N°d'ordre: .....

République Algerienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la Recherche scientifique

Université Djillali Liabès de Sidi Bel Abbès
Faculté des Sciences Exactes
Département d'informatique
Laboratoire EEDIS

Thèse de Doctorat en Sciences

Domaine : Informatique
Filière : Informatique
Spécialité : Réseaux des systèmes informatiques

Par

Mr TAMI Abdelaziz

Sécurité du routage dans les protocoles de routage multichemins

Soutenu le 26-07-2021 devant le jury :

Pr.	ADJOUDJ Réda	UDL SBA	Président du jury
Dr.	MEKKAOUI Kheireddine	U. Saida	Examinateur
Dr.	BABA AHMED Zakarya	U. Chlef	Examinateur
Pr.	BOUKLI-HACENE Sofiane	UDL SBA	Directeur de thèse
Dr.	ALI-CHERIF Moussa	UDL SBA	Co-Directeur de thèse

Année Universitaire : 2020 - 2021

Je dédie ce modeste travail à : Mes très chers parents pour tous leurs sacrifices et grâce à vous je n'ai manqué de rien « MERCI »

Remerciements

Cette thèse est le fruit de plusieurs années de travail et de l'engagement de plusieurs personnes qui font partie de mon parcours de recherche. Je voudrais exprimer dans ces lignes mes sincères remerciements à tous ceux qui ont contribué de près ou de loin à participer dans ce travail par leurs aides, leurs encouragements, leurs motivations, leurs conseils. Qu'ils trouvent ici les expressions de ma gratitude et ma reconnaissance.

Au début, je demande à Dieu pardon et miséricorde envers mon estimé enseignant M. ALI CHERIF Moussa, que Dieu ait pitié de lui et le fasse vivre dans son paradis et je remercie profondément mon directeur de thèse, Pr. BOUKLI-HACENE Sofiane, pour leurs soutiens, leurs conseils, leurs remarques, leurs patiences et surtout leurs confiances qu'il m'on toujours accordés depuis le début de ce travail jusqu'à l'achèvement de cette thèse. Je tiens également à les remercient pour leurs suivis tout au long de ces années de recherche. Ce travail n'aurait jamais pu aboutir sans l'aide qui mon accordés. Je leurs expriment particulièrement toute ma gratitude et ma reconnaissance.

Je suis très reconnaissant envers tous les membres du jury pour la grande attention qu'ils ont bien voulu porter à mon travail, je remercie ainsi le Pr. ADJOUDJ Réda de l'université de Sidi Bel Abbes, Dr. MEKKAOUI Kheireddine de l'université de SAÎDA et Dr. BABA AHMED Zakaria de l'université de Chlef pour avoir accepté de participer à mon jury de soutenance.

Je tiens à remercier également l'ensemble des enseignants avec qui j'ai eu le plaisir de travailler. Je voudrais aussi remercier tous mes amis. Je leurs exprime ma gratitude pour leurs encouragements et leurs soutiens moral qu'ils mont apportés. Je remercie en particulier mon ami Hamami Abdelkrim et je lui partage le fruit de ce travail.

Mes plus chaleureux remerciements vont également à ma famille, en particulier ma mère, mon père, mes frères, mes sœurs, pour leurs soutiens et leurs encouragements durant toute cette période à l'élaboration de ce travail.

Enfin, mes remerciements les plus sincères s'adressent à ma femme qui à toujours été avec moi pour m'encourager et pour m'avoir accompagnée pendant toutes ces années de recherche. Je pense toujours à ma petite fille Sirine et mes deux petits fils Mohamed et Tarek Amir.

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Contexte

Actuellement et avec l'apparition des technologies sans fil, les réseaux mobiles ad hoc sont devenus des moyens nécessaires pour rechercher et communiquer les informations dans les systèmes de communication. Un réseau mobile ad hoc ou MANET (Mobile Ad hoc NETwork) est un ensemble d'entités ou nœuds mobiles qui possèdent des interfaces sans fil et déplacent librement, interconnectés entre eux, formant un réseau d'une topologie dynamique, sans l'aide d'aucune infrastructure fixe ni d'administration centralisée. Nous assistons à une utilisation des réseaux mobiles ad hoc dans plusieurs domaines d'application à savoir : les applications commerciales, les applications conçues pour l'environnement, les applications destinées pour les opérations de secours, les applications utilisées dans le domaine militaire, les applications liées à l'éducation. De ce fait, les réseaux mobiles ad hoc doivent garantir les exigences de sécurité telle que : l'authentification, l'intégrité, la non-répudiation, la disponibilité et la confidentialité des données afin de protéger les informations communiquées dans ces réseaux. Toutefois, due aux caractéristiques des réseaux mobiles ad hoc, tel que : la topologie dynamique, la bande passante limitée, les contraintes d'énergie, la sécurité physique limitée, ces réseaux rencontrent divers défis de sécurisation. Ainsi, puisque la transmission des paquets de données est effectuée par voie Hertzienne, il est très facile pour un nœud malveillant de nuire à cette transmission. En effet, les réseaux ad hoc sont vulnérables à plusieurs types d'attaques, spécifiquement l'écoute ou l'interception des paquets, leurs suppressions ou modification, leurs retransmissions ou même leurs endommagements.

Le routage est une fonction fondamentale pour acheminer les paquets de données entre les nœuds mobiles participant à la communication dans le réseau mobile ad hoc. Généralement, il existe trois catégories de protocoles de routages à savoir : réactifs, proactifs et hybrides. Dans cette thèse, nous nous focaliserons essentiellement nos travaux de recherche sur les protocoles de routages réactifs, en particulier sur le protocole de routage multi-chemins AOMDV (Ad hoc On-demand Multipath Distance Vector).

L'attaque trou noir (blackhole) est l'une des plus dangereux attaques dans ce type de protocole de routage. En effet, dans l'attaque trou noir, le nœud malveillant s'annonce comme ayant le plus court chemin vers le nœud de destination, en falsifiant une réponse d'une requête envoyer vers le nœud source qui permet d'établir une route erronée. Dès la réception de cette fausse réponse, le nœud source ignore toutes les autres réponses envoyées par d'autres nœuds, en croyant que le nœud malveillant possède le bon chemin, il commence la transmission des paquets de données

vers ce nœud malveillant. Ensuite, le nœud malveillant absorbe tous les paquets de données reçus. En conséquence, il élimine la communication entre les nœuds source et destination, il provoque la perturbation du bon fonctionnement du protocole de routage, et il affecte les performances du réseau.

Contribution de la thèse

Ce travail rentre dans le cadre de l'étude du problème de la sécurité du routage dans les protocoles de routage multi-chemins dans les réseaux mobiles ad hoc. L'objectif de ce travail de recherche est de proposer une amélioration du protocole de routage multi-chemins AOMDV et qui comporte des mécanismes de sécurité contre les attaques trou noir.

Notre travail de recherche s'articule à la proposition d'un nouveau protocole améliorer comporte de nouveaux mécanismes permettant la transmission des données dans les réseaux mobiles en évitant les paquets émis par les nœuds malveillants qui peuvent falsifier le choix d'une route tout en utilisant les performances qui peuvent être tirées à partir des protocoles de routages multi-chemins. Nous avons fait une proposition d'une extension du protocole de routage AOMDV pour concevoir un autre protocole plus sécurisé et plus fiable pour assurer la transmission des paquets de données entre les nœuds d'un réseau mobile.

La contribution de ce travail de recherche comprend deux parties principales à savoir : étude de l'impact des attaques trou noir sur les performances du protocole de routage AOMDV dans le premier lieu, celle-ci nous permis de comprendre le comportement des nœuds malveillants et d'analyser leurs effets sur les performances du protocole de routage AOMDV et leur fonctionnement dans cette situation. Ensuite, la proposition d'un mécanisme capable de détecter et d'isoler ces attaques dans un deuxième lieu. Toutefois. Dans la première partie afin d'analyser les impacts des attaques trou noir sur le protocole AOMDV, nous allons implémenter le protocole BHAOMDV sous plusieurs attaques trou noir. Dans la deuxième partie afin de détecter et d'isoler les nœuds attaquants nous allons implémenter IDSAOMDV (Intrusion Detection System for AOMDV) comme solution contre les attaques trou noir. Pour implémenter les protocoles BHAOMDV et IDSAOMDV, nous allons utiliser le fameux simulateur des réseaux à savoir *NS*2.35 (Network Simulator).

Organisation de la thèse

La thèse est organisée en trois chapitres.

Le chapitre suivant sur les réseaux mobiles ad hoc qui représente le domaine de base de notre travail de recherche, qui joue un rôle principal associé par les recherches et les évolutions technologiques et les techniques de transmission. Nous présentons ainsi, les définitions énoncées des réseaux mobiles ad hoc, la modélisation et la représentation graphique d'un réseau mobile ad hoc, les caractéristiques générales et les applications essentielles de ces réseaux engendrés dans ce domaine, apprécié leurs avantages et leurs inconvénients, expliquer le routage et les différents proto-

coles de routage étudier dans la littérature, examiner la sécurité dans les réseaux mobiles ad hoc et exposer les différentes attaques spécifiaient pour ces réseaux.

Le deuxième chapitre s'articule sur les protocoles de routage multi-chemins dans les MANETs. Dans ce chapitre, nous détaillons les principaux composants de base des protocoles de routage multi-chemins, il s'agit de la découverte des routes, la maintenance des routes et l'allocation du trafic, afin d'expliquer les étapes nécessaires pour acheminer les paquets communiquer entre les nœuds dans un réseau ad hoc par le protocole de routage associer. Nous donnons ensuite les détails des avantages du routage multi-chemins les plus reconnais à savoir, la tolérance aux pannes, l'agrégation de la bande passante, la réduction du délai de découverte de route, l'équilibrage de la charge, et la sécurité. Nous exprimons ensuite une variété des protocoles de routage multi-chemins les plus connus, afin d'expliquer leurs caractéristiques et leurs principaux fonctionnalités.

Le troisième chapitre présente notre contribution. Dans ce chapitre nous adoptons la sécurité du routage dans les protocoles de routage multi-chemins. Nous étudions les attaques trou noir auxquelles le routage est traité et proposons un nouveau mécanisme pour sécuriser la communication et les paquets de données transmises par ce type de routage. La première section de ce chapitre dresse un état de l'art dans lequel nous étudions les solutions inclues dans les travaux de recherche existant dans la littérature pour résoudre le problème de la sécurité contre les attaques trou noir, nous décrivons aussi leurs avantages, leurs inconvénients et leurs limites. Puis nous détaillons notre solution de sécurité proposée dans le cadre de ce travail de recherche, nous présentons ainsi l'implémentation et les simulations effectuées, nous examinons aussi les résultats obtenus, puis une étude détaillée de comparaison des performances de notre solution proposée avec d'autres solutions existantes, nous présentons ensuite une synthèse sur cette étude de comparaison.

Enfin, nous concluons notre travail de recherche par une synthèse générale, en rappelant notre contribution, en éclairons les limites de notre solution proposée et nous suggérons quelques perspectives associées à notre thèse pour les futures recherches.

Les réseaux mobiles Ad hoc 1

Sommaire

Introduction

Dans les deux dernières décennies, les réseaux mobiles ad hoc où MANETs (Mobile Ad hoc NETwork) ont connu de grandes évolutions dans les domaines appliquant la technologie sans fil. Un réseau mobile ad hoc est composé par la réunion d'un ensemble autonome d'entités ou de nœuds mobiles utilisant des interfaces radio interconnectés entre eux sans infrastructure fixe et sans contrôle central. Ces nœuds mobiles se déplacent librement en formant une topologie dynamique. Chaque nœud participant au réseau ad hoc a la capacité de retransmettre les données aux autres nœuds selon un protocole de routage bien déterminé. Le protocole de routage permet l'établissement des itinéraires entre les pairs de nœuds qu'ils se situent physiquement les unes à coté des autres afin d'acheminer les données d'un nœud source vers un nœud de destination.

