Distance Vector*
SAR	*Security aware Ad hoc Routing*
SEAD	*Secure Efficient Ad hoc Distance vector*
SLSP	*Secure Link State Routing Protocol*
SOLSR	*Secure Optimized Link State Routing*
SRP	*Secure Routing Protocol*
TCP	*Transport Control Protocol*
UDP	*User Datagram Protocol*
VANET	*Vehicular Ad hoc NETwork*

Introduction générale

1. Contexte Général

La conception de périphériques sans fil tels que les téléphones cellulaires, les ordinateurs portables, les assistants numériques personnels (PDA) et les micro-capteurs a permis le développement de réseaux mobiles ad hoc (MANETs) [10] dans lesquels un groupe de nœuds sans fil forment un réseau entre eux. Contrairement aux réseaux filaires et cellulaires, un réseau sans fil ad hoc ne dépend d'aucune infrastructure établie ou administration centralisée, telle qu'une station de base ou un routeur, pour la communication. C'est pourquoi on l'appelle aussi des réseaux sans infrastructure. MANET est un réseau autonome de nœuds mobiles sans fil qui se déplace librement et de manière aléatoire, en s'organisant de manière arbitraire. Par conséquent, la topologie du réseau est de nature dynamique et change rapidement et d'une manière imprévisible. Ces réseaux ne disposent pas d'infrastructure fixe pour la livraison de paquets de bout en bout. Par conséquent, les nœuds agissent à la fois en tant qu'hôte et en tant que routeur pour la transmission de paquets sur le réseau. Ces dernières années, les réseaux sans fil ad hoc ont trouvé des applications dans les réseaux véhiculaires (VANETs) [61], militaires, lors de catastrophes naturelles, de conférences commerciales, d'environnements éducatifs et de maisons intelligentes.

Comme le fonctionnement du MANET nécessite la coopération des nœuds participants du réseau, la sécurité est une préoccupation majeure pour ces réseaux. De nombreuses applications [4], en particulier le militaire et de secours, reposent sur des réseaux ad hoc, où l'application des exigences de sécurité est plus difficile à appliquer que dans les réseaux filaires traditionnels. Le routage sécurisé est également difficile en raison de l'absence d'administration centralisée sur le réseau et chaque nœud doit faire confiance aux autres nœuds pour acheminer leurs paquets. Ainsi, la présence de nœuds qui se comportent mal dans le réseau peut facilement perturber le fonctionnement du réseau et endommager la communication au sein du réseau. Par conséquent, la sécurité du routage est un aspect important qui doit être intégré aux MANETs pour réussir la communication entre les nœuds. Ainsi, en fournissant un routage sécurisé grâce à la détection de mauvaise conduite et d'atténuation dans les réseaux MANETs est un sujet de recherche important et critique. Dans le cadre de cette thèse, l'attaque par trou noir, qui est une attaque contre la sécurité dans les réseaux mobiles ad hoc, est examinée et des solutions sont proposées et évaluées pour maintenir

un niveau optimal de performance du réseau en présence de nœuds malveillants.

2. Motivation

Les réseaux MANETs occupent aujourd'hui une place très importante en termes de recherche et d'investissement par rapport aux réseaux filaire en raison de leurs caractéristiques appropriées, telles que le déploiement rapide et l'absence d'infrastructure ou de point d'accès centralisé. Pour ces raisons, les MANETs sont particulièrement souhaitables pour de nombreuses applications telles que les champs de batailles, les situations catastrophiques, les conférences virtuelles, etc. En outre, le routage dans ces réseaux est très sensible aux menaces à la sécurité pour les raisons suivantes :

- Les nœuds mobiles dans les réseaux MANETs communiquent en coopération en raison de l'absence d'infrastructures comme les routeurs et autres.
- En raison des liens sans fil et de l'architecture ouverte des MANETs, tout le monde peut rejoindre et quitter le réseau à tout moment, de sorte qu'un nœud malveillant peut également rejoindre le réseau afin de perturber le fonctionnement du routage.
- Dans les réseaux MANETs, certains protocoles de routage très couramment utilisés sont AODV [47], OLSR [19] et DSR [22]. Ces protocoles de routage sont développés sur la base de certaines hypothèses, telles qu'il n'existe aucun nœud malveillant sur le réseau et que tous les nœuds se font confiance. En raison de ces hypothèses, les nœuds malveillants peuvent causer des problèmes de sécurité dans les MANETs via diverses attaques de routage et de transfert de données.
- Un autre problème concerne les contraintes de ressources. Par exemple, presque tous les nœuds font confiance à une batterie épuisable dans les MANETs, ce qui permet aux attaquants de l'exploiter pour compromettre le réseau.
- La topologie dynamique des MANETs rend plus difficile la détection des nœuds malveillants.

La sécurisation des réseaux MANETs reste un problème complexe [32]. Tout d'abord, les mécanismes de sécurité traditionnels utilisés dans les réseaux avec infrastructure ne peuvent pas être applicables aux MANETs. Aussi, MANET souffre non seulement du même type d'attaques dans les réseaux filaires, telles que l'usurpation d'adresse IP, les attaques de dénis de service et la distorsion des messages, mais également des nouvelles attaques provoquées par les caractéristiques uniques des MANETs, telles que les attaques par trous noirs, les attaques par trous de ver et l'attaque d'abandon de paquets. Par exemple, l'attaque par trou

noir peut se produire lorsqu'un nœud malveillant se déclare comme ayant le chemin le plus court vers un nœud dont il veut intercepter les paquets. Cela permet au nœud malveillant de s'insérer entre les nœuds communicants, puis de supprimer tous les paquets. MANET est plus ouvert à ce type d'attaque car la communication est basée sur une confiance mutuelle entre les nœuds participants et il n'existe aucune surveillance centralisée de leur comportement correct.

3. Objectifs et contributions

Dans le cadre de cette thèse, nous nous sommes intéressés aux problèmes de sécurité des communications entre les nœuds dans les réseaux mobiles ad hoc. Pour cela, notre objectif principal consiste à proposer des mécanismes de sécurité tout en tenant compte de plusieurs contraintes qui caractérisent ce genre de réseaux. Dans un premier temps et afin de justifier le choix de la sélection de l'attaque du trou noir, nous avons évalué les performances du protocole de routage AODV sous l'influence des attaques de trous noirs, d'inondations et de précipitation suivant les critères de la taille du réseau, la mobilité, la charge de trafic et le nombre d'adversaires.

La deuxième étape de notre étude, consiste à sécuriser les protocoles de routage des réseaux mobiles ad hoc. Puisque le routage a un rôle primordial dans l'acheminement des paquets de données entre les nœuds du réseau. Donc, il est indispensable de bloquer toutes les tentatives qui visent à modifier ces fonctionnalités par un nœud malveillant.

Afin de sécuriser les protocoles de routage des réseaux MANETs, nous avons proposé une nouvelle approche pour éliminer un ou plusieurs nœuds de trous noirs sur le protocole de routage réactif AODV. Dans cette approche proposée, le nœud intermédiaire transmet seulement le valide paquet de réponse d'itinéraire au nœud suivant. Ensuite, pour assurer la sécurité dans le protocole de routage proactif OLSR, nous avons proposé une solution basée sur des signatures numériques et des chaînes de hachage pour authentifier et vérifier l'intégrité de l'information dans les messages de contrôle avec l'inclusion des timestamps et la position géographique, obtenue par un dispositif GPS [35], afin de prévenir les attaques du rejeu et les attaques de trous de vers. De plus, nous avons proposé la construction d'un système de détection d'intrusion qui combine le système d'inférence neuro adaptatif (ANFIS) [21] et l'algorithme d'optimisation des essaims de particules (PSO) [26]. Cette approche de détection repose sur l'hypothèse qu'une attaque par trou noir provoque une

utilisation anormale de la part d'un nœud malveillant, pour détecter ces anomalies l'IDS doit être habile à distinguer entre un comportement normal et une attaque, pour cela avant de passer à l'étape de la détection, l'IDS établit un profil normal auquel il compare les nouvelles utilisations du réseau.

4. Structure de la thèse

Cette thèse est organisée en six chapitres comme suit :

Le chapitre 1 débute par une étude descriptive des réseaux mobiles ad hoc : leurs caractéristiques, leurs avantages et leurs domaines d'applications variés ainsi que leurs défis. Ensuite, les besoins en sécurité pour ces réseaux mobiles sont définis telles que l'authentification, confidentialité, intégrité, non répudiation et autres services de sécurité. Cependant, nous devons comprendre les vulnérabilités et les attaques contre les MANET afin de leur proposer des solutions de sécurité appropriées. Une brève introduction sur les vulnérabilités spécifiques aux MANETs est décrite et une classification détaillée des attaques est présentée. Ainsi que les différentes attaques au niveau du routage ad hoc est donnée.

Dans le chapitre 2, Nous avons réalisé une étude synthétique des travaux existant dans la littérature sur la sécurité dans les réseaux mobiles ad hoc, en vue de déterminer les principaux aspects dont doivent tenir compte nos contributions.

Une évaluation de performances du protocole de routage AODV sous l'influence des attaques sera réalisée dans le chapitre 3, afin de déterminer l'attaque du trou noir en tant qu'attaque de base dans la conception de nos extensions. Le chapitre se termine par l'illustration et l'interprétation des résultats obtenus et une conclusion. Le chapitre 4 est consacré principalement à la présentation de notre première contribution. Nous avons modifié dans le mécanisme de routage dans le protocole AODV pour éliminer un ou plusieurs nœuds de trous noirs. Les résultats des simulations réalisées pour évaluer les performances de l'approche proposés sont présentés et discutés à la fin du chapitre.

Dans le chapitre 5, nous proposons une solution pour sécuriser la découverte de topologie proactive à l'aide d'un protocole de routage préexistant, le routage à état de liens optimisé (OLSR). La solution proposée est basée sur des signatures numériques et des chaînes de hachage pour authentifier et vérifier l'intégrité de l'information dans les messages de contrôle avec l'inclusion des timestamps et la position géographique, obtenue par

un dispositif GPS, afin de prévenir les attaques du rejeu et les attaques de trous de vers.

La suite possible des travaux est envisagée dans le chapitre 6, par la construction d'un système de détection d'intrusion qui combine le système d'inférence neuro adaptatif (ANFIS) et l'algorithme d'optimisation des essaims de particules (PSO).

Enfin, nous terminons ce rapport par un bilan sur les travaux effectués et des perspectives de travaux futurs.

Chapitre 1

Généralités sur les réseaux mobiles ad hoc

Sommaire

1.1 Introduction

Les avancées remarquables de la technologie des réseaux sans fil et le besoin de créer rapidement des réseaux sans infrastructure préexistante, dans des situations urgentes et

des endroits parfois hostiles, ont favorisé le développement des réseaux mobiles ad hoc de façon prodigieuse. Un réseau mobile ad hoc est un système distribué, composé de plusieurs entités mobiles et autonomes, capables de communiquer entre elles sans l'existence d'une infrastructure centralisée. Ces entités communiquent via des fréquences radio et peuvent s'auto-organiser et coopérer pour fournir des services.

Dans ce chapitre, nous introduisons le concept des réseaux mobiles ad hoc, leurs caractéristiques, leurs avantages et leurs domaines d'application, ainsi que leurs défis. Nous abordons par la suite les besoins de la sécurité dans les réseaux mobiles ad hoc. Enfin, nous classifions les différentes attaques dans les réseaux mobiles ad hoc.

1.2 Les réseaux mobiles ad hoc

Un réseau mobile ad hoc [10] est un réseau auto-configurable constitué automatiquement par une collection de nœuds mobiles sans infrastructure fixe. Ces appareils sans fil communiquent directement entre eux s'ils se trouvent dans la même plage de communication radio. Si elles sont hors de portée radio, la communication nécessitera la coopération d'autres nœuds. Par conséquent, chaque nœud mobile doit fonctionner non seulement en tant qu'hôte mais également en tant que routeur.

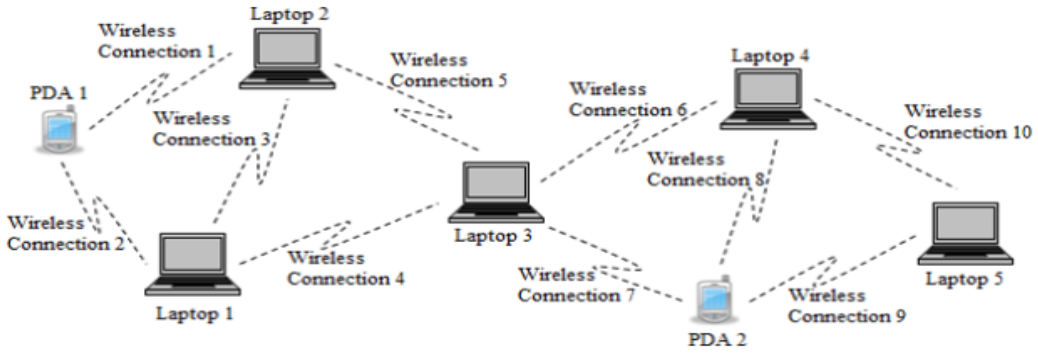


FIGURE 1.1 – Réseau mobile ad hoc

La figure 1.1 définit un réseau mobile ad hoc. Comme le montre cette figure, les nœuds ne dépendent pas d'un point d'accès ou d'une station de base pour communiquer entre eux. En fait, les nœuds utilisent leurs voisins immédiats pour transmettre leurs communications. Les nœuds commencent par découvrir leur voisinage (les nœuds qui sont dans leur zone de couverture) et à chaque fois que l'un d'entre eux souhaite communiquer, il envoie son

message à ses voisins qui à leur tour l'envoient à leurs voisins et ainsi de suite. Ce processus est répété jusqu'à ce que le message atteigne le nœud de destination.

1.2.1 Caractéristiques des réseaux mobiles ad hoc

Les MANETs ont diverses caractéristiques qui les différencient des autres réseaux, comme les réseaux filaires et les réseaux sans fil avec infrastructure, tels que :

Absence d'infrastructure : MANET ne dépend pas d'une station de base ou de point d'accès. Tous les nœuds du réseau se déplacent dans un environnement distribué sans point de rattachement à l'ensemble du réseau, fonctionnent en mode peer-to-peer étendu et se comportent comme un routeur indépendant. MANET est formé sur la base de la collaboration entre eux pour établir la communication dans un but particulier.

Topologie du réseau dynamique : Dans les MANETs, les nœuds sont autonomes et capables de se déplacer de manière arbitraire. Cette mobilité rend la topologie du réseau dynamique car elle peut changer de manière aléatoire et à des moments imprévisibles. Ce changement de topologie a un impact sur les liens unidirectionnels et bidirectionnels des nœuds. Par exemple, un nœud (routeur) peut à tout moment quitter ou rejoindre le réseau.

Canal de communication sans fil : les nœuds MANET utilisent un support sans fil pour communiquer les uns avec les autres. L'utilisation de ces liaisons sans fil rend le réseau vulnérable à des attaques telles que l'écoute et les interférences actives. De plus, les réseaux sans fil ont généralement des bandes passantes plus faibles que les réseaux filaires.

Ressources limitées : Les sources d'énergie telles que des batteries sont nécessaires pour la communication des nœuds mobiles. Malheureusement, les nœuds mobiles ont une capacité de calcul, mémoire et ressources énergétiques limitées, l'épuisement de leurs énergies dépend du traitement effectué au niveau du nœud tel que les opérations de transmission, de réception et les calculs complexes, etc.

Vulnérabilité aux différentes attaques : Les réseaux mobiles ad hoc sont des réseaux qui héritent des mêmes vulnérabilités que les réseaux sans fil traditionnels et sont en plus sensibles aux autres attaques liées à leurs propres caractéristiques.

1.2.2 Avantages des réseaux mobiles ad hoc

Les réseaux mobiles ad hoc ont réussi à s'imposer en tant qu'une technologie prometteuse. Leurs caractéristiques et notamment la mobilité et l'absence d'infrastructures élargissent leurs champs d'applications. Nous pouvons citer les points forts des réseaux mobiles ad hoc comme suit :

Le coût de déploiement est faible : les réseaux ad hoc peuvent être déployés à la volée, c'est pourquoi aucune infrastructure plus coûteuse, telle que des câbles de cuivre ou des câbles de données, n'est requise.

Déploiement simple et rapide : Les réseaux ad hoc sont très pratiques et faciles à déployer, car il n'y a pas de câbles impliqués. Ainsi, le temps de mise en œuvre est réduit.

Flexible : les MANETs peuvent être temporairement mis en place à tout moment dans n'importe quel endroit.

Topologie dynamique : la topologie du réseau ad hoc peut changer de façon dynamique au fil du temps. En comparaison avec la topologie des réseaux locaux, il est très facile de changer la topologie du réseau d'un réseau mobile ad hoc.

Réseau en endroit hostile : Dans les environnements difficiles à atteindre tels que les régions montagneuses, les réseaux mobiles ad hoc sont très pratiques. Un autre exemple de lieux hostiles est le champ de bataille.

1.2.3 Applications des réseaux mobiles ad hoc

Le déploiement d'un réseau MANET est facile en raison de l'absence de mise en place d'une infrastructure de communication. La plupart du temps, ce type de réseaux est requis dans les applications militaires et les opérations de secours d'urgence. Mais lentement, les MANETs sont entrés dans les domaines du jeu, de la détection, de la conférence, de l'informatique collaborative et distribuée [4]. Ci-dessous, nous identifions un ensemble représentatif des applications des MANETs.

Services militaires : Les services militaires sont l'un des domaines d'application les plus discutés et les plus communs dans les réseaux mobiles ad hoc, où l'installation de toute infrastructure fixe n'est pas possible dans les territoires ennemis ou sur des terrains

inhospitaliers. Dans cet environnement, MANET fournit le mécanisme de communication requis-en un rien de temps. Ici, les soldats sont considérés comme les nœuds mobiles. Le réseau doit donc rester connecté même si les soldats se déplacent librement. Ce support est fourni par le MANET. Une autre application dans ce domaine peut être la coordination des objets militaires et du personnel sur le champ de bataille. Par exemple, le chef d'un groupe de soldats peut vouloir transmettre un message à tous les soldats ou à un groupe de soldats impliqués dans l'opération. Dans cette situation, un protocole de routage sécurisé et fiable devrait être capable de faire le travail.

Services d'urgence : Celles-ci résultent de catastrophes naturelles lorsque toute l'infrastructure de communication est en désarroi (par exemple, tsunamis, ouragans, tremblements de terre, etc.) où la restauration rapide des communications est essentielle. En utilisant des réseaux mobiles ad hoc, une infrastructure pourrait être mise en place en quelques heures au lieu de jours / semaines requis pour les communications filaires.

Éducation : Universités et campus, salles de classe virtuelles, communications ad hoc lors de réunions et de conférences.

Réseaux de capteurs : Le réseau de capteurs est un cas particulier de réseaux ad hoc où la mobilité n'est généralement pas prise en compte. Cependant, la puissance de la batterie est un facteur clé dans les capteurs. Chaque capteur est équipé d'un émetteur-récepteur, d'un petit microcontrôleur et d'une source d'énergie. Les capteurs relaient les informations d'autres appareils pour transporter les données vers un moniteur central. Les capteurs sont utilisés pour détecter les conditions environnementales telles que la température, la pression, l'humidité, etc. Dans ce cas, ils forment un réseau ad hoc pour collecter les informations souhaitées. La mobilité peut également être intégrée dans le réseau de capteurs où ils sont destinés à étudier le comportement des tornades ou à étudier le comportement des patients à l'hôpital.

Réseau personnel : Les dispositifs de communication personnels tels que les ordinateurs portables, les PDA (Personal Digital Assistant) et les téléphones mobiles créent un réseau pour partager des données entre eux appelé PAN (Personal Area Network). Le PAN couvre une très courte portée pour la communication et peut être utilisé pour une communication ad hoc entre les dispositifs.

1.2.4 Défis des réseaux mobiles ad hoc

Les principaux défis dans la conception et l'exploitation de MANET proviennent de l'absence d'entité centralisée, tels que des stations de base, des points d'accès et des serveurs, une topologie changeant dynamiquement et un moyen de communication sans fil ouvert. Ce qui suit représente certains des défis des réseaux mobiles ad hoc :

Gestion de l'énergie : «La gestion de l'énergie est définie comme le processus de gestion des sources et des consommateurs d'énergie dans les nœuds ou dans le réseau dans son ensemble, afin d'améliorer la durée de vie du réseau». Les nœuds des réseaux mobile ad hoc agissent à la fois comme hôtes et comme routeurs, et ils sont exploités par des batteries dont la durée de vie est limitée. Ainsi, la gestion de l'énergie et la consommation sont importantes pour eux. Mais la plupart des protocoles conçus pour le routage et la sécurité sont adaptés aux réseaux filaires, qui supposent la présence de nœuds statiques, ayant une alimentation électrique et qui n'ont pas considéré la consommation électrique comme un problème.

Qualité de services (Routage) : L'objectif principal du routage est de trouver le bon et le meilleur chemin vers la destination. Le meilleur chemin vers une destination est basé sur plusieurs critères tels que le numéro du saut, la route sécurisée, l'utilisation de l'alimentation et la stabilité de la liaison sans fil. En raison de la mobilité dans les réseaux MANET, les liens sont souvent rompus et les itinéraires ne sont pas stables. La conception d'un protocole de routage qui s'adapte à tous les changements de routage est donc la principale exigence de MANET.

Performances du contrôle de transmission : Les principaux objectifs des protocoles de couche de transport incluent l'établissement et le maintien de connexions de bout en bout jusqu'à la fin de la transmission des données, la livraison de bout en bout fiable des paquets de données, le contrôle de flux et le contrôle de congestion. Le principal problème pour un protocole de contrôle de transmission (TCP) est qu'il ne sera pas capable de faire la distinction entre la présence de la mobilité dans le réseau et la congestion du réseau. Par conséquent, TCP doit être amélioré de manière significative pour améliorer le débit dans le réseau.

Sécurité : La sécurité des communications dans un réseau mobile ad hoc est très importante, en particulier dans les applications militaires. Le support d'accès ouvert et partagé, les contraintes de ressources, la topologie dynamique, la confiance sur d'autres

nœuds pour le bon fonctionnement du réseau sont certaines des caractéristiques de ces réseaux qui posent des défis substantiels dans la conception de la sécurité. La présence de ces caractéristiques uniques explique le besoin de solutions de sécurité pour MANET afin d'obtenir une communication de données sécurisée, une protection contre les attaques de sécurité et des performances réseau souhaitables.

1.3 Les objectifs de la sécurité

Les objectifs de base en sécurité pour les réseaux mobiles ad hoc sont les mêmes que ceux des réseaux filaires ou sans fil avec infrastructure. Les services de sécurité reposent sur quatre concepts fondamentaux : l'authentification de l'utilisateur, la confidentialité, l'intégrité des données et le trafic réseau et enfin la non-répudiation des utilisateurs.

1.3.1 Authentification

L'authentification est le processus permettant la vérification de l'identité d'un nœud ou d'une source d'information dans le réseau. Ceci est important pour garantir un véritable accès au réseau. Donc, il est nécessaire que les nœuds désirant communiquer entre eux aient besoin de vérifier l'identité de chacun pour s'assurer qu'ils communiquent avec une partie autorisée. Sans authentification, un adversaire pourrait se faire passer pour un nœud, obtenant ainsi un accès non autorisé à des ressources et des informations sensibles et interférant avec les opérations des autres nœuds.

1.3.2 Confidentialité

La confidentialité est le processus qui consiste à conserver les informations (données) envoyées illisible aux ceux qui ne sont pas autorisé à les connaître. La transmission d'informations sensibles nécessite la confidentialité. Les informations de routage et d'acheminement de paquets doivent également rester confidentielles. Les attaques contre la confidentialité visent à avoir accès à des données privées ou confidentielles, par exemple les noms d'utilisateur et les mots de passe, les numéros de cartes de crédit, les rapports secrets, etc. Pour garder la confidentialité, il est nécessaire de communiquer avec le bon partenaire. Dans le contexte de réseaux mobiles ad hoc, la confidentialité consiste à refuser l'accès aux

informations échangées entre deux nœuds du réseau par n'importe quel nœud malveillant ou indésirable. Cependant, les réseaux ad hoc se caractérisent par la diffusion générale de l'information, ce qui constitue un véritable défi pour la confidentialité.

1.3.3 Intégrité

L'intégrité est la capacité de garantir que le message reçu est le vrai qui n'a pas été falsifié ou modifié sans autorisation préalable durant sa transition de la source à la destination. Ceci est essentiel dans des situations telles que les opérations bancaires, les opérations militaires et les contrôles d'équipement. Comme pour la confidentialité, l'intégrité peut s'appliquer à un flux de messages, à un seul message ou à des champs sélectionnés dans un message. L'intégrité garantit que les parties autorisées sont uniquement autorisées à modifier les informations ou les messages afin qu'ils ne soient jamais corrompus. Donc, ce service assure une protection contre la modification intentionnelle (par un nœud malveillant) ou accidentelle (erreurs liées à la propagation radio). Dans les réseaux mobiles ad hoc, le message peut être modifié pour des raisons non-malveillantes, comme la corruption de paquet au niveau de propagation de radio. En fait, l'intégrité peut être appliquée de manière indirecte avec des protocoles de sécurité qui la confidentialité et l'authentification.

1.3.4 Non-répudiation

Le but de la non-répudiation est lié au fait que si une entité envoie ou reçoive un message, l'entité ne peut pas nier que le message a été envoyé par elle ou a été reçu. En d'autres termes, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. Autrement dit, la non-répudiation assure qu'une transaction (envoi / réception / action) ne peut pas être niée. Cela est très pratique pour la détection et l'isolation des nœuds compromis. Par exemple, si un nœud reçoit un message (paquet) erroné de la part d'un nœud malicieux, la non-répudiation permet au nœud récepteur du paquet d'accuser l'émetteur avec une preuve et informer les autres nœuds de la compromission du nœud émetteur du paquet erroné.

1.3.5 Autres services de sécurité

Nous définissons d'autres paramètres de sécurité utilisés dans l'analyse des aspects de sécurité de réseau mobile ad hoc qui sont les suivants :

Disponibilité : Les services ou les ressources devraient être disponibles pour les utilisateurs authentiques chaque fois que nécessaire même en présence de panne dans le réseau. En d'autres termes, la disponibilité consiste à assurer la continuité du service fourni par un nœud pour les utilisateurs autorisés du réseau, même en présence d'une attaque. Ce service permet non seulement de sécuriser le système mais le rend aussi tolérant aux défaillances. Ainsi, les ressources doivent rester disponibles jusqu'à ce que la panne soit réparée.

Autorisation d'accès et comptabilité : Les nœuds participant à un réseau doivent disposer des autorisations appropriées pour accéder aux ressources partagées sur ce réseau. Dans un réseau MANET, les nœuds devraient pouvoir empêcher les autres d'accéder à des informations privées sur leurs appareils. De plus, dans certains cas, les politiques d'autorisation sont accompagnées de mécanismes de comptabilisation pour suivre l'utilisation des ressources pour obtenir des informations statistiques sur le réseau.

Anonymat : L'anonymat signifie que toutes les informations qui peuvent être utilisées pour identifier le propriétaire ou l'utilisateur actuel du nœud doivent par défaut être gardées privées et ne pas être distribuées par le nœud lui-même ou le logiciel du système. Ce critère est étroitement lié à la préservation de la vie privée, dans lequel nous devrions essayer de protéger la confidentialité des nœuds contre la divulgation arbitraire à d'autres entités.

Scalabilité : La scalabilité n'est pas directement liée à la sécurité, mais c'est une question très importante qui a un grand impact sur les services de sécurité. Un réseau ad hoc peut être constitué de centaines voire de milliers de nœuds. Les mécanismes de sécurité doivent être évolutifs pour gérer un réseau aussi important.

Contrôle d'accès : ce service a pour rôle de déterminer la méthode et la politique qui permet à un utilisateur ou à un nœud d'accéder aux données ou services. Seuls les nœuds autorisés peuvent former, détruire, rejoindre ou quitter un groupe (cluster par exemple).

1.4 Vulnérabilités et attaques dans les réseaux mobiles ad hoc

Après avoir présenté les bases des réseaux mobiles ad hoc, nous examinons maintenant les différentes vulnérabilités et attaques que l'on peut trouver dans ce type de réseau [11].

1.4.1 Vulnérabilités des réseaux mobiles ad hoc

L'utilisation des liens sans fil facilite considérablement les attaques contre les réseaux mobiles ad hoc, que ce soit par une simple écoute indiscrète ou par des attaques plus nuisibles tels que la défaillance intentionnelle d'un service (déni de service). Contrairement aux réseaux classiques (réseaux filaires) où les attaquants doivent avoir un accès physique au réseau ou contournant plusieurs couches de défense telles que les passerelles et les pare-feu, dans les MANETs, il suffit que l'attaquant soit dans le champ de transmission d'un nœud pour pouvoir intercepter les communications de ce dernier. Finalement, dans quelques contextes tels que les réseaux de capteurs, les nœuds ont moins de protection physique et peuvent donc être capturés, corrompus et détournés à des fins malveillantes.

La majorité des réseaux autonomes et auto-organisés, et notamment les réseaux mobiles ad hoc, s'appuient sur des algorithmes coopératifs exigeant l'implication de tous les nœuds du réseau, afin d'assurer le fonctionnement des services majoritaires. Par exemple, les protocoles de routage sont plus vulnérables dans les réseaux mobiles ad hoc que dans les réseaux avec infrastructure, car chaque nœud doit agir comme un routeur pour ses voisins. Les nœuds pourraient, par exemple, décider de supprimer ou de modifier les informations de routage qu'ils reçoivent de leurs voisins ou d'injecter de fausses informations de routage. Ces comportements peuvent être préjudiciables au bon fonctionnement du réseau puisque le routage est l'un des noyaux de base du fonctionnement des réseaux informatiques. Un autre comportement malveillant, plus facile à réaliser, mais tout aussi nuisible pour le bon fonctionnement du réseau est le comportement égoïste prétendu d'un nœud. En d'autres termes, certains nœuds peuvent refuser d'acheminer les paquets des autres pour préserver leurs ressources matérielles.

1.4.2 Classification des attaques dans les réseaux mobiles ad hoc

Les attaques dans les réseaux MANETs peuvent généralement être classées en deux catégories principales, à savoir les attaques passives et les attaques actives [43]. Une attaque passive obtient des données échangées dans le réseau sans perturber le fonctionnement des communications, tandis qu'une attaque active implique une interruption, une modification ou une fabrication de l'information, perturbant ainsi le fonctionnement normal d'un MANET.

Quelques exemples d'attaques passives sont l'écoute indiscrète, l'analyse du trafic et la surveillance du trafic. Des exemples d'attaques actives incluent le brouillage, l'emprunt d'identité, la modification, le déni de service (DoS) et le message rejoue. Les attaques passives peuvent être surmontées en utilisant des mécanismes de cryptage puissants, ce qui rend l'obtention d'informations utiles impossible aux attaquants à partir des données interceptées, alors que les attaques actives sont très difficiles à surmonter.

Les attaques actives peuvent être classées en deux catégories, les attaques externes et les attaques internes selon le domaine des attaques. Les attaques externes sont effectuées par les nœuds qui n'appartiennent pas au domaine du réseau. De telles attaques peuvent être évitées en utilisant des techniques de cryptage et des pare-feu puissants. Les attaques internes proviennent de nœuds compromis, qui font en réalité partie du réseau. Les attaques internes sont plus sévères par rapport aux attaques externes puisque l'attaquant connaît des informations précieuses et secrètes, et possède des droits d'accès privilégiés. Ce nœud tente de collecter des informations de sécurité et peut avoir accès aux droits protégés du réseau. Puisque le nœud compromis est un nœud autorisé dans le réseau, il est très difficile d'identifier les attaques internes.

Les attaques peuvent également être classées selon la couche sur laquelle elles interviennent. La figure 1.2 montre la classification des attaques dans les réseaux mobiles ad hoc pour différentes couches du modèle OSI [41].

Chaque couche dans les protocoles de communication de réseau ad hoc a ses propres vulnérabilités. Dans la couche physique, les nœuds mobiles ainsi que les liens de communication sont vulnérables aux attaques passives et actives. L'écoute passive, le brouillage de signal, les attaques par déni de service (DoS) et la falsification de matériel physique sont parmi les attaques les plus populaires dans cette couche [2]. De telles attaques pourraient être rendues moins utiles en cryptant le signal de communication, en utilisant une techno-

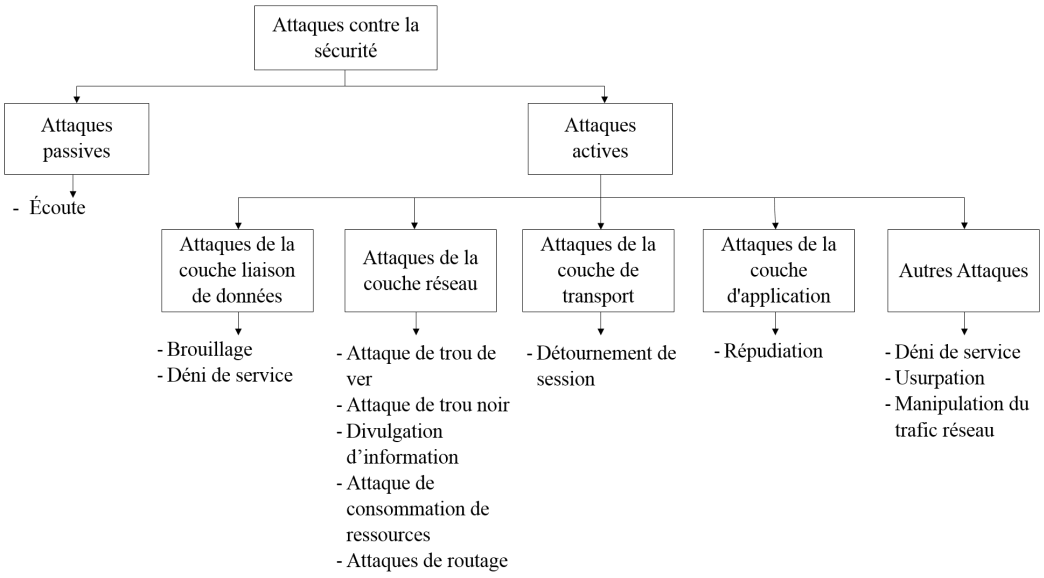


FIGURE 1.2 – Classifications des attaques dans les réseaux MANETs

logie de communication à spectre étalé et en utilisant un matériel résistant à l'altération.

Le brouillage de liens et les attaques DoS menacent également les réseaux MANETs au niveau de la couche de liaison de données. À cette couche, les adversaires peuvent bloquer les liens de communication en envoyant d'énormes données aux réseaux, ou en rejouant des paquets inutiles pour épuiser les ressources des réseaux. Des algorithmes de cryptographie coûteux et des mesures de sécurité plus sophistiquées seraient très utiles à cette couche pour protéger les réseaux et faire la distinction entre les paquets valides et invalides traversés dans les réseaux.

Les attaquants menacent également les réseaux mobiles ad hoc dans les couches de transport et d'application. Au niveau de la couche de transport, les messages sont échangés de bout en bout en utilisant des routes sécurisées établies dans la couche réseau. Pour cette raison, il est très important d'assurer la sécurité de la couche réseau pour assurer une communication fiable au niveau de la couche de transport. Comme les autres types de réseaux, les attaquants peuvent toujours trouver une faille dans les applications des réseaux ad hoc et utiliser cette vulnérabilité pour lancer des attaques sur la couche application. Cependant, puisque des attaques similaires se produisent également dans les autres types de réseaux, les solutions régulières utilisées dans les réseaux filaires pourraient être réutilisées pour défendre les réseaux ad hoc contre les attaques de la couche application.

En plus de fournir des routes fiables pour échanger des messages dans la couche de transport, la couche réseau fournit également le service le plus critique du MANET, qui est le protocole de routage. Plusieurs protocoles de routage ont été introduits pour fournir une communication fiable entre les nœuds, mais moins d'attention aux aspects de sécurité alors que la conception de tels protocoles a ouvert de nombreux trous de sécurité à cette couche [54]. La couche réseau dans MANETs est susceptible de diverses attaques telles que l'espionnage avec une intention malveillante, l'usurpation de la transaction de contrôle et / ou de paquets de données, la modification / altération malveillante du contenu de paquet et les attaques de déni de service, les attaques de trou de ver et les attaques de trou noir [38][39].

1.4.3 Attaques au niveau du routage ad hoc

Le routage est l'un des mécanismes les plus essentiels dans les réseaux MANETs. Des mécanismes de routage incorrects et non sécurisés dégraderont non seulement les performances des réseaux ad hoc, mais rendront également ces réseaux vulnérables à de nombreuses attaques de sécurité. L'un des éléments de base dans le mécanisme de routage est le paquet de routage, qui est utilisé pour établir et maintenir les relations entre les nœuds dans les réseaux. L'importance du paquet de routage l'a fait une cible principale par les attaquants pour lancer des attaques contre les réseaux mobiles ad hoc [8][32].

Les attaques contre les paquets de routage sont classées en fonction de l'emplacement et de la propriété des attaques [58]. Les classifications sont illustrées à la figure 1.3.

Dans une telle classification, les informations ou les messages pourraient être déviés du flux d'opérations normal en utilisant des attaques de modification, d'interception, d'interruption ou de fabrication. Dans un cas plus grave, les attaquants pourraient également utiliser n'importe quelle combinaison de ces attaques pour perturber le flux d'information normal [24].

1.4.3.1 Modification

Dans une attaque de modification de message, les adversaires apportent des modifications aux paquets de routage et mettent ainsi en danger l'intégrité des paquets dans les réseaux. Puisque les nœuds des réseaux mobiles ad hoc sont libres de se déplacer et s'auto-

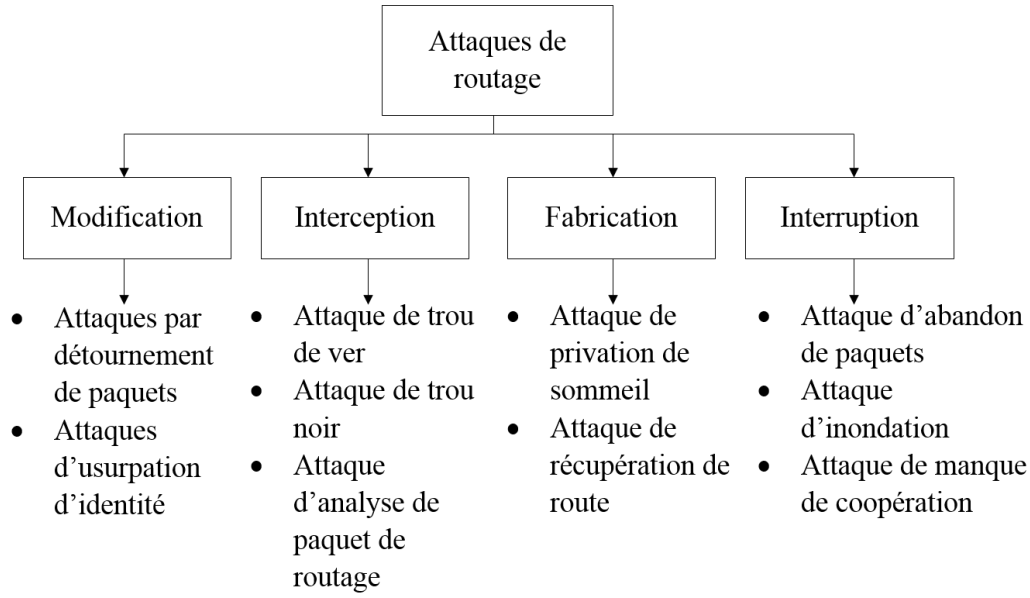


FIGURE 1.3 – Classifications des attaques au niveau du routage

organiser, les relations entre les nœuds peuvent parfois inclure les nœuds malveillants. Ces nœuds malveillants pourraient exploiter les relations sporadiques dans le réseau pour participer au processus d'acheminement de paquets, et lancer ensuite les attaques de modification de message. Des exemples d'attaques qui peuvent être classées dans les attaques de modification de message sont les attaques par détournement de paquets et les tentatives d'usurpation d'identité.

- **Attaques par détournement de paquets**

Dans une attaque par détournement de paquet, des nœuds malveillants réacheminent le trafic de leur chemin d'origine pour les amener à atteindre les mauvaises destinations [23]. Les attaquants pourraient mal acheminer un paquet pour qu'il reste dans le réseau plus longtemps que sa durée de vie, le rendant ainsi abandonné du réseau. En conséquence, le nœud source doit retransmettre les paquets perdus et cela consommera plus de la bande passante, ainsi que d'augmenter la surcharge dans les réseaux.

- **Attaques d'usurpation d'identité**

Les attaques d'usurpation d'identité, également appelées les attaques de spoofing, sont des attaques où le nœud malveillant prend l'identité d'un autre nœud dans le réseau [6]. En usurpant l'identité d'un autre nœud, les attaquants peuvent recevoir des messages de

routage dirigés vers les nœuds qu'ils ont truqués. Les attaques d'emprunt d'identité sont possibles dans les MANETs car la plupart des protocoles de routage ad hoc actuels n'authentifient pas les paquets de routage. En conséquence, les nœuds malveillants pourraient exploiter cette lacune pour se faire passer pour un autre nœud en modifiant le contenu des paquets.

1.4.3.2 Interception

Les attaquants peuvent lancer les attaques d'interception pour obtenir un accès non autorisé aux messages de routage qui ne leur sont pas intentionnellement envoyés. Ce type d'attaque compromet l'intégrité des paquets car de tels paquets peuvent être modifiés avant d'être transmis au saut suivant. En outre, les paquets interceptés pourraient également être analysés avant de passer à la destination, violant ainsi la confidentialité. Des exemples d'attaques qui peuvent être classées sous les attaques d'interception sont les attaques de trou de ver, les attaques de trou noir et les attaques d'analyse de paquet de routage.

- **Attaque de trou de ver**

Dans l'attaque de trou de ver, un nœud compromis dans les réseaux ad hoc se combine avec un attaquant externe pour créer un raccourci dans le réseau. En créant ce raccourci, ils pourraient tromper le nœud source pour gagner dans le processus de découverte d'itinéraire et lancer plus tard les attaques d'interception. Les paquets provenant de ces deux attaquants collus sont généralement transmis en utilisant une connexion câblée pour créer l'itinéraire le plus rapide de la source au nœud de destination. De plus, si les nœuds de trou de ver maintiennent systématiquement les fausses routes, ils pourraient définitivement empêcher d'autres routes d'être établies. Par conséquent, les nœuds intermédiaires résident le long de ces routes refusées qui ne peuvent pas participer aux opérations réseau.

- **Attaque de trou noir**

Dans cette attaque, les nœuds malveillants trompent tous leurs nœuds voisins pour leur attirer tous les paquets de routage. Comme dans les attaques de trou de ver, des nœuds malveillants pourraient lancer les attaques de trous noirs en annonçant eux-mêmes aux nœuds voisins comme ayant l'itinéraire le plus optimal vers les destinations demandées. Cependant, contrairement aux attaques de trou de ver où plusieurs attaquants se sont associés pour attaquer un nœud voisin, dans les attaques du trou noir, un seul attaquant peut être impliqué et il menace tous ses nœuds voisins.

Parmi toutes les attaques, les attaques de trous noirs sont faciles à constituer et elles sont capables de nuire à l'efficacité du réseau en partitionnant le réseau, de sorte que les informations importantes n'atteignent pas leurs destinations. L'attaque du trou noir est un problème important qui peut survenir dans les réseaux mobiles ad hoc, en particulier dans les protocoles de routage à la demande populaires comme AODV [37][36].

- **Attaque d'analyse de paquet de routage**

Puisque aucune action perturbatrice ne se produit, l'analyse des paquets de routage peut être classée comme l'une des attaques passives contre les MANETs. Une façon de lancer cette attaque est d'exploiter le mode de promiscuité utilisé dans le réseau ad hoc. En mode promiscuité, si le nœud A est le voisin des deux nœuds B et C à un instant donné, le nœud A peut toujours entendre les transmissions entre les nœuds B et C. En exploitant cette nature, le nœud A est capable d'analyser les paquets interceptés transmis entre les nœuds B et C. En outre, des nœuds malveillants pourraient également lancer cette attaque en exploitant la nature dans un routage multi-sauts. Dans le routage multi-sauts, les paquets doivent être transmis à travers plusieurs nœuds intermédiaires avant d'atteindre la destination réelle. Les nœuds malveillants peuvent exploiter cette opportunité en se plaçant à n'importe quel emplacement le long de la route pour participer au processus de transfert de messages et lancer ultérieurement les attaques d'analyse de paquets de routage.

1.4.3.3 Fabrication

Au lieu de modifier ou d'interrompre les paquets de routage existants dans le réseau, les nœuds malveillants pourraient également fabriquer leurs propres paquets pour provoquer le désordre dans les opérations du réseau. Ils pourraient lancer les attaques de fabrication de message en injectant des paquets énormes dans les réseaux comme dans les attaques de privation de sommeil. Cependant, les attaques de fabrication de messages ne sont pas seulement lancées par les nœuds malveillants, mais peuvent également provenir des nœuds internes qui se comportent mal, comme dans les attaques de récupération de route.

- **Attaque de privation de sommeil**

Ce type d'attaque est en réalité plus spécifique aux réseaux mobiles ad hoc. Le but est d'épuiser les ressources limitées des nœuds mobiles (par exemple les puissances de batterie), en les rendant constamment occupés à traiter des paquets inutiles. Dans un protocole de routage, les attaques de privation de sommeil peuvent être lancées en inondant

le nœud ciblé avec des paquets de routage inutiles. Par exemple, les attaquants pourraient inonder n'importe quel nœud dans les réseaux en envoyant un nombre énorme de paquets de demande de route (RREQ), de réponse d'itinéraire (RREP) ou d'erreur d'acheminement (RERR) au nœud ciblé. En conséquence, ce nœud particulier est incapable de participer aux mécanismes de routage et de rendre inaccessible par les autres nœuds dans les réseaux.

- **Attaque de récupération de route**

Les attaques de récupération de route sont lancées par les nœuds internes gourmands dans les réseaux. Dans un réseau mobile ad hoc, il n'y a aucune garantie que chaque paquet transmis atteigne avec succès le nœud de destination souhaité [55]. Les paquets peuvent ne pas atteindre le nœud de destination à cause des défaillances naturelles du réseau ou peuvent être attaqués par les adversaires. Par conséquent, pour sauver leurs paquets de telles défaillances, les nœuds internes se conduisant mal peuvent dupliquer et retransmettre leurs paquets bien qu'aucun message d'erreur d'envoi n'ait été reçu. Les effets des attaques de récupération de route peuvent être plus graves s'il existe de nombreux nœuds gourmands dans les réseaux. En plus de drainer plus de ressources dans les nœuds intermédiaires et de destination, cette attaque peut également entraîner la consommation de bande passante inutile.

1.4.3.4 Interruption

Les attaques d'interruption sont lancées pour empêcher les paquets de routage d'atteindre les nœuds de destination. Les adversaires pourraient le faire en attaquant les paquets de routage ou en attaquant les nœuds mobiles dans le réseau. En fait, la plupart des attaques lancées lors des attaques de modification, d'interception et de fabrication visent à interrompre les opérations normales des réseaux ad hoc. Par exemple, les adversaires visant à interrompre le service de disponibilité dans les réseaux peuvent détruire tous les chemins d'accès à un nœud victime particulier en utilisant les attaques de modification de message. Dans une attaque de fabrication de message, les adversaires pourraient surcharger les réseaux en injectant d'énormes paquets inutiles. Des exemples d'attaques qui pourraient être classées dans la catégorie des attaques d'interruption sont les attaques d'abandon de paquets, les attaques d'inondation et les attaques de manque de coopération.

- **Attaque d'abandon de paquets**

L'interruption directe des paquets de routage peut être effectuée en utilisant les at-

taques par abandon de paquets. Dans une attaque par abandon de paquet standard, un adversaire collabore comme d'habitude dans le processus de découverte d'itinéraire et lance les attaques par abandon de paquets constantes s'il est inclus comme l'un des nœuds intermédiaires. De plus, au lieu de laisser tomber tous les paquets en permanence, les adversaires peuvent varier leurs techniques en utilisant des attaques aléatoires, sélectives ou périodiques, pour aider à dissimuler leur comportement d'interruption [17].

- **Attaque d'inondation**

Les adversaires peuvent également interrompre les opérations normales dans le processus de transfert de paquets en inondant les nœuds de destination ciblés avec d'énormes paquets inutiles. Les nœuds sous les attaques d'inondation sont incapables de recevoir ou transmettre aucun paquet ainsi tous les paquets dirigés vers eux seront écartés du réseau.

- **Attaque de manque de coopération**

Le manque de coopération des nœuds internes pour participer aux opérations du réseau peut également être considéré comme une tentative de lancer une attaque de refus de service. Dans de telles attaques, les nœuds internes sont découragés de coopérer dans les opérations de réseau parce que la participation à de telles opérations épuisera leurs ressources. Les nœuds internes qui se comportent mal peuvent utiliser des stratégies différentes pour économiser leurs ressources limitées. Ils peuvent refuser de transmettre les paquets de l'autre nœud, ne pas renvoyer le rapport d'erreur de routage à l'expéditeur en cas d'échec de la transmission des paquets ou éteindre leurs appareils lorsqu'ils n'envoient aucun paquet dans les réseaux.

1.5 Conclusion

Les réseaux mobiles ad hoc ont des caractéristiques uniques qui les différencient des autres réseaux filaires et sans fil, tels que l'absence de l'infrastructure, facile à déployer et permet la mobilité. Ces caractéristiques rendent ce type de réseau essentiel pour les réseaux de communication de la future génération, mais ils présentent également des défis tels que la sécurité, la gestion de l'énergie et la qualité de service.

Ce chapitre a examiné toutes les informations générales sur les réseaux mobiles ad hoc. Les caractéristiques, les avantages, les applications et les défis des réseaux mobiles

ad hoc. Les applications de ce type de réseau comprennent les applications militaires, l'informatique collaborative et distribuée et les opérations d'urgence. De plus, nous avons détaillé les besoins en sécurité dans ces réseaux. Ce chapitre aborde également les attaques et les vulnérabilités associées à la sécurisation des MANETs. Une classification des attaques dans les MANETs est présentée, ainsi qu'une description des attaques au niveau du routage est aussi présentée.

Dans le chapitre suivant de notre thèse on va détailler l'ensemble des propositions qui visent à sécuriser les réseaux mobiles ad hoc.

Chapitre 2

La sécurité des réseaux mobiles ad hoc

Sommaire

2.1 Introduction

La sécurité est devenue une préoccupation majeure afin de fournir une communication protégée entre les nœuds mobiles dans un environnement hostile. Contrairement aux réseaux filaires, les caractéristiques uniques des réseaux mobiles ad hoc posent un certain

nombre de défis non triviaux à la conception de sécurité, tels qu'une architecture de réseau de bout en bout ouverte, un support sans fil partagé, des contraintes de ressources rigoureuses et une topologie réseau hautement dynamique. Ces défis plaident clairement en faveur de la création de solutions de sécurité multibarrière qui assurent à la fois une protection étendue et des performances réseau souhaitables.

Dans la littérature, Il existe plusieurs propositions qui tentent de contrer les menaces de sécurité mentionnées dans la section précédente, et offrent une protection contre les attaques malveillantes et les comportements égoïstes. Ces solutions proposées sont soit une modification dans le mécanisme des protocoles de routage existant (par exemple AODV ou OLSR), soit de nouveaux protocoles de routage sécurisés autonomes basées sur quelques primitives cryptographiques telles que le chiffrement et la signature numérique, ou bien l'utilisation des systèmes de détection d'intrusion.

Dans ce chapitre, nous présentons dans un premier temps les solutions basées sur la modification dans le mécanisme du protocole de routage spécifiquement AODV, ensuite nous décrivons des solutions en utilisant des primitives cryptographiques. Et finalement, nous présentons les systèmes de détections d'intrusion IDS avec quelques travaux existant dans la littérature qui utilisent les IDS.

2.2 Modification dans le mécanisme du protocole de routage

Dans cette section, nous présentons les vulnérabilités du protocole de routage AODV et un aperçu de certaines des approches pour résoudre le problème de la mauvaise conduite pour le protocole AODV.

2.2.1 Vulnérabilité du protocole AODV

Les auteurs du papier [42] analysent les attaques internes contre le protocole AODV du point de vue d'un attaquant. En effet, leurs études classe les actions abusives en quatre catégories, qui sont : la suppression des paquets (Drop (DR)), Modifier et Transférer (Modify and Forward (MF)), Forge réponse (Forge Reply (FR)), Forge active (Active Forge (AF)).

— DR : La suppression des paquets est quand l'attaquant supprime tous les paquets du protocole de routage reçus.
— MF : Pour Modifier et Transférer est quand l'attaquant modifie un ou plusieurs champs dans un paquet de routage, puis transmet le paquet à son voisin (s).
— FR : La Forge réponse est lorsque l'attaquant envoie un faux paquet route reply en réponse à la demande d'un paquet route request reçue. La Forge réponse est principalement liée à l'utilisation abusive des messages RREQ et RREP.
— AF : la Forge active est lorsque l'attaquant envoie un paquet de routage falsifié sans être déclenché par la réception d'un paquet de routage.

La figure 2.1 montre la taxinomie pour l'utilisation abusive du protocole de routage AODV.

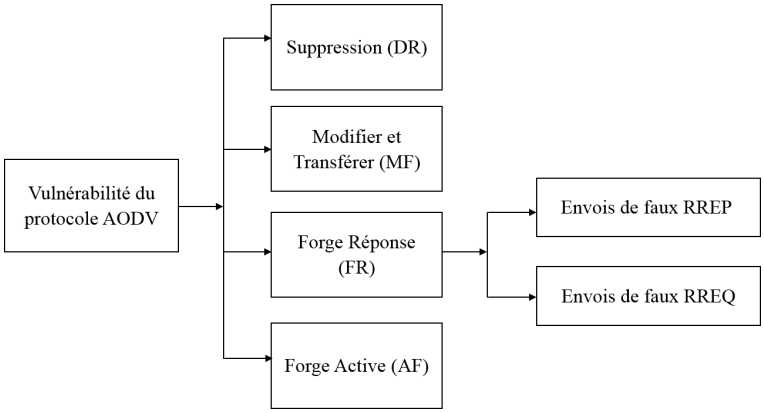


FIGURE 2.1 – Taxonomie de la vulnérabilité du protocole AODV

2.2.2 Revue de littérature

L'étude [53] a proposé une modification du protocole de routage AODV pour y introduire un aspect de sécurité, pour la détection et l'isolation des nœuds malveillants qui source d'attaque de type du trou gris ou l'attaque du trou noir. Dans ce travail, le nœud intermédiaire recevant un paquet RREP détecte le nœud malveillant qui envoie de fausses informations de routage en calculant une valeur de pic. Cette valeur de pic est la valeur maximale possible du numéro de séquence que n'importe quel RREP peut avoir dans l'état actuel. Le nœud recevant un RREP compare le numéro de séquence dans le paquet RREP avec la valeur de pic calculée. Si le numéro de séquence est supérieur à la valeur de pic, le RREP est considéré comme frauduleux et il est marqué comme DO_NOT_CONSIDER

et le nœud qui envoie ce paquet est considéré comme malveillant. Le nœud intermédiaire envoie alors tous les RREP au nœud source. Le nœud source rejette alors tous les RREP marqué comme DO_NOT_CONSIDER et sélectionne un véritable RREP.

L'approche du mécanisme de mise en cache des paquets RREP est utilisée dans le papier [20] pour surmonter le problème de l'attaque du trou noir. Dans leur approche, ils comptent les paquets RREP reçus par le nœud source, puis la source choisit le chemin approprié en ignorant le premier paquet RREP. Comme il y a une grande possibilité d'implication de nœud malveillant dans le chemin du premier paquet RREP.

L'étude [28] a proposé une solution pour la détection de l'attaque du trou noir en modifient le protocole de routage AODV à la source et à la destination. Cette approche ajoute une fonction supplémentaire au nœud source ainsi qu'au nœud de destination, de sorte qu'à chaque fois qu'un message RREP ou RREQ parvient au nœud intermédiaire, il vérifie le numéro de séquence des paquets et le compare à une valeur de seuil. La valeur de seuil est définie pour trois tailles du réseaux, petite, moyenne et grande taille.

Le nœud source vérifie le numéro de séquence de destination à partir de la valeur de seuil. Si le numéro de séquence de destination dans le paquet RREP est inférieur au numéro de séquence de valeur de seuil, il est considéré comme un nœud normal et établit le chemin entre le nœud source et le nœud de destination. Sinon le paquet est rejetté.

Par contre, le nœud de destination reçoit plusieurs messages RREQ provenant de ses nœuds voisins. Le nœud de destination compare le numéro de séquence du RREQ et le numéro de séquence de sa table de routage. Si ce numéro de séquence RREQ est supérieur au numéro de séquence de sa table de routage, il sélectionne le numéro de séquence RREQ sinon il sélectionne le numéro de séquence de sa table de routage. Le numéro de séquence sélectionné par le nœud de destination doit être incrémenté de un et comparé avec la valeur de seuil. S'il est supérieur ou égal à la valeur de seuil, le numéro de séquence sera mis à jour par zéro, sinon le nœud de destination va utiliser dans le message RREP le numéro de séquence incrémenté.

Les auteurs du papier [31] ont utilisé l'approche du numéro de séquence. Dans leur méthode, tous les numéros de séquence mentionnés dans le paquet RREP sont stockés avec l'ID de nœud correspondant dans une RR-table (Route Request). Ensuite, si le premier numéro de séquence de destination dans la table est beaucoup plus grand que le numéro de séquence du nœud source. Ce nœud sera identifié comme nœud malveillant et l'entrée sera immédiatement supprimée de la table. La solution proposée maintient également l'identité

du nœud malveillant en tant que MN-ID (Malicious Node), de sorte que les messages de contrôle provenant de ce nœud peuvent être supprimés. En outre, il n'est pas nécessaire de transférer les messages de contrôle de ce nœud malveillant. De plus, la table RR est vidée une fois qu'une demande de route est choisie à partir de celle-ci.

2.3 Les protocoles de routage sécurisés

Afin d'analyser les solutions existantes de manière structurée, nous les avons classées en trois catégories [40]. Des solutions basées sur la cryptographie, des solutions basées sur une chaine de hachage unidirectionnelle et des solutions hybrides. Pour les solutions basées sur la cryptographie, il existe deux sous-catégories ; solutions basées sur la cryptographie symétrique et solutions basées sur la cryptographie asymétrique.

2.3.1 Solutions de cryptographie symétrique

a. Protocole de routage sécurisé (SRP)

Le protocole de routage sécurisé (SRP) développé par Papadimitratos et Haas [45], est un protocole conçu pour sécuriser les protocoles de routage à la demande qui utilisent la diffusion comme méthode d'interrogation d'itinéraire. Les auteurs ont mentionné qu'il peut être appliqué en tant qu'extension d'une multitude de protocoles de routage réactif existants, en particulier le DSR [22]. Une association de sécurité (SA) est requise entre un nœud source et un nœud de destination. On suppose que le SA peut être établi en utilisant une clé partagée entre les deux nœuds communicants.

Un en-tête SRP tel que représenté sur la figure 2.2 est ajouté au paquet du protocole de routage de base. Le nœud source initie la découverte d'itinéraire, en envoyant un paquet de demande d'acheminement identifié par un numéro de séquence de requête (QSEQ), un identificateur de requête aléatoire (QID) et la sortie d'une fonction de hachage de clé. La fonction de hachage de clé prend l'en-tête IP, l'en-tête du protocole de routage de base et la clé partagée.

Les nœuds intermédiaires diffusent le paquet aux nœuds voisins et mettent à jour leur table de routage. Cependant, s'ils ont le même QID dans leur table de routage, la requête est supprimée. Lorsque la requête a atteint le nœud de destination, elle vérifie que la requête

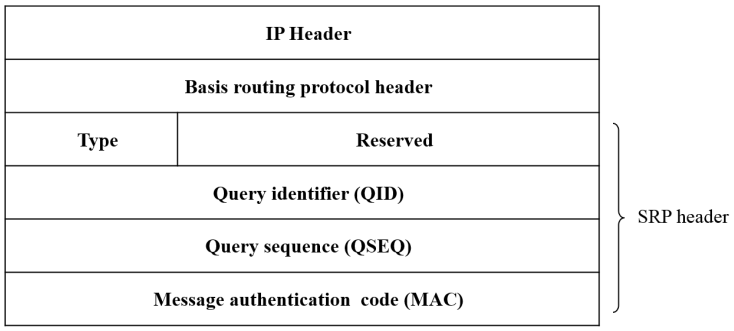


FIGURE 2.2 – En-tête de paquet SPR

n'est pas périmée ou rejouée via le QSEQ et il vérifie les métriques de sécurité en calculant le hachage à clé. Après vérification, le nœud de destination génère un certain nombre de réponses avec des routes différentes, de sorte qu'il fournit à la source une image de topologie aussi diverse que possible. Ces paquets de réponses incluent les informations de chemin de la source à la destination, les numéros QSEQ et QID. Les métriques de sécurité de la réponse sont assurées par la même méthode que la demande d'itinéraire, en calculant le code d'authentification de message (MAC). Après avoir reçu le paquet de réponse, le nœud source vérifie les numéros QSEQ et QID, puis calcule le MAC et compare la sortie avec le champ MAC de l'en-tête SRP. Selon une vérification réussie, le nœud source est assuré que la demande est atteinte à la destination et que la réponse n'a pas été corrompue sur son chemin de la source à la destination.

b. Protocole de routage ad hoc conscient de la sécurité (SAR)

Le protocole SAR [60] est une approche du routage ad hoc qui incorpore des attributs de sécurité en tant que paramètres dans la découverte d'itinéraire. Cependant, les protocoles de routage traditionnels non sécurisés trouvent le chemin le plus court entre deux nœuds, tandis que le SAR peut découvrir un chemin avec les attributs de sécurité souhaités. Par exemple, le critère d'une route valide peut être lorsque chaque nœud de l'itinéraire doit avoir une clé partagée particulière.

SAR peut être étendu à tous les protocoles de routage ad hoc à la demande (tels que AODV ou DSR) afin d'intégrer la mesure de sécurité dans les messages de demande de route. Une implémentation de SAR basée sur AODV est présentée par les auteurs. Le paquet de demande de route a un champ supplémentaire (RQ_SEC_REQUIREMENT) qui indique le niveau de sécurité requis de l'itinéraire qu'elle souhaite découvrir. Ce champ n'est défini qu'une seule fois par l'expéditeur et ne change pas pendant la découverte

de l'itinéraire. Un nœud intermédiaire qui reçoit le paquet vérifie s'il peut satisfaire aux exigences de sécurité. Si le nœud peut fournir la sécurité requise, il peut participer au routage et le paquet de demande de route est transmis à ses propres voisins, mettant à jour un nouveau champ appelé RQ_SEC_GURANTEE pour indiquer le niveau maximal de sécurité qu'il peut fournir. Et si le nœud intermédiaire ne peut pas satisfaire à l'exigence de sécurité, il abandonne simplement le paquet de demande d'itinéraire. Lorsque le nœud de destination reçoit le paquet de demande de route, il peut être sûr de l'existence d'un itinéraire de la source à la destination et cette route satisfait aux exigences de sécurité définies par l'expéditeur. Le nœud de destination envoie un paquet RREP avec un champ supplémentaire (RP_SEC_GUARANTEE) qui indique la sécurité maximale disponible sur le chemin. La valeur du champ RQ_SEC_GURANTEE est ensuite copiée dans RP_SEC_GUARANTEE. Le paquet de RREP revient le long du chemin inverse et les nœuds intermédiaires qui sont autorisés à participer au routage, mettent à jour sa table de routage conformément à la spécification AODV et enregistrent également la nouvelle valeur RP_SEC_GUARANTEE. Cette valeur indique la sécurité maximale disponible sur le chemin d'accès.

Un inconvénient majeur dans le SAR est qu'il implique un surcoût important pour le processus de routage, puisque chaque nœud intermédiaire doit effectuer une opération de chiffrement / déchiffrement.

2.3.2 Solutions de cryptographie asymétrique

a. Routage authentifié pour les réseaux ad hoc (ARAN)

Le protocole ARAN décrit dans [54], est un protocole de routage sécurisé basé sur les protocoles à la demande. ARAN utilise un mécanisme cryptographique afin d'atteindre les objectifs de sécurité d'authentification, d'intégrité des messages et de non-répudiation.

Il comprend deux étapes opérationnelles distinctes, la première étape est le processus de certification préliminaire qui nécessite l'existence d'une autorité de certification (CA) de confiance. Tous les nœuds qui souhaitent se connecter au réseau doivent contacter l'autorité de certification et demandent un certificat pour son adresse et sa clé publique. Cette autorité de certification distribue sa clé publique à tous les nœuds du réseau. La deuxième étape opérationnelle du protocole est le processus de découverte d'itinéraire qui fournit une authentification de bout en bout. Cela garantit que la destination prévue a

bien été atteinte. Le nœud initiateur démarre la communication en diffusant un paquet de découverte d'itinéraire (Route Discovery Packet (RDP)) à ses voisins. Le RDP comprend un identifiant de type de paquet ("RDP"), le certificat du nœud initiateur, un nonce, un Timestamp et l'adresse du nœud de destination, tous signés avec la clé privée du nœud initiateur. Chaque nœud intermédiaire valide la signature et vérifie que le certificat de la source n'a pas expiré, met à jour sa table de routage avec le voisin à partir duquel il a reçu le RDP, signe le contenu du message, ajoute son propre certificat et transmet le message à ses voisins enlever le certificat et la signature du nœud précédent. La signature empêche les attaques d'usurpation qui peuvent altérer les routes ou former des boucles. Après avoir reçu le RDP, le nœud de destination répond avec un paquet de réponse (REP). Le REP contient un identificateur de type de paquet ("REP"), l'adresse du nœud source, le certificat de destination, un nonce et le Timestamp associé. De plus, le nœud de destination signe le REP de manière similaire à la découverte d'itinéraire. Chaque nœud supprime le certificat et la signature du saut précédent et les remplace par les siens avant de les transmettre au saut suivant, sauf que le REP est unicasté le long du chemin inverse. Lorsque la source reçoit le REP, elle vérifie la signature de la destination et le nonce retourné par la destination. La figure 2.3 illustre le processus de découverte d'itinéraire dans ARAN.