Dans ce chapitre, nous présentons un aperçu des différents aspects en relation avec les réseaux mobiles ad hoc. Tout d'abord, une brève définition est exposée sur les réseaux mobiles ad hoc. Ensuite, la modélisation, les importantes caractéristiques, les principales applications, les avantages et inconvénients des MANETs sont abordés. Nous détaillons ensuite le routage et les différents protocoles de routage envisagés. Nous décrivons par la suite les attaques dans les réseaux mobiles ad hoc. Enfin, nous présentons une conclusion de ce chapitre.

1.1 Définition d'un réseau mobile ad hoc

Plusieurs chercheurs ont défini le réseau mobile ad hoc (Corson & Macker 1999; Ubéda 2008; Lu 2004). En voici les détails :

Un réseau mobile ad hoc est constitué de plateformes mobiles (par exemple, un routeur, un routeur avec plusieurs hôtes et périphériques de communication sans fil) appelés "nœuds" qui sont libres de se déplacer de manière arbitraire. Les nœuds peuvent être situés dans ou sur des avions, des navires, des camions, des voitures, et mêmes sur des personnes ou de très petits périphériques. Ainsi, un MANET est un système autonome de nœuds mobiles. Le système peut fonctionner de manière isolée ou avoir des passerelles vers un réseau fixe et une interface avec ce dernier. Cependant, les nœuds MANET sont équipés d'émetteurs et de récepteurs sans fil utilisant des antennes qui peuvent être omnidirectionnelles (diffusion), hautement directionnelles (point à point), éventuellement orientables ou une combinaison des deux. Les nœuds forment une topologie qui peut changer avec le temps lorsque les nœuds se déplacent ou ajustent leurs paramètres de transmission et de réception (Corson & Macker 1999).

Un réseau mobile ad hoc est un groupe de terminaux mobile indépendant de toute infrastructure, communiquant par ondes radio, où chacun de ces terminaux offrant un service de relais pour accepter un message ne lui était pas destiné à le retransmettre à un autre terminal du réseau qui est hors de portée radio de l'émetteur initial de ce message, comme présenter sur la *figure*1.1 (Ubéda 2008).

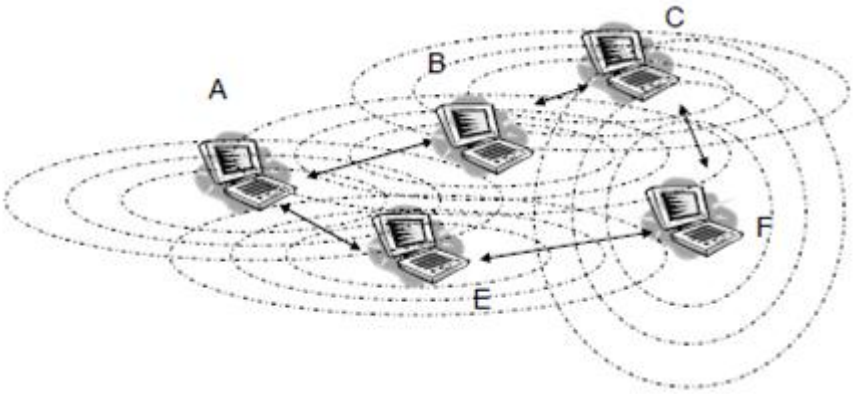

FIGURE 1.1 – *Exemple d'un réseau ad hoc (Ubéda 2008)*

La figure 1.1 représente un exemple de réseau ad hoc, où le terminal A souhaitant envoyer un message au terminal C demandera au terminal B de servir de relais ou consécutivement aux terminaux E et F, dans le même but. Cependant, deux routes sont possibles pour atteindre le terminal C à partir du terminal A, dans ce cas, on parle du routage pour décider comment le nœud A peut savoir la route pour transférer un message vers le nœud C. Le routage sera traité dans une autre section de ce chapitre.

Han dans (Lu 2004), explique que les réseaux mobiles ad hoc n'ont pas de routeurs fixes, chaque nœud peut être routeur. Tous les nœuds sont capables de mouvement et peuvent être connectés dynamiquement de manière arbitraire. Cependant, les responsabilités relatives à l'organisation et au contrôle du réseau sont réparties entre les terminaux eux-mêmes. L'ensemble du réseau est mobile et les terminaux individuels sont autorisés à se déplacer librement. Ainsi, certaines paires de terminaux peuvent ne pas être en mesure de communiquer directement entre elles et doivent relayer sur d'autres terminaux pour que les messages soient remis à leurs destinations.

1.2 Modélisation d'un réseau ad hoc

La modélisation prend une place croissante dans tous les domaines d'intervention. Actuellement, la modélisation par la théorie des graphes voit son champ d'application s'élargir. Un graphe n'est rien d'autre qu'une représentation symbolique d'un réseau (Mansouri & Bouhlel 2014). Autrement dit, la modélisation d'un réseau ad hoc par la théorie des graphes consiste à utiliser les concepts et les algorithmes de la théorie des graphes pour représenter graphiquement la topologie d'un réseau ad hoc.

D'après (Chelius 2004), la nature du médium est l'une des principales difficultés dans la conception et l'étude d'algorithmes adaptés aux réseaux ad hoc. Effectivement, le lien radio se distingue des liens filaires par plusieurs particularités : il n'est pas isolé mais localement diffus, sa qualité dépend de l'environnement extérieur et il peut être utilisé simultanément en plusieurs points suffisamment distants (réutilisation spatiale). Ainsi, le médium radio est caractérisé principalement par la diffusion radio (broadcast) et la réutilisation spatiale du médium.

Pour la première caractéristique, le lien radio est diffus. En effet, une onde radio se propage de manière omnidirectionnelle autour du nœud émetteur. Un paquet radio émis d'un nœud "u" vers un nœud "v" est également reçu par l'ensemble des nœuds voisins de u. Le voisinage de u, noté $\Gamma 1(u)$, représente l'ensemble des nœuds du réseau capables de recevoir et de comprendre un signal radio émis par "u".

Pour la deuxième caractéristique, la portée limitée des transmissions radio permet une réutilisation spatiale du médium. Pratiquement, deux nœuds ad hoc peuvent émettre en même temps sur le même médium radio s'ils sont à une distance assez grande l'un de l'autre. Cette distance dépend de la puissance d'émission ainsi que de l'atténuation du signal radio.

Un réseau ad hoc peut-être représenté formellement par un graphe G = (V, E) où V représente l'ensemble des nœuds du réseau et E l'ensemble des liens radio (figure 1.2).

Γ 1(u) = (v|(u, v)$\in$ E) représente le voisinage de u.

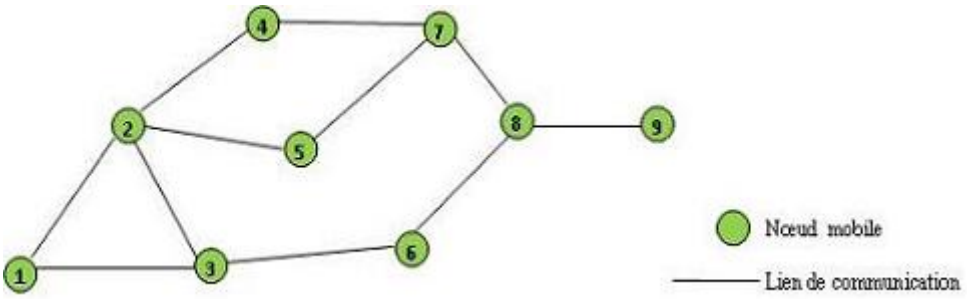

FIGURE 1.2 – *Représentation graphique d'un réseau ad hoc*

1.3 CARACTÉRISTIQUES DES RÉSEAUX MOBILES AD HOC

Plusieurs caractéristiques pour les réseaux mobiles ad hoc sont envisagées. Les principales caractéristiques sont les suivantes (Corson & Macker 1999) :

Topologies dynamiques

Les nœuds sont libres de se déplacer de manière arbitraire, ainsi la topologie du réseau qui est généralement multi-sauts peut changer aléatoirement et rapidement à des moments imprévisibles, et peut-être constituée de liens bidirectionnel et unidirectionnel.

Liaisons à capacités variables et bande passante limitée

Les liaisons sans fil auront toutefois une capacité inférieure à celles de leurs homologues câblées. De plus, le débit réalisé par les communications sans fil – dû aux effets des accès multiples, de la perte, du bruit et des interférences, etc. – est souvent beaucoup moins que le taux de transmission maximale d'une radio.

Contraintes d'énergie

L'ensemble ou une partie des nœuds d'un MANET peuvent dépendre de batteries ou d'autres moyens épuisables pour leur énergie. Pour ces nœuds, le critère de conception du système le plus important pour l'optimisation peut être la conservation de l'énergie.

Sécurité physique limitée

Les réseaux sans fil sont généralement plus exposés aux menaces pour la sécurité physique que les réseaux câblés fixes. La possibilité accrue d'attaques d'espionnage, d'usurpation d'identité et de déni de service doit être soigneusement examinée. Les techniques existant pour la sécurité des liaisons sont souvent appliquées dans les réseaux sans fil pour réduire les menaces à la sécurité. Comme avantage, la nature décentralisée du contrôle de réseau dans les MANETs offre une robustesse supplémentaire par rapport aux points de défaillances uniques d'approches plus centralisées.

1.4 Domaines d'application des réseaux ad hoc

Une application ad hoc est une application à organisation automatique composée d'appareils mobiles formant un réseau P2P (pair-à-pair en anglais peer-to-peer) où les communications sont possibles en raison de la proximité des appareils à une distance physique. MANET peut être utilisé pour constituer l'infrastructure de base des applications ad hoc. De nombreuses applications sont maintenues par les réseaux mobiles ad hoc. Dans cette section, nous présentons les principales applications (Subhankar 2005) :

Conférence mobile

Les réseaux ad hoc permettent la téléconférence mobile pour les utilisateurs qui ont besoin de collaborer en dehors de leur bureau, lorsque aucune infrastructure réseau n'est disponible. Il existe un besoin croissant d'environnements informatiques mobiles où différents membres d'un projet doivent collaborer à la conception et au développement. Les utilisateurs doivent partager des documents, transférer et télécharger des fichiers et échanger des idées.

Espace personnel et réseau domestique

Les réseaux ad hoc conviennent tout à fait aux applications de réseau domestique et personnel. Les appareils mobiles dotés de cartes Bluetooth ou WLAN peuvent être facilement configurés pour former un réseau ad hoc. Avec la connectivité Internet à la maison, ces appareils peuvent facilement être connectés à Internet. Par conséquent, l'utilisation de ce type de réseaux ad hoc a des applications pratiques et une facilité d'utilisation.

Services d'urgence

Lorsque l'infrastructure de réseau existante cesse de fonctionner ou est endommagée à la suite d'une catastrophe telle que des tremblements de terre, des ouragans, des incendies, etc., des réseaux ad hoc peuvent être facilement déployés pour fournir des solutions aux services d'urgence. Ces réseaux peuvent également être utilisés pour des opérations de recherche et de sauvetage, la récupération des données des patients à distance depuis des hôpitaux et de nombreux autres services utiles.

Points d'accès public

Dans les aéroports, les gares, et les centres commerciaux, les réseaux ad hoc permettent aux utilisateurs de créer leur propre réseau et de communiquer instantanément entre eux. Les réseaux ad hoc peuvent également être utilisés à des fins de divertissement, par exemple pour fournir une connectivité instantanée aux jeux multi-utilisateurs. En outre, la connectivité Internet des ménages peut être fournie par un point d'accès communautaire.

Applications militaires

Sur le champ de bataille, MANET peut être déployé pour assurer la communication entre les soldats sur le terrain. Différentes unités militaires sont censées communiquer et coopérer les unes avec les autres dans une zone spécifiée. Dans ces types d'environnements à faible mobilité, MANET est utilisé pour les communications où pratiquement aucune infrastructure de réseau n'est disponible.

Commerce mobile

Les réseaux ad hoc peuvent être utilisés pour effectuer des paiements électroniques à tout moment, n'importe où. Les utilisateurs professionnels peuvent extraire de manière dynamique les informations relatives aux clients / aux ventes et créer des rapports à la volée.

Applications informatiques omniprésentes et embarquées

Avec l'émergence des nouvelles générations d'appareils mobiles portables intelligents, l'informatique omniprésente devient une réalité. Comme prédit par certains chercheurs (Weiser 1993), des ordinateurs omniprésents seront autour de nous, nous confiant toujours certaines tâches sans effort conscient. Ces machines réagiront également aux environnements changeants et fonctionneront en conséquence. Ces appareils mobiles formeront un réseau ad hoc, rassembleront diverses informations localisées et informeront parfois les utilisateurs automatiquement.

Services basés sur la localisation

MANET, lorsqu'il est intégré aux informations de localisation, fournit des services utiles. Le GPS (Global Positioning System), un système

de radionavigation par satellite, est un outil très efficace pour déterminer l'emplacement physique d'un appareil. Un hôte mobile dans un MANET connecté à un récepteur GPS sera en mesure de déterminer son emplacement physique actuel. Par exemple, un groupe de touristes utilisant des PDAs (Personal Digital Assistant) avec des cartes de réseau local sans fil installées avec une connectivité GPS peut former un MANET. Ces touristes peuvent ensuite échanger des messages et se localiser grâce à ce MANET. Les véhicules sur une autoroute peuvent former un réseau ad hoc pour échanger des informations sur la circulation. De plus, les services d'information basés sur la localisation peuvent être fournis par les MANETs. Par exemple, vous pouvez annoncer des informations spécifiques à un lieu, telles que des restaurants et des centres commerciaux (push), et récupérer des informations dépendantes de votre lieu, telles que des guides de voyage, des cinémas, des pharmacies, etc.

Réseau de capteurs

C'est un type particulier de réseau ad hoc hybride. Il existe un nombre croissant d'applications pratiques pour les capteurs minuscules dans diverses situations. Une fois déployés, ces dispositifs peu coûteux peuvent fournir des informations précises sur la température, les produits chimiques, les conditions environnementales critiques (par exemple, générer des alarmes d'incendie sauvage) et les comportements tels que les mouvements de certains animaux, etc. Les capteurs dotés d'applications RFID (Radio Frequency Identification) sont utilisés pour suivre les collectes d'inventaire et de péages. De plus, ces appareils peuvent également être utilisés pour des applications de sécurité. Cependant, une fois déployés, ces capteurs ont une puissance de batterie limitée et la durée de vie de la batterie peut déterminer la durée de vie du capteur.

1.5 Avantages et inconvénients

Les avantages des réseaux ad hoc

D'après (Dipobagio 2009), Il existe de nombreuses raisons pour lesquelles il vaut mieux utiliser des réseaux ad hoc que des réseaux infrastructures. La plus grande force de l'ad hoc est son indépendance vis-à-vis de toutes infrastructures. Par conséquent, il est possible d'établir un réseau ad hoc dans toutes les situations difficiles. Voici les avantages des réseaux ad hoc (Dipobagio 2009), (Bakshi *et al.* 2013) :

Aucune infrastructure et moindre coût

Il existe des situations dans lesquelles un utilisateur d'un système de communication ne peut pas s'appuyer sur une infrastructure. L'utilisation d'un service à partir d'une infrastructure peut être coûteuse pour des applications spécifiques. Dans une zone à très faible densité, comme le désert, la montagne ou une zone isolée, il n'est pas impossible d'établir une infrastructure. Mais si nous comparons la fréquence à laquelle les

gens utilisent le service d'infrastructure et le nombre de données transmises par jour avec le coût d'installation, de maintenance et de réparation, c'est peut-être trop cher. Presque le même problème avec le réseau militaire. Il est évidemment très inutile de construire une infrastructure sur un champ de bataille. Outre le coût d'installation, l'ennemi peut détruire l'infrastructure en peu de temps. Un réseau indépendant de l'infrastructure est nécessaire dans les deux cas.

Mobilité

Les nœuds mobiles sans fil peuvent se déplacer en même temps dans différentes directions. Bien que l'algorithme de routage puisse résoudre ce problème, les simulations de performances montrent qu'il existe un niveau de seuil de mobilité de nœud tel que le fonctionnement du protocole commence à échouer. Les exemples les plus courants sont les réseaux militaires, les opérations d'urgence / de sauvetage, les efforts en cas de catastrophe. Dans ces scénarios, nous ne pouvons pas compter sur une connectivité centralisée. Les MANET prennent en charge la mobilité des nœuds. Nous pouvons toujours communiquer avec nos appareils mobiles tant que la destination est accessible.

Décentralisé et robuste

Un autre avantage des réseaux ad hoc est qu'ils sont intrinsèquement très robustes. Imaginez que pour une raison quelconque, l'une des stations de base ne fonctionne pas. Dans ce cas, tous les utilisateurs de cette station de base perdront la connectivité à d'autres réseaux. Dans les réseaux ad hoc, vous pouvez éviter un tel problème. Si un nœud quitte le réseau ou ne fonctionne pas, vous pouvez toujours avoir une connectivité à d'autres nœuds et peut-être que vous pouvez utiliser ces nœuds pour effectuer plusieurs sauts de votre message vers les nœuds de destination, tant qu'il existe au moins un moyen d'accéder au nœud souhaité.

Routeur gratuit

Se connecter à Internet sans avoir besoin d'un routeur sans fil est le principal avantage de l'utilisation d'un réseau ad hoc. Pour cette raison, la gestion d'un réseau ad hoc peut être plus abordable que le réseau traditionnel, car nous n'avons pas le coût supplémentaire d'un routeur.

La vitesse

La création d'un réseau ad hoc à partir de zéro nécessite quelques modifications de paramètres et aucun matériel ou logiciel supplémentaire. Si vous avez besoin de connecter plusieurs ordinateurs rapidement et facilement, un réseau ad hoc est la solution idéale.

Tolérance aux pannes

MANET prend en charge les échecs de connexion, car les protocoles de routage et de transmission sont conçus pour gérer ces situations.

Connectivité

L'utilisation de points ou de passerelles centralisées n'est pas nécessaire pour la communication au sein du MANET, en raison de la collaboration entre les nœuds dans la tâche de livraison des paquets.

Installation rapide

Le niveau de flexibilité pour la mise en place de MANET est élevé, car ils ne nécessitent aucune installation ou infrastructure préalable et, par conséquent, ils peuvent être montés et démontés en très peu de temps.

Les inconvénients des réseaux ad hoc

Selon (Dipobagio 2009), la communication sans fil est très célèbre de nos jours, l'utilisation du sans fil peut améliorer l'apparence des pièces, car moins de câbles sont utilisés. La faiblesse de la liaison sans fil a un impact ad hoc. Un débit de données inférieur, une sécurité et un contrôle d'accès moyen sont des problèmes courants dans les communications sans fil. Voici les inconvénients des réseaux ad hoc.

Taux d'erreur plus élevé

Contrairement à la transmission filaire, la transmission sans fil peut résoudre le problème de la caractéristique de l'onde électronique. Dans une pièce libre sans obstacle l'onde électronique se propage linéairement indépendamment de sa fréquence. Il y a rarement une telle situation. L'obstacle provoque une ombre, une réflexion, une diffusion, un évanouissement, une réfraction, une diffraction de l'onde. Cette propagation peut conduire à des paquets transmis brouillés et donc reçus par erreur.

Débit de données inférieur

L'un des plus gros problèmes des réseaux ad hoc est la réduction des débits de données. La caractéristique de l'onde radio, qui est utilisée pour la communication sans fil, empêche la communication sans fil de transmettre des données mieux que la communication filaire. Une fréquence plus élevée peut transmettre plus de données, mais elle est alors plus vulnérable aux interférences et fonctionne bien à courte portée.

Topologie dynamique et évolutivité

Parce que les réseaux ad hoc ne permettent pas les mêmes types de techniques d'agrégation qui sont disponibles pour les protocoles de routage Internet standard, ils sont vulnérables aux problèmes d'évolutivité. Étant donné que les nœuds du MANET sont mobiles, le routage change au fur et à mesure que les nœuds se déplacent. Les informations de connectivité actuelles doivent être propagées à tous les participants du réseau. Les messages de contrôle doivent être envoyés fréquemment sur le réseau. Le nombre accru de messages de contrôle alourdit la bande passante disponible. Par conséquent, les protocoles ad hoc sont généralement conçus

pour réduire le nombre de messages de contrôle, par exemple en conservant les informations actuelles. Un bon algorithme pour les réseaux ad hoc doit être capable d'évaluer et de comparer l'évolutivité relative des réseaux face à l'augmentation du nombre de nœuds et de la mobilité des nœuds. Il est très important de savoir combien de messages de contrôle sont nécessaires. Nous pouvons donc contrôler l'utilisation de la bande passante.

Sécurité

En raison de la nature dynamique sans infrastructure distribuée et du manque de points de surveillance centralisés, les réseaux ad hoc sont vulnérables à divers types d'attaques. Contrairement au canal filaire, le canal sans fil est accessible à la fois aux utilisateurs légitimes du réseau et à l'attaquant malveillant. Par conséquent, les réseaux ad hoc sont sensibles aux attaques allant des attaques passives telles que l'écoute du trafic de routage à des attaques actives telles que les interférences. Surtout pour MANET, la consommation d'énergie et les capacités de calcul limitées, en raison de la limitation de l'énergie, empêchent d'exécuter des algorithmes lourds de calcul comme les algorithmes à clé publique. D'autres problèmes de sécurité, tels que la disponibilité, l'authenticité, l'intégrité, la confidentialité et la vie privée, sont discutés dans (Vanhala 2000). Plus de détails sont expliqués dans la section «La sécurité dans les réseaux mobiles ad hoc».

Limitation d'énergie

Un réseau MANET permet aux nœuds mobiles de communiquer en l'absence d'infrastructure fixe. Par conséquent, ils fonctionnent avec une alimentation par batterie. En raison de ces limitations, ils doivent disposer d'algorithmes économes en énergie et fonctionnent avec des ressources de traitement et de mémoire limitées. L'utilisation de la bande passante disponible sera limitée car les nœuds peuvent ne pas être en mesure de sacrifier l'énergie consommée en fonctionnant à pleine vitesse de liaison. C'est aussi très ennuyeux, lors de la réception de données de quelqu'un avec PDA, la batterie est presque épuisée. Il est nécessaire de répéter le processus de transfert après la recharge. Par conséquent, un MANET ne convient pas pour un réseau permanent.

1.6 Le routage dans les réseaux ad hoc

1.6.1 Définition du routage

Le routage est un processus qui sélectionne les chemins par lesquels les unités de données de protocole PDU (Protocol Data Unit), appelées paquets, se propagent de la source à la destination. C'est la fonction principale de la couche réseau dans les architectures de protocole ISO/OSI et TCP/IP (Kabeto 2000).

Les deux fonctions principales effectuées par un algorithme de routage sont : la sélection de routes pour diverses paire origine-destination et la

remise des messages à leur destination correcte une fois que les routes sont sélectionnées. La deuxième fonction est conceptuellement simple en utilisant une variété de protocoles et de structures de données (appelées tables de routage) (Bertsekas & Gallager 1992).

Selon (Yang & Wang 2008), Un protocole de routage se compose de deux composants : un algorithme de calcul de chemin et un schéma de transfert de paquets. Cependant, il existe trois algorithmes de calcul de chemin : la découverte d'itinéraire basée sur les inondations, l'algorithme de Dijkstra et l'algorithme Bellman-Ford, qui sont tous largement utilisés dans le routage sans fil. Dans la découverte d'itinéraire basée sur l'inondation, pour rechercher un chemin vers un nœud de destination, un nœud source inonde un message de demande d'itinéraire à travers l'ensemble du réseau pour explorer plusieurs chemins simultanément et le nœud de destination sélectionne un seul chemin parmi tous les chemins recherchés comme chemin entre le nœud source et le nœud de destination. Dans l'algorithme de Dijkstra ou l'algorithme de Bellman-Ford, un nœud source collecte des informations de topologie du réseau via des échanges de messages périodiques entre les nœuds voisins. Sur la base des informations collectées, le nœud source calcule ses chemins vers les autres nœuds. Ainsi, dans les réseaux sans fil, deux schémas de transfert de paquets sont souvent utilisés dans différents protocoles de routage, le routage source et le routage saut par saut. Dans le routage source, un nœud source place le chemin complet d'un flux dans ses en-têtes de paquet et les nœuds intermédiaires transmettent les paquets en conséquence. Dans le routage saut par saut, un nœud source met uniquement les adresses de destination dans ses en-têtes de paquet. Un nœud intermédiaire transmet les paquets en fonction de sa table de routage, qui stocke les prochains sauts pour atteindre chaque adresse de destination.