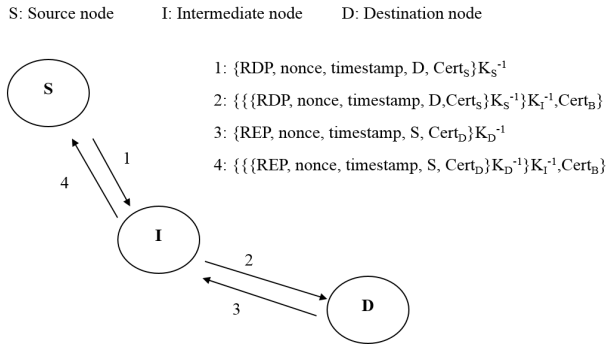


FIGURE 2.3 – Découverte de route dans le protocole ARAN

2.3.3 Prévention en utilisant des chaînes de hachage One Way

a. Vecteur de distance ad hoc sécurisé et efficace (SEAD)

Le protocole SEAD [15] est un protocole de routage de réseau ad hoc sécurisé basé sur la conception du protocole de routage DSDV [48], en particulier sur la version DSDVSQ de ce protocole. SEAD utilise une chaîne de hachage pour authentifier le nombre de sauts et les numéros de séquence et n'implique aucune opération cryptographique asymétrique.

Dans SEAD, chaque nœud crée sa chaîne de hachage en appliquant une fonction de hachage unidirectionnelle à une valeur aléatoire. De plus, des éléments particuliers de la chaîne de hachage sont utilisés pour sécuriser les mises à jour du protocole de routage. Cependant, le protocole est basé sur l'hypothèse de l'existence d'un certain mécanisme afin d'authentifier un élément d'une chaîne de hachage entre deux nœuds. Par conséquent, lorsqu'un nœud envoie ou transmet une mise à jour de routage, il inclut une valeur de la chaîne de hachage pour chaque entrée de cette mise à jour. D'une manière qu'un nœud inclut l'adresse du nœud de destination, la métrique et le numéro de séquence de la destination de sa table de routage et la valeur de hachage du haché de la valeur de hachage reçue dans l'entrée de mise à jour de routage à partir de laquelle elle a appris cette route vers cette destination. Si la mise à jour concerne elle-même, le nœud inclut sa propre adresse, met la métrique à 0 et le numéro de séquence au numéro de séquence suivant, et la valeur de hachage au premier élément dans sa propre chaîne de hachage correspondant à ce numéro de séquence. Les nœuds recevant une mise à jour de routage vérifient l'authentification de chaque entrée du message, en hachant la valeur de hachage reçue de chaque entrée le nombre correct de fois et ils sont comparés à la valeur de hachage authentique antérieure. Selon cette comparaison, la mise à jour de routage est soit acceptée comme authentifiée, soit supprimée. En utilisant cette technique, les autres nœuds peuvent uniquement augmenter la mesure dans une mise à jour de routage, mais pas la diminuer.

b. Ariadne

Ariadne [16] est un protocole de routage ad hoc réactif sécurisé basé sur le DSR [22] ; ce protocole est développé par les mêmes auteurs que le protocole SEAD décrit ci-dessus. Au lieu d'utiliser les mécanismes de sécurité hop-hop comme dans le protocole SEAD, la proposition Ariadne suit une approche de bout-en-bout.

La conception d'Ariadne peut être considérée comme comportant trois étapes : Authentification de ROUTE REQUEST par cible, techniques d'authentification des données dans ROUTE REQUEST et ROUTE REPLY, et technique de hachage par Hop.

- Authentification de ROUTE REQUESTs par cible : cette étape consiste à vérifier l'authenticité de la ROUTE REQUEST, qu'elle est remplie lorsque le nœud initiateur inclut un MAC calculé avec une clé partagée sur des données uniques, par exemple un Timestamp, dans la ROUTE REQUEST.
- Techniques d'authentification des données dans ROUTE REQUEST et ROUTE REPLY : cette étape permet au nœud initiateur d'authentifier chaque nœud indivi-

duel dans la liste des nœuds de la ROUTE REPLY. De même, le nœud cible peut authentifier chaque nœud dans la liste de nœuds de la ROUTE REQUEST, afin que ROUTE REPLY ne retourne que le long des chemins qui contiennent des nœuds légitimes. Selon les auteurs, l'authentification peut être effectuée en utilisant l'un des trois schémas suivants : secrets partagés entre chaque paire de nœuds, secrets partagés entre nœuds communicants combinés avec le protocole d'authentification de diffusion TESLA [49] qui nécessite une synchronisation temporelle lâche ou une signature numérique.

- Technique de hachage par saut : Une fonction de hachage unidirectionnelle est utilisée pour vérifier qu'aucun nœud n'a été supprimé de la liste des nœuds dans la ROUTE REQUEST. Pour modifier ou supprimer un saut précédent, un attaquant doit être capable d'inverser la fonction de hachage à une seule voie, ce qui s'est avéré irréalisable.

2.3.4 Solutions hybrides

a. Protocole de vecteur de distance à la demande ad hoc sécurisé (SAODV)

Le protocole sécurisé SAODV [62] est une extension du protocole de routage AODV. Les extensions proposées utilisent des signatures cryptographiques pour authentifier les champs non mutables des messages, et une chaîne de hachage à sens unique pour sécuriser le champ du nombre de sauts dans les messages RREQ et RREP, qui est le seul champ mutable d'un message AODV. Le protocole nécessite l'existence d'un mécanisme de gestion de clés qui permet à chaque nœud d'obtenir des clés publiques auprès des autres nœuds participant au réseau mobile ad hoc.

Les informations relatives aux signatures et aux chaînes de hachage sont transmises avec le message AODV en tant que message d'extension que les auteurs appellent extension de signature. Ces extensions SAODV comprennent les champs suivants. Le champ de fonction de hachage indique quelle fonction de hachage doit être utilisée. Le nombre maximal de sauts de champ spécifie le nombre maximal de nœuds qu'un paquet est autorisé à traverser. Le champ hash est un nombre généré aléatoirement appelé SEED. Enfin, le champ de top hash est calculé en hachant la valeur dans le champ hash le maximum du nombre de sauts de fois. Le format des extensions de signature SAODV est représenté sur la figure 2.4.

Chaque fois qu'un nœud émet une RREQ ou un paquet RREP génère un nombre

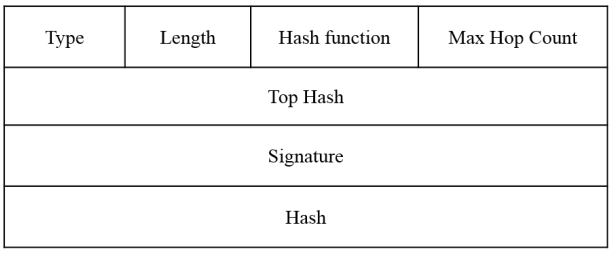


FIGURE 2.4 – En-tête de paquet SAODV

aléatoire (seed) et définit le champ de hachage à la valeur de départ, définit le champ de nombre de sauts maximum sur le champ TTL de l'en-tête IP, spécifie le champ de fonction de hachage par l'identifiant de la fonction de hachage qu'il va utiliser, et applique la fonction de hachage au seed le maximum du nombre de sauts de fois, le résultat calculé est défini sur le champ de Top Hash. En outre, le nœud signe numériquement tous les champs du message, à l'exception du champ de nombre de sauts de l'en-tête AODV et du champ de hachage de l'en-tête de l'extension SAODV. Après avoir reçu une RREQ ou une RREP, le nœud intermédiaire vérifie le champ du nombre de sauts dans le paquet AODV en comparant le résultat du hachage du nombre maximal de sauts moins le nombre de sauts de fois pour le champ hash avec la valeur du champ top hash. Si la vérification échoue, le paquet sera abandonné par le nœud. Le nœud intermédiaire hache une fois l'ancienne valeur du champ Hash dans l'extension de signature, avant de rediffuser un message RREQ à ses voisins ou de transmettre un RREP.

b. Protocole de routage d'état de lien sécurisé (SLSP)

Le protocole SLSP [44] est un schéma proposé pour sécuriser le routage proactif pour les réseaux ad hoc mobiles et la distribution des informations d'état de liaison pour les locaux et les topologies sectorielles. SLSP peut être utilisé comme solution autonome pour le routage proactif des états de liaison ou comme partie de la structure de routage hybride lorsqu'elle est associée à un protocole de routage ad hoc réactif. Cependant, le SLSP requiert l'existence d'une paire de clés asymétriques pour chaque interface réseau d'un nœud.

SLSP comporte trois étapes principales : la distribution des clés publiques, la découverte des voisins et les mises à jour de l'état des liens.

- Distribution de clé publique : pour fonctionner efficacement sans gestion de clé centrale, chaque nœud diffuse sa clé publique aux nœuds de sa zone à l'aide de

paquets PKD (Public Key Distribution). Ensuite, les nœuds de réception valident leurs mises à jour d'état de liaison ultérieures à partir du nœud source.

- Découverte du voisin : les informations sur l'état du lien du nœud sont également diffusées périodiquement à l'aide du protocole NLP (Neighbor Lookup Protocol), une partie interne de SLSP. Chaque nœud envoie son adresse MAC et l'adresse IP de l'interface réseau actuelle à ses voisins en diffusant des messages hello NLP signés. Le NLP d'un nœud génère une notification pour informer le SLSP lorsque des divergences suspectes sont observées, par exemple que deux voisins utilisent la même adresse IP ou qu'un nœud utilise la même adresse MAC que le nœud de détection, etc. En recevant la notification, le protocole de routage se décharge immédiatement les paquets suspects.
- Mises à jour d'état de liaison : les paquets de mise à jour d'état de liaison (Link State Update (LSU)) sont identifiés par l'adresse IP du nœud initiateur et incluent un numéro de séquence de 32 bits, ce qui fournit un large espace de mises à jour. Chaque mise à jour comprend un nombre de sauts représentant le nombre de sauts parcourus par les mises à jour SLSP. Une chaîne de hachage est utilisée pour authentifier le nombre de sauts, et les valeurs de chaîne de hachage sont effectuées via l'ancre de la chaîne de hachage, qui est incluse dans la partie numériquement signée d'un message LSU. Lors de la réception du LSU, les nœuds vérifient la signature attachée en utilisant une clé publique du nœud d'origine. Le champ hops_traversed du LSU est défini sur le haché hops_traversed, le TTL est décrémenté et le paquet est rediffusé.

c. OLSR sécurisé

Pour sécuriser le protocole de routage OLSR, les auteurs de [13] proposent de signer tout le trafic de contrôle OLSR pour chaque saut avec un algorithme de signature numérique (SHA-1). Cependant, ils ne considèrent pas les champs variables dans les messages, tels que le nombre de sauts et le TTL. De plus, une seule signature est utilisée puisque plusieurs messages OLSR soient empilés dans un seul paquet OLSR. L'utilisation de cette approche hop-by-hop ne fournit pas de signatures de bout en bout, ce qui signifie que le digest ne représente pas une signature de confiance provenant de la source, mais seulement une signature de l'expéditeur garantissant la source du message dans le saut précédent.

Un nœud qui n'a pas accès à la clé secrète partagée ne peut pas produire le bon digest. Tous les récepteurs exécutant le protocole OLSR sécurisé rejettent les messages avec des digests incorrects. Les signatures sont transmises dans leurs propres messages. Cela permet

d'assurer la compatibilité avec les nœuds qui n'exécutent pas de protocole OLSR sécurisé, mais aussi parce que le Timestamp est transmis avec la signature.

Quatre paquets différents sont définis. Le premier, qui est le message signature représenté dans la figure 2.5, et trois autres messages (figures 2.6, 2.7, et 2.8) utilisés dans l'échange du Timestamp. Tous les messages sont envoyés dans le corps d'un paquet OLSR.

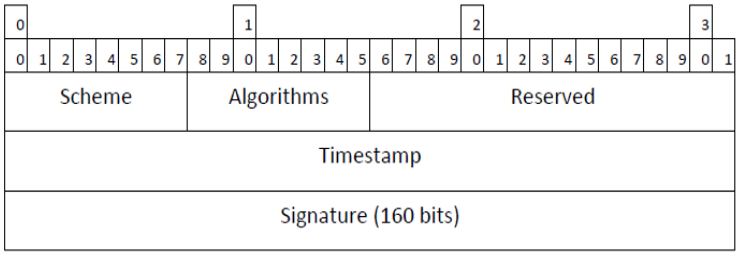


FIGURE 2.5 – Le message de signature élémentaire (Secure OLSR)

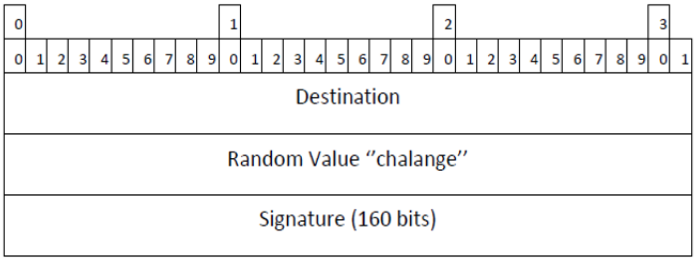


FIGURE 2.6 – Le message de challenge pour l'échange du timestamp (Secure OLSR)

En outre, leur solution empêche les attaques de rejeux en utilisant des Timestamps dans l'extension sécurisée du protocole OLSR. Pour échanger ces Timestamps lors de la connexion initiale entre deux nœuds, un mécanisme d'échange de Timestamp bidirectionnel est utilisé. Leur approche ne repose pas sur la synchronisation du temps entre les nœuds du réseau.

2.4 Les systèmes de détection d'intrusions dans les réseaux mobiles ad hoc

Pour les réseaux conventionnels, de nombreux IDS ont été proposés, mais ces IDS ne peuvent pas être directement appliqués sur des environnements ad hoc mobiles en raison

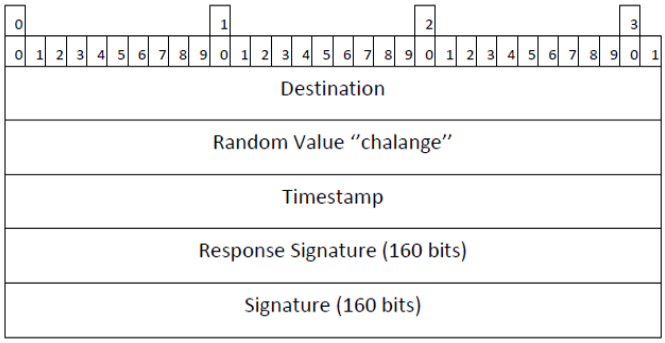


FIGURE 2.7 – Le message de challenge-response pour l'échange du timestamp (Secure OLSR)

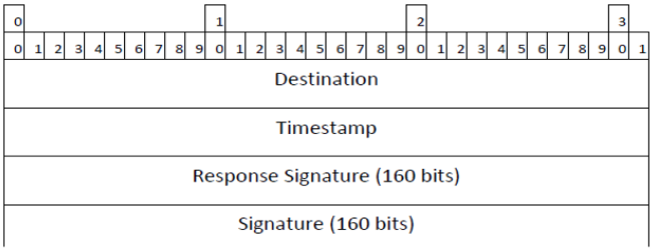


FIGURE 2.8 – Le message de response- response pour l'échange du timestamp (Secure OLSR)

de leurs caractéristiques différentes. Pour cette raison nous présentons dans cette section les systèmes de détection d'intrusion, ensuite nous discutons de la taxonomie des IDS qui comprend les composants de l'IDS, la classification IDS, les techniques de détection d'intrusion et les architectures IDS pour les MANET. Et finalement, les principales solutions de détection d'intrusion proposées dans la littérature sont présentées.

2.4.1 Les systèmes de détection d'intrusion

Lorsqu'un ensemble d'actions tente de compromettre les attributs de sécurité tels que la confidentialité, l'intégrité, la non-répudiation et la disponibilité des ressources, ces actions sont considérées comme des intrusions, et la détection de telles intrusions est appelée système de détection d'intrusion, désigné par son acronyme anglais IDS (Intrusion Detection System). Le développement d'un IDS est motivée par l'environnement MANETs car les techniques de prévention ne suffisent pas, les systèmes les plus sécurisés sont vulnérables aux attaques internes et de nouvelles intrusions émergeant continuellement alors que de nouvelles techniques sont nécessaires pour se défendre contre eux.

Puisqu'il y a toujours de nouvelles intrusions qui ne peuvent être évitées, IDS est introduit pour détecter les violations possibles d'une politique de sécurité en surveillant les activités du système et la réponse. De plus, les IDS sont connus comme la deuxième ligne de défense, car lorsqu'une intrusion s'est produite, IDS entre en scène. Si nous détectons l'attaque une fois qu'elle arrive dans le réseau, une réponse peut être lancée pour empêcher ou minimiser les dommages au système. Cela permet également d'améliorer les techniques de prévention en fournissant des informations sur les techniques d'intrusion.

2.4.2 Taxonomie des systèmes de détection d'intrusion

La fonctionnalité de base d'un IDS dépend de trois composants principaux tels que la collecte de données, la détection et la réponse. Le composant de collecte de données est chargé de collecter les données provenant de diverses sources telles que les données d'audit du système, les données de trafic réseau, etc. Aussi chargé du prétraitement de données : transfert des données dans un format commun, stockage des données et envoie les données au module de détection. Le module de détection est chargé d'analyser les données collectées pour détecter les intrusions, et si une activité suspecte est détectée, l'IDS génère une alarme

par le module de réponse.

Les systèmes de détection d'intrusion (IDS) utilisent des différentes sources de données qui sont les entrées du système : données d'audit basées sur l'hôte, données basées sur les traces d'activité réseau, paquets réseau ou des données de table de routage, etc. Basé sur les données d'audit, IDS peut être catégorisé comme système de détection d'intrusion hôte (Host based Intrusion Detection System (HIDS)) et système de détection d'intrusion réseau (Network based Intrusion Detection System (NIDS)), où HIDS souligne uniquement le système d'exploitation d'un hôte particulier et détecte les activités suspectes sur l'hôte, et NIDS est responsable de surveiller les paquets réseau et détecte les attaques dans le réseau. Il existe également des systèmes de détection d'intrusion qui utilisent à la fois HIDS et NIDS. Par exemple, un système peut utiliser NIDS et également HIDS pour des hôtes importants dans les réseaux tels que des serveurs, des bases de données, etc.

Dans la littérature, il existe à la fois des IDS distribués et centralisés. Dans [50], il y a une étude des IDS distribués actuels qui montre que la plupart des DIDS sont organisés hiérarchiquement autour d'un nœud central et que peu d'entre eux sont complètement distribués. Généralement, seule la collecte de données est effectuée de manière distribuée dans les DIDS.

Trois techniques de détection d'intrusion sont présentées dans la littérature. La première technique est la technique de détection basée sur l'anomalie. Il détecte les intrusions sur la base du comportement normal du système. Cette technique peut détecter les attaques nouvelles ou inconnues, mais avec des taux de faux positifs élevés. Il existe diverses techniques dans la littérature qui ont été appliquées pour la détection d'anomalies telles que les approches statistiques, le datamining et les approches basées sur les réseaux de neurones [7]. La deuxième technique est la technique de détection basée sur les signatures, qui détecte les intrusions sur les bases d'une signature d'attaque prédéfinie. L'inconvénient de cette technique est qu'elle ne peut pas détecter des nouvelles attaques, mais elle a de faibles taux de faux positifs, de sorte qu'elle est généralement utilisée par les IDS à but commercial. La dernière technique est la détection d'intrusions basée sur les spécifications. Dans cette technique, nous spécifions d'abord l'ensemble des contraintes sur un protocole ou un programme particulier, puis les intrusions sont détectées en tant que des violations de l'exécution de ces spécifications. Elle est présentée comme une alternative prometteuse qui combine les forces des techniques de détection basées sur des anomalies et des signatures, permettant de détecter des attaques connues et inconnues avec un taux de faux positifs plus bas. Elle peut détecter de nouvelles attaques qui ne suivent pas les spécifica-

tions du système. De plus, elle ne déclenche pas de fausses alarmes lorsque le programme ou le protocole a un comportement inhabituel mais légitime, puisqu'elle utilise des spécifications légitimes du programme ou du protocole. Le principal problème de cette technique est qu'il faut plus de temps pour définir les spécifications détaillées de chaque protocole / programme.

Lorsqu'une intrusion est détectée dans le réseau, une réponse appropriée est déclenchée conformément à la politique de réponse. Cependant, les réponses peuvent être passives ou actives. Les réponses passives ne font que déclencher l'alarme et informer l'autorité concernée. Les réponses actives tentent d'atténuer les effets des intrusions et sont divisées en deux groupes : ceux qui cherchent à contrôler le système attaqué et ceux qui cherchent à contrôler le système attaquant [33]. Le premier essaie de restaurer le système endommagé en supprimant des processus, en mettant fin à des connexions réseau, etc. Et, le dernier tente d'empêcher les tentatives futures d'un attaquant, ce qui peut être nécessaire pour des applications militaires.

L'architecture d'un IDS dans les MANETs peut être classée en IDS autonome, distribué et coopératif, et hiérarchique.

Dans l'architecture IDS autonome, un IDS s'exécute indépendamment sur chaque nœud pour déterminer les intrusions. Il collecte les données d'audit sur son propre nœud, car il n'y a pas de communication avec les autres nœuds du réseau. L'architecture IDS autonome est adaptée à une infrastructure de réseau plate.

Puisque les nœuds dans les MANET ont seulement des données locales, une architecture IDS distribuée et coopérative est généralement utilisée pour fournir une approche de détection plus éclairée. Dans cette architecture, chaque nœud a son agent IDS local et communique avec les agents des autres nœuds pour échanger des informations, prendre des décisions et répondre. De la même manière, cette architecture convient également à l'infrastructure de réseau plate.

La dernière architecture est l'IDS hiérarchique qui est une sorte d'architecture distribuée et coopérative plus adaptée aux réseaux multicouches. Dans cette architecture, le réseau peut être divisé en groupes tels que les clusters, les zones où certains nœuds (têtes de cluster, nœuds interzones, etc.) ont plus de responsabilités (communication avec d'autres clusters, zones) que les autres nœuds du même cluster. Il en est de même du point de vue de la détection d'intrusion : chaque nœud du cluster effectue une détection locale tandis que les têtes de cluster et les nœuds interzones effectuent une détection globale.

2.4.3 Travaux antérieurs sur les IDS ad hoc

Dans cette section, nous nous concentrons sur les recherches effectuées sur les techniques de logique floue basées sur IDS dans les réseaux MANETs.

Les auteurs de l'étude [1] ont proposé une optimisation d'un système de détection d'intrusion basé sur la logique floue. Leur approche automatise le processus de production d'un système flou en utilisant un ANFIS pour l'initialisation du système d'inférence floue, puis ils optimisent le système initialisé en utilisant les algorithmes génétiques. Dans leur travail, ils ont prouvé que leur IDS optimisé proposé contre l'attaque de trou noir surpasse les systèmes estimés normaux contre la même attaque.

Dans l'étude [29], les auteurs ont conçu un protocole de routage basé sur la confiance pour MANET en cluster. Le but principal de leur schéma de routage est d'obtenir le chemin le plus fiable pendant le temps de transmission du paquet du nœud source au nœud de destination. Leur mécanisme évite le choix d'un nœud malveillant qui agit comme un nœud réel dans un réseau ad hoc. Dans leur article, ils expliquent comment la tête de cluster calcule sa matrice de score de confiance en fonction de la composition max-min basée sur la logique floue de nœuds hautement fiables.

Les auteurs de l'étude [9] ont proposé un nouveau schéma utilisant un classificateur neuro-flou sous forme binaire pour les réseaux mobiles ad hoc afin d'identifier le comportement des activités courantes, c'est-à-dire normales ou anormales. Leurs résultats expérimentaux montrent que l'approche proposée est capable d'identifier des attaques connues (attaque de privation de sommeil) et inconnues (attaque par paquets) dans des réseaux mobiles ad hoc avec un taux positif élevé et un faible taux de faux positifs.

Le papier [3] a proposé un système pour détecter le comportement malveillant des nœuds par système de détection d'intrusion avec une technique de logique floue et identifié les attaques telles que l'attaque de trou noir et l'attaque de trou gris. Ce système empêche également les attaques en utilisant un mécanisme efficace de blocage des nœuds. Le système proposé comprend trois blocs principaux : la catégorisation d'attaque, l'implémentation floue et l'estimation floue. Dans leur module d'implémentation floue, ils ont utilisé le nombre de paquets abandonnés par le nœud.

Les auteurs du papier [30] ont proposé un système de détection d'intrusion basée sur la logique floue pour une prévention des attaques dans MANET. Ils ont utilisé une machine à vecteurs de support (Support Vector Machine (SVM)[14]) pour distinguer les nœuds

malveillants des nœuds légitimes. Ensuite, les règles floues sont utilisées pour isoler les nœuds malveillants pour la prévention de l'intrusion.

L'étude [5], a également proposé une architecture sécurisée basée sur la logique floue pour MANET dans laquelle la classification des nœuds et la détection des activités malveillantes sont effectuées par un détecteur flou, en considérant le taux de livraison des paquets (Packet Delivery Ratio (PDR)), transmission de paquets (Packet Forwarding (PF)) et l'énergie résiduelle (Residual Energy (RE)) en tant que paramètres d'entrée. Après avoir détecté une activité malveillante, une étude comparative est effectuée sur la base de paramètres tels qu'un rapport de livraison de paquets, un débit moyen, un transfert total de paquets et un pourcentage de détection avec variation de la vitesse du nœud.

Les auteurs du papier [56] ont proposé une technique de logique Di-Fuzzy qui fournit une détection en deux phases pour le paquet de données malveillantes et calcule la fiabilité du paquet de données afin d'assurer la communication entre les troupes de guerre dans différentes localités. Leur technique comporte trois étapes, à savoir la sélection de la tête de cluster, la technique de logique floue et la détection d'intrusion. La sélection de la tête de cluster de leur solution est basée sur le nœud avec l'énergie maximale pour améliorer la durée de vie du réseau.

Ces systèmes de détection d'intrusion proposés (sauf la solution [1]) avec l'utilisation de la logique floue reposent sur l'expérience du chercheur pour bien comprendre le système afin de choisir le nombre de fonctions d'appartenance pour chaque ensemble flou, la forme, et la position de chacun. En outre, il faut un effort de la part du chercheur pour définir la base de règles pour ce système flou (en remarquant que même avec un chercheur expert de haut niveau, ces paramètres sont difficiles à optimiser). Afin de voir l'efficacité du processus d'optimisation dans la découverte des attaques, nous favorisons l'utilisation d'un système flou basé sur les capacités d'adaptation et d'apprentissage pour le système de détection d'intrusion dans MANET.

2.5 Conclusion

Les réseaux mobiles ad hoc sont une nouvelle technologie, de plus en plus utilisée dans de nombreuses applications. Ces réseaux sont plus vulnérables aux attaques que les réseaux filaires. Comme ils ont des caractéristiques différentes, les techniques de sécurité

classiques ne sont pas directement applicables. Les chercheurs se concentrent actuellement sur le développement de nouvelles méthodes de prévention, de détection et mécanisme de réponse pour les MANET.

Dans ce chapitre, nous avons donné un aperçu sur les techniques proposées dans la littérature pour sécuriser les réseaux mobiles ad hoc. Ces techniques proposées soit une modification dans le mécanisme des protocoles de routage existant (par exemple AODV ou OLSR), soit de nouveaux protocoles de routage sécurisés autonomes basées sur quelques primitives cryptographiques telles que le chiffrement et la signature numérique, ou bien l'utilisation des systèmes de détection d'intrusion, avec différentes techniques de détection d'intrusions, architectures et mécanismes de réponse. Cette analyse réalisée dans l'état de l'art nous a permet d'orienter la suite de nos travaux. C'est pour cela, nous nous sommes concentrés sur la contribution / nouveauté apportée par chaque solution.

Le prochain chapitre a pour objet de présenter une évaluation de performances du protocole de routage AODV sous l'influence des attaques.

Chapitre 3

Evaluation de performances du protocole AODV sous l'influence des attaques

Sommaire

3.1 Introduction

Dans le premier chapitre, nous avons apporté une vue sur un ensemble d'attaquants au niveau du routage dans les réseaux mobiles ad hoc, et leur classification selon l'emplacement et la propriété des attaques. Pour rendre la sécurité du réseau incassable contre ces différents

types d'attaque, il est indispensable de développer un schéma de sécurité capable de prendre en compte le comportement malveillant des nœuds. La défense contre ces attaques n'est assurée qu'avec une compréhension profonde de ces attaques. Par conséquent, la simulation et l'étude des attaques permettent d'offrir une vision sur les performances du protocole de routage sous l'influence des attaques, et elle permet également aux chercheurs de tester leurs algorithmes de sécurité pour les améliorer.

Le but de ce chapitre est d'évaluer, de simuler et de comparer des attaques par trou noir, par inondation et par précipitation pour comprendre le comportement du protocole de routage AODV lors de ces attaques.

3.2 Les métriques utilisées dans notre simulation

Les mesures de performance suivantes sont prises en compte pour l'évaluation du comportement malveillant du protocole de routage AODV lors d'attaques de trous noirs, d'inondations et de précipitation [39] :

3.2.1 Taux de paquets délivrés

Le taux de paquets délivrés (en anglais est : Packet Delivery Ratio (PDR)) est le rapport entre le nombre total de paquets reçus par les nœuds de destination et le nombre total de paquets générés par les nœuds sources. Il est utilisé pour calculer le taux de perte des paquets de données lors de la transmission de données sur le réseau. Il évalue le taux de perte et mesure à la fois l'exactitude et l'efficacité des protocoles de routage ad hoc. Un taux de paquets délivrés plus élevé est espéré dans n'importe quel réseau.

$$PDR = \frac{\sum \text{nombre de paquets reçus par les nœuds de destination}}{\sum \text{nombre de paquets générés par les nœuds sources}} * 100 \qquad (3.1)$$

3.2.2 Délai de bout-en-bout

Le délai de bout-en-bout de paquets de données est le temps consommé par les paquets de données pour atteindre les destinations respectives. Cette métrique comprend tout le

retard pris par le routeur pour trouver le chemin dans le réseau : mise en mémoire tampon, transmission, propagation, retransmission. Le délai moyen de bout en bout pour un paquet P qui a été envoyé par le nœud N en tant que nœud source et reçu avec succès au niveau du nœud de destination est le suivant :

$$\text{Délai moyen de bout en bout} = \frac{\sum (\text{TA - TE})}{\sum \text{nombre de paquets de données reçus}} \tag{3.2}$$

Où TA désigne le temps d'arrivée du paquet P au nœud destination, et TE est le temps d'envoi du paquet P par le nœud N. Le délai moyen de bout en bout inférieur est le meilleur. Un protocole de routage a de meilleures performances s'il garantit un délai de bout-en-bout minimal.

3.2.3 Débit

Le débit peut être défini comme le nombre de bits réussis par unité de temps transmis par le réseau d'une source à une destination. Le débit est représenté en bits par seconde. Les facteurs qui affectent le débit dans les réseaux ad hoc sont les changements fréquents de topologie et la bande passante limitée. Dans tout le réseau, un débit plus élevé est le facteur le plus essentiel.

L'expression mathématique est la suivante :

$$\text{Débit} = \frac{\sum (\text{nombre total des bits reçues})}{\text{la durée de la simulation}} \tag{3.3}$$

3.3 Modélisation de la simulation et Scénarios

Les simulations sont effectuées à l'aide du simulateur de réseau NS-2.35 [18] pour évaluer l'effet du trou noir, des inondations et des attaques de précipitation sur le protocole de routage AODV dans les réseaux MANETs. Nous utilisons un modèle de points de cheminement aléatoire comme modèle de mobilité et définissons la source du trafic au débit binaire constant (CBR : Constant Bit Rate) ; les nœuds se déplacent dans une zone de

500 m x 500 m ; nous avons utilisé une taille de paquet de 512 octets. Nous avons utilisé les paramètres de simulation cités dans le tableau 3.1 pour chaque cas, en faisant varier le nombre de nœuds, la mobilité, le nombre de connexions et le nombre des attaquants avec des simulations successives.

Paramètre	**Valeur**
Simulateur	NS2(version 2.35)
Temps de simulation	200s
Taille du réseau	500 x 500 m
Protocole de routage	AODV
Type de trafic	CBR
Taille de paquets	512 octet
Nombre de nœuds	10 to 80
Nombre de connexions	1 to 20
Nombre de nœuds malveillants	1 to 5
Modèle de mobilité	RandomWaypoint
Temps de pause	10s
Taux de transmission	0.25
Portée de transmission	50m
Vitesse des nœuds	0-30m/s

TABLE 3.1 – Les paramètres de simulations

3.4 Résultats et interprétation

Nous évaluons les performances du protocole de routage AODV contre les attaques par trous noirs, par inondations et par précipitation en modifiant la taille du réseau, la mobilité, la charge de trafic et le nombre d'adversaires, comme indiqué dans les sous-sections suivantes.