D'après (Bertsekas & Gallager 1992), le routage dans un réseau implique généralement un ensemble assez complexe d'algorithmes qui fonctionnent de manière plus ou moins indépendante, tout en se supportant mutuellement par l'échange de services ou d'informations. La complexité est due à un certain nombre de raisons. Premièrement, le routage nécessite une coordination entre tous les nœuds du réseau. Deuxièmement, le système de routage doit faire face aux défaillances des liaisons et des nœuds, ce qui nécessite une redirection du trafic et une mise à jour des informations du routage. Troisièmement, pour obtenir des performances élevées, l'algorithme de routage peut avoir besoin de modifier ses routes lorsque certaines zones du réseau deviennent encombrées.

1.6.2 Les problèmes rencontrés par un protocole de routage

Les principaux problèmes rencontrés par un protocole de routage sont les suivants(Murthy & Manoj 2004) :

Mobilité

L'une des propriétés les plus importantes des réseaux sans fil ad hoc est la mobilité associée aux nœuds. La mobilité des nœuds entraîne des ruptures de chemin fréquentes, des collisions de paquets, des boucles tran-

sitoires, des informations de routage obsolètes et des difficultés de réservation des ressources.

Contrainte de bande passante

Le canal étant partagé par tous les nœuds de la région de diffusion (toute région dans laquelle tous les nœuds peuvent entendre tous les autres nœuds), la bande passante disponible par liaison sans fil dépend du nombre de nœuds et du trafic qu'ils traitent. Ainsi, seule une fraction de la bande passante totale est disponible pour chaque nœud.

Canal partagé et sujet aux erreurs

Le taux d'erreur sur les bits dans un canal sans fil est très élevé (de l'ordre de 10^{-5} à 10^{-3}) par rapport à celui de ses homologues câblés (de l'ordre de 10^{-12} à 10^{-9}). Les protocoles de routage conçus pour les réseaux sans fil ad hoc devraient en tenir compte. La prise en compte de l'état de la liaison sans fil, du rapport signal sur bruit et de la perte de chemin pour le routage dans les réseaux sans fil ad hoc peut améliorer l'efficacité du protocole de routage.

Conflit dépendant de l'emplacement

La charge sur le canal sans fil varie en fonction du nombre de nœuds présents dans une région géographique donnée. Cela alourdit le conflit pour le canal lorsque le nombre de nœuds augmente. La forte contention pour le canal entraîne un nombre élevé de collisions et un gaspillage ultérieur de bande passante. Un bon protocole de routage devrait comporter des mécanismes intégrés permettant de répartir la charge du réseau de manière uniforme sur l'ensemble du réseau, de manière à éviter la formation de régions où la contention des canaux est élevée.

Autres contraintes de ressources

Les contraintes sur les ressources telles que la puissance de calcul, la charge de la batterie et le stockage en mémoire-tampon limitent également la capacité d'un protocole de routage.

1.6.3 Les exigences d'un protocole de routage

Les principales exigences d'un protocole de routage dans les réseaux sans fil ad hoc sont les suivantes (Murthy & Manoj 2004) :

Délai d'acquisition de la route

Le délai d'acquisition de la route pour un nœud qui n'a pas de route vers un nœud de destination particulier doit être aussi minime que possible. Ce délai peut varier en fonction de la taille du réseau et de la charge du réseau.

Reconfiguration rapide de la route

Les changements imprévisibles de la topologie du réseau exigent que le protocole de routage soit capable d'effectuer rapidement une reconfiguration de route afin de gérer les ruptures de chemin et les pertes de paquets ultérieures.

Routage sans boucle

Il s'agit d'une exigence fondamentale de tout protocole de routage afin d'éviter un gaspillage inutile de la bande passante du réseau. Dans les réseaux sans fil ad hoc, en raison du mouvement aléatoire des nœuds, des boucles transitoires peuvent se former dans la route ainsi établie. Un protocole de routage devrait détecter ces boucles de routage transitoires et prendre des mesures correctives.

Approche de routage distribué

Un réseau sans fil ad hoc est un réseau sans fil entièrement distribué et l'utilisation des approches de routage centralisées dans un tel réseau peut consommer une grande quantité de bande passante.

Surcharge de contrôle

Les paquets de contrôle échangés pour trouver une nouvelle route et maintenir les routes existantes doivent être maintenus minime que possible. Les paquets de contrôle consomment une bande passante précieuse et peuvent provoquer des collisions avec des paquets de données, réduisant ainsi le débit du réseau.

Évolutivité

L'évolutivité est la capacité du protocole de routage à s'adapter correctement (c'est-à-dire à fonctionner efficacement) dans un réseau comportant un grand nombre de nœuds. Cela nécessite une réduction de la surcharge de contrôle et une adaptation du protocole de routage à la taille du réseau.

fourniture de la qualité de service

Le protocole de routage devrait être en mesure de fournir un certain niveau de qualité de service (QoS) demandé par les nœuds ou la catégorie du flux. Les paramètres de QoS peuvent être la bande passante, le délai, le rapport de livraison des paquets et le débit.

Sécurité et confidentialité

Le protocole de routage dans les réseaux sans fil ad hoc doit être résilient aux menaces et aux vulnérabilités. Il doit disposer d'une fonctionnalité intégrée permettant d'éviter la consommation de ressources, le déni de service, l'usurpation d'identité et les attaques similaires possibles contre un réseau sans fil ad hoc.

1.6.4 Classification des protocoles de routages

Plusieurs protocoles de routages sont proposés pour les réseaux mobiles ad hoc. Ces protocoles peuvent être classés en trois catégories : routage proactif, routage réactif et routage hybride.

Les protocoles de routage proactifs

Les protocoles proactifs sont directement inspirés des protocoles de routage déployés sur Internet et sont donc des adaptations du routage à l'état des liens et des routages à vecteur de distance. Leur caractéristique commune est que chaque nœud de réseau ad hoc maintient localement une table de routage pour envoyer des données à n'importe quel nœud du réseau. Avec ces protocoles, les terminaux échangent périodiquement des informations au-delà de leur voisinage direct pour maintenir en permanence des «tables» décrivant le réseau, totalement ou partiellement, afin de décider des itinéraires à emprunter lors de la transmission des messages ; ils sont parfois appelés routage ad hoc piloté par table. Selon la fréquence de mise à jour des tables d'informations, ou la fréquence de transmission des messages de mise à jour, ces tables reflètent assez fidèlement l'état du réseau. Si la fréquence est plus élevée, alors le protocole a une meilleure chance de résister à la dynamique du réseau, mais d'un autre côté, lorsque cette fréquence de mise à jour est plus élevée, alors la bande passante utilisée pour ces messages de contrôle est plus grande et n'est donc pas disponible pour les transmissions de données (Ubéda 2008).

Les protocoles de routage réactifs

Les algorithmes de routage réactif ad hoc réduisent au minimum l'utilisation des messages de contrôle pour économiser la bande passante. Les informations vitales pour le calcul d'une route entre deux nœuds du réseau ne sont recherchées que lorsqu'une demande pour cette route est exprimée par les couches de protocole supérieures. Les protocoles de cette classe tentent de garder les routes utilisées et uniquement celles aussi à jour que possible. La quantité de bande passante utilisée pour les messages de contrôle est particulièrement sensible au nombre de routes (implémentation et maintenance) et peut-être bien inférieure à un protocole proactif lorsque ce nombre est inférieur. L'inconvénient majeur de ce type de protocole est le délai important nécessaire entre une demande de transmission de message et la transmission effective lorsque la route n'a pas encore été créée (Ubéda 2008).

Les protocoles de routage hybrides

Les protocoles de routage hybrides combinent les techniques utilisées dans les deux protocoles de routage proactif et réactif pour générer les routes entre les nœuds. Dans ce type de protocole, le réseau est partitionné en plusieurs zones. Ainsi, dans le cas où les nœuds voisins à une certaine distance proche dans la zone prédéfinie, les fonctionnalités des protocoles proactifs sont utilisées. Si les nœuds voisins sont éloignés de cette zone, les

fonctionnalités des protocoles réactifs sont utilisées. Cependant, les protocoles hybrides héritent également un certain nombre d'inconvénients des protocoles réactifs et proactifs.

1.7 La sécurité dans les réseaux mobiles ad hoc

La sécurisation des réseaux mobiles ad hoc est très difficile et complexe dû aux caractéristiques des réseaux mobiles ad hoc tels que la liberté de déplacement, la mobilité et l'auto-organisation des nœuds. Autrement dit, les nœuds eux-mêmes prennent la charge d'exécuter toutes les fonctions possibles au sein d'un réseau tel que l'envoi, la réception, le transfert des paquets, ainsi que toutes les tâches qui sont exigées par le protocole de routage mis en réseau. Cependant, puisque les seuls moyens physiques de communiquer entre les nœuds sont les interfaces sans fil et dû aux caractéristiques des ondes radio, les paquets transmis par les nœuds sont toujours en danger extérieur par d'autres nœuds en dehors du réseau et même par des nœuds malveillants dans le même réseau.

1.7.1 Les critères de sécurité

Les critères de sécurité les plus utilisés sont discutés dans plusieurs recherches (Zhou & Haas 1999; Rachedi 2008). Les réseaux mobiles ad hoc sont très sensibles à la sécurité. Afin d'évaluer la sécurité des réseaux ad hoc, il est très important de garantir certains critères comme : la disponibilité, la confidentialité, l'intégrité, l'authentification et la non-répudiation, voici leurs explications :

La disponibilité

La disponibilité permet de garantir que l'accès et la fourniture des services mise en réseau sont assurés pour tous les nœuds participant à la communication dans le réseau à tout moment et au bon moment malgré la présence des attaques par déni de service.

La confidentialité

Les nœuds autorisés sont les seules à accéder aux informations confidentielles. Dans certaines situations, les informations sensibles ne sont pas divulguées aux nœuds non autorisés à accèdes aux informations communiquées dans le réseau. La confidentialité garantit aussi que les informations du routage doivent rester confidentielles dans certains cas. Ce qui assure que les nœuds malveillants ne doivent jamais avoir la possibilité d'écouter ou d'accéder à ces informations. L'utilisation des techniques de la cryptographie peut garantir la confidentialité.

L'intégrité

L'intégrité garantit que les messages communiqués ne sont pas modifiés, dupliqués ou altérés par des nœuds non autorisés. Dans certains cas, un message peut être corrompu à défaut de réduction de la propagation

des ondes radio, l'intégrité assure aussi que les messages ne sont jamais corrompus durant leurs transmissions. L'utilisation des techniques de la cryptographie et le hachage peuvent garantir l'intégrité.

L'authentification

Permet au nœud de s'assurer de l'identité du nœud avec lequel il communique. En effet, s'il y a un défaut dans l'authentification, un nœud malveillant peut prend le rôle d'un nœud légitime et effectué un accès non autorisé à des ressources sensibles et peut injecter des faux messages.

Non-répudiation

La non-répudiation garantit que l'émetteur d'un message ne peut pas nier qu'il soit l'origine de l'envoi de ce message. La non-répudiation est utile pour la détection et l'isolation des nœuds compromis. La technique du certificat électronique peut garantir la non-répudiation. Certains objectifs de sécurité utilisée dans l'analyse des aspects de sécurité réseau mobile Ad hoc tels que : l'autorisation d'accès, le contrôle d'accès, et autres objectifs sont expliqués dans (Rachedi 2008).

1.7.2 Vulnérabilités des réseaux mobiles ad hoc

La vulnérabilité a été discutée dans plusieurs recherches (Li & Joshi 2008; Jadye 2016; Kumar 2011; Aluvala *et al.* 2016). En général, le réseau ad hoc mobile est par nature peu sûr : il n'existe pas de ligne de défense aussi claire en raison de la liberté des nœuds de se joindre, de quitter et de se déplacer à l'intérieur du réseau ; certains des nœuds peuvent être compromis par l'adversaire et par conséquent avoir des comportements malveillants difficiles à détecter ; L'absence de mécanisme centralisé peut poser problème lorsqu'il est nécessaire de disposer d'un tel coordonnateur centralisé ; une alimentation électrique limitée peut causer des problèmes égoïstes et l'évolution constante de l'échelle du réseau a imposé des exigences plus élevées en matière d'évolutivité des protocoles et des services du réseau mobile ad hoc. En conséquence, par rapport au réseau câblé, le réseau mobile ad hoc aura besoin d'un système de sécurité plus robuste pour en assurer la sécurité (Li & Joshi 2008).

Une vulnérabilité est une faiblesse du système de sécurité. Un système particulier peut être vulnérable à la manipulation de données non autorisée car le système ne vérifie pas l'identité d'un utilisateur avant d'autoriser l'accès aux données. Certaines de ces vulnérabilités sont les suivantes (Kumar 2011) :

Absence de gestion centralisée

MANET n'a pas de serveur de surveillance centralisé. L'absence de gestion rend la détection difficile des attaques car il n'est pas orienté de surveiller le trafic dans un réseau ad hoc très dynamique et à grande échelle. L'absence de gestion centralisée entravera la gestion de la confiance pour les nœuds.

Disponibilité des ressources

La disponibilité des ressources est un problème majeur dans MANET. Assurer une communication sécurisée dans un environnement aussi changeant, ainsi qu'une protection contre des menaces et des attaques spécifiques, conduit au développement de divers schémas et architectures de sécurité. Les environnements de collaboration ad hoc permettent également la mise en œuvre des mécanismes de sécurité auto-organisés.

Evolutivité

En raison de la mobilité des nœuds, l'échelle du réseau ad hoc change constamment. L'évolutivité est donc un problème majeur en matière de sécurité. Le mécanisme de sécurité doit être capable de gérer un réseau aussi bien grand que petit.

Coopérativité

L'algorithme de routage pour les MANETs suppose généralement que les nœuds sont coopératifs et non malveillants. En conséquence, un attaquant malveillant peut facilement devenir un agent de routage important et perturber le fonctionnement du réseau en désobéissant aux spécifications du protocole.

Topologie dynamique

La topologie dynamique et l'appartenance à des nœuds modifiables peuvent perturber la relation de confiance entre les nœuds. La confiance peut également être perturbée si certains nœuds sont détectés comme étant compromis. Ce comportement dynamique pourrait être mieux protégé avec des mécanismes de sécurité distribués et adaptatifs.

Alimentation électrique limitée

Les nœuds du réseau ad hoc mobile doivent prendre en compte une alimentation restreinte, ce qui posera plusieurs problèmes. Un nœud du réseau ad hoc mobile peut se comporter de manière égoïste lorsqu'il est constaté que l'alimentation est limitée.

1.7.3 Classification des attaques

Les réseaux ad hoc souffrent de certaines vulnérabilités et attaques (Lundberg 2000). Les attaques peuvent être subdivisées en deux catégories possibles ($figure$1.3, $figure$1.4) : les attaques passives, lorsque l'attaquant tente uniquement de découvrir des informations précieuses en écoutant le trafic de routage ; les attaques actives, qui se produisent lorsque l'attaquant injecte des paquets arbitraires dans le réseau dans le but, la désactivation du réseau par exemple. Dans la littérature, plusieurs façons sont envisagées pour classer les attaques (Ait-Salem 2011; Murthy & Manoj 2004; Bhattacharyya *et al.* 2011; Monnet 2015; Mishra & Nadkarni 2003). Ces attaques sont détaillées comme suit :

Attaques passives

Les attaques passives impliquent une «écoute» non autorisée des paquets de routage. L'attaque pourrait être une tentative d'obtenir des informations de routage à partir desquelles l'attaquant pourrait extrapoler des données sur les positions de chaque nœud par rapport aux autres. Les attaques passives incluent les canaux secrets, l'analyse du trafic, le reniflement pour compromettre les clés, etc. Par exemple, un attaquant qui écoute toutes les mises à jour de routage transmises dans une certaine partie du réseau ad hoc peut commencer à reconstituer quels nœuds sont proches les uns des autres (à un ou deux sauts) et quels nœuds sont éloignés les uns des autres (de nombreux sauts) (Mishra & Nadkarni 2003).

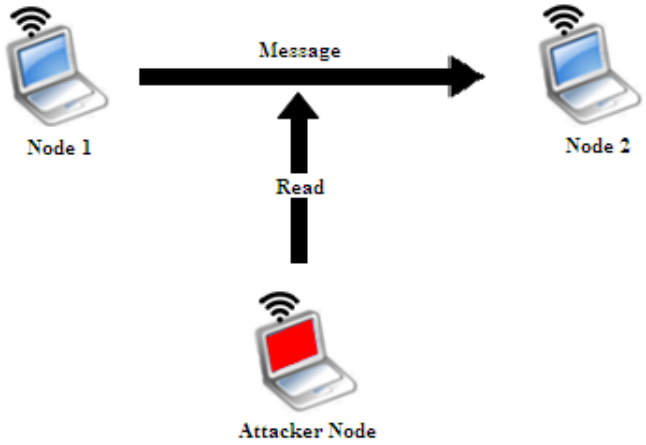

FIGURE 1.3 – *L'attaque passive*

Une attaque passive ne perturbe pas le fonctionnement du réseau ; l'adversaire récupère les données échangées sur le réseau sans les modifier. Ici, l'exigence de confidentialité peut être violée si un adversaire est également capable d'interpréter les données recueillies par surveillance. Généralement l'attaque passive implique uniquement d'écouter le trafic de routage pour découvrir des informations précieuses. Il est difficile de détecter les attaques passives car de telles attaques ne détruisent pas les opérations des protocoles de routage et le fonctionnement du réseau lui-même n'est pas affecté. Un moyen de surmonter ces problèmes consiste à utiliser des mécanismes de cryptage puissants pour crypter les données en cours de transmission, empêchant ainsi les oreilles indiscrètes d'obtenir des informations utiles à partir des données saisies. L'autre moyen consiste à transmettre des parties d'un message sur plusieurs chemins disjoints et à les réassembler à la destination (Mishra & Nadkarni 2003; Murthy & Manoj 2004; Wang & Tseng 2007; Karlof & Wagner 2003; Chan & Perrig 2003; Burgod 2009).

Attaques actives

Les attaques actives impliquent des actions effectuées par des adversaires, par exemple, la réplication, la modification et la suppression des données échangées. Les adversaires tentent activement de changer le com-

portement du protocole dans les attaques actives tandis que les adversaires sont subtils dans leurs activités dans les attaques passives. Les informations divulguées par inadvertance aux attaquants passifs par les paquets de protocole peuvent être utilisées pour lancer des attaques actives. Les attaques actives sur le réseau à partir de sources extérieures sont destinées à dégrader ou à empêcher le flux de messages entre les nœuds. Les attaques externes actives sur le protocole de routage ad hoc peuvent être décrites collectivement comme des attaques par déni de service, provoquant une dégradation ou un arrêt complet de la communication entre les nœuds. Un type d'attaque implique l'insertion de paquets étrangers dans le réseau afin de pouvoir utiliser la congestion. Une méthode d'attaque plus subtile consiste à intercepter un paquet de routage, à modifier son contenu et à le renvoyer dans le réseau. L'attaquant peut également choisir de ne pas modifier le contenu du paquet mais plutôt de le rejouer sur le réseau à des moments différents, en introduisant des informations de routage obsolètes vers les nœuds. Le but de cette forme d'attaque est de confondre les nœuds de routage avec des informations contradictoires, retardant les paquets ou les empêchant d'atteindre leur destination. Pour effectuer une attaque active, l'attaquant doit être capable d'injecter des paquets arbitraires dans le réseau. Le but peut être d'attirer des paquets destinés à d'autres nœuds vers l'attaquant pour analyse ou simplement de désactiver le réseau. Une attaque active peut parfois être détectée, ce qui fait des attaques actives une option moins invitante pour la plupart des attaquants (Mishra & Nadkarni 2003).

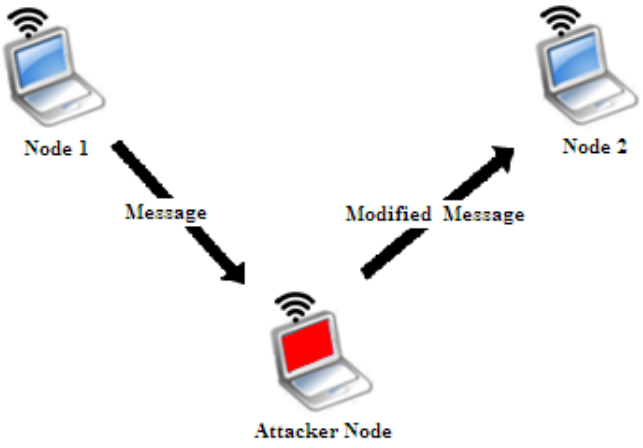

FIGURE 1.4 – *L'attaque active*

Une attaque active peut tenter de perturber le mécanisme de routage, de modifier intentionnellement les messages de routage, d'obtenir une authentification ou une autorisation ou même de contrôler l'ensemble du réseau en générant de faux paquets dans le réseau ou en modifiant ou en supprimant des paquets légitimes envoyés par d'autres nœuds. Les attaques actives peuvent être subdivisées en attaques externes et internes (Wang & Tseng 2007), comme illustrer sur la *figure*1.5.

Attaques externes

Les attaques externes sont généralement des attaques actives ciblées, par exemple pour provoquer une congestion, propager des informations de routage incorrectes, empêcher les services de fonctionner correctement ou les arrêter complètement. Les attaques externes peuvent généralement être évitées en utilisant des mécanismes de sécurité standard tels que les pare-feu, le chiffrement, etc (Mishra & Nadkarni 2003).

Attaques internes

Les attaques internes sont généralement des attaques plus graves, car les nœuds internes malveillants appartiennent déjà au réseau en tant que parties autorisées et sont donc protégés par les mécanismes de sécurité offerts par le réseau et ses services. Ainsi, ces initiés malveillants, qui peuvent même opérer dans un groupe, peuvent utiliser les moyens de sécurité standard pour protéger réellement leurs attaques. Une attaque interne est une menace grave pour les réseaux ad hoc. L'attaque peut diffuser des informations de routage erronées vers d'autres nœuds du réseau. Un nœud compromis est classé comme une attaque interne. La détection de telles informations erronées dans les informations de routage est difficile car les nœuds compromis sont capables de générer des signatures valides à l'aide de leurs clés privées. La distinction entre un attaquant réel et un changement de topologie peut également être problématique car la topologie du réseau ad hoc change de manière dynamique (Mishra & Nadkarni 2003).