Type d'attaque	**Désignation**
Blackhole	Trou noir
Flooding	Innondation
Rushing	Précipitation

TABLE 3.2 – Type d'attaques

3.4.1 Effet de la densité du réseau

Le nombre de nœuds varie de 10 à 80, le nombre de connexions pour 10 nœuds est 5 et pour 20 à 80 nœuds est 10. La vitesse est réglée sur 10 m/s et le temps de pause sur 10 s. Les figures 3.1, 3.2, 3.3 montrent le comportement de l'AODV lors d'attaques avec la taille de réseau variable. Nous pouvons conclure de l'analyse de la figure 3.1 que le taux de paquets délivrés sous attaque par trou noir diminue de manière significative, tandis que le taux de paquets délivrés lors d'inondations et d'attaques de précipitation est légèrement inférieur à celle de l'AODV. La figure 3.2 montre que le délai moyen de bout en bout diminue dans tous les cas. Le débit diminue considérablement avec l'existence de l'attaque du trou noir, comme le montre la figure 3.3.

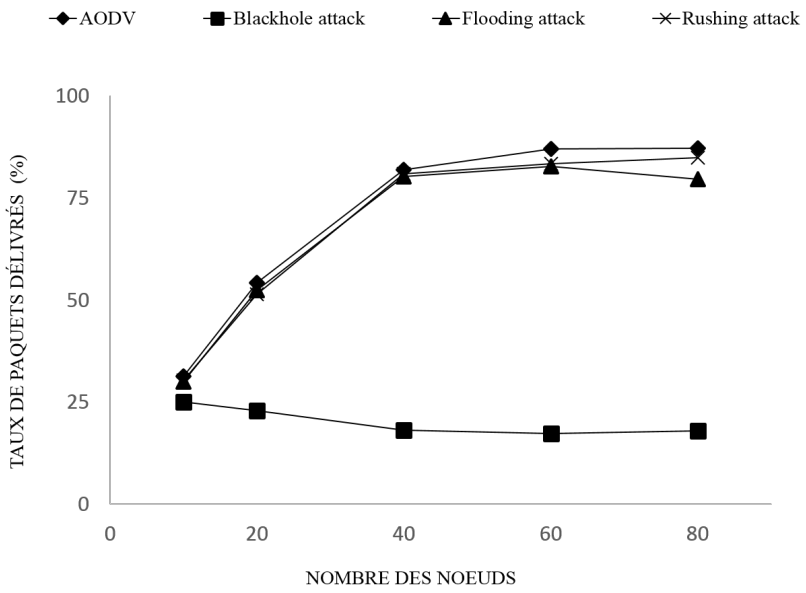


FIGURE 3.1 – Taux de paquets délivrés Vs. Le nombre des noeuds

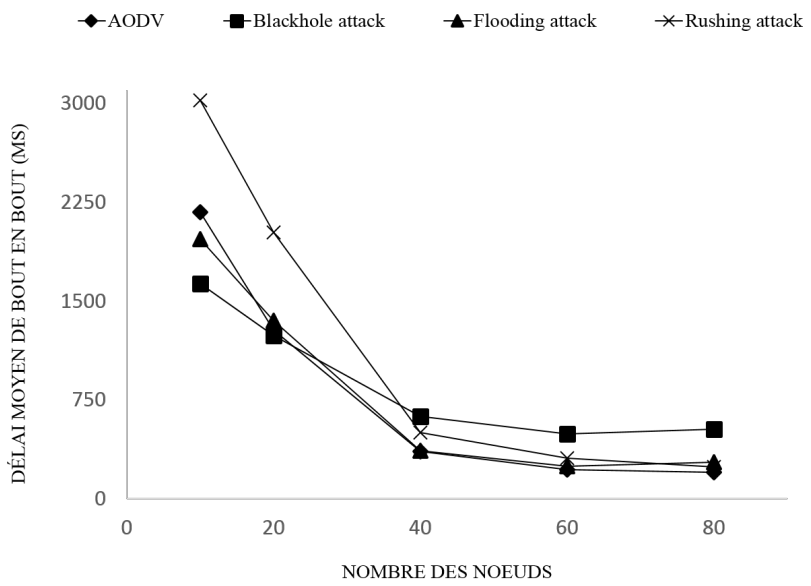


FIGURE 3.2 – Délai moyen de bout en bout Vs. Le nombre des noeuds

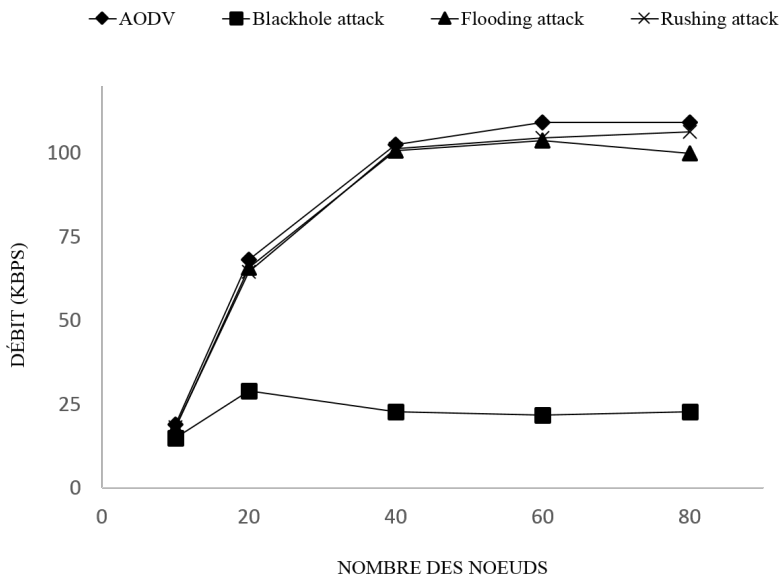


FIGURE 3.3 – Débit Vs. Le nombre des noeuds

3.4.2 Effet de la mobilité

Les figures 3.4, 3.5, 3.6 montrent l'effet de la mobilité sur le protocole de routage AODV en faisant varier la vitesse de 0 m/s à 30 m/s en maintenant la taille du réseau à 50, le nombre de connexions à 10 et le temps de pause à 10 s. Le taux de paquets délivrés sous une attaque par trou noir est inférieur à l'AODV, alors que sous les attaques par inondations et par précipitation, le taux de paquets délivrés est presque équivalent à celle de l'AODV standard, comme le montre la figure 3.4. Le délai moyen de bout en bout de trou noir augmente considérablement par rapport aux autres cas dans la figure 3.5. Le débit moyen est inférieur en présence d'une attaque par trou noir que lors d'une attaque par inondation ou par précipitation ou de l'AODV standard, comme le montre la figure 3.6.

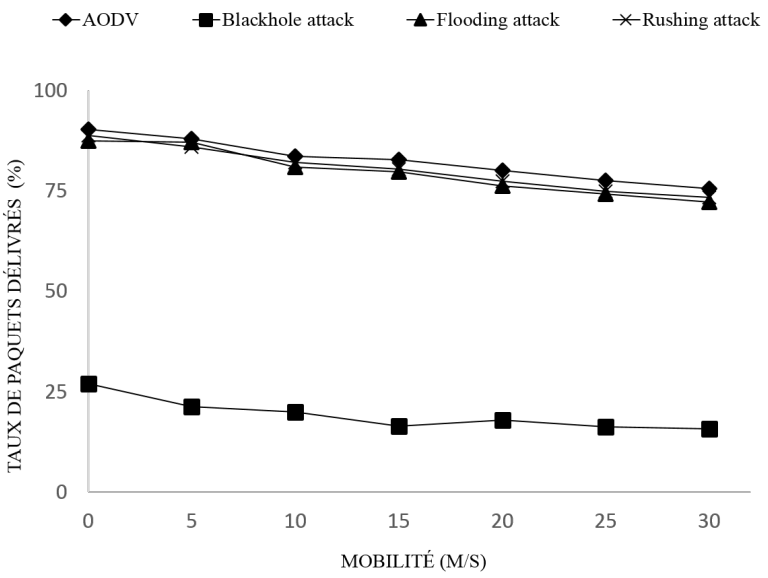


FIGURE 3.4 – Taux de paquets délivrés Vs. La mobilité

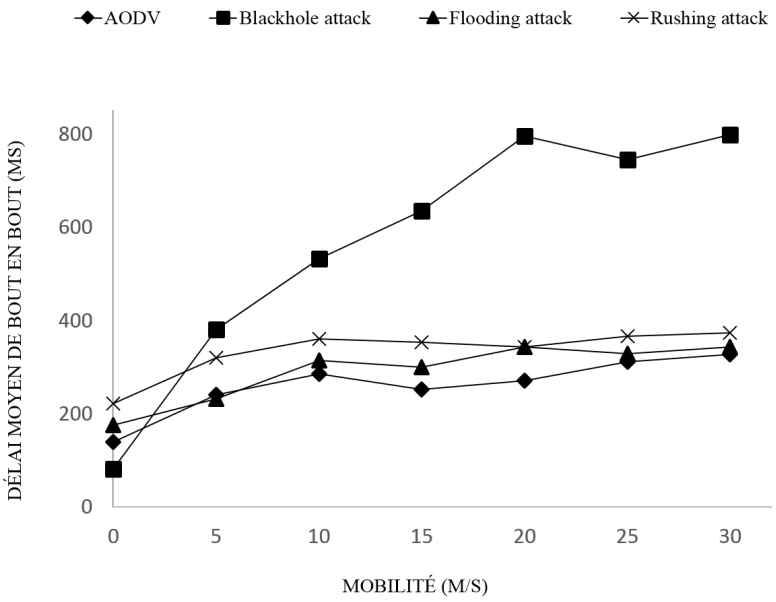


FIGURE 3.5 – Délai moyen de bout en bout Vs. La mobilité

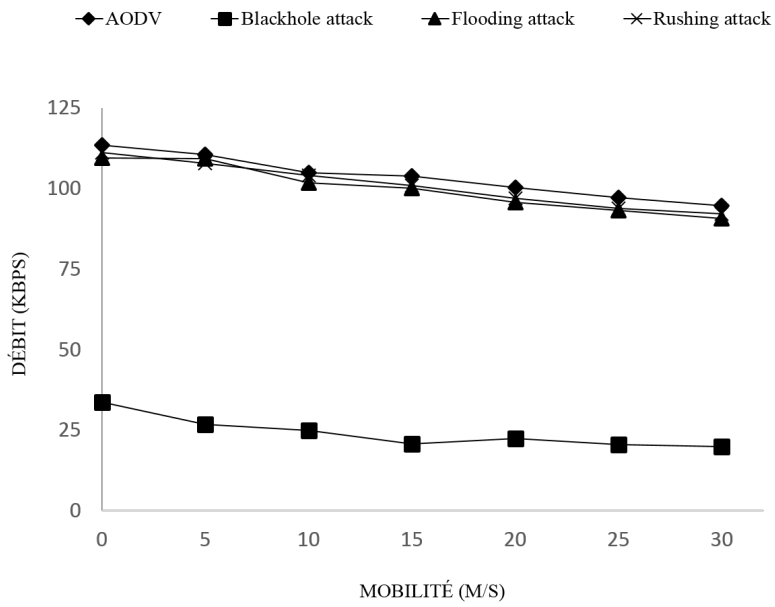


FIGURE 3.6 – Débit Vs. La mobilité

3.4.3 Effet de la charge de trafic

Le nombre de connexions varie de 1 à 20 en maintenant la taille du réseau à 50, la vitesse à 10 m/s et le temps de pause à 10 s. Les figures 3.7, 3.8, 3.9 présentent les effets de la charge de trafic pour AODV et AODV en cas d'attaques de trous noirs, d'inondations et de précipitation. Comme le nombre de connexions augmente, les pertes de paquets augmentent en raison de la congestion. Par conséquent, le taux de paquets délivrés pour l'AODV standard commence à diminuer à mesure que le nombre de sources augmente, comme le montre la figure 3.7. Le taux de paquets délivrés sous l'attaque par trou noir est plus affecté que les attaques par inondations et les attaques par précipitation. La figure 3.8 montre le délai moyen de bout en bout de l'AODV et de l'AODV sous attaques, on peut observer qu'il y a une augmentation significative du délai moyen de bout en bout avec l'effet du trou noir, comparativement à au protocole AODV normal. Le graphique du débit pour l'attaque par inondation et par précipitation est légèrement inférieur à celui de l'AODV, tandis que le débit pour l'attaque du trou noir est considérablement inférieur à celui de l'AODV, comme le montre la figure 3.9.

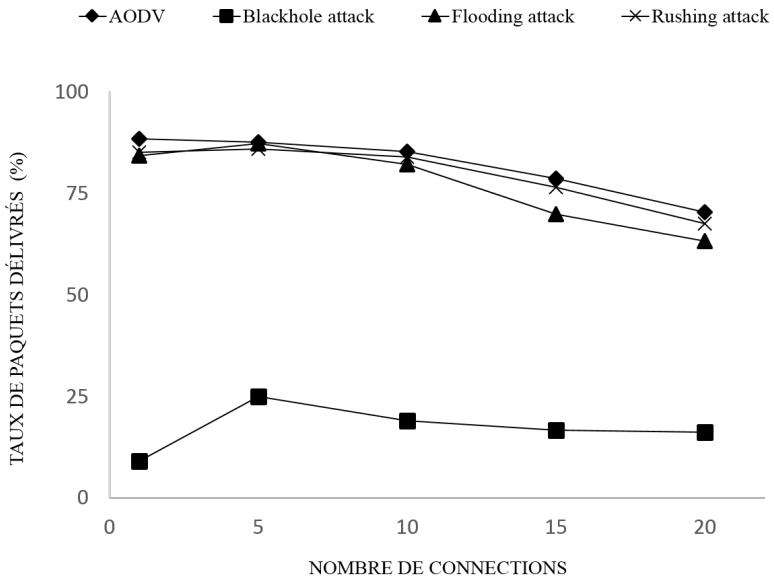


FIGURE 3.7 – Taux de paquets délivrés Vs. Le nombre de connexions

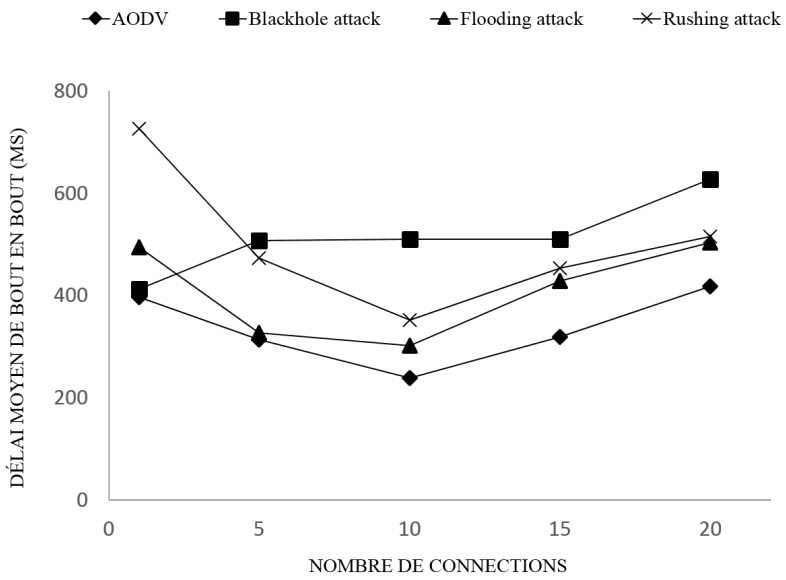


FIGURE 3.8 – Délai moyen de bout en bout Vs. Le nombre de connexions

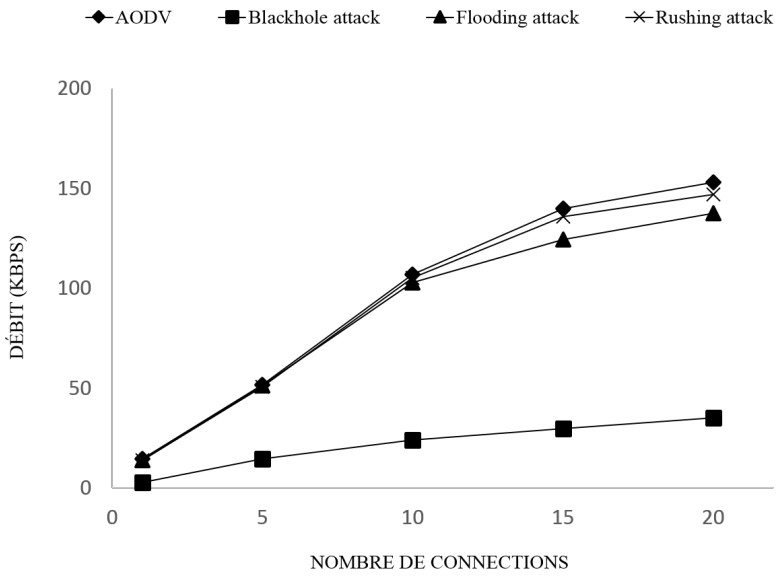


FIGURE 3.9 – Débit Vs. Le nombre de connexions

3.4.4 Effet du nombre des nœuds malveillants

Les figures 3.10, 3.11, 3.12 présentent l'effet du nombre des nœuds malveillants sur le protocole de routage AODV en augmentant le nombre d'attaquants de 1 à 5, la taille du réseau est de 50, la vitesse maximale est 10 m/s, le temps de pause est 10 s et le nombre de connexions est 10. Nous constatons que quand le nombre de nœuds malveillants augmente, le taux de paquets délivrés et le débit de l'AODV sous attaques commence à diminuer, nous constatons aussi que le taux de paquets délivrés et le débit de l'AODV sous attaque du trou noir est le plus affecté que d'autres attaques comme le montrent les figures 3.10 et 3.12 . La figure 3.11 montre le délai moyen de bout en bout de l'AODV en cas d'attaque, à partir de la figure, le délai moyen de bout en bout de l'attaque par inondation et de l'attaque par précipitation augmente lorsque le nombre d'attaquants augmente, tandis que le délai moyen de bout en bout du trou noir diminue.

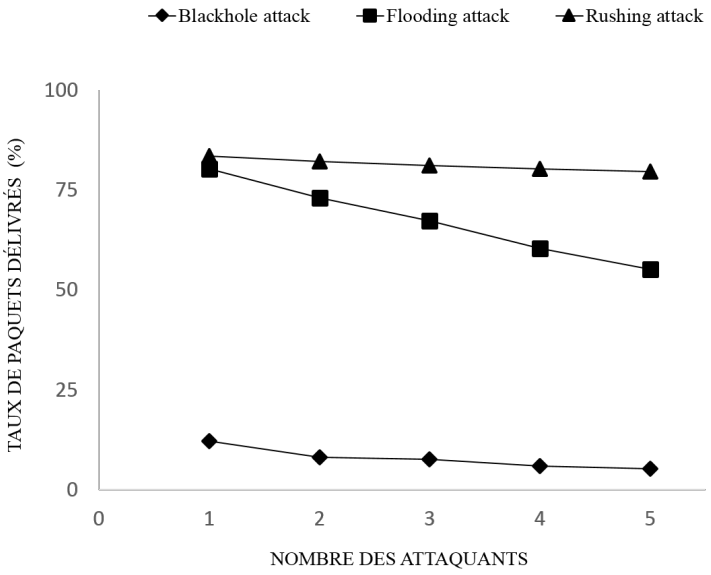


FIGURE 3.10 – Taux de paquets délivrés Vs. Le nombre des attaquants

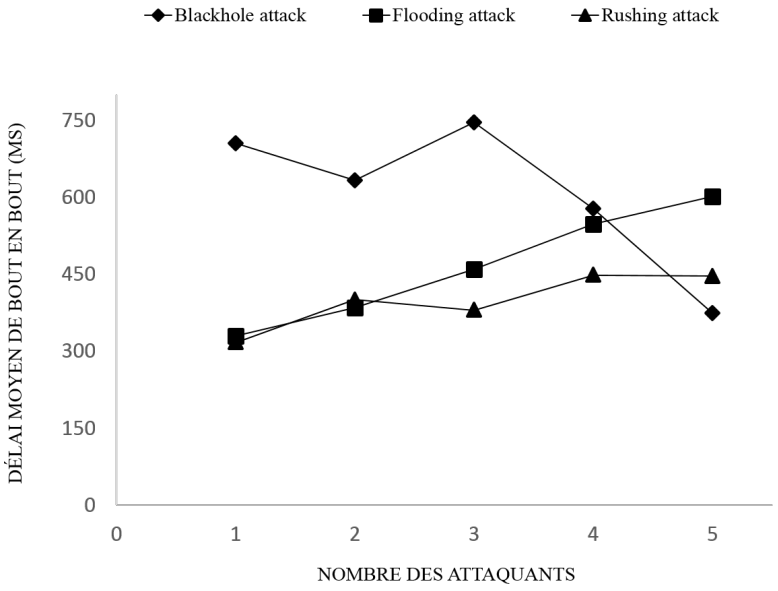


FIGURE 3.11 – Délai moyen de bout en bout Vs. Le nombre des attaquants

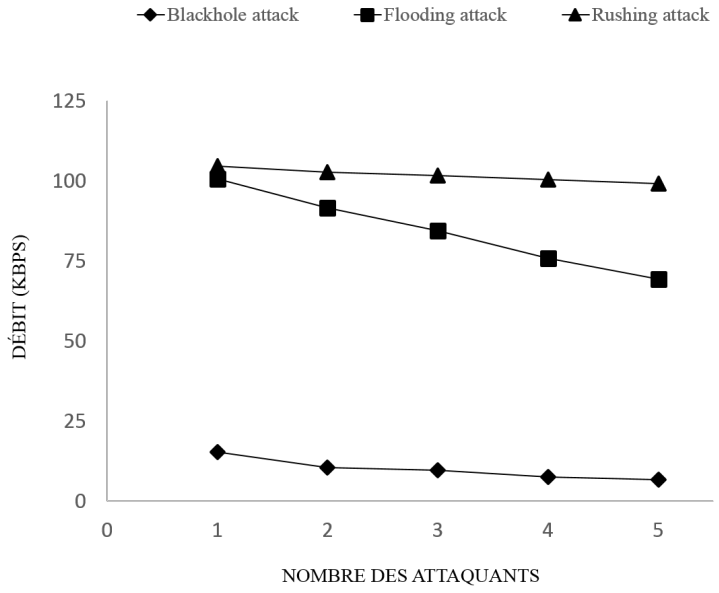


FIGURE 3.12 – Débit Vs. Le nombre des attaquants

3.4.5 Les paquets supprimés dans les attaques

Nous avons calculé le taux des paquets supprimés pour les attaques du trou noir et des attaques par précipitation. L'attaque par inondation provoque un déni de service, dans ce cas-là, il n'y a pas de suppression de paquets. Pour cette raison, nous calculons le taux de paquets supprimés uniquement pour l'attaque du trou noir et l'attaque par précipitation. La figure 3.13 montre que l'attaque du trou noir supprime de nombreux paquets, tandis qu'une attaque par précipitation supprime quelques paquets. Le résultat de cette différence est que l'attaque de trou noir envoie une réponse d'itinéraire avec un numéro de séquence plus élevé au nœud source pour être dans l'itinéraire choisi, alors que dans l'attaque par précipitation, les paquets ne seront supprimés que si l'itinéraire choisi contenait l'attaquant. Pour la simulation, nous avons analysé avec 50 nœuds, une vitesse maximale de 10 m/s, un temps de pause de 10 s, un nombre de connexions de 5 et un attaquant.

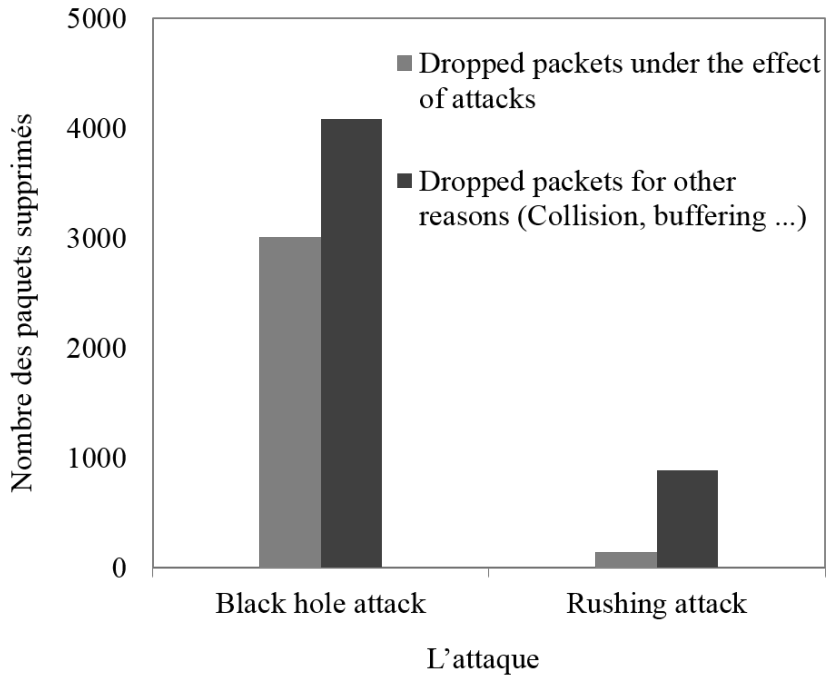


FIGURE 3.13 – Calcul des paquets supprimés

3.5 Conclusion

Dans ce chapitre, nous avons analysé l'impact de certaines attaques contre les réseaux MANETs qui sont principalement des trous noirs, des inondations et des attaques par précipitation. Ces attaques ont été implémentées dans NS-2 en utilisant le protocole de routage AODV. Ensuite, nous avons comparé les performances de l'AODV sous attaques avec l'AODV d'origine en termes du taux de paquets délivrés, de délai moyen de bout en bout et le débit. À partir des simulations, nous concluons que les performances de l'AODV se dégradent sous les attaques, que ce soit en raison de la taille du réseau, de la mobilité ou de la charge de trafic. Par conséquent, le taux de paquets délivrés diminue dans le réseau avec l'attaque du trou noir. En outre, nous avons observé que le délai moyen de bout en bout est plus élevé dans l'attaque du trou noir. Le débit du réseau est réduit avec l'attaque des trous noirs par rapport aux attaques par inondation et par précipitation. Par conséquent, l'attaque du trou noir a un effet significatif sur les performances du réseau.

Dans le chapitre suivant nous allons présenter nos différentes contributions pour sécuriser le routage dans les réseaux MANETs.

Chapitre 4

Sécurisation des protocoles de routage ad hoc

Sommaire

4.1 Introduction

Dans le chapitre précédent, nous avons constaté que l'attaque du trou noir a un effet significatif sur les performances du réseau MANET. Cette attaque peut être facilement lancée sur des protocoles de routage réactifs comme AODV. Dans l'attaque du trou noir, un nœud malveillant peut drainer tous les paquets de données en réclamant faussement un nouvel itinéraire ou l'itinéraire le plus court chemin vers le nœud de destination, sans avoir aucune route active vers la destination spécifiée, et les absorbe sans les transmettre au nœud de destination.

De plus les protocoles de routage pour les réseaux mobiles ad hoc (MANET) ont été développés sans tenir compte des exigences de sécurité. Par conséquent, la plupart des

chercheurs se concentrent sur ce sujet.

L'objectif de ce chapitre est de présenter les différentes contributions visant à résoudre les problèmes relatifs à la sécurité du processus de routage dans les réseaux MANETs. D'abord, on va présenter notre solution pour sécuriser le protocole de routage réactif AODV contre l'attaque du trou noir, puis nous proposons une nouvelle approche pour assurer la sécurité dans le protocole de routage proactif OLSR.

4.2 Cas du protocole de routage réactif : AODV

4.2.1 Solution proposée

Dans cette section, nous décrirons en détail notre solution proposée [38] pour empêcher l'attaque du trou noir. En effet, nous avons modifié les procédures recvReply (Packet * p), recvRequest (Packet * p) et le paquet de réponse de route (Route REPly packet (RREP)), comme indiqué dans la figure 4.1 et le Tableau 4.1 illustre les champs du paquet RREP.

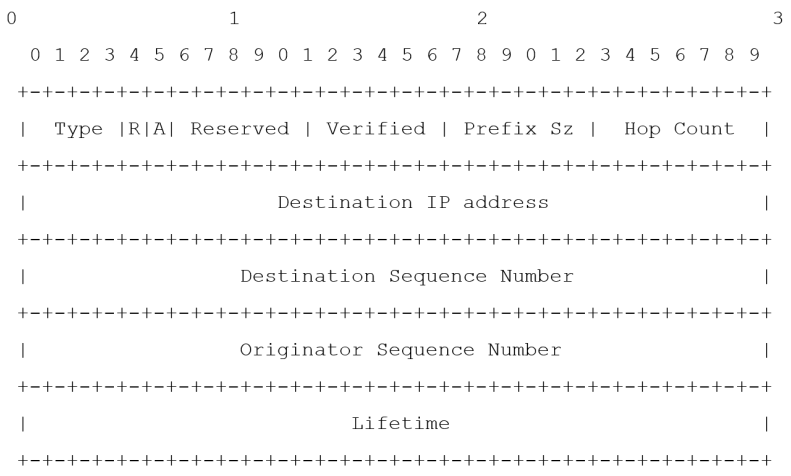


FIGURE 4.1 – Format du message de réponse de route modifié (RREP)

Selon le protocole AODV, le nœud source doit diffuser le paquet RREQ pour trouver un chemin pour atteindre le nœud de destination. Le nœud de destination, ou tout nœud intermédiaire ayant le chemin, peut renvoyer la réponse au nœud source. Ensuite, par défaut, le nœud source accepte le premier paquet RREP suffisamment récent qui lui arrive. Dans notre approche, comme le protocole AODV standard, le nœud de destination ou le nœud

Type	Forcé à 2.
R	Drapeau de réparation ; utilisé pour la multidiffusion.
A	Acquittement requise.
Réservé	Envoyé en tant que 0 ; ignoré à la réception.
Verified	Un bit spécifie le paquet de réponse de route si elle est valide ou non, comme illustré ci-dessous : 0 fait référence à la RREP invalide 1 fait référence à la RREP valide
Prefix Sz	S'il est différent de zéro, la taille de préfixe 5 bits spécifie que le saut suivant indiqué peut être utilisé pour tous les nœuds ayant le même préfixe de routage (défini par la taille de préfixe) que la destination demandée.
Nombre de sauts	Nombre de sauts de l'adresse IP de l'expéditeur à l'adresse IP de destination. Pour les demandes de routage multidiffusion, cela indique le nombre de sauts effectués par le membre de l'arbre de multidiffusion qui envoie le RREP.
Adresse IP de destination	Adresse IP de la destination pour laquelle un itinéraire est fourni.
Numéro de séquence de destination	Le numéro de séquence de destination associé à la route.
Numéro de séquence de l'initiateur	Adresse IP du nœud à l'origine du RREQ pour lequel l'itinéraire est fourni.
Durée de vie	Durée, en millisecondes, pendant laquelle les nœuds recevant le RREP considèrent la route comme valide.

Table 4.1 – Champs du paquet RREP

intermédiaire génère le paquet RREP, mais génère aussi un autre paquet RREP, comme étant une confirmation du premier paquet avec un numéro de séquence incrémenté par un. Par conséquent, nous avons deux messages RREP du nœud de destination ou un nœud intermédiaire ayant l'itinéraire vers la destination, l'un avec le numéro de séquence normal et l'autre avec le numéro de séquence normal + 1, et les deux ont le champ VERIFIED mis à 0. Sur le nœud intermédiaire qui reçoit le paquet RREP, il stocke les informations

sur le paquet de réponse, puis il vérifie notre champ ajouté VERIFIED s'il est mis à 0 ou 1. S'il est 0, cela signifie que notre paquet n'est pas encore vérifié ou c'est un paquet invalide, sinon le paquet est vérifié et valide et il doit être transmis au nœud suivant. Dans le cas où le champ VERIFIED est mis à 0, si le nœud intermédiaire reçoit un deuxième paquet de réponse, il doit vérifier si le numéro de séquence de la première réponse est le numéro de séquence de la seconde moins un, si la vérification est vraie, il définit ensuite le champ VERIFIED à 1 et transmet le paquet. En outre, lorsque le nœud intermédiaire reçoit un autre paquet de réponse d'itinéraire du nœud malveillant qui effectue une attaque de trou noir avec un numéro de séquence de destination très élevé. La même procédure est suivie ; la vérification est le numéro de séquence du premier paquet de réponse doit être le numéro de séquence du deuxième paquet de réponse moins un. Si la vérification est fausse, le champ VERIFIED est laissé à 0 et ignore le paquet.

Notre solution permet d'éviter l'attaque du trou noir ainsi qu'une attaque multiple du trou noir. De plus, les messages de contrôle du nœud malveillant ne sont pas transférés dans le réseau.

Notre approche est basée sur les quatre étapes détaillées ci-dessous :

Algorithme 1 : Notre approche détaillée

Étape 1 : (Processus d'initialisation)
Démarre la phase de découverte de route avec le noeud source S.
Étape 2 : (Génération de RREPs)
Le nœud de destination ou le nœud intermédiaire génère deux paquets de réponses sur la route avec deux numéros de séquence de destination différents, le second doit être incrémenté par un.

```
sendReply( seqno, // Numéro de séquence de destination
    VERIFIED = 0, ) ; // Champ ajouté
sendReply( seqno+1, // Numéro de séquence de destination
    VERIFIED = 0, ) ; // Champ ajouté
```

Étape 3 : (Vérification de RREPs)

```
si (noeud intermédiaire reçoit RREP) alors
    si (la première fois que le nœud reçoit RREP) alors
        Stocker l'adresse IP et le seqno du noeud ;
        si (RREP est valide) alors
            Transférer le RREP ;
    sinon
        si (le nœud reçoit plus d'une RREP) alors
            Stocker l'adresse IP et le seqno du noeud ;
            si (RREP est invalide) alors
                si (nouveau seqno de RREP == ancien seqno de RREP + 1) alors
                    VERIFIED = 1 ; (Marquer RREP comme valide)
                    Transférer le RREP ;
                sinon
                    Ignorer le RREP ;
            sinon
                Transférer le RREP ;
```

Étape 4 : (Continuer le processus par défaut)
Le nœud source envoie des données au nœud de destination à partir de la route sélectionnée.