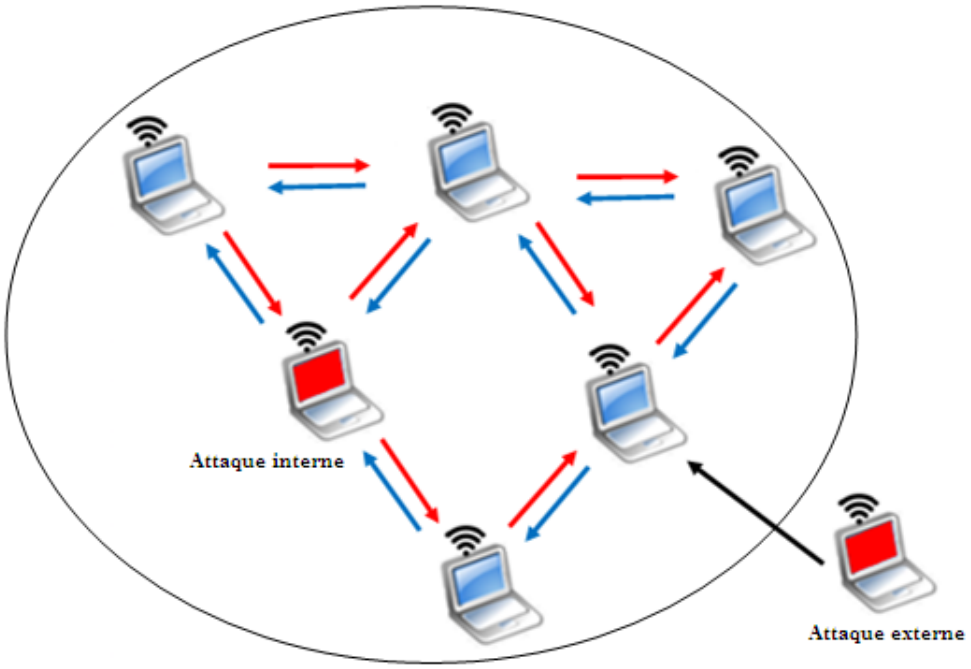

FIGURE 1.5 – *L'attaque interne et l'attaque externe*

1.7.4 Les principales attaques

Les attaques sur un protocole de routage de réseau ad hoc appartiennent généralement à l'une des deux catégories suivantes : attaques de perturbation ou d'interruption de routage et attaques de consommation de ressources. Dans la première catégorie des attaques, l'attaquant tente de faire acheminer des paquets de données légitimes de manière dysfonctionnelle. Dans la deuxième catégorie des attaques, l'attaquant injecte des paquets dans le réseau afin de consommer des ressources réseau précieuses telles que la bande passante ou des ressources de nœud telles que la mémoire (stockage) ou la puissance de calcul. Du point de vue de la couche d'application, les deux attaques sont des instances d'attaque par déni de service (DoS) (Hu *et al.* 2005).

Dans cette section, nous exposons quelques attaques spécifiques contre le routage dans les réseaux ad hoc, telles que : l'attaque trou noir (Blackhole Attack), l'attaque trou gris (Greyhole Attack), l'attaque trou de ver (Wormhole Attack), l'attaque précipitée (Rushing Attack) et l'attaque par déni de service (DoS attack pour Denial of Service attack).

L'attaque trou noir (Blackhole attack)

Un trou noir est un nœud malveillant qui répond faussement à toute requête de route RREQ (Route Request) sans avoir de route active vers la destination spécifiée et abandonne tous les paquets de réception (Vishnu *et al.* 2010). Dans cette attaque, un nœud malveillant utilise le protocole de routage pour s'annoncer comme ayant le chemin le plus court vers le nœud dont il veut intercepter les paquets (Deng *et al.* 2002) (*figure*1.6).

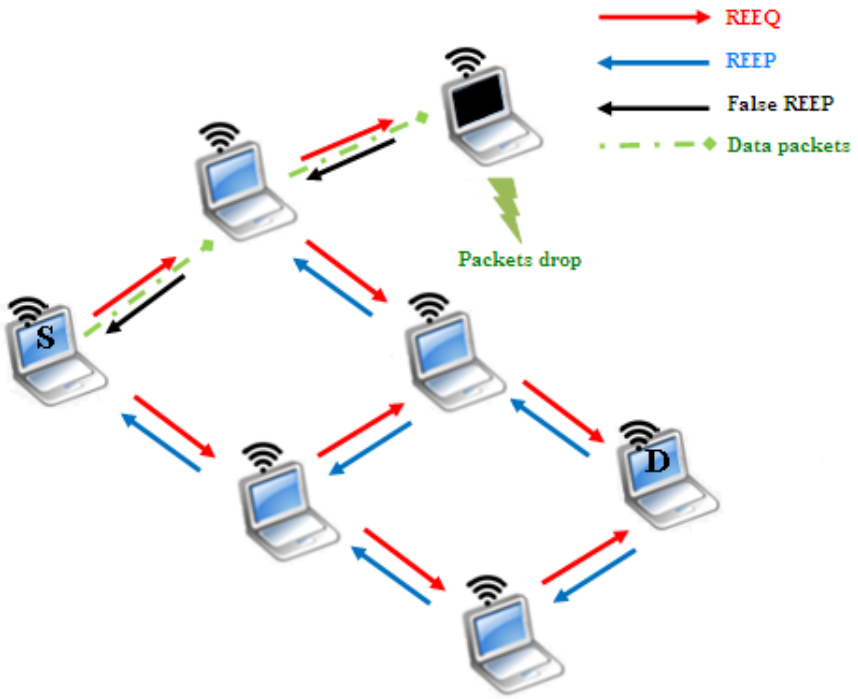

FIGURE 1.6 – *L'attaque trou noir*

Un attaquant peut également créer un trou noir de routage, dans lequel tous les paquets sont rejetés : en envoyant des paquets de routage falsifiés, l'attaquant pourrait router tous les paquets pour une destination donnée vers lui-même, puis les ignorer (Hu *et al.* 2005). Si ces nœuds malveillants travaillent ensemble en tant que groupe, les dégâts seront très graves. Ce type d'attaque s'appelle l'attaque coopérative par trou noir (Vishnu *et al.* 2010) (*figure*1.7).

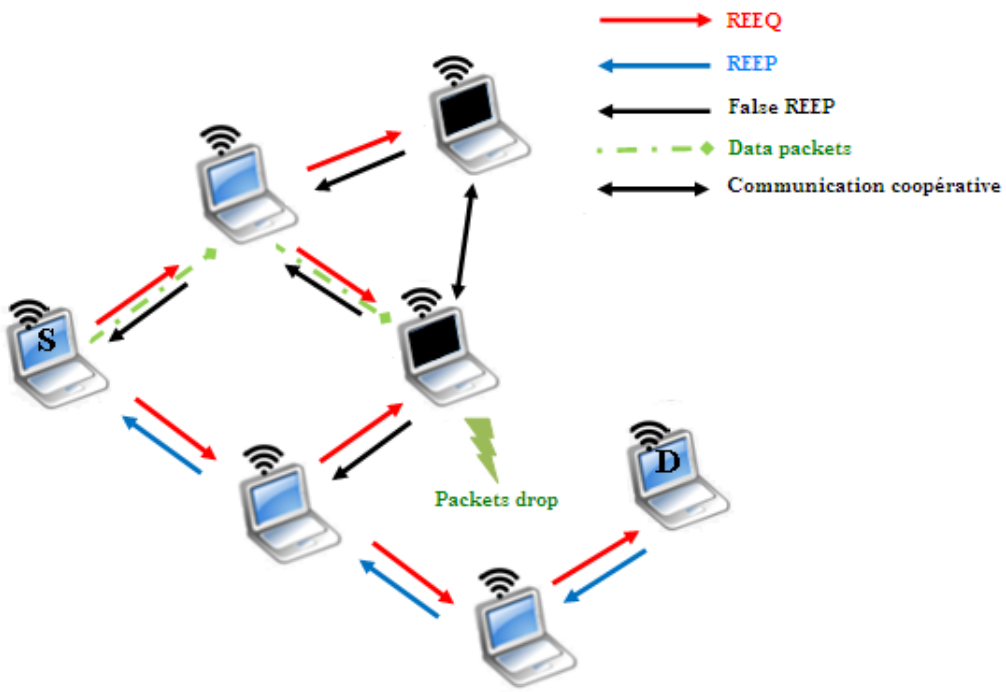

FIGURE 1.7 – *L'attaque coopérative par trou noir*

L'attaque trou gris (Greyhole Attack)

Une attaque trou gris est une variante de l'attaque trou noir, où le nœud malveillant n'est pas initialement malveillant, il le devient un peu plus tard (Vishnu *et al.* 2010). Un attaquant pourrait créer un trou gris, dans lequel il éliminera sélectivement certains paquets mais pas d'autres, par exemple, les paquets de routage mais pas les paquets de données (Hu *et al.* 2005).

L'attaque par trou de ver (Wormhole Attack)

Dans cette attaque, un attaquant enregistre un paquet, ou des bits individuels d'un paquet, à un emplacement du réseau, tunnels le paquet (éventuellement sélectivement) vers un autre emplacement et le rejoue à cet endroit. L'attaque par trou de ver peut constituer une menace sérieuse dans les réseaux sans fil, en particulier contre de nombreux protocoles de routage dans le réseau ad hoc et les systèmes de sécurité sans fil basé sur la localisation (Hu *et al.* 2003a). Un type d'attaque de perturbation de routage plus subtil est la création d'un trou de ver dans le réseau (Hu *et al.* 2003a), utilisant une paire de nœuds attaquants A et B reliés via

une connexion réseau privée. Chaque paquet que A reçoit du réseau ad hoc, le transfère à travers le trou de ver à B pour être ensuite rediffusé par B ; de la même façon, B peut envoyer tous les paquets de réseau ad hoc à A. Une telle attaque perturbe potentiellement le routage en court-circuitant le flux normal de paquets de routage et les attaquants peuvent également créer une coupe de sommet virtuelle qu'ils contrôlent (Hu *et al.* 2005). L'attaquant peut ensuite exploiter le trou de ver pour rejeter tous les paquets de données au lieu de les transmettre, ce qui crée une attaque permanente par déni de service (aucune autre route menant à la destination ne peut être découverte tant que l'attaquant maintient le trou de ver pour les paquets RREQ), ou la suppression ou la modification sélective de certains paquets de données (Hu *et al.* 2003a).

L'attaque précipitée (Rushing Attack)

L'attaque précipitée (rushing attack) est une attaque malveillante qui cible les protocoles de routage à la demande qui utilisent la suppression des doublons sur chaque nœud. Un attaquant diffuse rapidement les demandes de routage sur l'ensemble du réseau, supprimant toute demande de routage légitime ultérieure lorsque les noeuds les abandonnent en raison de la suppression des doublons (Hu *et al.* 2005).

Un attaquant précipitant plus puissant peut employer un trou de ver (Hu *et al.* 2003a) pour précipiter les paquets. Dans ce cas, l'attaquant transmet simplement tous les paquets de contrôle (mais pas les paquets de données) reçus sur un nœud (l'attaquant) vers un autre nœud du réseau (par exemple, un deuxième attaquant). Cela forme un tunnel dans le réseau, où les paquets atteignant une extrémité du tunnel sont diffusés à l'autre extrémité. Si le tunnel assure un transit beaucoup plus rapide que les transitaires légitimes, les nœuds situés à une extrémité du tunnel ne pourront généralement pas découvrir les itinéraires actifs vers l'autre extrémité du tunnel, car ils découvriront généralement les itinéraires empruntant le tunnel. En général, un tunnel câblé (dans lequel les deux attaquants ont une connexion câblée entre eux) assurera un transit plus rapide que le transfert sans fil natif (multi-sauts), car le délai de traitement des noeuds dans la transmission est beaucoup plus long que le temps de propagation (Hu *et al.* 2003b).

Attaque par déni de service (DoS Attack)

L'attaque DoS survient lorsque la bande passante du réseau est détournée par un nœud malveillant. Il se présente sous de nombreuses formes : la méthode classique consiste à inonder toute ressource centralisée afin que le réseau ne fonctionne plus correctement ou ne se bloque plus. Par exemple, une demande de route est générée chaque fois qu'un nœud doit envoyer des données à une destination particulière. Un nœud malveillant peut générer de fréquentes demandes de route inutiles pour rendre les ressources réseau indisponibles pour les autres nœuds (Deng *et al.* 2002).

Conclusion

Dans ce chapitre nous avons exposé les réseaux mobiles ad hoc comme un grand champ d'études relier par les recherches conçues pour les développements technologiques et les techniques de communication. Nous avons présenté les concepts et les notions conçus pour les réseaux mobiles ad hoc, détaillé leurs modélisations, leurs principales caractéristiques et applications, examiné certains de leurs avantages et inconvénients, expliqué le routage et les différents protocoles de routage aperçus dans la littérature, discuté la sécurité dans les réseaux mobiles ad hoc et exposé les attaques au sein de ces réseaux. Le chapitre suivant détail les protocoles de routage multi-chemins dans les réseaux mobiles ad hoc.

Les protocoles de routage multi-chemins dans les MANETs

2

Sommaire

Introduction

Durant les récentes années, les réseaux mobiles ad hoc ont connu de plus en plus d'importance avec le développement des technologies sans fil et leurs utilisations dans les dispositifs mobiles afin de satisfaire les besoins d'échanger, de communiquer, de transmet et de partager les données dans les réseaux mobiles. D'après (Zhang & Zhou 2003) un réseau ad hoc est un ensemble de nœuds mobiles sans fil forment dynamiquement un réseau local ou un autre réseau temporaire sans utiliser aucune infrastructure de réseau existante ni aucune administration centralisée. Les réseaux ad hoc peuvent être formés, fusionnés ou partitionnés en réseaux distincts, sans nécessairement s'appuyer sur une infrastructure fixe pour gérer l'opération. Chaque nœud mobile fonctionne non seulement en tant qu'hôte, mais également en tant que routeur, en envoyant et en transmettant des paquets à d'autres nœuds mobiles du réseau qui peuvent ne pas se trouver dans la portée de transmission sans fil direct les uns des autres. Chaque nœud du réseau est conforme à un protocole de routage ad hoc lui permettant de découvrir des chemins à sauts multiples, ce qui signifie qu'un paquet d'un nœud source à un nœud de destination peut transiter par plusieurs nœuds du réseau. Cependant, le routage détient un rôle indispensable dans l'établissement des liens de communications et l'acheminement des paquets de données entre les nœuds dans les réseaux mobiles ad hoc.

Plusieurs protocoles de routage ont été proposés dans la littérature et peuvent être subdivisés en deux classes à savoir les protocoles à chemin unique et à multi-chemins. Les protocoles de routage à chemin unique cherchent à construire un seul chemin valide entre les nœuds source et destination à travers des nœuds intermédiaires. Les exemples des protocoles de routage à chemins uniques les plus connues sont : AODV (Perkins & Royer 1999; Perkins *et al.* 2003), DSR (Johnson 1994; Johnson & Maltz 1996; Johnson *et al.* 2007), DSDV (Perkins & Bhagwat 1994). Alors que, les protocoles de routage multi-chemins cherchent à construire plusieurs chemins valident entre les nœuds source et destination. Les exemples des protocoles de routage à chemins multiples sont : AOMDV (Marina 2001; Marina 2006), AODVM (Ye *et al.* 2003), AODV-BR (Lee & Gerla 2000), SMR (Lee & Gerla 2001), SMORT (Reddy & Raghavan 2007), CHAMP (Valera *et al.* 2003).

Après cette introduction, ce chapitre est organisé comme suite : nous évoquons les composants de base des protocoles de routage multi-chemins, nous discutons ainsi, la découverte de routes, la maintenance de routes et l'allocation du trafic. Puis nous présentons une synthèse des principaux avantages du routage multi-chemins, il s'agit de la tolérance aux pannes, l'agrégation de la bande passante, la réduction du délai de découverte de route, l'équilibrage de charge, et la sécurité. Ensuite, nous détaillons les principaux protocoles de routage multi-chemins. Enfin, une conclusion de ce chapitre est présentée.

2.1 Les composants de bases des protocoles de routage multi-chemins

Dans la littérature, plusieurs chercheurs en discuter les composants du routage multi-chemins (Mueller *et al.* 2003; Tsai & Moors 2006; Murshedi *et al.* 2016; Gopi 2014; Bargaoui 2016). Généralement trois composants de base reflètent les tâches principales du routage multi-chemins, il s'agit de : la découverte de routes, la maintenance de routes et l'allocation du trafic. Ci-dessous leurs détails.

Découverte de routes

Le processus de découverte de routes consiste à la détermination des chemins disponibles pour une paire de nœuds source et destination. Un protocole peut utiliser différents critères pour déterminer tous ou le sous-ensemble des chemins possibles qu'ils souhaitent découvrir dans le processus de découverte de routes (Tsai & Moors 2006).

L'un des principaux critères est la disjonction des chemins, qui classe l'indépendance des chemins en termes de ressources partagées. Trois principaux types de disjonction de chemin sont envisagés, à savoir : les chemins à nœuds disjoints, les chemins à liens disjoints et les chemins non disjoints. Les chemins à nœuds disjoints où chemins totalement disjoints, n'ont aucun nœud ni lien en commun. Ainsi, les chemins à liens disjoints n'ont pas de liens en commun, mais peuvent avoir des nœuds en commun. Ainsi que, les chemins non disjoints peuvent avoir des nœuds et des liens en commun. La figure 2.1 donne des exemples des différents types de chemins disjoints. Les chemins SXD, SYD et SZD n'ont pas de liens ou de nœuds en commun et sont donc des nœuds disjoints (figure 2.1 (a)). Les chemins SXYZD et SYD ont le nœud Y en commun et ne sont donc que des liens disjoints (figure 2.1 (b)). Les chemins SXD et SXYD ont le nœud X et le lien SX en commun et sont donc non disjoints (figure 2.1 (c)) (Mueller *et al.* 2003).

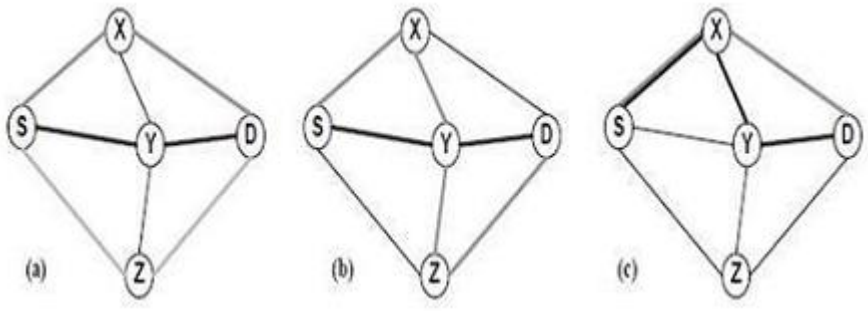

Figure 2.1 – *Exemples des différents types de chemins disjoints*

Sélection des chemins et distribution du trafic

Après la découverte de plusieurs chemins, un autre problème à résoudre est le nombre de chemins à sélectionner pour la transmission de données. Par conséquent, afin de répondre aux exigences de performance

de l'application visée, proposer un mécanisme de sélection de chemin pour choisir un certain nombre de chemins constitue un élément important de la conception d'un protocole de routage multi-chemins de haute performance. Après avoir sélectionné un ensemble de chemins parmi les chemins découverts, le protocole de routage multi-chemins doit maintenant déterminer comment répartir le trafic sur les chemins sélectionnés. Divers mécanismes d'attribution de trafic sont utilisés pour répartir les données entre les chemins sélectionnés (Gopi 2014).

Maintenance de routes

Due à la mobilité des nœuds dans les réseaux mobiles ad hoc, les chemins peuvent échouer en raison de défaillance des liens ou des nœuds, ce qui nécessite la maintenance de routes. Le processus de maintenance de routes permet la régénération des chemins existants après la découverte du chemin initial (Tsai & Moors 2006).

Dans le routage multi-chemins, la découverte de routes peut être déclenchée chaque fois que l'un des chemins échoue ou seulement après que tous les chemins ont échoué. Si tous les chemins échouent avant de procéder à la découverte, il en résultera un délai avant que de nouveaux chemins ne soient disponibles. Cela pourrait dégrader la qualité de service de l'application. Cependant, le lancement d'une découverte de routes chaque fois que l'un des chemins échoués peut entraîner des frais généraux élevés. La découverte de routes en cas d'échec de N chemins, où N est inférieur au nombre de chemins disponibles, peut constituer un compromis entre les deux options (Mueller *et al.* 2003).

2.2 Les avantages du routage multi-chemins

D'après (Siddiqui *et al.* 2007), Les protocoles de routage multi-chemins (Garcia-Luna-Aceves & Mosko 2005) ont été initialement conçus pour assurer la fiabilité (Ganjali & Keshavarzian 2004) et la qualité de service dans les réseaux ad hoc. Mais leur nature de résilience aux attaques a été rapidement identifiée comme une caractéristique de sécurité importante. En effet, avec les protocoles de routage à un seul chemin, il est facile pour un adversaire de lancer des attaques de routage. Un nœud compromis contrôlé par l'adversaire peut participer à la découverte d'itinéraire entre deux nœuds d'extrémité sans être remarqué. Par conséquent, l'adversaire peut contrôler le mécanisme de routage et interrompre les services à tout moment.

Le routage multi-chemins est nécessaire pour une communication sécurisée lorsque la récupération d'itinéraire ne peut pas être garantie d'être effectuée assez rapidement en raison de la grande mobilité du système. Avec les chemins de secours, le trafic peut être redirigé chaque fois que nous avons une panne d'itinéraire, réduisant ainsi le temps de récupération d'itinéraire (Burmester & Van Le 2004).

Plusieurs avantages peuvent être obtenu due à l'utilisation du routage multi-chemins (Lou *et al.* 2006; Gurung & Saikia 2015; Bargaoui 2016; Tsai & Moors 2006; Mueller *et al.* 2003; Narware *et al.* 2019). De nombreuses études ont été mentionnés dans (Ploumidis *et al.* 2017) indiquant

que l'utilisation de plusieurs chemins peut offrir de nombreux avantages en termes de débit, de délai, de fiabilité, équilibrage de la charge, sécurité et efficacité énergétique. Les principaux avantages du routage multi-chemins sont les suivants :

Tolérance aux pannes

Selon (Tsai & Moors 2006), les protocoles de routage multi-chemins peuvent offrir une tolérance aux pannes en faisant acheminer des informations redondantes vers la destination via des chemins alternatifs. Cela réduit la probabilité que la communication soit interrompue en cas de défaillance de la liaison. Des algorithmes plus sophistiqués utilisent le codage source (Ayanoglu *et al.* 1993) pour réduire la surcharge du trafic due à une redondance excessive, tout en maintenant le même degré de fiabilité. Cette augmentation de la résilience des routes dépend en grande partie de mesures telles que la diversité ou la disjonction des chemins disponibles.

Du point de vue de la tolérance aux pannes, le routage multi-chemins peut fournir une résilience de routage. Pour illustrer cela, considérons la figure 2.2, où le nœud S a établi trois chemins vers le nœud D. Si le nœud S envoie le même paquet le long des trois chemins, tant qu'au moins un des chemins n'échoue pas, le nœud D recevra le paquet. Bien que le routage des paquets redondants ne soit pas le seul moyen d'utiliser plusieurs chemins, il montre comment le routage multi-chemins peut offrir une tolérance aux pannes en cas de défaillance de la route (Mueller *et al.* 2003).

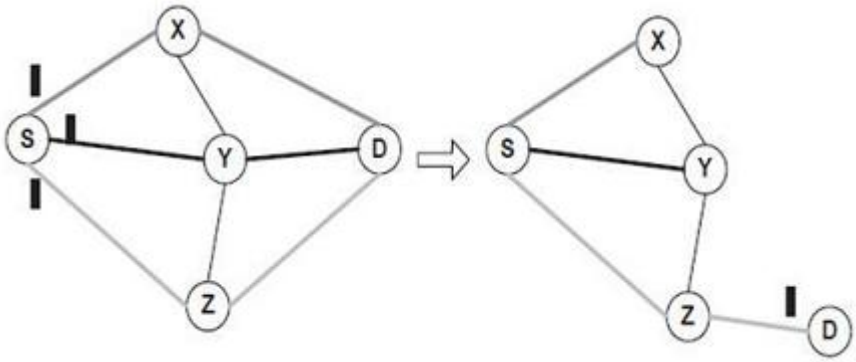

FIGURE 2.2 – *Exemple d'une tolérance aux pannes*

D'après la figure 2.2, le nœud source S achemine le même paquet vers le nœud de destination D le long des chemins SXD, SYD et SZD. Lorsque le nœud D se déplace, les chemins SXD et SYD sont interrompus, mais le chemin SZD peut toujours livrer le paquet au nœud D (Mueller *et al.* 2003).