4.2.2 Méthodologie d'évaluation

4.2.2.1 Environnement de simulation

Les simulations sont effectuées à l'aide du simulateur de réseau NS-2 (v-2.35), afin d'analyser les performances de notre solution proposée par rapport aux attaques de trous noirs. Sur une taille du réseau de 500x500 m, 25 nœuds sont distribués aléatoirement, ils exécutent une fois le protocole de routage standard AODV et une autre fois le protocole de routage M-AODV (Modified AODV) pour comparer les deux protocoles sous l'attaque du trou noir. Les nœuds malveillants sont distribués aléatoirement. Cinq paires ont été choisies aléatoirement pour la communication de données, chacune envoyant 512 octets

par seconde. Tous les nœuds ont été déplacés dans un modèle de points aléatoires, avec des vitesses aléatoires comprises entre 0 et 30 m/s. De plus, le temps de pause des nœuds est de 10 secondes. Les paramètres de simulation sont résumés dans le tableau 4.2. Par conséquent, chaque point de données représente une moyenne de vingt exécutions.

Paramètre	**Valeur**
Taille du réseau	500x500 m
Nombre de nœuds	25
Temps de simulation	200s
Portée de transmission	50m
Modèle de mobilité	Random way point
Taux de transmission	0.25
Taille de paquets	512 Bytes
Protocole de routage	AODV / Modified-AODV
mobilité des nœuds	0-30 m/s
Nombre d'attaquants du trou noir	1 and 5
Nombre de connections	5
Type de trafic	UDP–CBR
Temps de pause	10s

TABLE 4.2 – Les paramètres de simulations

4.2.2.2 Métriques utilisées pour la simulation

Afin d'évaluer la performance de notre approche, nous avons utilisé les métriques suivantes :

- **Taux de paquets délivrés (PDR).**
- **Délai moyen de bout en bout.**
- **Surcharge de routage normalisée :** cette métrique indique le nombre de paquets de contrôle de routage générés par paquets de données transmis.

4.2.3 Résultats de la simulation et analyse

La figure 4.2 et la figure 4.3 montrent le taux de paquets délivrés d'AODV, notre solution et AODV sous des attaques de trous noirs lorsque la mobilité des nœuds varie. Il est clair d'après les chiffres que la performance de notre approche est supérieure à celle

d'AODV sous une attaque par trou noir, que ce soit pour un ou plusieurs attaquants. Le PDR de l'AODV sous une attaque était d'environ 15%, tandis que le PDR de l'AODV modifié en présence d'une attaque était d'environ 60%, ce taux est augmenté de 45%. De même, le PDR de l'AODV lors d'attaques multiples était d'environ 7%, ce qui a été augmenté de 43% par rapport à notre système en cas d'attaques multiples. De plus, le PDR du protocole de routage AODV sans aucune attaque est d'environ 64%, ce qui est dû à la congestion du réseau.

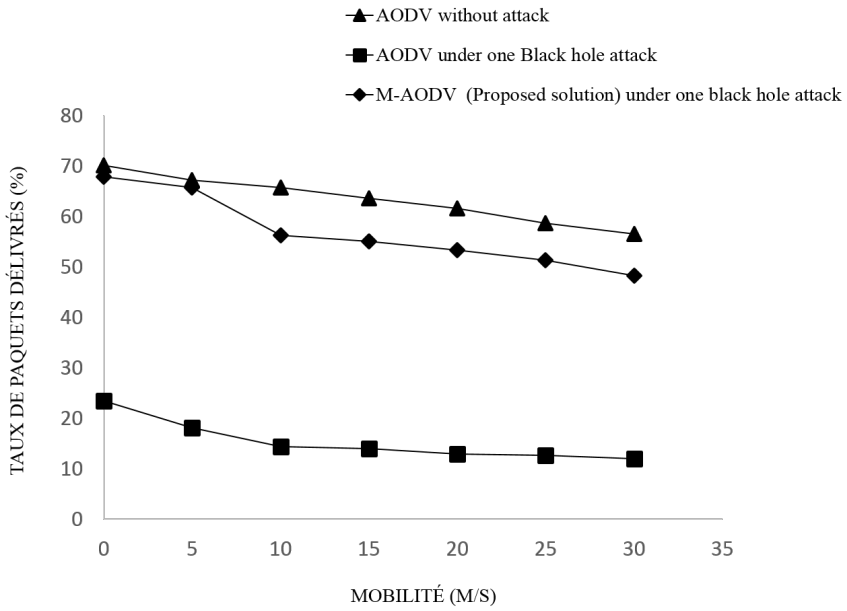


FIGURE 4.2 – Taux de paquets délivrés Vs. mobilité avec un attaquant

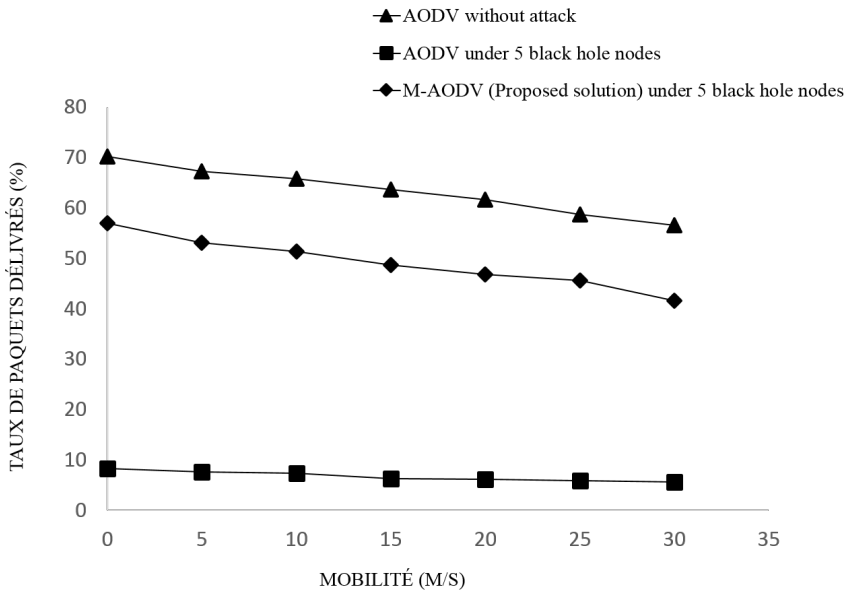


FIGURE 4.3 – Taux de paquets délivrés Vs. mobilité avec cinq attaquants

D'après les figures 4.4 et 4.5, on peut observer que, lorsque le protocole AODV modifié est utilisé, le délai moyen de bout en bout augmente par rapport au protocole de routage standard AODV sans attaque. De plus, nous observons que notre approche sous une attaque est légèrement augmentée dans le délai moyen de bout en bout, par rapport aux attaques multiples. Ceci est dû au temps d'attente supplémentaire dans chaque nœud intermédiaire avant d'envoyer la réponse, et quand il y a une attaque multiple, notre approche nécessite plus de temps pour calculer la bonne réponse d'itinéraire que quand une attaque existe.

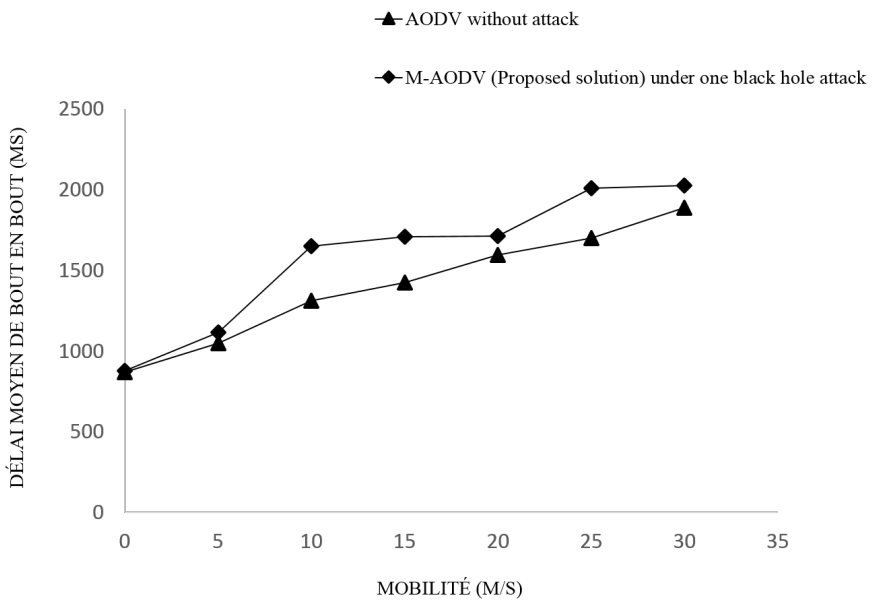


FIGURE 4.4 – Délai moyen de bout en bout Vs. mobilité avec un attaquant

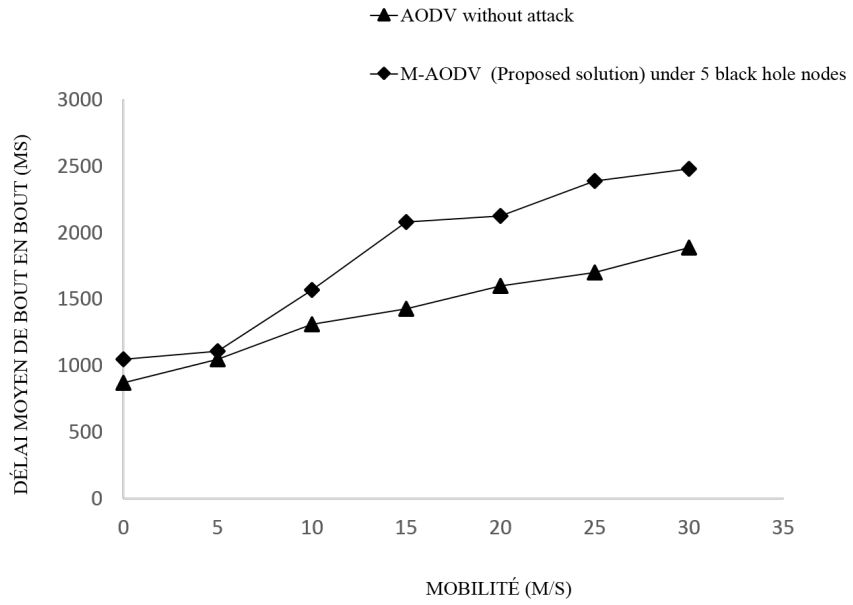


FIGURE 4.5 – Délai moyen de bout en bout Vs. mobilité avec cinq attaquants

La surcharge du routage normalisée est illustrée dans les figures 4.6 et 4.7 , avec une mobilité variable. Dans notre AODV modifié, la surcharge de routage sous un ou plusieurs

nœuds malveillants est légèrement supérieure à celle de l'AODV standard en raison du processus supplémentaire nécessaire pour éviter la sélection de nœuds malveillants. La surcharge de routage normalisée pour AODV en cas d'attaque de trou noir, que ce soit une ou plusieurs attaques est très élevée par rapport à l'AODV sans attaque. Cela est dû au fait que les nœuds de trous noirs envoient de fausses réponses aux paquets de demande de route, ce qui compromet le protocole de routage, puis le protocole commence à mal se comporter et à générer des paquets de routage supplémentaires.

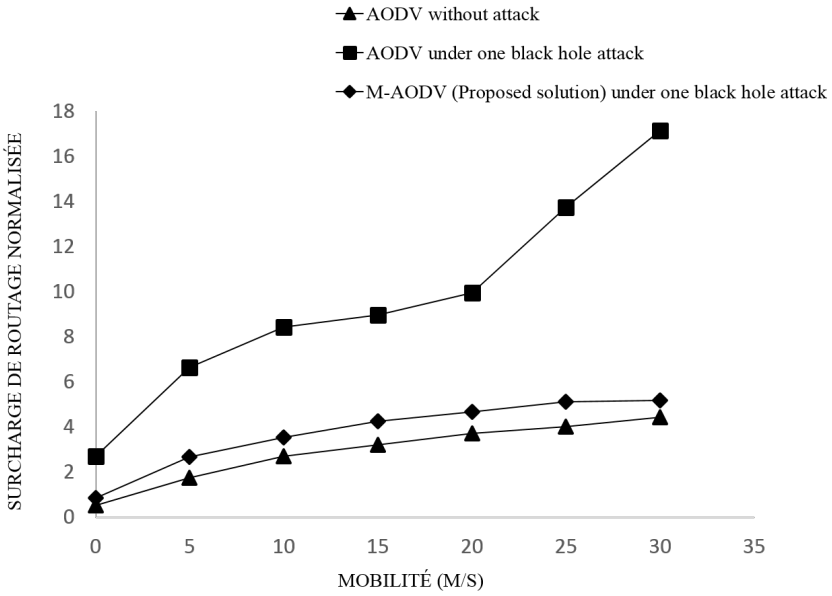


FIGURE 4.6 – NRL Vs. mobilité avec un attaquant

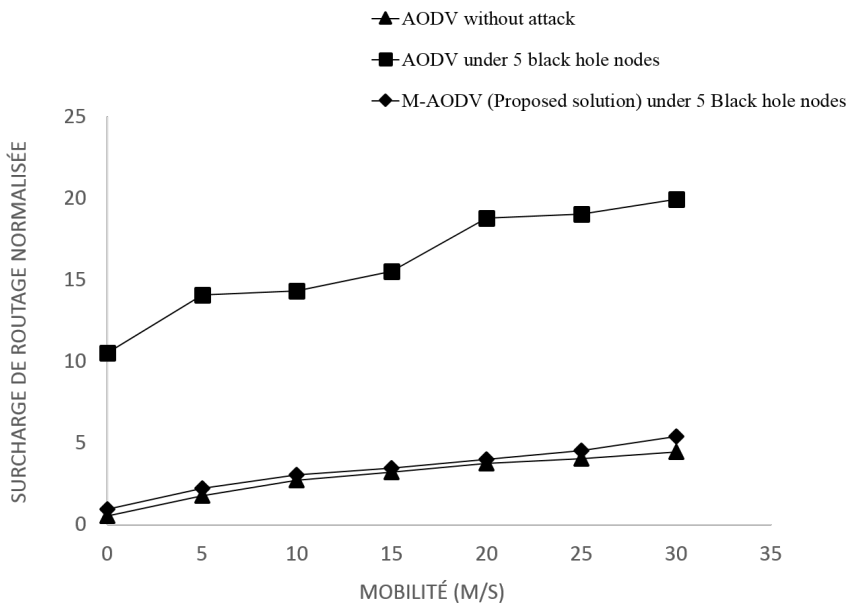


FIGURE 4.7 – NRL Vs. mobilité avec cinq attaquants

Nous avons calculé le nombre de paquets envoyés, supprimés et reçus dans les deux cas avec une attaque de trou noir et cinq attaquants dans le protocole de routage AODV standard, ainsi que dans notre AODV modifié, comme le montrent les figures 4.8 et 4.9 . Dans cette simulation, 25 nœuds se déplacent de manière aléatoire avec une vitesse maximale de 10 m/s, 10 secondes pour le temps de pause, le nombre de connexions est de 5 et le nombre de paquets circulant sur le réseau est de 2849 paquets. D'après la simulation, nous affirmons clairement que le système que nous proposons a surmonté l'attaque du trou noir lorsqu'il n'y a qu'une seule attaque du trou noir et même lorsqu'il y a plusieurs attaquants. Pour la différence entre les paquets envoyés et la somme des paquets supprimés et reçus est due aux paquets supprimés en cas de collision ou de mise en mémoire tampon ou pour d'autres raisons.

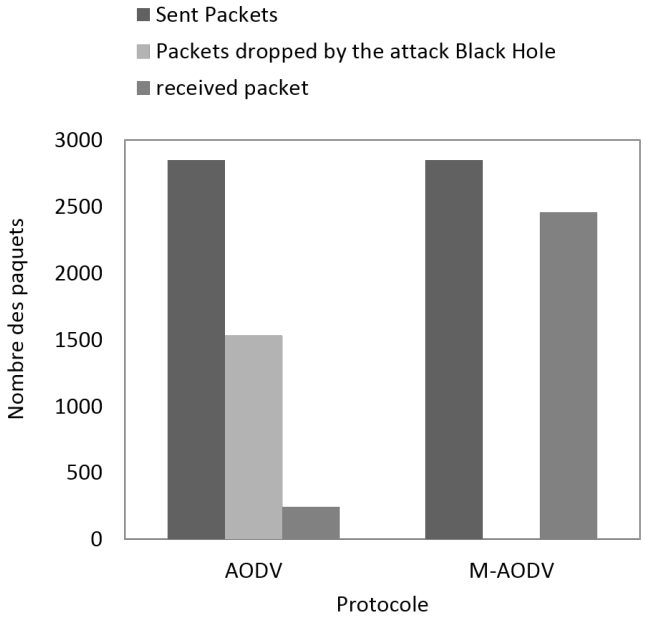


FIGURE 4.8 – Nombre de paquets traversant le réseau avec un attaquant

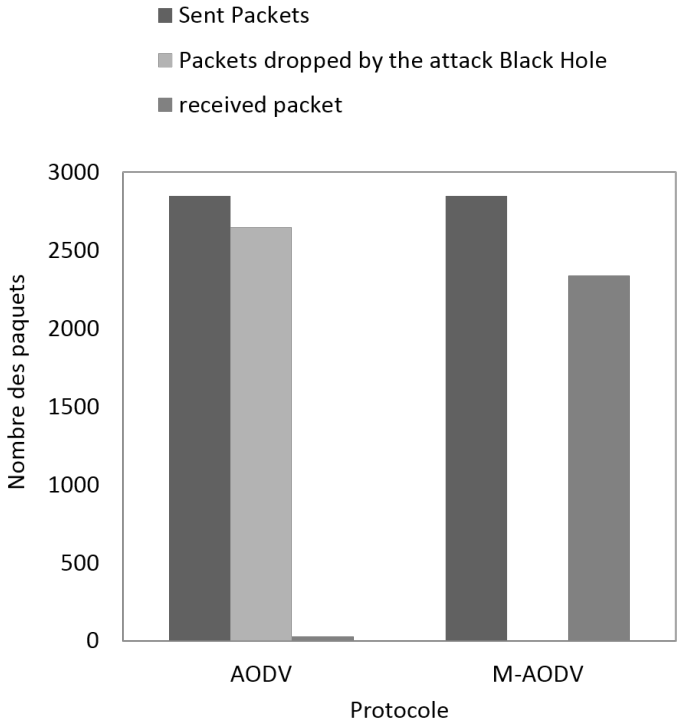


FIGURE 4.9 – Nombre de paquets traversant le réseau avec cinq attaquants

4.3 Cas du protocole de routage proactif : OLSR

4.3.1 Hypothèses

La couche physique et la couche de liaison de données sont vulnérables à certaines attaques telles que le brouillage, les interceptions, les écoutes indiscrètes, l'analyse du trafic et l'interruption des protocoles de contrôle d'accès au support. Il existe des mécanismes de sécurité pour remédier à ces vulnérabilités. Cependant, dans ce chapitre, nous ignorons les attaques sur ces deux couches.

En outre, les liaisons sont supposées être bidirectionnelles, par exemple, lorsque le nœud A est capable de transmettre au nœud B, de même B peut transmettre à A.

Nous supposons que les principaux problèmes de distribution et de gestion des clés sont résolus. Par conséquent, seul un nœud légitime peut obtenir une paire de clés publique / privée, nommée KA^- et KA^+ pour le nœud A. Cette gestion des clés supposée permet à tout nœud légitime de connaître la clé publique de tous les autres nœuds.

Dans ce travail, nous supposons également que tous les nœuds équipés de dispositifs GPS capables de fournir des informations de localisation pour chaque nœud.

Enfin, nous supposons que le réseau peut dupliquer, réorganiser ou corrompre les paquets en cours de transmission.

4.3.2 Paquets de routage sécurisés

Le protocole OLSR étant un protocole de routage proactif, l'échange de messages de contrôle est périodique entre les nœuds afin de gérer le routage des paquets de données. Par conséquent, les messages de contrôle doivent être authentifiés pour empêcher la création de faux itinéraires vers une destination quelconque. De plus, tous ces paquets de données sont transmis dans un format de paquet unifié appelé "paquets OLSR", comme le montre la figure 4.10.

Les champs des paquets de contrôle OLSR peuvent être divisés en deux catégories : les uns ne sont pas mutables pendant une transmission ; un autre est mutable, tel que le temps de vie (TTL) et le nombre de sauts (HC). Nous avons utilisé deux mécanismes pour

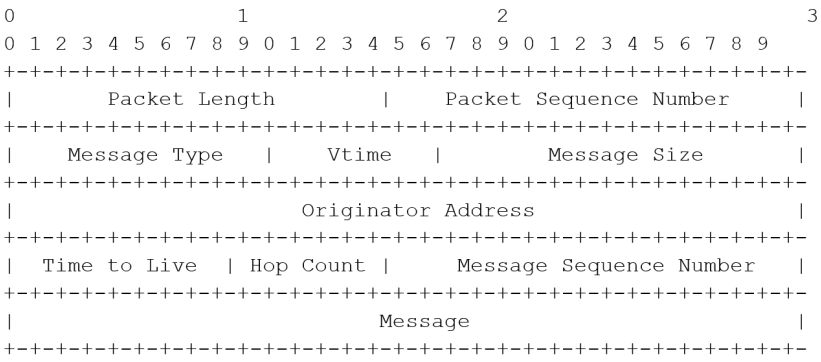


FIGURE 4.10 – Format de paquet OLSR

sécuriser les messages OLSR : les signatures numériques pour garantir que les champs non mutables sont inchangés avant la réception et les chaînes de hachage pour sécuriser les informations mutables dans les messages.

Les messages HELLO sont utilisés pour détecter et signaler les voisins d'un seul saut. Par conséquent, le TTL du message HELLO est défini sur 1, puisque les voisins ne les transfèrent pas. Pour cette raison, nous considérons les informations de TTL et HC dans le paquet HELLO comme des champs non mutables. Ainsi, dans notre plan, l'extension de signature attribuée au message HELLO n'utilisera pas les chaînes de hachage, contrairement aux autres messages de contrôle qui sont des paquets TC, MID et HNA. Les extensions de signature sont les suivantes (voir figure 4.11 et figure 4.12).

Les extensions de signature OLSR de sécurité améliorée (SE-OLSR) illustrées sur la figure 4.11 et la figure 4.12 sont générées par l'expéditeur de chaque message de contrôle OLSR et transmises avec le message de contrôle. Ces signatures doivent être le dernier message du paquet, de manière à ce que chaque message de contrôle soit suivi de sa propre extension de signature. Enfin, l'en-tête du paquet OLSR est ajusté pour inclure la taille de l'extension de signature dans le champ de taille. Comme le montre la Fig. 4.13.

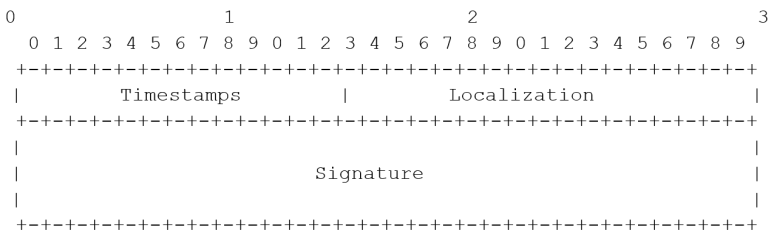


FIGURE 4.11 – Format des extensions de sécurité du paquet Hello

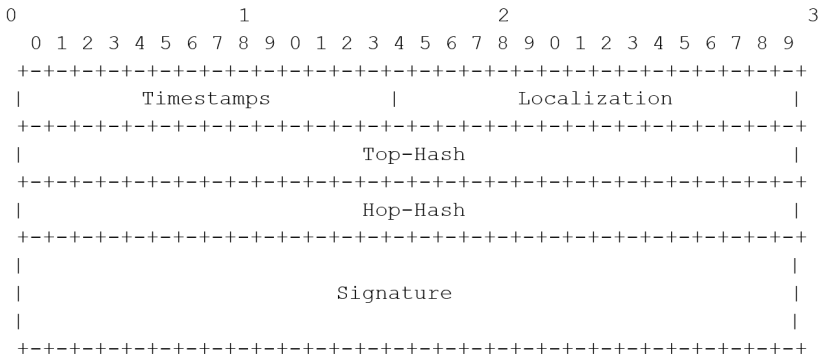


FIGURE 4.12 – Format des extensions de sécurité des paquets TC, MID, HNA

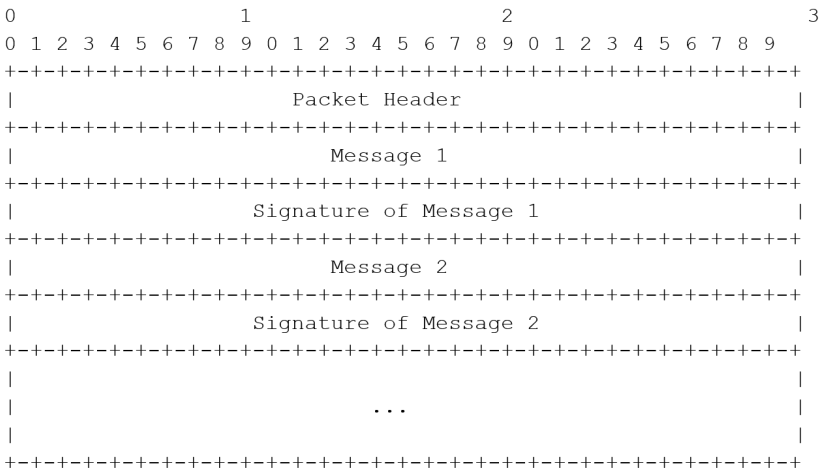


FIGURE 4.13 – Format de paquet OLSR avec les signatures

4.3.2.1 Signatures numériques SE-OLSR

Les signatures numériques sont utilisées pour authentifier et vérifier l'intégrité des données non mutables dans le message de contrôle. Par conséquent, l'utilisation de signatures numériques asymétriques est requise. De plus, les signatures numériques asymétriques utilisent deux clés spécialement corrélées. Contrairement aux signatures symétriques qui nécessitent la même clé dans le processus de création et de vérification d'une signature. Cependant, le message OLSR traversant plusieurs sauts, de sorte que l'utilisation de la signature de clé asymétrique protégerait les paquets contre les nœuds compromis.

- **Création de signature**

Un nœud génère un message de contrôle et signe les champs non mutables avec sa clé privée. De plus, la création des extensions de signature suit les étapes ci-dessous :

- ✓ Le paquet Hello ne sera pas transmis. Par conséquent, tous les champs du paquet seront signés. Parce que nous considérons que les champs mutables du paquet Hello sont inchangeables. Ainsi, la signature est : signature = sign (paquet Hello).
- ✓ Les autres messages de contrôle (TC, HNA et MID) sont transmis sur le réseau. Ensuite, le champ TTL est décrémenté de 1 et le nombre de sauts est augmenté de 1. En conséquence, les champs non mutables sont signés de la même manière, mais nous utilisons des chaînes de hachage pour TTL et Hop Count qui sont des champs mutables. La signature est donc : signature = sign (Le contenu inchangé).

• **Vérification de la signature** A la réception, un nœud récepteur vérifie la signature numérique avec la clé publique de l'expéditeur. Cependant, si une modification est notée par un nœud, l'extension de signature et son message de contrôle correspondant seront ignorés.

De plus, chaque saut du nœud suivant vérifie l'extension de signature de TC, MID et HNA, jusqu'à ce que le champ TTL devienne 0. Cependant, les voisins ne vérifient que l'extension de signature affectée au paquet Hello.

4.3.2.2 Protection des champs variables TTL et Hop Count

Les chaînes de hachage servent à protéger les champs mutables d'un message de routage OLSR. Cependant, deux champs de hachage sont ajoutés à chaque message de contrôle (le message TC, HNA et MID) : les champs Top-Hash et Hop-Hash présentés dans la figure 4.12.

Lorsqu'un nœud génère un nouveau message de contrôle à l'exception du paquet Hello, il effectue les opérations suivantes :

- ✓ Génère une valeur aléatoire appelée Seed.
- ✓ Définit le champ Hop-Hash sur la valeur Seed. (Hop-Hash = Seed).
- ✓ Calcule le champ Top-Hash en hachant la valeur de la Seed TTL fois. Top-Hash = $H^{\mathrm{TimeToLive}}(\mathrm{Seed})$

  Où : H est une fonction de hachage ;

  $H^{i}(x)$ est le résultat de l'application de la fonction H à x i fois.

Le nœud suivant exécute la procédure suivante lors de la réception d'un message de contrôle (message TC, HNA et MID) :

- ✓ Applique la fonction de hachage HTTL moins HC à la valeur du champ Hop-Hash. $H^{\text{TimeToLive-HopCount}}$(Hop-Hash).
- ✓ Comparez la valeur résultante à la valeur du champ Top-Hash.
  - — Si les deux valeurs sont égales, le message sera transmis et le nœud modifie le champ Hop-Hash en le hachant une fois dans l'extension de signature pour prendre en compte le nouveau saut. (Hop-Hash = H (Hop-Hash))
  - — Le message sera ignoré lorsque les deux valeurs ne sont pas égales.

En raison de la propriété unidirectionnelle d'une fonction de hachage, le champ Hop-Hash ne peut pas être modifié.

4.3.2.3 Timestamp ou estampille temporelle

Pour éviter les attaques du rejeu, un mécanisme du timestamp est requis pour chaque message de routage. Un timestamp est essentiellement une information au moment de la génération du message de l'expéditeur. Afin de permettre à un destinataire de savoir si un message est nouveau ou bien s'il y a un rejeu dans le message. De plus, le protocole OLSR peut déterminer quelles informations sont plus récentes en examinant le MSN (numéro de séquence de message) et le numéro de séquence ANSN (Advertised Neighbor Sequence Number). Ce mécanisme est suffisant pour le fonctionnement du protocole de routage de base, mais pas pour assurer une sécurité complète. Par exemple, les deux champs ne sont que des valeurs de 16 bits qui impliquent que le débordement se produira assez fréquemment. La méthode d'utilisation d'un mécanisme du timestamp dans un protocole diffère grandement selon les horloges des entités communicantes si elles sont synchronisées ou non. Dans la suite, nous allons expliquer les deux approches :

• **Horloges synchronisées** Pour chaque message émis par un nœud, un timestamp unique lui est associé. Par conséquent, à la réception d'un message, le nœud récepteur peut comparer le timestamp du message à son heure actuelle (la valeur de son horloge). Le message est accepté lorsque la différence des deux temps n'est pas supérieure à un seuil prédéfini. Par conséquent, l'attaque par rejeu serait difficile.

• **Horloges non synchronisées** Si les horloges des entités communicantes ne sont pas synchronisées, la différence du timestamp du message et l'heure actuelle du récepteur devient sans signification. Ainsi, avant qu'un nœud destinataire puisse vérifier le timestamp,

il doit avoir une certaine connaissance du temps de l'expéditeur.

Ainsi, nous adoptons une synchronisation d'horloge des nœuds. En fait, pour tout message de contrôle généré ou transmis par un nœud, un timestamp est inclus. Ensuite, un nœud de réception vérifie la validité de timestamp en comparant le timestamp avec son heure actuelle ; la différence ne doit pas dépasser un seuil prédéfini. De plus, la sécurisation des timestamps à modifier nécessite une authentification.

4.3.2.4 Position géographique

Pour protéger le réseau contre une attaque de trou de ver dans le protocole de routage OLSR, nous utilisons la solution présentée dans [52]. Cette approche est basée sur la position géographique et nécessite le déploiement d'une infrastructure de clé publique et la synchronisation des timestamp entre tous les nœuds. Dans cette solution, un expéditeur du message de contrôle intègre sa position actuelle et son heure actuelle dans le paquet. Lors de la réception d'un message d'un voisin, les nœuds comparent leurs données géographiques aux données géographiques reçues. Si la distance est supérieure à la portée de transmission maximale, le nœud juge que le message peut être tunnelé par une attaque de trou de ver. Ensuite, le message de routage faux est détecté et ignoré.

4.4 Conclusion

Dans ce chapitre, nous avons proposé une solution pour éviter l'attaque du trou noir et les multiples attaquants de trous noirs sur le protocole de routage réactif AODV. Selon les résultats de la simulation, notre solution apporte une amélioration significative du taux de paquets délivrés avec un délai moyen de bout en bout et une surcharge de routage normalisée acceptable lorsque la mobilité des nœuds augmente. Par conséquent, nous avons conclu que notre approche proposée montre des performances supérieures à celles de l'AODV en présence d'un ou de plusieurs nœuds de trous noirs.

Dans notre deuxième proposition pour sécuriser le protocole de routage proactif OLSR, nous avons utilisé des signatures numériques pour authentifier et vérifier l'intégrité des données non mutables dans les messages de contrôle. Pour les champs mutables, nous avons utilisé le mécanisme des chaînes de hachage. De plus, notre proposition offre une protection contre les attaques de trous de ver à l'aide de la position géographique, qui peut

être obtenue à l'aide de dispositifs de système de positionnement global (GPS) intégrés au matériel de chaque nœud. Comparée aux protocoles de routage de sécurisation existants, notre solution est légère. En raison des paquets Hello les plus fréquents sur le réseau, n'utilise pas les chaînes de hachage, car nous considérons toutes les informations du paquet HELLO comme des champs non mutables.

Dans le chapitre suivant, nous avons proposé la construction d'un système de détection d'intrusion (IDS) qui combine le système d'inférence neuro adaptatif (ANFIS) et l'algorithme d'optimisation des essaims de particules (PSO).

Chapitre 5

Système de détection d'intrusion basé sur la logique floue

Sommaire

5.1 Introduction

D'après le chapitre précédent, on a constaté que les techniques de prévention des intrusions ne sont pas des solutions suffisantes pour que les MANETs éliminent les nœuds compromis. Pour cette raison, l'existence d'un système de détection d'intrusion (IDS) devient un composant essentiel de la sécurité pour les MANETs c'est pourquoi il est connu comme la deuxième ligne de défense de tout réseau.

La logique floue [59] est un outil mathématique robuste dont l'applicabilité a été prouvée dans les IDS. Par conséquent, de nombreux chercheurs ont proposé des IDS basé sur la logique floue pour les MANETs, mais la plupart des systèmes flous proposés, leurs règles floues sont basées sur les connaissances expertes humaines qui manquent d'adaptation.

Ce chapitre explore l'utilisation d'un système flou basé sur des capacités d'adaptation et d'apprentissage pour un système de détection d'intrusion dans les réseaux MANETs. À cette fin, le système ANFIS (Adaptive Neuro Fuzzy Inference System) [21] est utilisé pour automatiser le processus de production d'un système flou, puis nous optimisons notre système en utilisant l'optimisation des essaims de particules (Particle Swarm Optimization (PSO)) [25]. Cela se fait en extrayant une base de données du réseau simulé, puis nous extrayons les paramètres appropriés de la base de données, puis un processus de mappage vers ces paramètres avec une sortie cible. De plus, nous transmettons les paramètres extraits et la sortie cible à l'ANFIS pour générer le système FIS. Et enfin, nous passons notre FIS à l'algorithme PSO pour l'optimisation.

5.2 Approche proposée

De nombreux travaux rapportés dans la littérature concernant la détection des attaques de trous noirs sont fournis par l'utilisation du système d'inférence floue (FIS), qui nécessite des connaissances humaines pour choisir le nombre de fonctions d'appartenance pour chaque ensemble flou, la position et la forme de chacun. Les règles floues sont également basées sur leurs expériences. Par conséquent, ces paramètres sont difficiles à optimiser même avec un chercheur expert de haut niveau. Par conséquent, un système optimisé est requis pour générer automatiquement les règles floues et les fonctions d'appartenance. Dans ce chapitre, une approche bénéficiant de la combinaison du système d'inférence neuro adaptatif (ANFIS) et de l'optimisation des essaims de particules (PSO) [37] est proposée pour détecter l'attaque du trou noir. Dans cette approche, le PSO est appliqué pour améliorer la performance de l'ANFIS en ajustant les fonctions d'appartenance et en minimisant par la suite l'erreur. Les prévisions de l'ANFIS permettent de reconstituer le comportement futur de l'attaquant et donc de le détecter.

5.2.1 Paramètres d'entrée

Les paramètres d'entrée qui sont extraits du réseau doivent être des paramètres les plus affectés par l'existence d'une attaque de trou noir, dans notre cas serait le rapport de paquet transmis (Forward Packet Ratio (FPR)) et le numéro de séquence de destination moyen (Average Destination Sequence Number (ADSN)). Ces paramètres sont extraits du réseau par l'écoute du trafic d'une manière promiscuité. Par conséquent, chaque nœud du réseau doit créer une table de voisinage pour chacun de ses nœuds voisins directs. Dans cette table, les paramètres suivants doit être stocké :

- **Rapport de paquet transmis (FPR) :** Cette valeur de paramètre est calculée sur la base du nombre de paquets que le voisin a envoyé sur le nombre de paquets de données transférés à un voisin. La première valeur peut être calculée en comptant le numéro du paquet de données chaque fois que le voisin direct envoie une donnée en mode promiscuité. Ensuite, la deuxième valeur peut être calculée en créant un compteur et en l'incrémentant chaque fois que le nœud envoie un paquet de données à ce voisin.

$$\text{FPR} = \frac{\text{(Nombre de paquets que le voisin envoie)}}{\text{Nombre de paquets de données transmis au voisin}} \tag{5.1}$$

- **Numéro de séquence de destination moyen (ADSN) :** Dans le paquet RREP de l'AODV, la destination transmet son numéro de séquence mis à jour. Le numéro de séquence d'un nœud particulier dépend du nombre de connexions du nœud respectif sur le réseau. Un nœud ayant une valeur élevée du numéro de séquence de destination est supposé être un nœud fiable dans l'AODV. Un nœud malveillant sur le réseau affichera une valeur élevée de son numéro de séquence de destination pour faire semblant d'être une destination. Ainsi, si un nœud est un nœud de trou noir, il transmettra le numéro de séquence de destination le plus élevé et prétend être la destination. Nous pouvons donc vérifier le comportement du nœud en fonction du numéro de séquence. Pour vérifier les variations du numéro de séquence, nous calculons la moyenne de la différence de numéro de séquence de destination dans chaque intervalle de temps entre le numéro de séquence précédent dans la liste de voisins et le paquet RREP. L'intervalle de temps pour mettre à jour le numéro de séquence de destination moyenne est dès qu'un nœud transmet un paquet RREP.

Dans le cas normal, la valeur FPR doit être proche de 1, car quand un nœud source envoie un paquet de données, le nœud intermédiaire transmet ce paquet de données au nœud de destination. Dans le cas malveillant, la valeur FPR serait proche de 0, car lorsqu'un nœud source envoie un paquet de données, le nœud malveillant supprime ces données. ADSN est égal à la moyenne des numéros de séquence de destination que le nœud reçoit de son voisin chaque fois qu'il envoie un paquet RREP. Dans le cas normal, ce nombre moyen sera faible. Au contraire, quand une attaque par trou noir existe, ce nombre moyen sera élevé, car ce nœud malveillant souhaite attirer tous les paquets.

5.2.2 Optimisation de l'essaim de particules (PSO)

L'optimisation des essaims de particules est une approche heuristique de l'optimisation des fonctions de prise de décision continues et discontinues proposée par Kennedy et Eberhart en 1995 [25]. L'algorithme PSO est un algorithme de recherche basé sur la population basé sur le comportement biologique et sociologique des animaux, tels que les troupeaux d'oiseaux à la recherche de leur nourriture.

Dans la méthode PSO, chaque solution potentielle est représentée sous la forme d'une particule dans une population (appelée essaim). La position des particules est constamment modifiée dans un espace de recherche multidimensionnel jusqu'à atteindre l'équilibre ou l'état optimal ou jusqu'à ce que les restrictions de calcul soient dépassées.

Considérons un problème d'optimisation avec D variables, un essaim de N particules est initialisé de manière à ce que chaque particule soit assignée à une position arbitraire dans l'hyperespace dimensionnel D afin que la position de chaque particule corresponde à une réponse possible pour la question d'optimisation. Soit x la position d'une particule (coordonnée) et v la vitesse de vol de la particule sur un espace de solution. Chaque individu x dans l'essaim est marqué en utilisant une fonction de notation, qui obtient une valeur de remise en forme représentant la résolution du problème.

La meilleure position antérieure d'une particule est représentée par Pbest et Gbest signifie la meilleure particule parmi toutes les particules de l'essaim. Par la suite, toutes les particules qui survolent l'espace de la solution dimensionnelle D doivent suivre les règles mises à jour pour les nouvelles positions, jusqu'à ce que la position optimale globale soit trouvée. Les règles de mise à jour déterministes et stochastiques suivantes montrent comment la position et la vitesse d'une particule sont mises à jour :

$$v_i(t) = \omega v_i(t-1) + \rho_1(x_{pbest_i} - x_i(t)) + \rho_2(x_{Gbest} - x_i(t)) \tag{5.2}$$

$$x_i(t) = x_i(t-1) + v_i(t) \tag{5.3}$$

où ω représente un poids d'inertie, $\rho 1$ et $\rho 2$ sont des variables aléatoires. Les variables aléatoires sont définies comme $\rho 1 = r1C1$ et $\rho 2 = r2C2$, avec $r1$, $r2 \sim U(0,1)$, et C1 et C2 sont des constantes d'accélération positive.

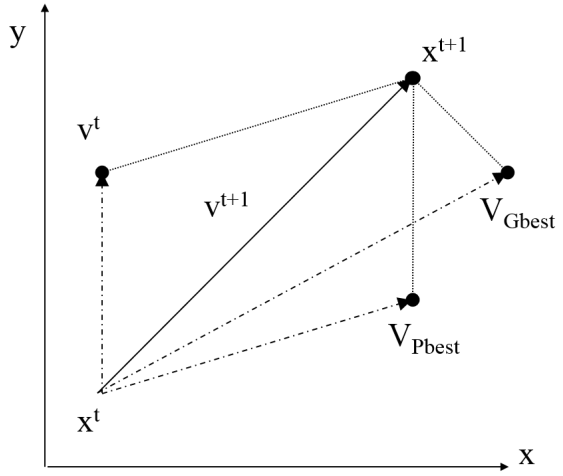


FIGURE 5.1 – Mise à jour du mécanisme de positionnement de PSO

La figure 5.1 illustre le mécanisme de recherche de l'algorithme PSO en utilisant la règle de mise à jour de la vitesse et de la position dans (6.2) et (6.3). C1 et C2 représentent les poids des termes d'accélération stochastique qui poussent une particule vers Pbest et Gbest, respectivement. Les petites valeurs des constantes d'accélération permettent à une particule de s'éloigner des régions cibles. En revanche, des valeurs élevées de cette constante provoquent un déplacement brutal des particules vers les régions cibles. Dans cette étude, les constantes C1 et C2 sont toutes deux établies à 2,0, suivant la pratique typique de [26]. Une correction appropriée de l'inertie ω dans (3) fournit un équilibre entre les explorations globales et locales, ainsi que le nombre d'itérations lors de la recherche d'une solution optimale. Une fonction de correction d'inertie "Approche de pondération par inertie (Inertia Weight Approach (IWA))" est utilisée dans cet article. Au cours de l'IWA, la masse d'inertie ω est modifiée selon l'équation suivante :

$$\omega = \omega_{max} - \frac{(\omega_{max} - \omega_{min})}{Itr_{max}} Itr \tag{5.4}$$

En (6.4), ω_{max} et ω_{min} représentent les poids d'inertie initiale et finale, le nombre maximum d'itérations est représenté par Itr_{max}, et le nombre actuel d'itérations est représenté par Itr.

5.2.3 Système d'inférence adaptative neuro-floue (ANFIS)

Le système d'inférence neuro-floue adaptative (ANFIS) a été introduit par Jang [21], faisant référence à la combinaison d'un réseau de neurones artificiels (Artificial Neural Network (ANN)) [57] et de systèmes flous [27] pour produire un outil de traitement puissant. Dans un système neuro-flou, les réseaux de neurones extraient automatiquement les règles floues des données numériques et, grâce au processus d'apprentissage, les fonctions d'appartenance sont ajustées de manière adaptative. De plus, les paramètres liés aux fonctions d'appartenance changeront en fonction du processus d'apprentissage.

La figure 5.2 montre l'architecture de l'ANFIS. ANFIS peut être décrit comme un réseau de neurones multicouches, il est composé de cinq couches, pour lesquelles chaque couche correspond à la réalisation d'une étape d'un système d'inférence floue du type Takagi Sugeno [34].

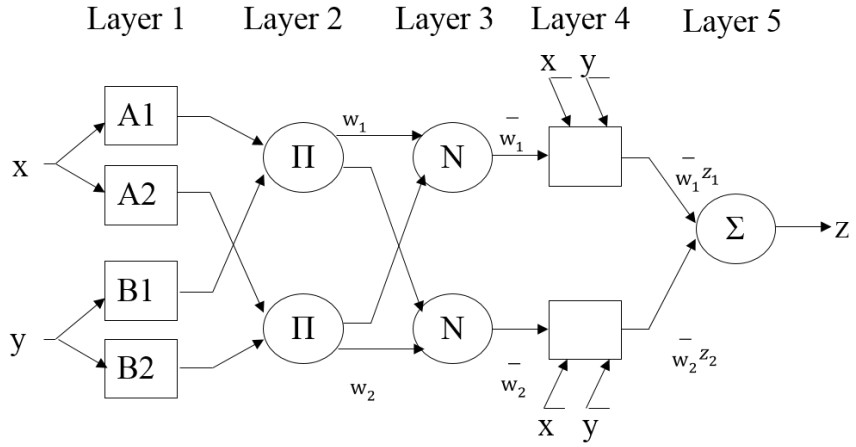


FIGURE 5.2 – Architecture de l'ANFIS

Soit O_i^j la sortie du nœud $i^{ème}$ dans la couche j.

La couche 1 contient des fonctions d'appartenance (MF) des variables d'entrée et des valeurs d'entrée de flux pour la couche suivante. Chaque nœud i de la $1^{ère}$ couche est un nœud adaptatif avec une fonction de nœud :

$$O_i^1 = \mu A_i(x), \qquad i = 1, 2 \tag{5.5}$$

$$O_i^1 = \mu B_{i-2}(y), \qquad i = 3, 4 \tag{5.6}$$

où x (ou y) est l'entrée du $i^{ème}$ nœud et A_i (ou B_{i-2}) est une étiquette linguistique associée à ce nœud. Habituellement, les fonctions d'appartenance utilisées pour A et B sont des fonctions en forme de cloche dont les montants les plus bas et les plus élevés sont respectivement 0 et 1. Cette fonction d'appartenance est présentée dans (7) :

$$O_i^1 = \frac{1}{1 + |\frac{x - r_i}{p_i}|^{2q_i}} \tag{5.7}$$

où $\{p_i, q_i, r_i\}$ sont l'ensemble de paramètres des MF. Lorsque les valeurs de ces paramètres changent, la fonction en forme de cloche varie en conséquence, présentant ainsi différentes formes de fonctions d'appartenance sur l'étiquette linguistique A_i (ou B_{i-2}).

Dans la $2^{ème}$ couche, chaque nœud $\prod$ multiplie les signaux entrants et envoie le produit sous la forme :

$$O_i^2 = w_i = \mu A_i(x) \mu B_i(y), \qquad i = 1, 2 \tag{5.8}$$

La sortie de chaque nœud indique la force de déclenchement d'une règle.

Dans la $3^{ème}$ couche, chaque nœud N calcule la proportion de la $i^{ème}$ règle de la force de déclenchement par rapport à la somme des forces de déclenchement de toutes les règles :

$$O_i^3 = \bar{w_i} = \frac{w_i}{w_1 + w_2}, \qquad i = 1, 2 \tag{5.9}$$

Les sorties de cette couche sont nommées comme forces de déclenchement normalisées.

Dans la $4^{ème}$ couche, chaque nœud calcule la contribution de la $i^{ème}$ règle aux valeurs de sortie résultantes à partir de l'inférence des règles.

$$O_i^4 = \bar{w}_i z_i = \bar{w}_i(a_i x + b_i y + c_i), \qquad i = 1, 2 \tag{5.10}$$

où w_i est la sortie de la couche précédente (couche 3) et $\{a_i, b_i, c_i\}$ sont le jeu de paramètres. Ces paramètres sont appelés paramètres conséquents.

La $5^{ème}$ couche ou la couche de sortie contient un seul nœud $\sum$, qui calcule la sortie globale en tant que somme de tous les signaux entrants :

$$O_i^5 = \sum_i \bar{w}_i z_i = \frac{\sum\limits_i w_i z_i}{\sum\limits_i w_i} \tag{5.11}$$

Dans ce chapitre, la méthode PSO a été utilisée pour aider l'ANFIS à ajuster les paramètres des fonctions d'appartenance. Le principal avantage de la technique PSO est qu'elle est moins coûteuse en calculs pour une taille de topologie de réseau donnée. Dans cette étude, les fonctions d'appartenance considérées sont de forme triangulaire.

5.2.4 Algorithme ANFIS-PSO

Dans cette section, notre système optimisé proposé est décrit étape par étape et présenté dans la figure 5.3.

Première étape (1) : Il existe deux types de mises à jour d'apprentissage : l'apprentissage en ligne et l'apprentissage par lots. Le premier type d'apprentissage met à jour le réseau après chaque exemple et l'autre type attend l'ensemble complet de l'apprentissage, puis met à jour le réseau, qui est celui choisi pour le système proposé. Pour que cela soit possible, une base de données doit être extraite du réseau. Cela se fait en créant un enregistreur de table de voisinage qui enregistre toute l'activité de la table des voisins dans tous les nœuds du réseau. Ensuite, un processus de mappage doit être mis en place, où les activités normales avec un niveau de fidélité élevé (10 dans notre cas) et les activités anormales avec un niveau de fidélité faible (0 dans notre cas). Après le processus de mappage

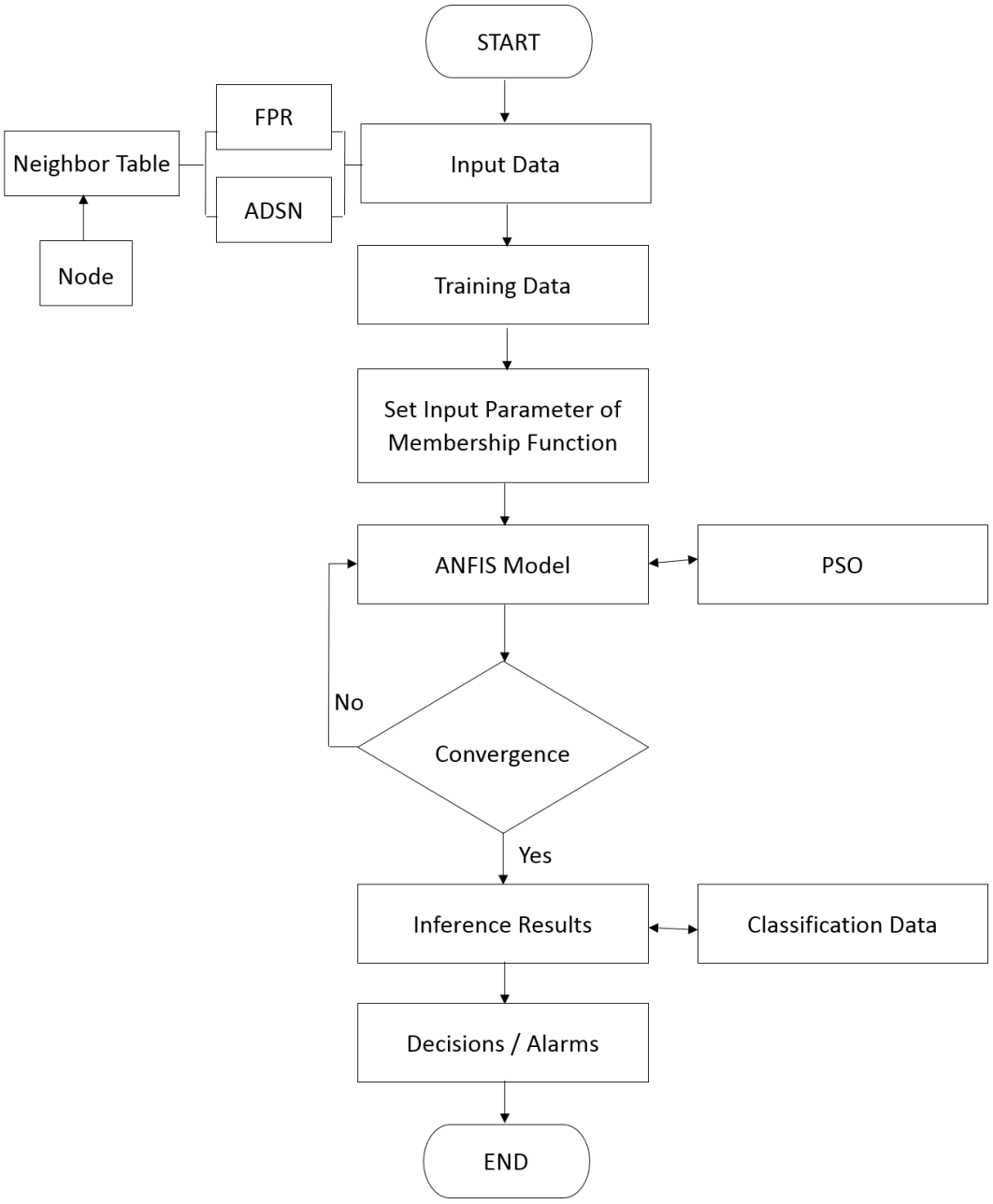


FIGURE 5.3 – Organigramme de l'approche proposée

des données, les paramètres d'entrée FPR et ADSN doivent être calculés à partir de la base de données comme expliqué précédemment, donc trois ensembles de données sont présentés : l'ensemble FPR et l'ensemble ADSN comme ensembles d'entrée et l'ensemble cible FL comme ensemble de sortie. Les données entières sont divisées en deux groupes : ensemble de données de formation (deux tiers des ensembles de données complets) et ensemble de

données de test (le reste des ensembles de données).

La deuxième étape (2) : consiste à former l'ANFIS avec l'ensemble de données de formation à partir de la mise en œuvre de l'étape précédente. Le processus de formation permet au système d'ajuster ses paramètres en tant qu'entrées / sorties. L'ANFIS est formé jusqu'à ce que le nombre de fois désigné soit atteint ou que les résultats soient obtenus avec un minimum d'erreur. Après avoir défini les données d'apprentissage, le type de fonctions d'appartenance et le nombre de fois, le système est optimisé en ajustant les paramètres des fonctions d'appartenance. Nous utilisons PSO pour former les paramètres associés aux fonctions d'appartenance du système d'inférence floue.

Troisième étape (3) : Soit N le nombre de fonctions d'appartenance, donc nous créons un vecteur de dimension N. Ce vecteur contient les paramètres de la fonction d'appartenance et sera optimisé par l'algorithme PSO. La fonction de remise en forme est définie comme l'erreur quadratique moyenne (MSE).

Quatrième étape (4) : Dans cette étape, nous définissons les paramètres associés à l'algorithme PSO, comme indiqué dans le tableau 5.1.

Paramètre	**Valeur**
Nombre de particules	25
Nombre d'itérations	2000
Accélération cognitive C1	2.0
Accélération sociale C2	2.0
Poids d'inertie initial ω_{min}	0.9
Poids d'inertie final ω_{max}	0.4

TABLE 5.1 – Paramètres de l'algorithme PSO

Les paramètres sont initialisés de manière aléatoire lors de la première étape et sont ensuite mis à jour en utilisant l'algorithme PSO. A chaque itération, l'un des paramètres de la fonction d'appartenance est mis à jour. Par exemple, dans la première itération, pi est mis à jour, puis dans la deuxième itération qi est mis à jour et après la mise à jour de tous les paramètres, à nouveau la première mise à jour des paramètres est considérée et ainsi de suite. Ces paramètres sont regroupés dans un vecteur qui est mis à jour à chaque itération. L'algorithme PSO est utilisé pour optimiser les paramètres de la fonction d'appartenance. Il est décrit ci-dessous :

a) Initialiser les positions et les vitesses de la population. Pour chaque particule, les

vecteurs de position et de vitesse sont initialisés aléatoirement avec la même taille que celle présentée par la taille du problème ;

b) Évaluer la capacité de chaque particule (Pbest). Si la valeur est meilleure que la valeur actuelle de la particule individuelle, Pbest réinitialise la position actuelle de la particule et met à jour la valeur individuelle. Si le meilleur de toutes les particules de valeurs individuelles est mieux que la valeur globale du Gbest actuel, réinitialiser l'emplacement des meilleures particules ;

c) Mesurer la fonction fitness de chaque particule (Pbest) et stocker les particules ayant la meilleure valeur fitness (Gbest) ;

d) Changer la vitesse en fonction de la position Pbest et Gbest ;

e) Mettre à jour les particules ;

f) Arrêtez si la condition est vérifiée. Si le nombre actuel d'itérations atteint le nombre maximal par défaut ou si le résultat atteint un seuil d'erreur minimal, arrêtez l'itération et collectez la meilleure solution.

Cinquième étape (5) : Extraire la sortie de l'ANFIS en utilisant les paramètres trouvés par l'algorithme PSO.

Sixième étape (6) : Le résultat final correspond à la prédiction de notre approche.

5.3 Évaluation des performances

Dans cette section, nous décrivons les simulateurs utilisés, les paramètres de simulation et les mesures de performance.

5.3.1 Simulateurs utilisés

Dans ce chapitre, nous avons utilisé trois simulateurs : Network Simulator NS-2 (v-2.35) [18], utilisé dans la simulation du réseau mobile MANET, la simulation de l'attaque du trou noir et l'IDS optimisé contre les nœuds de trous noirs. Le deuxième simulateur est MATLAB [46], utilisé dans l'étape ANFIS, et l'étape PSO dans notre algorithme proposé, le dernier simulateur utilisé est le QTFUZZYLITE [51], qui sert à encoder le système d'inférence flou en code C++ afin de l'ajouter dans notre IDS en NS2.

5.3.2 Paramètres de simulation

Dans ces simulations, nous considérons que 50 nœuds mobiles se déplacent à l'intérieur d'un champ carré de 800 x 800 m. Une paire à vingt paires ont été choisies au hasard pour la communication de données, chacune envoyant 512 octets par seconde. Tous les nœuds ont été déplacés dans un modèle de points aléatoires, avec des vitesses aléatoires comprises entre 0 et 10 m / s. De plus, le temps de pause entre les mouvements est de 5 secondes avec 200 secondes de temps simulé. Pour le nœud malveillant est également distribué de manière aléatoire. Tous les paramètres de simulation sont résumés dans le tableau 5.2. Chaque point de données représente une moyenne de vingt exécutions différentes.

Paramètre	**Valeur**
Taille du réseau	800x800 m
Nombre des nœuds	50
Temps de simulation	200s
Portée de transmission	50m
Modèle de mobilité	Random way point
Taux de transmission	0.25
Taille de paquets	512 Bytes
Protocole de routage	AODV / AODV-with attack / IDS-AODV
mobilité des nœuds	0-10 m/s
Nombre d'attaquants du trou noir	1
Nombre de connections	1 to 10
Type de trafic	UDP–CBR
Temps de pause	5s

Table 5.2 – Les paramètres de simulations

Nous exécutons le réseau dans trois situations.

— Situation 1 : nous simulons le réseau sans la présence d'une attaque par trou noir.
— Situation 2 : nous simulons le réseau en présence d'une attaque par trou noir et sans présence d'IDS.
— Situation 3 : nous simulons le réseau sous l'attaque du trou noir et la présence de notre système de détection d'intrusion proposé.

5.3.3 Métriques utilisés pour l'évaluation

Afin d'évaluer la performance de notre protocole, nous avons utilisé les métriques suivantes :

- **Taux de paquets délivrés (PDR).**
- **Délai moyen de bout en bout.**
- **Surcharge de routage normalisée.**

De plus, deux paramètres de performance ont été utilisés pour évaluer les performances du système proposé en cas d'attaque par un trou noir, le taux de détection (DR) et le taux de fausse alarme (FAR). Ils peuvent être calculés à l'aide de la matrice de confusion du tableau 5.3 et définis comme suit :

$$DR = TP/(TP + FN) \times 100 \tag{5.12}$$

$$FAR = FP/(TN + FP) \times 100 \tag{5.13}$$

Avec :

TP = Enregistrement de connexion d'attaque classé comme attaque (TP).
FP = Enregistrement de connexion d'attaque classé comme normal (FP).
TN = Enregistrement de connexion normal classé comme normal (TN).
FN = Enregistrement de connexion normale classée comme attaque (FN).

5.4 Résultats expérimentaux et discussion

Les performances de notre IDS proposé sont évaluées et comparées avec le système de détection d'intrusion optimisé qui utilise l'ANFIS et les algorithmes génétiques (GA) pour l'optimisation proposé dans [1]. La simulation fonctionnait sur un ordinateur portable avec un processeur Core i5 et 4 Go de RAM avec Linux Ubuntu version 12.04 en tant que système d'exploitation. Chaque exécution est exécutée avec des paires de sources et de destinations aléatoires d'une à vingt paires, chacune simulant le réseau dans quatre

Matrice de confusion (**Métriques standard**)		**Étiquette de connexion prédite**	
		Normal	**Intrusions (Attaque du trou noir)**
Etiquette de connexion réelle	**Normal**	Vrai Négatif (TN)	Fausse Alarme (FP)
	Intrusions (attaque de trou noir)	Faux négatifs (FN)	Attaques correctement détectées (TP)

TABLE 5.3 – Matrice de confusion pour l'évaluation des intrusions (attaques)

situations différentes (AODV de base, avec attaque du trou noir, avec notre IDS proposé et IDS optimisé proposé dans [1]).

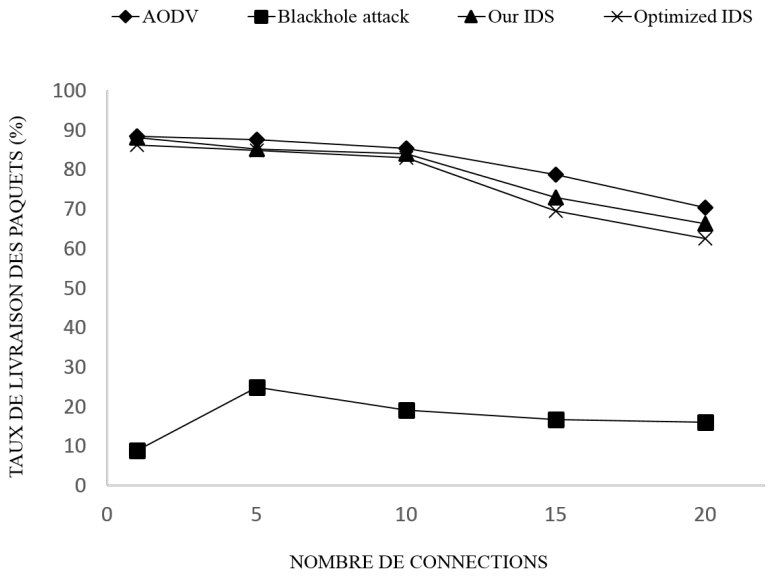


FIGURE 5.4 – Taux de paquets délivrés vs. Nombre de connexions

La figure 5.4 montre la variation du taux de livraison des paquets avec la modification du numéro de connexion. À mesure que le nombre de connexions augmente, la perte de paquets augmente en raison de la congestion ; par conséquent, le diagramme PDR pour l'AODV standard commence à diminuer au fur et à mesure que le nombre de sources augmente. Il est clair à partir de la figure que le PDR de notre IDS proposé est supérieur

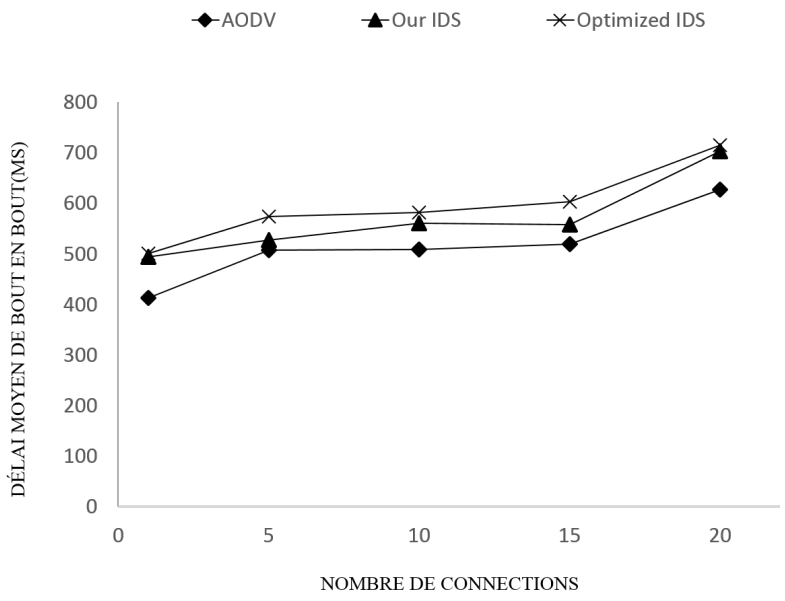


FIGURE 5.5 – Délai moyen de bout en bout vs. Nombre de connexions

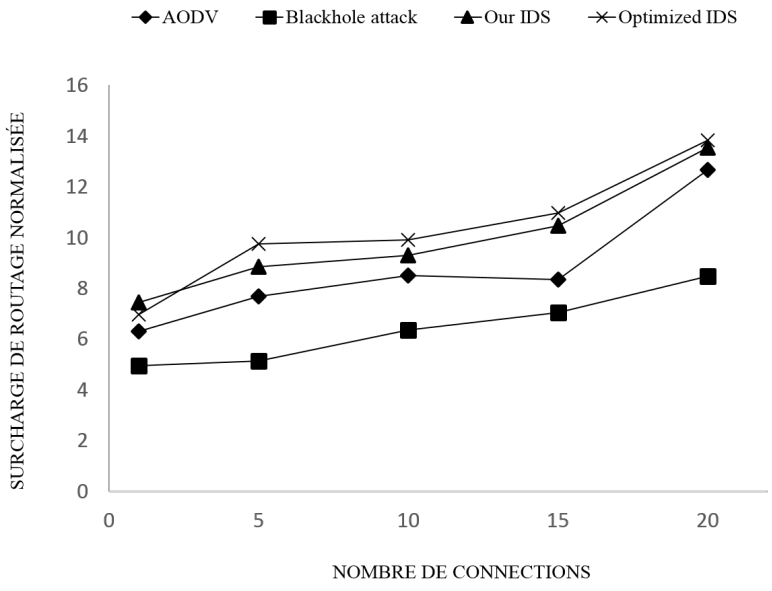


FIGURE 5.6 – Surcharge de routage normalisée vs. Nombre de connexions

à celui de l'AODV de base sous l'attaque de trou noir ou à l'IDS optimisé. La figure 5.5 illustre le délai moyen de bout en bout. Tous les protocoles ont un délai moyen de bout en bout plus élevé avec un nombre élevé de connexions. Principalement parce que les itinéraires fréquents tombent en panne à cause de la mort des nœuds intermédiaires et de la mobilité. En outre, nous observons que notre IDS et l'IDS optimisé utilisant ANFIS + GA sous une attaque par trou noir sont légèrement augmentés dans le délai moyen de bout en bout, par rapport à l'AODV standard. Cela est dû au temps d'attente supplémentaire dans chaque nœud intermédiaire avant l'envoi du paquet de réponse. La surcharge de routage normalisée est illustrée dans la figure 5.6 tout en faisant varier le nombre de connexions. Comme nous pouvons le voir, la surcharge de routage normalisée de notre système IDS et l'IDS basé sur ANFIS et GA sont légèrement supérieurs à ceux de l'AODV standard en raison du processus supplémentaire nécessaire pour éviter la sélection de nœuds malveillants. En outre, l'utilisation des messages d'alarme afin d'informer les autres nœuds de l'attaque du trou noir. La NRO dans le cas de l'AODV sous attaque par trou noir est inférieure aux autres situations, car le nœud malveillant manipule le réseau pour penser qu'il délivre les paquets de données alors que ce n'est pas le cas.

Dans le cadre de l'évaluation de la mesure de classification de notre IDS et de l'IDS optimisé proposé dans [1], le taux de détection et le taux de fausse alarme ont été réalisés dans le tableau 5.4. Les résultats montrent que notre IDS proposé présente les meilleures performances avec un taux de détection élevé et un faible taux de fausses alarmes lorsque nous faisons varier le nombre de connexions. En conséquence, il est prouvé que l'utilisation de notre IDS proposé fournit un IDS très robuste comparé à l'IDS optimisé qui utilise ANFIS et GA.

Nombre de connexions	Notre IDS		IDS optimisé	
	Taux de détection (DR)	Taux de fausse alarme (FAR)	Taux de détection (DR)	Taux de fausse alarme (FAR)
1	99.83%	0.76%	99.75%	0.85%
5	99.81%	0.99%	99.82%	1.23%
10	99.34%	1.33%	99.30%	1.29%
15	98.30%	1.77%	98.21%	1.93%
20	98.35%	2.10%	98.11%	2.76%

TABLE 5.4 – Taux de détection et taux de fausses alarmes

5.5 Conclusion

Dans ce chapitre, nous avons proposé une nouvelle méthode pour détecter et prévenir l'effet d'une attaque de trou noir. Dans notre nouvelle méthode, nous initialisons le FIS par l'approche ANFIS, puis nous optimisons le système initialisé en utilisant l'algorithme PSO. L'efficacité de cette approche est évaluée en la comparant à un IDS optimisé proposé par un autre auteur utilisant l'approche ANFIS associée à GA. Selon les résultats expérimentaux, notre approche a une bonne efficacité de détection contre les attaques de trous noirs, mais avec une légère augmentation de la surcharge de routage normalisée.

Conclusion générale et perspectives

Les réseaux mobiles ad hoc (MANETs) ont attiré beaucoup d'attention dans le milieu de la recherche au cours de ces dernières années. Cela s'explique par les progrès récents de l'informatique mobile et de la technologie sans fil et par les applications potentielles qui pourraient être réalisées à l'aide de ces réseaux, allant des applications civiles et commerciales simples aux services d'urgence et aux opérations sur le champ de bataille complexes à haut risque. Bien que les nœuds MANET partagent de nombreuses propriétés avec leurs homologues sur un réseau filaire traditionnel, ils présentent certains défis uniques liés à la nature inhérente du support de communication sans fil, de la fonction distribuée de leur mécanisme d'accès au support et des fréquents changements topologiques associés à leur mobilité. En raison des caractéristiques uniques des MANETs, ces réseaux sont extrêmement vulnérables aux attaques par rapport aux réseaux filaires ou aux réseaux sans fil basés sur l'infrastructure.

Au cours de ces dernières années, beaucoup d'efforts de recherche ont été consacrés à trouver des solutions liés à la sécurité des MANETs. Notamment, les attaques sur les protocoles de routage qu'ont fait l'objet d'une attention considérable. Cette thèse traite le problème de la sécurité des communications entre les nœuds. Plus précisément, nos travaux permettent de sécuriser les protocoles de routage des réseaux mobiles ad hoc. Puisque, le routage est une fonctionnalité fondamentale pour le bon fonctionnement de tout réseau.

Pour atteindre cet objectif nous avons commencé par une étude sur le protocole de routage AODV sous l'influence des attaques. Nous avons simulé ce protocole en utilisant NS2 (Network Simulator), afin d'examiner l'impact de la densité, la mobilité, le nombre des connexions et le nombre des nœuds malveillants dans le réseau sur les performances du routage selon les critères de taux de paquets délivrés, délai moyen de bout en bout et le débit. De cette étude, nous avons constaté que le taux de paquets délivrés diminue dans le réseau avec l'attaque du trou noir. Aussi, nous avons observé que le délai moyen de bout en bout est plus élevé dans l'attaque du trou noir. Et le débit du réseau est faible avec l'attaque des trous noirs par rapport aux autres attaques. Cela nous a permis de déduire que l'attaque du trou noir a un effet significatif sur les performances du réseau.

Pour aborder la problématique (sécurité contre l'attaque du trou noir), nous avons divisé notre étude en trois grands axes que nous avons traités séparément et conjointement. Nous

avons commencé par une modification dans le mécanisme de routage d'AODV pour la défense d'un ou plusieurs attaques du trou noir. Ensuite nous avons proposé une solution qui assure l'authentification et l'intégrité du trafic de contrôle pour le protocole de routage d'état de lien optimisé (OLSR). Cette dernière solution n'empêche pas toutes les attaques, comme l'attaque du trou de ver car cette attaque ne requiert aucune modification des paquets de routage. Pour remédier ce problème, nous avons proposé un système de détection d'intrusion basée sur la logique floue contre les attaques du trou noir comme deuxième ligne de défense.

Dans notre proposition pour sécuriser le protocole de routage AODV, nous avons modifié le mécanisme du protocole afin d'éviter l'attaque du trou noir par un seul ou plusieurs attaquants. Notre solution est allégée par rapport aux autres solutions proposées, parce que le nœud intermédiaire transmet seulement le valide paquet de réponse d'itinéraire au nœud suivant. Mais, notre solution reste faible contre les nœuds compromis.

Dans le deuxième axe de notre travail, nous avons sécurisé le protocole proactif de routage OLSR en utilisent des signatures numériques pour authentifier et vérifier l'intégrité des données non mutables du paquet de contrôle. Pour les champs mutables, nous avons utilisé le mécanisme des chaînes de hachage. En outre, cette proposition offre également une protection contre l'attaque de trou de ver à l'aide de la position géographique qui peut être obtenue en utilisant des dispositifs GPS (Global Positioning System) intégrés dans le matériel de chaque nœud.

En comparant notre approche proposée avec des protocoles de routage sécurisé existants, nous trouvons que notre solution est allégée, puisque il n'utilise pas les chaines de hachages dans les paquets Hello qui sont les plus fréquents dans le réseau.

Cependant, cette solution cryptographique de signature numérique ne permet pas d'empêcher toute les attaques qui visent le protocole de routage OLSR, comme l'attaque de trou de ver car cette attaque ne requiert aucune modification des paquets de routage.

De plus, notre approche suppose que les nœuds de réseaux coopèrent entre eux et qu'ils ne sont pas compromis, c'est-à-dire qu'ils ne sont pas égoïstes et ils n'ont pas pour but le dysfonctionnement du réseau. Pour lutter contre ce type de nœud, il est indispensable d'utiliser un système de détection d'intrusion comme deuxième ligne de défense.

Dans le troisième axe de notre travail, nous avons présenté un système de détection d'intrusion basée sur la logique floue contre les attaques du trou noir. Pour ce faire, le

système ANFIS (Adaptive Neuro Fuzzy Inference System) est utilisé pour automatiser le processus de production d'un système flou, puis nous optimisons notre système en utilisant l'optimisation des essaims de particules (Particle Swarm Optimization (PSO)). Cela se fait en extrayant une base de données du réseau simulé, puis nous extrayons les paramètres appropriés de la base de données, puis un processus de mappage vers ces paramètres avec une sortie cible. De plus, nous transmettons les paramètres extraits et la sortie cible à l'ANFIS pour générer le système FIS. Et enfin, nous passons notre FIS à l'algorithme PSO pour l'optimisation.

Dans la littérature, plusieurs travaux sur les IDS dans les réseaux MANETs ont été proposés qui utilisent les systèmes d'inférence floue (FIS), cependant ces solutions nécessitent des connaissances humaines pour choisir le nombre de fonctions d'appartenance pour chaque ensemble flou, la position et la forme de chacun. Les règles floues sont également basées sur leurs expériences. Contrairement à notre solution proposée qui génère automatiquement les règles floues et les fonctions d'appartenance.

Ces différentes contributions donnent lieu à plusieurs travaux de recherche futurs, tels que :

— La première phase concerne l'analyse d'autres comportements malveillants que l'étude effectuée dans le chapitre 3, notamment l'attaque de trous de ver sous les protocoles proactifs et réactifs dans les réseaux MANETs, en utilisant des différents paramètres de simulation, et nous envisageons de concevoir une solution pour prévenir ces attaques.
— Comme deuxième objectif, nous souhaitons améliorer l'approche proposée dans le chapitre 4, par l'envoie des paquets d'alarme depuis les nœuds qui détectent l'attaquant afin d'informer les autres nœuds du réseau quand il y a une attaque du trou noir pour l'isoler.
— Ensuite, nous envisageons également de se focaliser sur la gestion des clés dans l'approche proposée dans le chapitre 5, en se basent sur une architecture en cluster d'une façon que seulement les nœuds légitimes peuvent obtenir une paire de clés (publique / privée).
— De plus, nous souhaitons d'établir plus de simulations dans le chapitre 5, en implémentent l'ensemble des extensions cryptographiques proposés sous le simulateur Network Simulator NS-2 afin de mesurer l'impact de ces extensions sur le protocole de routage proactif OLSR.
— En dernier, nous nous concentrons sur le prolongement de notre IDS proposé dans le

chapitre 6 pour détecter plus d'attaques que l'attaque du trou noir dans un réseau ad hoc mobile.

Annexe A

Protocole de routage ad hoc

Le protocole de routage est nécessaire lorsqu'un réseau souhaite transmettre une information d'un nœud à un autre. La tâche d'un protocole de routage implique deux phases : premièrement, trouver le meilleur chemin optimal et deuxièmement, échanger les informations avec succès entre les nœuds du réseau en utilisant le chemin optimal.

Le routage dans les réseaux mobiles ad hoc est difficile en raison de ses caractéristiques dynamiques (changement de la topologie du réseau augmente la complexité du routage entre les nœuds mobiles). Ce qui a conduit aux chercheurs de proposer des nombreux protocoles de routage pour MANET, ces protocoles de routage trouvent un itinéraire pour acheminer le paquet depuis la source vers la destination d'une façon correcte. Par conséquent, les études sur divers aspects des protocoles de routage de MANET sont un domaine de recherche actif depuis de nombreuses années.

Les protocoles de routage conçus pour les réseaux mobiles ad hoc doivent s'adapter rapidement aux changements fréquents et imprévisibles de la topologie. Les protocoles de routage existant pour MANET sont classés en fonction de différents critères tels que le moment et la manière dont les informations de routage sont échangées etc. Fondamentalement, les protocoles de routage ad hoc peuvent être classés en trois types selon la structure du réseau à savoir :

- ✓ Routage hiérarchique,
- ✓ Routage basé sur positionnement géographique,
- ✓ Routage à plat.

Dans le routage hiérarchique, les nœuds du réseau sont organisés d'une manière dynamique en partitions appelées clusters, puis les clusters sont à nouveau regroupés en une partition plus grande appelée super clusters. Ceci est bien adapté aux grands réseaux. Dans le cas du routage assisté par positionnement géographique, le protocole utilise des informations géographiques pour spécifier la destination plutôt que l'adresse de nœud logique.

Dans le protocole de routage à plat, tous les nœuds du réseau sont égaux, c'est-à-dire que chaque nœud joue le même rôle dans le réseau. Chaque nœud suit le même algorithme de routage que n'importe quel autre nœud du réseau. Le routage à plat est simple et efficace pour les petits réseaux. Les protocoles de routage à plat sont classés en deux catégories principales basées sur le mécanisme de mise à jour des informations de routage, à savoir :

- ✓ Protocoles proactifs ou protocoles pilotés par table,
- ✓ Protocoles réactifs ou protocoles de routage à la demande.

C'est la classification qui nous intéresse et qu'on maintient pour la suite.

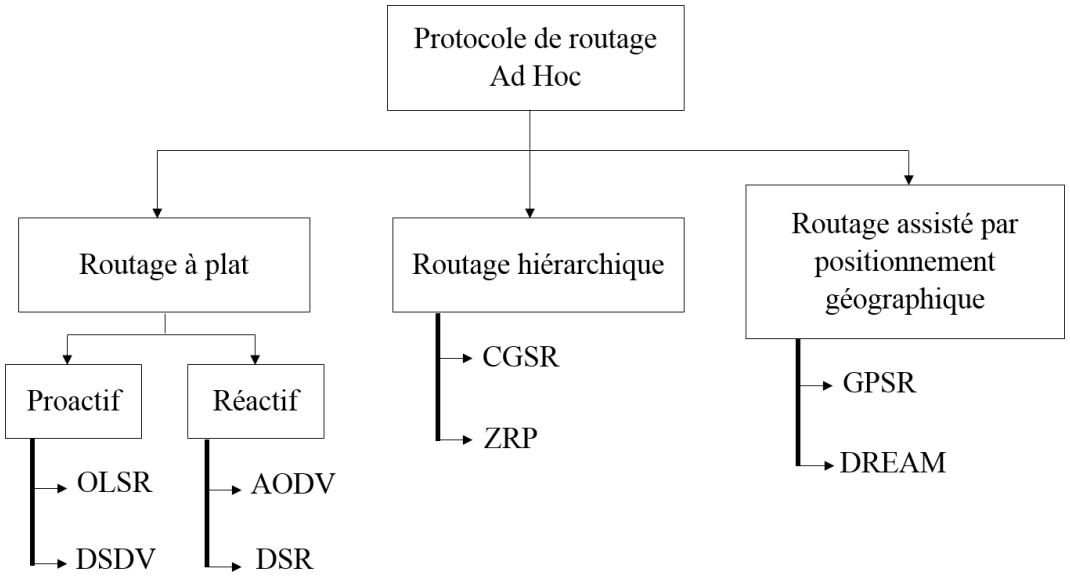


FIGURE A.1 – Illustre la classification des protocoles de routage dans les MANETs

A.1 Protocoles de routage proactifs

Les protocoles de routage proactif maintiennent des informations de routage cohérentes et à jour entre les nœuds source et destination du réseau en propageant les informations de routage de manière périodique. Ces protocoles de routage sont parfois appelés protocole de routage piloté par table parce que chaque nœud du réseau conserve les informations de routage dans sa table de routage. Parfois, on parle également de routage pré-calculé, car les itinéraires vers toutes les destinations sont calculés à l'avance.

La principale caractéristique des approches proactives est que chaque nœud du réseau

maintient à tout moment un itinéraire vers tous les autres nœuds du réseau. La création et la maintenance de l'itinéraire sont réalisées grâce à une combinaison de mises à jour périodiques et de mises à jour déclenchées par des événements. Les mises à jour périodiques des informations de routage sont effectuées indépendamment des caractéristiques de mobilité et de trafic du réseau. D'un autre côté, chaque fois qu'un événement comme l'ajout ou la suppression d'un nœud dans le réseau entraîne des mises à jour déclenchées par un événement. Les approches proactives ont l'avantage que les itinéraires sont disponibles au moment où ils sont nécessaires. Donc, il n'y a pas de latence. Mais le protocole de routage proactif ne convient pas aux grands réseaux ou aux réseaux à forte mobilité, car il augmente considérablement la surcharge, ce qui entraîne une consommation de la bande passante.

Le protocole de routage proactif inclut le protocole le protocole de routage d'état de lien optimisé (OLSR) et le protocole vecteur de distance séquencé par destination (DSDV).

a. Le protocole de routage d'état de lien optimisé (OLSR)

Le protocole OLSR (Optimized Link State Routing Protocol) [19] est un algorithme proactif d'état des liens pour les réseaux mobiles ad hoc. Le protocole OLSR est également appelé en tant que protocole piloté par table dans lequel chaque nœud stocke et met à jour de manière permanente les routes vers toutes les destinations de sa table de routage. Par conséquent, le principal avantage de la nature proactive est d'avoir tous les itinéraires immédiatement disponibles en cas de besoin.

Le trafic de contrôle dans le protocole OLSR est échangé par le biais de deux types de messages : les messages HELLO et les messages de contrôle de topologie (Topology Control (TC)). Les messages Hello sont utilisés pour la détection des voisins et le calcul des relais multipoints (MPR), et pour les déclarations de la topologie, le protocole est basé sur les messages TC. Il y a également un message de déclaration d'interface multiple (MID) qui est utilisé pour informer les autres nœuds que le nœud d'annonce peut avoir plusieurs adresses d'interface OLSR. Un autre type de messages en OLSR est HNA (Host and Network Association), qui est utilisé pour déclarer les informations sur l'hôte et le réseau associé. Grâce aux messages HNA, OLSR offre la possibilité de routage vers les adresses externes.

L'optimisation de base dans le protocole OLSR est l'utilisation de relais multipoints (MPR) pour diffuser ses messages dans le réseau. Seuls les MPR d'un nœud retransmettent ses messages de diffusion (TC, MID, HNA) sur l'ensemble du réseau, au lieu de permettre

à chaque nœud de les diffuser, comme dans la A.2(a). Pour cette raison, la surcharge de routage pour OLSR est réduite. La figure A.2(b) montre un nœud S avec ses voisins directs et ses voisins à deux sauts. Comme illustré dans la figure, le nœud S doit choisir seulement quatre nœuds parmi ses voisins directs pour communiquer avec tous les nœuds voisins dans deux sauts.

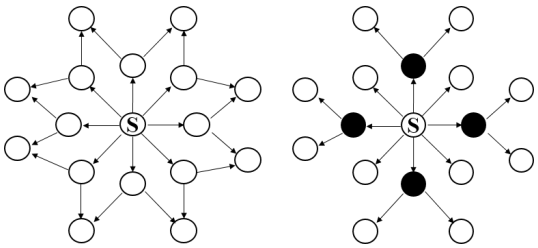


FIGURE A.2 – (a) Inondation classique (b) Inondation MPR

b. Le protocole vecteur de distance séquencé par destination (DSDV)

Le protocole DSDV (Destination Sequenced Distance Vector) [48] est un protocole de routage proactif basé sur l'algorithme distribué de Bellman Ford [12]. Dans ce protocole de routage, chaque nœud mobile maintient une table comportant du voisin du saut suivant et de la distance par rapport à la destination en termes de nombre de sauts. Il utilise des numéros de séquence pour les nœuds de destination afin de déterminer la «fraîcheur» d'un itinéraire particulier, afin d'éviter toute boucle de routage de courte ou de longue durée. Si deux itinéraires ont le même numéro de séquence, celui avec la plus petite métrique de distance est annoncé. Le numéro de séquence est incrémenté à chaque mise à jour envoyée par l'hôte. Tous les hôtes diffusent périodiquement leurs tables aux nœuds voisins afin de conserver une vue actualisée du réseau. Les tables peuvent être mises à jour de deux manières : soit progressivement, soit par un vidage complet. Une mise à jour incrémentielle est effectuée lorsque le nœud n'observe aucun changement majeur dans la topologie du réseau. Un vidage complet est effectué lorsque la topologie du réseau change de manière significative ou lorsqu'une mise à jour incrémentielle nécessite plus d'une NPDU (unité de données par paquets réseau). Considérons la topologie de réseau illustrée à la figure A.3. Comme indiqué dans le tableau A.1, chaque nœud de la table de routage pour ce réseau conserve une route vers tous les autres nœuds du réseau pendant la phase d'établissement de la route.

Chaque fois qu'une liaison est interrompue sur le réseau, le nœud d'extrémité du lien rompu propage un message de mise à jour de la table de routage avec le poids du lien rompu affecté à l'infini. Ce message est diffusé par chaque nœud à ses voisins. Un lien

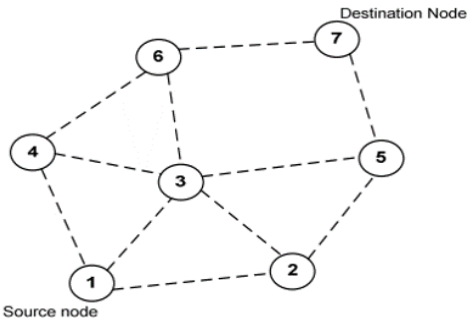


FIGURE A.3 – Graphe de topologie du réseau

Destination	**saut suivant**	**métrique**	**numéro de séquence**
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

TABLE A.1 – Table de routage pour le nœud 1

brisé est désigné par un numéro de séquence impair et un lien ordinaire par un numéro de séquence pair. Lorsque le nœud 1 veut envoyer des données au nœud 7, il vérifie le prochain saut du voisin pour le nœud 7, qui est 2, et lui transmet le paquet de données. La figure A.4 illustre le cas où le nœud 7 se déplace hors de la plage des nœuds 6 et 5. Ainsi, les liens 6-7 et 7-5 sont rompus et la table de routage de 1 est maintenant réorganisée comme indiqué dans le tableau A.2. Lorsque le nœud 4 entend la demande de mise à jour du nœud 7 avec un numéro de séquence supérieur, il diffuse ces informations vers tous les nœuds. Cela atteint finalement le nœud 1, qui modifie le saut suivant, la métrique et l'entrée du numéro de séquence dans la table de routage pour le nœud 7.

DSDV garantit des itinéraires sans boucle vers chaque destination et trouve également le chemin optimal. Il utilise un délai de stabilisation moyen pour éviter les mises à jour fréquentes de la table de routage et les fluctuations causées par deux annonces de routage similaires, dans un ordre incorrect des numéros de séquence.

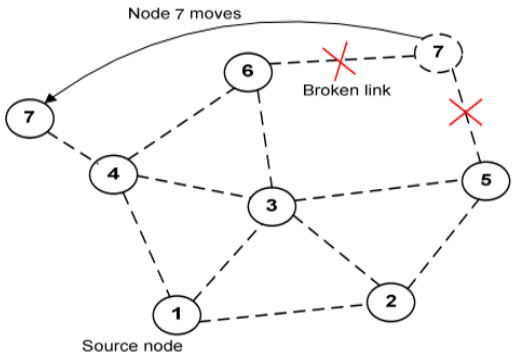


FIGURE A.4 – Graphe de topologie du réseau lorsque le nœud 7 se déplace

Destination	saut suivant	métrique	numéro de séquence
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	4	2	S98_7

TABLE A.2 – Table de routage modifiée pour le nœud 1

A.2 Protocoles de routage réactifs

Les techniques de routage réactif sont également appelées routage à la demande ou protocole de routage initié par la source. Dans ces protocoles de routage, les informations de routage ne sont pas gérées par les nœuds s'il n'y a pas de communication entre les nœuds source et cible. Ces protocoles sont parfois appelés à la demande car les itinéraires ne sont calculés que sur la base de la demande. Lorsqu'un nœud source souhaite envoyer des données à la destination, il vérifie d'abord sa table de routage pour déterminer s'il dispose d'un itinéraire. Si aucune route n'existe, il exécute une procédure de découverte d'itinéraire pour trouver le chemin d'accès à la destination. Par conséquent, la découverte d'itinéraire devient à la demande. Dans le protocole de routage réactif, il n'y aura pas de mise à jour périodique de la route comme dans le protocole de routage proactif. Ainsi, ils n'ont pas besoin d'utiliser les ressources pour maintenir un lien entre eux.

Le routage réactif est parfois appelé routage initié par la source car il crée les routes uniquement lorsque le nœud source le souhaite. Une fois qu'une route a été établie, elle

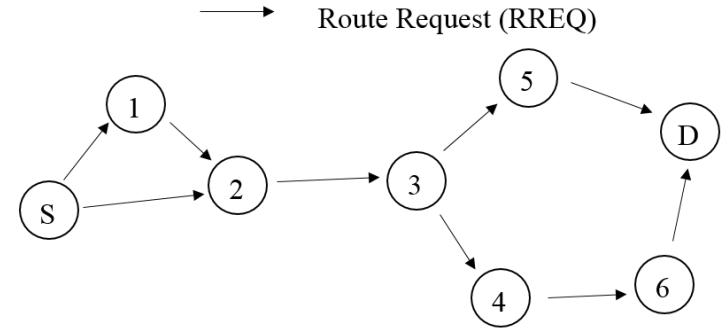
est maintenue par la procédure de maintenance de la route jusqu'à ce que le nœud de destination ne soit plus joignable le long de chaque chemin ou jusqu'à ce que la route ne soit plus désirée. Les protocoles de routage réactifs sont généralement considérés comme efficaces, car la découverte de la route est moins fréquente que le transfert de données, ce qui réduit la surcharge. Le trafic réseau provoqué par l'étape de découverte d'itinéraire est faible comparé à la largeur de bande de communication totale. Cela rend les protocoles de routage à la demande plus adaptés aux grands réseaux à faible trafic et à faible mobilité. Par conséquent, ils ont une surcharge de découverte de route plus réduite. Ainsi, cela économise de l'énergie et de la bande passante pendant l'inactivité. L'inconvénient du protocole de routage réactif est qu'il introduit une latence.

Des exemples de protocoles de routage réactifs sont le protocole routage Ad hoc On Demand Distance Vector (AODV), le routage à source dynamique (DSR).

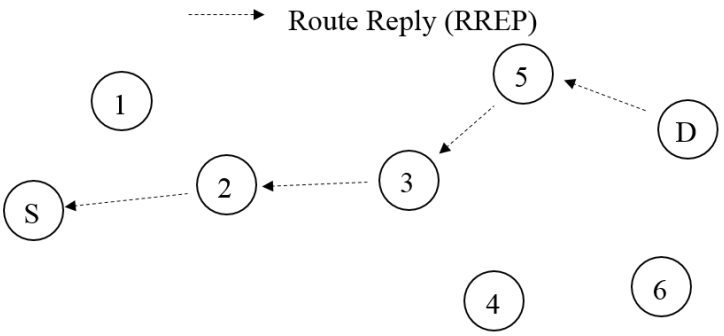
a. Le protocole Ad hoc On Demand Distance Vector (AODV)

Le protocole de routage AODV [47] est basé sur les algorithmes de DSDV et DSR (Dynamic Source Routing) [22]. Il s'agit d'un protocole réactif, puisque les routes ont été découvertes au moment où un nœud source doit envoyer des paquets de données à un nœud de destination pour lequel il n'a pas de route en cache.

AODV a deux fonctionnalités principales : (1) la découverte de la route (voir Fig. A.5) et (2) la maintenance de la route (voir Fig. A.6). L'approche de base de ce protocole pendant la phase de découverte de la route est d'établir un itinéraire en diffusant les paquets Route REQuest (RREQ) sur le réseau. Lorsque le nœud voisin reçoit le paquet RREQ, il vérifie d'abord s'il s'agit du nœud de destination pour ce paquet, et s'il est le cas, le nœud renvoie un paquet RREP (Route REPly). Si ce n'est pas le nœud de destination, il vérifie dans sa table de routage s'il dispose d'une route suffisamment récente vers le nœud de destination. Sinon, il retransmit le paquet RREQ en l'inondant à ses voisins. De plus, s'il dispose d'une route vers la destination, il peut renvoyer le RREP au nœud source en inversant les informations de route stockées dans le paquet RREQ.



(a) Inondation du paquet RREQ



(b) Unicasting du paquet RREP

FIGURE A.5 – Processus de découverte d'itinéraire de l'AODV

Dans la phase de maintenance de la route, si un nœud détecte un lien rompu, il envoie un message Route ERRor (RERR) au nœud source l'informant que le lien est rompu. Ensuite, le nœud source essaie un autre chemin disponible ou relance à nouveau le processus de découverte de la route. Un lien est rompu lorsqu'un nœud intermédiaire impliqué dans le processus de transmission de paquets sort de la plage de transmission de son voisin en amont.

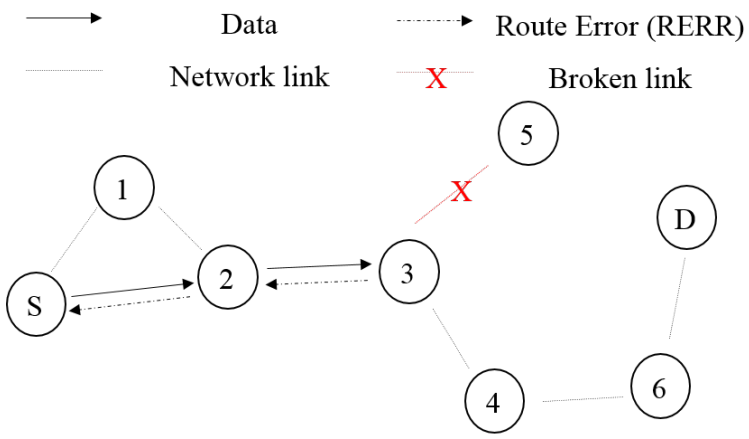


FIGURE A.6 – Processus de maintenance de route du protocole AODV

b. Le protocole Dynamic Source Routing

Le protocole "Routage à Source Dynamique" (DSR : Dynamic Source Routing) [22], implémente le « routage source » à la demande pour transmettre les paquets de données. Dans la technique de routage source, le chemin parcouru par le paquet est inclus dans l'en-tête du paquet de données à partir de la source.

Le protocole de routage DSR comprend deux phases principales, la découverte de la route et la phase de la maintenance de routes.

La découverte de la route : Dans cette phase de découverte, le nœud source établit un itinéraire en inondant les paquets RouteRequest à tous ses voisins. Chaque nœud voisin rediffuse à son tour les paquets vers ses voisins s'il ne l'a pas déjà fait ou s'il ne s'agit pas du nœud de destination, à condition que le compteur de durée de vie (TTL) soit supérieur à zéro. De plus, les identifiants de demande sont utilisés pour déterminer si une demande de route particulière a déjà été reçue par le nœud. Chaque nœud maintient une liste des paires <initiateur, id de demande> récemment reçues. Si deux demandes de route avec le même <initiateur, id de demande> sont reçues par un nœud intermédiaire, il n'en diffuse qu'une seule et abandonne l'autre. Cela empêche également la formation de boucles de routage dans le réseau. Lorsque le paquet atteint le nœud de destination, il renvoie un paquet de réponse (RREP) sur le chemin inverse vers la source. Ce paquet de réponse contient la route vers cette destination. Dans la figure A.7, le nœud source 1 lance un paquet RouteRequest pour obtenir un chemin pour le nœud de destination 15. Ce protocole utilise un cache de route sur chaque nœud qui stocke toutes les informations possibles extraites de la route

source contenues dans un paquet de données. Les nœuds peuvent également en savoir plus sur les routes voisines traversées par les paquets de données si elles sont exploitées en mode promiscuous (mode de fonctionnement dans lequel un nœud peut recevoir les paquets qui ne sont ni diffusés ni adressés à lui-même). Cette route en cache est également utilisée pendant la phase de découverte de la route. Si un nœud intermédiaire recevant une demande de route possède une route vers le nœud de destination dans son cache de route, il répond au nœud source en envoyant une RouteReply avec les informations de route complètes du nœud source au nœud de destination.

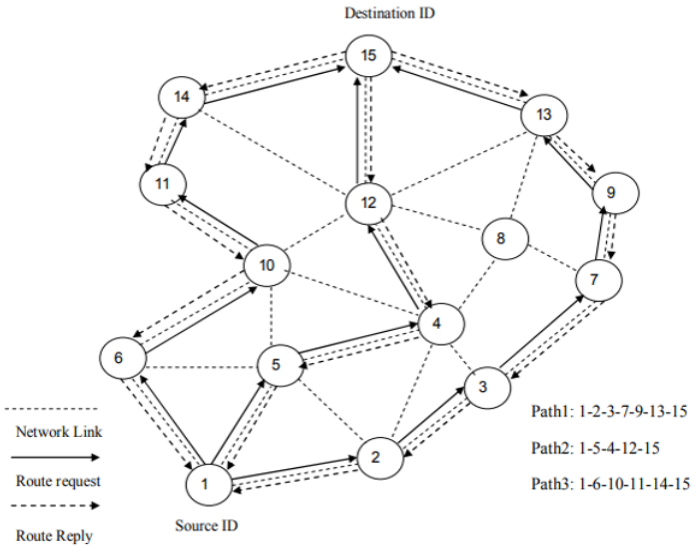


FIGURE A.7 – Découvert de la route dans le protocole DSR

Maintenance de la route : la phase de maintenance de la route est effectuée chaque fois qu'un lien est rompu entre deux nœuds. Une liaison défaillante peut être détectée par un nœud soit en surveillant passivement en mode promiscuous, soit en surveillant activement la liaison. Comme le montre la figure A.8, lorsqu'un nœud intermédiaire du chemin s'éloigne, provoquant la rupture d'une liaison sans fil (12-15), un paquet d'erreur de route (RERR) est renvoyé par le nœud intermédiaire au nœud d'origine. Le nœud source relance la procédure de découverte d'itinéraire pour rechercher un nouvel itinéraire vers la destination. Il supprime également toutes les entrées de route qu'il peut avoir dans son cache vers le nœud de destination.

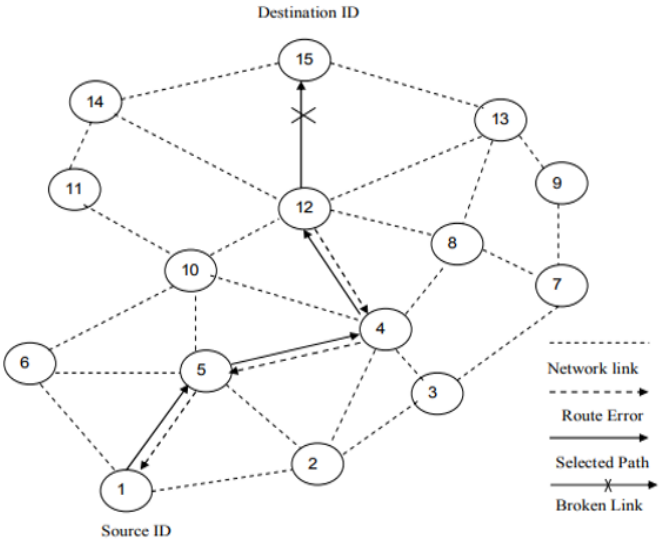


FIGURE A.8 – Maintenance de route du protocole DSR

Annexe B

Environnement de simulations network simulator 2

B.1 Présentation de Network Simulator 2

NS2 [18] est un simulateur d'événements discrets écrit en C ++, avec un interpréteur OTcl (Object Tool Command Langage) comme interface frontale. Le simulateur supporte une hiérarchie de classes en C ++ et une hiérarchie de classes similaire dans l'interpréteur OTcl. Les deux hiérarchies sont étroitement liées l'une à l'autre. Du point de vue de l'utilisateur, il existe une correspondance individuelle entre une classe de la hiérarchie interprétée et une classe de la hiérarchie compilée. La racine de cette hiérarchie est la classe Objet Tcl. Les utilisateurs créent de nouveaux objets de simulateur via l'interprète ; ces objets sont instanciés dans l'interpréteur et sont étroitement reflétés par un objet correspondant dans la hiérarchie compilée. La hiérarchie de classe interprétée est automatiquement établie à l'aide de méthodes définies dans la classe Tcl Class. Les objets instanciés par l'utilisateur sont reflétés par les méthodes définies dans la classe Tcl Object.

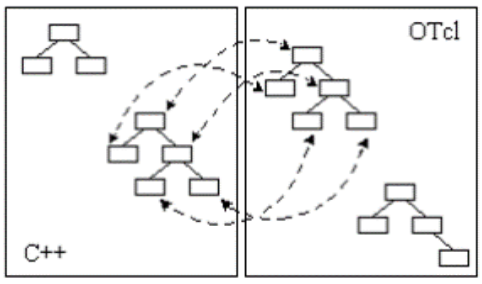


Figure B.1 – Dualité des classes de NS2

NS2 utilise deux langues parce que le simulateur a deux tâches à effectuer. D'une part, les simulations détaillées de protocoles nécessitent un langage de programmation système

capable de manipuler efficacement les octets, les en-têtes de paquets et de mettre en œuvre des algorithmes fonctionnant sur de grands ensembles de données. Pour ces tâches, la vitesse d'exécution est importante et le délai d'exécution moins important. D'autre part, une grande partie de la recherche sur le réseau implique des paramètres ou des configurations légèrement variables, ou une exploration rapide de plusieurs scénarios. Dans ces cas, le temps d'itération est plus important. Comme la configuration s'exécute une seule fois, l'exécution de cette partie de la tâche est moins importante. C ++ est rapide à exécuter mais plus lent à changer, ce qui le rend approprié pour une implémentation de protocole détaillée. OTcl fonctionne beaucoup plus lentement, mais peut être modifié très rapidement, ce qui le rend idéal pour la configuration de la simulation. Lorsqu'une simulation est terminée, NS2 génère un ou plusieurs fichiers de sortie textuels contenant des données de simulation détaillées, si cela est spécifié dans le script d'entrée OTcl. Les données peuvent être utilisées pour l'analyse de simulation ou comme entrée dans un outil d'affichage de simulation graphique appelé Network Animator (NAM). NAM possède une interface utilisateur graphique attrayante qui peut présenter graphiquement des informations telles que le débit et le nombre de pertes de paquets à chaque lien, bien que les informations graphiques ne puissent pas être utilisées pour une analyse de simulation précise.

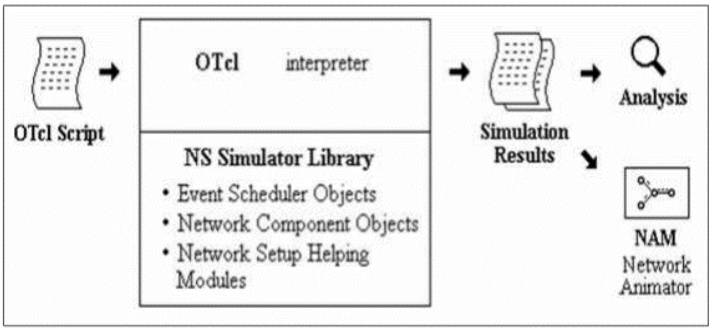


FIGURE B.2 – Vue simplifiée de NS2

La figure suivante décrit comment les différentes informations sont stockées dans les différents fichiers du simulateur NS2.

Parmi les sous-répertoires de ns-allinone-2.35, ns-2 est l'endroit qui contient toutes les implémentations du simulateur, les scripts de test de validation OTcl et des exemples de scripts OTcl. Dans ce répertoire, tous les codes OTcl situés dans un sous-répertoire appelé tcl, ainsi que la plupart du code C ++, qui implémente le planificateur d'événements, ainsi que les classes d'objets composant de réseau élémentaire, sont situés au niveau principal.

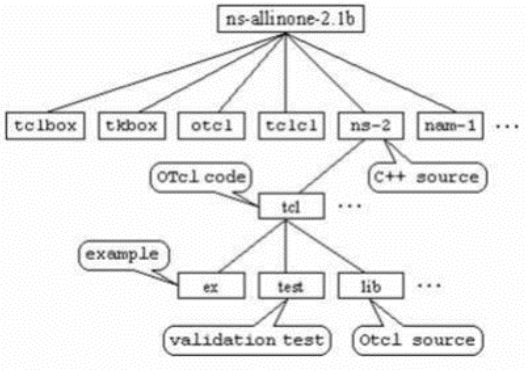


FIGURE B.3 – Structure du répertoire du NS

B.2 Notions de base sur le simulateur

B.2.1 Planificateur d'événements

NS2 est un simulateur d'événements. Il y a actuellement quatre planificateurs disponibles dans le simulateur, dont chacun est implémenté en utilisant une structure de données différente : une simple liste liée, un tas, une file d'attente calendrier (par défaut), et un type spécial appelé "temps réel". L'ordonnanceur en temps réel est destiné à l'émulation, ce qui permet au simulateur d'interagir avec un réseau réel. Actuellement, l'émulation est en cours de développement bien qu'une version expérimentale soit disponible. Les planificateurs d'événements sont utilisés pour planifier des événements tels que quand démarrer un agent cbr, quand envoyer /recevoir/déposer un paquet, etc. Ils sont également utilisés pour simuler le retard.

Les planificateurs d'événements s'exécutent en sélectionnant le prochain événement le plus ancien et en l'exécutant jusqu'à la fin (en appelant les composants réseau appropriés et en leur permettant d'effectuer l'action appropriée associée à l'événement), puis en revenant pour exécuter l'événement suivant. Le simulateur est mono-thread, il n'y a qu'un seul événement en cours d'exécution à un moment donné.

B.2.2 Nœud de base

Un nœud est un objet composé. Il est composé d'un objet d'entrée de nœud et de classificateurs. Il existe deux types de nœuds dans NS. Un nœud unicast a un classificateur

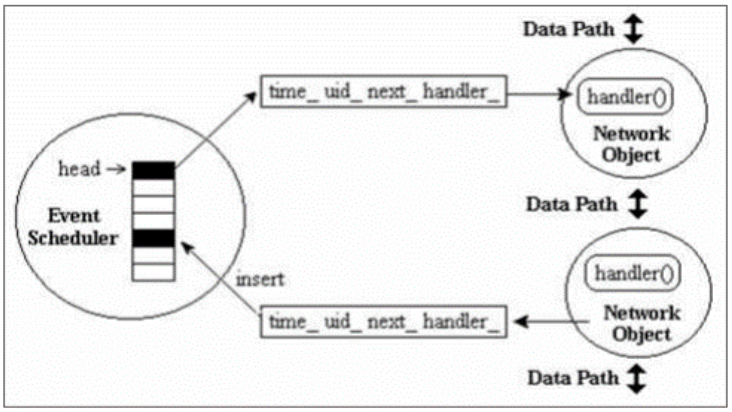


FIGURE B.4 – Planificateur d'événements

d'adresses qui effectue le routage monodiffusion et un classificateur de ports (les agents sont attachés aux ports). En outre, un nœud de multidiffusion possède un classificateur qui classifie les paquets de multidiffusion à partir de paquets unicast et un classificateur de multidiffusion qui effectue le routage multicast.

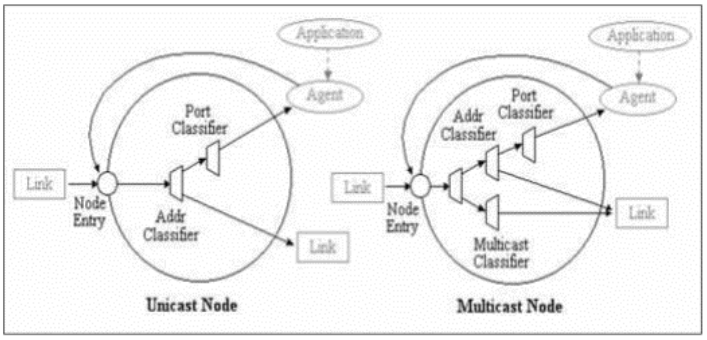


FIGURE B.5 – Structure de base du nœud dans NS2

B.2.3 Lien

Link est un objet composé en NS. Il relie deux nœuds. Nous pouvons créer des liens simplex et duplex en NS. Un lien duplex n'est rien d'autre que deux liens simplex dans les deux sens.

Lorsqu'un nœud veut envoyer un paquet via un lien, il place le paquet sur l'objet de file d'attente du lien. Les paquets retirés de la file d'attente de l'objet file d'attente sont

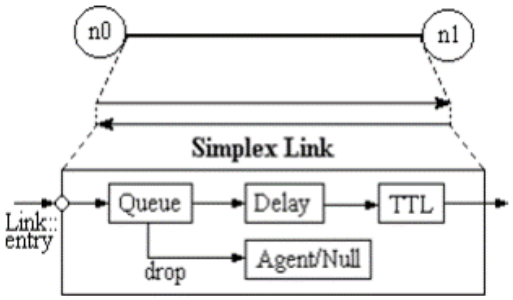


FIGURE B.6 – Lien simplex

transmis à l'objet délai. L'objet délai simule le délai de lien. L'envoi d'un paquet à un agent nul à partir de l'objet file d'attente simule la suppression du paquet. L'objet TTL calcule la durée de vie de chaque paquet reçu et met à jour le champ TTL du paquet.

B.2.4 Paquet

Les paquets sont les unités fondamentales d'échange entre les objets. Un paquet est composé d'une pile d'en-têtes et d'un espace de données facultatif.

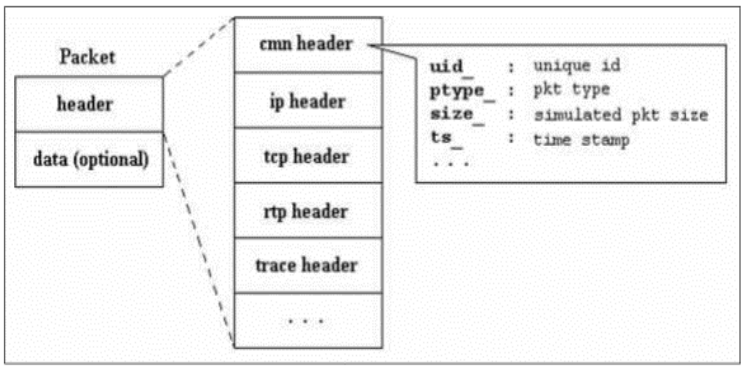


FIGURE B.7 – Lien simplex

Chaque en-tête de la pile correspond à une couche particulière. De plus, il existe un en-tête commun auquel toutes les couches peuvent accéder, ainsi qu'un en-tête de trace contenant des informations pour le support de trace. Les nouveaux protocoles peuvent définir leurs propres en-têtes de paquet ou étendre les en-têtes existants avec des champs supplémentaires.

B.2.5 Agent

Les agents sont utilisés dans la mise en œuvre de protocoles à différentes couches. Ils représentent des points d'extrémité où des paquets de couche réseau sont construits ou utilisés. Il existe plusieurs types d'agents pris en charge par NS2 au niveau de la couche de transport. Network Simulator dispose également d'agents de routage implémentant les différents protocoles de routage tels que DSDV, TORA, AODV et DSR.

Ci-dessous des exemples des agents au niveau de la couche de transport :

- Agent TCP : pour émettre un trafic TCP.
- Agent UDP : pour émettre un trafic UDP.
- Agent TCPSink : pour la réception du trafic TCP.
- Agent NULL : pour la réception des paquets UDP.

Bibliographie

[1] Abdel-Azim, Mohammed, Salah, Hossam El-Din et al. « Black Hole attack Detection using fuzzy based IDS ». In : *International Journal of Communication Networks and Information Security (IJCNIS)* 9.2 (2017).

[2] Al-Jaroodi, J. « Security issues in wireless mobile ad hoc networks at the network layer ». In : *University of Nebraska-Lincoln, Dept. of Computer Science and Engineering, Technical Report TR02-10-07* (2002).

[3] Balan, E Vishnu et al. « Fuzzy based intrusion detection systems in MANET ». In : *Procedia Computer Science* 50 (2015), p. 109-114.

[4] Bang, Ankur O et Ramteke, Prabhakar L. « MANET : History, challenges and applications ». In : *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2.9 (2013), p. 249-251.

[5] Bisen, Dhananjay et Sharma, Sanjeev. « Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET ». In : *National Academy Science Letters* 41.1 (2018), p. 23-28.

[6] Burg, Adam. « Ad-hoc network specific attacks ». In : *Seminar Ad-hoc network, Technische Universitaet Muenchen, 2003*. 2003.

[7] Cannady, James. « Artificial neural networks for misuse detection ». In : *National information systems security conference*. T. 26. Baltimore. 1998.

[8] Capkun, Srdjan, Buttyán, Levente et Hubaux, Jean-Pierre. « Self-organized public-key management for mobile ad hoc networks ». In : *IEEE Transactions on mobile computing* 1 (2003), p. 52-64.

[9] Chaudhary, Alka, Tiwari, VN et Kumar, Anil. « Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks ». In : *International Journal of Soft Computing and Networking* 1.1 (2016), p. 17-34.

[10] Corson, Scott et Macker, Joseph. « Mobile Ad-hoc networking (manet) : Routing protocol performance and evaluation considerations ». In : (1999).

[11] Ghaffari, Ali. « Vulnerability and security of mobile ad hoc networks ». In : *Proceedings of the 6th WSEAS international conference on simulation, modelling and optimization*. Citeseer. 2006, p. 124-129.

[12] Goldberg, Andrew et Radzik, Tomasz. *A heuristic improvement of the Bellman-Ford algorithm*. Rapp. tech. STANFORD UNIV CA DEPT OF COMPUTER SCIENCE, 1993.

[13] Hafslund, Andreas et al. « Secure Extension to the OLSR protocol ». In : *OLSR Interop and Workshop*. T. 1004. Citeseer. 2004.

[14] Hsu, Chih-Wei, Chang, Chih-Chung, Lin, Chih-Jen et al. « A practical guide to support vector classification ». In : (2003).

[15] Hu, Yih-Chun, Johnson, David B et Perrig, Adrian. « SEAD : Secure efficient distance vector routing for mobile wireless ad hoc networks ». In : *Ad hoc networks* 1.1 (2003), p. 175-192.

[16] Hu, Yih-Chun, Perrig, Adrian et Johnson, David B. « Ariadne : A secure on-demand routing protocol for ad hoc networks ». In : *Wireless networks* 11.1-2 (2005), p. 21-38.

[17] Huang, Yi-an et al. « Cross-feature analysis for detecting ad-hoc routing anomalies ». In : *null*. IEEE. 2003, p. 478.

[18] Issariyakul, Teerawat et Hossain, Ekram. « Introduction to Network Simulator 2 (NS2) ». In : *Introduction to Network Simulator NS2*. Springer, 2012, p. 21-40.

[19] Jacquet, Philippe et al. « Optimized link state routing protocol for ad hoc networks ». In : *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*. IEEE. 2001, p. 62-68.

[20] Jain, Ashish Kumar et Tokekar, Vrinda. « Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks ». In : *Pervasive computing (ICPC), 2015 international conference on*. IEEE. 2015, p. 1-6.

[21] Jang, J-SR. « ANFIS : adaptive-network-based fuzzy inference system ». In : *IEEE transactions on systems, man, and cybernetics* 23.3 (1993), p. 665-685.

[22] Johnson, David B et Maltz, David A. « Dynamic source routing in ad hoc wireless networks ». In : *Mobile computing*. Springer, 1996, p. 153-181.

[23] Joshi, Anupam et al. « Neighborhood Watch : An intrusion detection and response protocol for mobile ad hoc networks ». In : (2002).

[24] Kannhavong, Bounpadith et al. « A survey of routing attacks in mobile ad hoc networks ». In : *IEEE Wireless communications* 14.5 (2007).

[25] Kennedy, James. « Particle swarm optimization ». In : *Encyclopedia of machine learning*. Springer, 2011, p. 760-766.

[26] Kennedy, James. « The behavior of particles ». In : *International Conference on Evolutionary Programming*. Springer. 1998, p. 579-589.

[27] Kruse, Rudolf, Gebhardt, Joan E et Klowon, F. *Foundations of fuzzy systems*. John Wiley & Sons, Inc., 1994.

[28] Kumar, Raushan, Quyoom, Abdul et Gouttam, Devki Nandan. « To mitigate black hole attack in AODV ». In : *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on*. IEEE. 2015, p. 307-311.

[29] Kundu, Joydeep, Majumder, Koushik et De, Debashis. « An Efficient Trust-Based Routing Scheme by Max-Min Composition of Fuzzy Logic for MANET ». In : *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*. Springer. 2016, p. 435-440.

[30] Lakshmi, A Anna et Valluvan, KR. « Support vector machine and fuzzy-based intrusion detection and prevention for attacks in MANETs ». In : *International Journal of Mobile Network Design and Innovation* 6.2 (2015), p. 63-72.

[31] Lakshmi, K et al. « Modified AODV Protocol against Blackhole Attacks ». In : *in MANET", International Journal of Engineering and Technology Vol. 2*. Citeseer. 2008.

[32] Li, Huaizhi et al. « Secure routing in wired networks and wireless ad hoc networks ». In : *Department of Computer Science : Univ of Kentucky* (2002), p. 1-10.

[33] Liao, Hung-Jen et al. « Intrusion detection system : A comprehensive review ». In : *Journal of Network and Computer Applications* 36.1 (2013), p. 16-24.

[34] Mendel, Jerry M, John, Robert I et Liu, Feilong. « Interval type-2 fuzzy logic systems made simple ». In : *IEEE transactions on fuzzy systems* 14.6 (2006), p. 808-821.

[35] Misra, Pratap et Enge, Per. « Global Positioning System : signals, measurements and performance second edition ». In : *Massachusetts : Ganga-Jamuna Press* (2006).

[36] Moudni, Houda et al. « Attacks against aodv routing protocol in mobile ad-hoc networks ». In : *2016 13th international conference on computer graphics, imaging and visualization (cgiv)*. IEEE. 2016, p. 385-389.

[37] Moudni, Houda et al. « Fuzzy Logic based Intrusion Detection System against Black Hole Attack in Mobile Ad Hoc Networks ». In : *International Journal of Communication Networks and Information Security (IJCNIS)* 10.2 (2018).

[38] Moudni, Houda et al. « Modified AODV routing protocol to improve security and performance against black hole attack ». In : *Information Technology for Organizations Development (IT4OD), 2016 International Conference on*. IEEE. 2016, p. 1-7.

[39] Moudni, Houda et al. « Performance analysis of AODV routing protocol in MANET under the influence of routing attacks ». In : *Electrical and Information Technologies (ICEIT), 2016 International Conference on*. IEEE. 2016, p. 536-542.

[40] Moudni, Houda et al. « Secure routing protocols for mobile ad hoc networks ». In : *Information Technology for Organizations Development (IT4OD), 2016 International Conference on*. IEEE. 2016, p. 1-7.

[41] Murthy, C Siva Ram et Manoj, BS. *Ad hoc wireless networkd : Architestures and protocols*. Pearson Education India, 1900.

[42] Ning, Peng et Sun, Kun. « How to misuse AODV : a case study of insider attacks against mobile ad-hoc routing protocols ». In : *Ad Hoc Networks* 3.6 (2005), p. 795-819.

[43] Oppliger, Rolf. « Internet and Intranet Security ». In : *Artech House* (1998).

[44] Papadimitratos, Panagiotis et Haas, Zygmunt J. « Secure link state routing for mobile ad hoc networks ». In : *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*. IEEE. 2003, p. 379-383.

[45] Papadimitratos, Panagiotis et Haas, Zygmunt J. « Secure routing for mobile ad hoc networks ». In : *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*. T. 31. San Antonio, TX. 2002.

[46] Pekalska, Elzbieta et al. *Introduction to MATLAB*. University of Twente, Department of Applied Mathematics, 2006.

[47] Perkins, Charles, Belding-Royer, Elizabeth et Das, Samir. *Ad hoc on-demand distance vector (AODV) routing*. Rapp. tech. 2003.

[48] Perkins, Charles E et Bhagwat, Pravin. « Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers ». In : *ACM SIGCOMM computer communication review*. T. 24. 4. ACM. 1994, p. 234-244.

[49] Perrig, Adrian et al. « Efficient and secure source authentication for multicast ». In : *Network and Distributed System Security Symposium, NDSS*. T. 1. 2001. 2001, p. 35-46.

[50] Puttini, Ricardo S et al. « A modular architecture for distributed IDS in MANET ». In : *International Conference on Computational Science and Its Applications*. Springer. 2003, p. 91-113.

[51] Rada-Vilelahttp, J. *A Fuzzy Logic Control Library in C++*.

[52] Raffo, Daniele et al. « Securing OLSR using node locations ». In : *Wireless Conference 2005-Next Generation Wireless and Mobile Communications and Services (European Wireless), 11th European*. VDE. 2005, p. 1-7.

[53] Rutvij, HJ, Sankita, JP et Devesh, CJ. « A novel approach for gray hole and black hole attacks in mobile ad hoc networks ». In : *Second international conference on advanced computing and communication technologies, IEEE*. 2012.

[54] Sanzgiri, Kimaya et al. « A secure routing protocol for ad hoc networks ». In : *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*. IEEE. 2002, p. 78-87.

[55] Shafi, M Qaisar, Hussain, Faisal B et Ahmed, Usama. « Topology-based Efficient Downstream transport in wireless sensor networks ». In : *Emerging Technologies (ICET), 2010 6th International Conference on*. IEEE. 2010, p. 353-358.

[56] Theresa, W Gracy et Sakthivel, S. « Fuzzy based intrusion detection for cluster based battlefield MANET ». In : *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2017 IEEE International Conference on*. IEEE. 2017, p. 22-27.

[57] Wang, Sun-Chong. « Artificial neural network ». In : *Interdisciplinary computing in java programming*. Springer, 2003, p. 81-100.

[58] William, Stallings. « Cryptography and network security : principles and practice ». In : *Prentice-Hall, Inc* (1999), p. 23-50.

[59] Yen, John et Langari, Reza. *Fuzzy logic : intelligence, control, and information*. T. 1. Prentice Hall Upper Saddle River, NJ, 1999.

[60] Yi, Seung, Naldurg, Prasad et Kravets, Robin. « Security-aware ad hoc routing for wireless networks ». In : *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. ACM. 2001, p. 299-302.

[61] Yousefi, Saleh, Mousavi, Mahmoud Siadat et Fathy, Mahmood. « Vehicular ad hoc networks (VANETs) : challenges and perspectives ». In : *ITS Telecommunications Proceedings, 2006 6th International Conference on*. IEEE. 2006, p. 761-766.

[62] Zapata, Manel Guerrero et Asokan, Nadarajah. « Securing ad hoc routing protocols ». In : *Proceedings of the 1st ACM workshop on Wireless security*. ACM. 2002, p. 1-10.

Liste des Publications

Articles

1. **Moudni H.**, Er-rouidi M., Mouncif H., El Hadadi B. (2018) Fuzzy Logic based Intrusion Detection System against Black Hole Attack in Mobile Ad Hoc Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No. 2, pp. 366-373.
2. **Moudni H.**, Er-rouidi M., Faouzi H., Mouncif H., El Hadadi B. (2017) Enhancing Security in Optimized Link State Routing Protocol for Mobile Ad Hoc Networks. In : Sabir E., García Armada A., Ghogho M., Debbah M. (eds) Ubiquitous Networking. UNet 2017. Lecture Notes in Computer Science, vol 10542. Springer, Cham
3. Er-Rouidi, M., **Moudni, H.**, Faouzi, H., Mouncif, H., & Merbouha, A. (2017). Enhancing Energy Efficiency of Reactive Routing Protocol in Mobile Ad-Hoc Network with Prediction on Energy Consumption. International Arab Journal of Information Technology (IAJIT) (pp. 1-7)
4. Er-rouidi M., **Moudni H.**, Faouzi H., Mouncif H., Merbouha A. (2017) A Fuzzy-Based Routing Strategy to Improve Route Stability in MANET Based on AODV. In : El Abbadi A., Garbinato B. (eds) Networked Systems. NETYS 2017. Lecture Notes in Computer Science, vol 10299. Springer, Cham
5. Faouzi H., Er-rouidi M., **Moudni H.**, Mouncif H., Lamsaadi M. (2017) Improving Network Lifetime of Ad Hoc Network Using Energy Aodv (E-AODV) Routing Protocol in Real Radio Environments. In : El Abbadi A., Garbinato B. (eds) Networked Systems. NETYS 2017. Lecture Notes in Computer Science, vol 10299. Springer, Cham
6. Er-rouidi M., **Moudni H.**, Faouzi H., Mouncif H., Merbouha A. Improving Performance of Mobile Ad Hoc Network Using Clustering Schemes, The International Journal of Informatics and Communication Technology (IJ-ICT) Vol. 6, No. 2, August 2017, pp. 69-75.

Conférences internationales

1. **Houda MOUDNI**,Mohamed ER-ROUIDI,Hicham MOUNCIF, Benachir EL HADADI, " Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET", Procedia Computer Science, 2019, vol. 151, p. 1176-1181.
2. **Houda MOUDNI**, Mohamed ER-ROUIDI, Hicham MOUNCIF, Benachir EL HADADI, " Intrusion Detection in MANETs using Machine Learning Approaches ", The Fourth International Conference on Business Intelligence (CBI'18), April 25-27, 2018, Beni Mellal, Morocco.
3. **Houda MOUDNI**, Mohamed ER-ROUIDI, Hassan FAOUZI, Hicham MOUNCIF, Benachir EL HADADI, " Intrusion Detection System in Mobile Ad-hoc Networks using Machine Learning Techniques", The Third International Conference on Business Intelligence (CBI'17), March 29-31, 2017, Beni Mellal, Morocco.
4. **Houda MOUDNI**, Mohamed ER-ROUIDI, Hassan Faouzi, Hicham MOUNCIF, Benachir EL HADADI, "Anomaly traffic detection based on GPLVM and SVM", The International Arab Conference on Information Technology (ACIT'16), December 6-8, 2016, Beni Mellal, Morocco.
5. **Houda MOUDNI**, Mohamed ER-ROUIDI, Hicham MOUNCIF, Benachir EL HADADI, "A Security Enhanced in Optimized Link State Routing Protocol for Mobile Ad Hoc Networks", the fourth International Workshop on RFID and Adaptive Wireless Sensor Networks (RAWSN'16), May 17, 2016, Marrakech, Morocco.
6. **Houda MOUDNI**, Mohamed ER-ROUIDI, Hicham MOUNCIF, Benachir EL HADADI, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks", the Second Edition of the International Conference on Electrical and Information Technologies (ICEIT2016), May 5-7, 2016, Tangier, Morocco.
7. **H. Moudni**, M. Er-rouidi, H. Mouncif and B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks," 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, Morocco, 2016, pp. 1-7. IEEE.
8. **H. Moudni**, M. Er-rouidi, H. Mouncif and B. E. Hadadi, "Modified AODV routing protocol to improve security and performance against black hole attack," 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, Morocco, 2016, pp. 1-7. IEEE.

9. **H. Moudni**, M. Er-Rouidi, H. Mouncif and B. El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks," 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, Morocco, 2016, pp. 385-389. IEEE.
10. **Houda MOUDNI**, Mohamed ER-ROUIDI , Hicham MOUNCIF , Benachir EL HADADI, "Impact of Malicious Behavior on AODV Routing Protocol, Third International Conference on NETworked sYStems (NETYS'2015), May 13-15, 2015, Agadir , Morocco.
11. **Houda MOUDNI**, Mohamed ERROUIDI , Benachir ELHADADI, Hicham MOUNCIF, "Survey on the security of mobile ad hoc networks", First International Conference on business Intelligence (CBI'14), April 30, 2014, Beni Mellal , Morocco.
12. Mohamed ER-ROUIDI, **Houda MOUDNI**, Hicham MOUNCIF, Abdelkrim MERBOUHA, "A Balanced Energy Consumption in Mobile Ad hoc Network", Procedia Computer Science, 2019, vol. 151, p. 1182-1187.
13. Mohamed ER-ROUIDI, **Houda MOUDNI**, Hassan FAOUZI, Hicham MOUNCIF, Abdelkrim MERBOUHA, "Improving Performance of Mobile Ad Hoc Network Using Clustering schemes ", The Third International Conference on Business Intelligence (CBI'17), March 29-31, 2017, Beni Mellal, Morocco.
14. M. Er-Rouidi, **H. Moudni**, H. Mouncif and A. Merbouha, "An Energy Consumption Evaluation of Reactive and Proactive Routing Protocols in Mobile Ad-Hoc Network," 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, Morocco, 2016, pp. 437-441. IEEE.
15. Mohamed ER-ROUIDI, **Houda MOUDNI**, Hassan Faouzi, Hicham MOUNCIF, Abdelkrim Merbouha, "Energy Enhancement Of Ad Hoc On-Demand Distance Vector Routing Protocol for Maximum Lifetime in MANET", The International Arab Conference on Information Technology (ACIT'16), December 6-8, 2016, Beni Mellal, Morocco.
16. Hassan Faouzi, Mohamed ER-ROUIDI, **Houda MOUDNI**, Hicham MOUNCIF, Mohamed Lamsaadi, "Implementation and Comparison of AODV and DSDV in Multi-Channel Multi-Interface Ad Hoc Wireless Networks", The International Arab Conference on Information Technology (ACIT'16), December 6-8, 2016, Beni Mellal, Morocco.
17. Mohamed ERROUIDI, **Houda MOUDNI**, Abdelkrim MERBOUHA, Hicham MOUNCIF, "Performance Comparison of DSDV, AODV and DSR Routing Protocols for

MANETS", First International Conference on business Intelligence (CBI'14), April 30, 2014, Beni Mellal , Morocco.

18. Er-rouidi, M., **Moudni, H.**, Merbouha, A., & Mouncif, H. (2014). "A Survey on QoS Enhancements in AODV protocol for MANET". INTIS'2014, 13.