Délai réduit

Avec les protocoles de routage à chemin unique, la rupture de la route primaire signifie le lancement d'une nouvelle procédure de découverte de routes, engendrant ainsi un délai important. En utilisant le routage multi-chemins, ce délai peut être minimisé, grâce aux chemins alternatifs

découverts en parallèle à la route primaire. Ainsi, selon la technique de maintenance adoptée, le protocole de routage peut lancer une procédure de découverte de routes à chaque fois qu'un chemin tombe en panne ou bien reporter le lancement de cette procédure jusqu'au moment où tous les chemins alternatifs soient en panne (Bargaoui 2016).

Agrégation de la bande passante

Dans les réseaux sans fil, la bande passante est considérée comme une ressource primordiale. Tout en tenant compte de l'importance de la bande passante du réseau, l'approche multi-chemins avec le routage parallèle devient un travail intéressant à considérer (Suresh *et al.* 2017).

La répartition des données d'une même destination en plusieurs flux, chacun acheminé par un chemin différent, la bande passante effective peut être agrégée. Cette stratégie est particulièrement utile lorsqu'un nœud possède plusieurs liens à faible bande passante, mais nécessite une largeur de bande supérieure à celle qu'un lien individuel peut fournir. Le délai de bout en bout peut également être réduit en conséquence directe d'une bande passante plus importante (Tsai & Moors 2006).

Equilibrage de la charge

L'équilibrage de charge est une technique utilisée pour répartir la charge de travail sur plusieurs chemins ou plusieurs processeurs. Le terme d'équilibrage de charge est généralement évolué pour utiliser efficacement les ressources du réseau et réduire la congestion du réseau (Devikar *et al.* 2016).

Selon (Vermeulen *et al.* 2020), l'équilibrage de charge est utilisé pour augmenter la capacité globale du réseau et assurer la redondance et la résilience aux pannes. Deux types d'équilibrage de charge sont configurables sur les routeurs : déterministe et non déterministe. Lorsqu'un paquet arrive sur un routeur configuré avec un équilibrage de charge déterministe (c'est-à-dire, un équilibrage de charge par flux) et que plusieurs chemins de routage à coût égal sont disponibles vers la destination du paquet, le routeur choisit un chemin en calculant un hachage sur les champs d'en-tête du paquet. Cet ensemble de champs utilisé pour calculer le hachage est appelé l'identificateur de flux et comprend généralement soit les adresses source et de destination (par destination), soit les adresses et ports source et de destination (par flux). Deux paquets appartenant au même flux sont ainsi envoyés sur le même chemin, ce qui contribue à la performance des protocoles de transport qui réagissent aux paquets retardés ou dans le désordre, ainsi que permet aux boîtiers de médiation d'avoir une visibilité sur tous les paquets d'un flux. Non déterministe est également connu sous le nom d'équilibrage de charge par paquet. Dans cette configuration, lorsqu'un paquet arrive sur un routeur avec plusieurs chemins à coût égal vers la destination, le routeur sélectionne parmi les chemins de manière circulaire.

Sécurité

Le routage multi-chemins implique l'établissement de plusieurs chemins entre les nœuds source et destination. Ces chemins peuvent être utilisés pour une communication répliquée (ou redondante) afin de contrôler les attaques malveillantes. Le principal avantage de la communication via plusieurs chemins est qu'en exploitant la redondance, elle garantit la continuité du service, même lorsque l'adversaire est actif (Raj & Sumathi 2018). Ainsi, le routage multi-chemins peut être utilisé pour améliorer statistiquement la confidentialité des messages échangés entre les nœuds source et de destination. L'envoi de données confidentielles sur un chemin d'accès aide les attaquants à sécuriser facilement l'ensemble des données. Tandis que l'envoyer en parties sur différents chemins disjoints augmente la robustesse de la confidentialité car il est presque impossible d'obtenir toutes les parties d'un message divisées et envoyées sur plusieurs chemins existants entre la source et la destination (Vinod & Madhusudan 2012). En outre, la transmission de données chiffrées sur plusieurs chemins peut réduire considérablement le risque d'attaques d'interception, de relecture et d'espionnage. Cette propriété est particulièrement importante dans les environnements mobiles, car la communication sans fil est intrinsèquement plus vulnérable aux défaillances de sécurité (Wang *et al.* 2003). Cependant, pour des raisons de sécurité, les protocoles de routage multi-chemins à nœuds-disjoints sont préférables aux protocoles de routage multi-chemins à liens-disjoints, car si l'attaquant détruit le lien commun, dans ce cas, plusieurs chemins seront affectés (Reddy & Nagendra 2019).

2.3 Les principaux protocoles de routage multi-chemins

Le routage multi-chemins a connu un intérêt considérable dans plusieurs domaines d'application. Plusieurs études de recherche ont été proposées pour résoudre divers problèmes en relation avec le routage multi-chemins, à titre d'exemples : la sécurité du routage et la qualité de service.

Dans la littérature, plusieurs protocoles de routage multi-chemins ont été proposés, certains parmi eux sont basés sur les protocoles de routages à la demande comme AODV et DSR. Dans les sous-sections suivantes, les protocoles de routage multi-chemins les plus connus sont abordés. Nous présentons ainsi, leurs fonctionnalités et leurs caractéristiques fondamentales.

Certains protocoles de routages multi-chemins proposés sont présentés dans les sous-sections suivantes et sont exprimés respectivement à partir de leurs sources comme suit :

Le protocole de routage AOMDV

Le protocole AOMDV (Marina 2001; Marina 2006) est une extension du protocole de routage AODV (Perkins & Royer 1999; Perkins *et al.* 2003). C'est parmi les protocoles de routage réactif et à la demande permettant de créer plusieurs chemins dans le processus

de découvert de routes. Ce protocole garantit la liberté de boucle et la disjonction des chemins alternatifs.

AOMDV partage plusieurs caractéristiques avec AODV. Il est basé sur le concept de vecteur de distance et utilise une approche de routage saut par saut. De plus, AOMDV trouve également des chemins à la demande en utilisant une procédure de découverte de routes. La principale différence réside dans le nombre de chemins trouvés dans chaque découverte de routes. Dans AOMDV, la propagation du RREQ de la source vers la destination établit plusieurs chemins inverses tant au niveau des nœuds intermédiaires que de la destination. Plusieurs RREP (Route Reply) traversent ces chemins inverses pour former plusieurs chemins aller vers la destination au niveau des nœuds source et intermédiaire. Les règles de mise à jour de route AOMDV, appliquées localement sur chaque nœud, jouent un rôle clé dans le maintien des propriétés de liberté de boucle et de disjonction des chemins alternatifs.

Le protocole AOMDV s'articule sur quatre composants à savoir : structure de la table de routage, découverte de routes, maintenance de routes et transmission de paquets de données. Ci-après leurs descriptions en détail.

Table de routage

Les tableaux 2.1 et 2.2 montrent la différence entre la structure d'entrée de la table de routage entre AODV et AOMDV. L'entrée de la table de routage AOMDV comporte un nouveau champ «advertised_hop_count» pour le nombre de sauts annoncé. En outre, une liste de chemins est utilisée dans AOMDV pour stocker des informations supplémentaires pour chaque chemin alternatif, notamment : prochain saut (next_hop), dernier saut (last_hop), nombre de sauts (hop_count), et délai d'expiration (timeout). Les informations relatives au «last_hop» sont utiles pour vérifier la disjonction des chemins alternatifs.

Soit une destination d et un nœud i. Chaque fois que le numéro de séquence de destination pour d en i est mis à jour, le nombre de sauts annoncé correspondant est initialisé. Pour un numéro de séquence de destination donné, $hop\_count^d_{ik}$ indique le nombre de sauts du kth chemin (pour certains k) dans l'entrée de la table de routage pour d en i, c'est-à-dire $(next\_hop^d_{ik}, last\_hop^d_{ik}, hop\_count^d_{ik}) \in route\_list^d_i$.

Quand i est sur le point d'envoyer sa première annonce de route pour d, il met à jour le nombre de sauts annoncés comme suit :

$$advertised\_hop\_count^d_i := \begin{cases} \max\limits_k \{hop\_count^d_{ik}\} & i \neq d \\ 0 & \text{otherwise} \end{cases}$$

Lorsqu'un nœud reçoit une annonce de route, il appelle les règles de mise à jour de route AOMDV répertoriées dans l'algorithme1. Notez que les lignes (1) et (10) de l'algorithme1 garantissent la liberté de boucle, tandis que les lignes (12) et (15) vérifient la non-jonction des liaisons.

Table 2.1 – Structure d'entrée de la table de routage de AODV

destination	sequence number	hop count	next hop	timeout

Table 2.2 – Structure d'entrée de la table de routage de AOMDV

destination	sequence number	advertised hop count	route list			
			*next_hop*1 *next_hop*2 . .	*last_hop*1 *last_hop*2 . .	*hop_count*1 *hop_count*2 . .	*timeout*1 *timeout*2 . .

Algorithme 1 : Règles de mise à jour de route AOMDV.

if $(seq\_num_i^d < seq\_num_j^d)$ **then**
  /* enforces the sequence number rule */
  $seq\_num_i^d := seq\_num_j^d$;
  $advrtised\_hop\_count_i^d := \infty$;
  $route\_list_i^d := NULL$;
  if $(j = d)$ **then**
    /* neighbor is the destination */
    $insert(j, i, 1) intoroute\_list_i^d$;
  else
    $insert(j, last\_hop_{jk}^d, advrtised\_hop\_count_j^d + 1) intoroute\_list_i^d$;
    end if
else
  if$((seq_num_i^d = seq_num_j^d) and (advrtised_hop_count_i^d >$
  $advrtised\_hop\_count_j^d))$ then
  /* enforces the route acceptance rule */
  if $(j = d)$ **then**
    /* neighbor is the destination */
    if $((\nexists k1 : (next\_hop_{ik1}^d = j))\ and\ (\nexists k2 : (last\_hop_{ik2}^d = i)))$ **then**
      /* establishes uniqueness of next and last hops*/
      $insert(j, i, 1) intoroute\_list_i^d$;
      end if
  else
    if$((\nexists k3 : (next_hop_{ik3}^d = j)) and (\nexists k4 : (last_hop_{ik4}^d =$
    $last\_hop_{jk}^d)))$ then
    /* establishes uniqueness of next and last hops*/
    $insert(j, last\_hop_{jk}^d, advrtised\_hop\_count_j^d + 1) intoroute\_list_i^d$;
    end if
  end if

Découverte de routes

Comme en AODV, lorsqu'une source a besoin d'une route vers une destination, la source lance un processus de découverte de routes en générant une demande RREQ. Etant donné que la demande RREQ est

inondée sur l'ensemble du réseau, un nœud peut recevoir plusieurs copies du même RREQ. En AODV, seule la première copie de la RREQ est utilisée pour former des chemins inversés ; les copies qui arrivent plus tard sont simplement jetées. Notez que certaines de ces copies en double peuvent être utilisées utilement pour former des chemins inverses alternatifs. Ainsi, toutes les copies dupliquées sont examinées dans AOMDV pour rechercher d'autres chemins inverses potentiels, mais les chemins inversés ne sont formés qu'en utilisant les copies qui préservent la liberté de boucle et la disjonction de route parmi l'ensemble de chemins résultant. Ceci est assuré en appliquant les règles de mise à jour de route de l'algorithme1.

Lorsqu'un nœud intermédiaire obtient un chemin inverse via une copie RREQ, il vérifie s'il existe un ou plusieurs chemins d'acheminement valides vers la destination. Si tel est le cas, le nœud génère une RREP et le renvoie à la source le long du chemin inverse ; la RREP inclut un chemin direct qui n'a été utilisé dans aucune RREP précédente pour cette découverte de route. Dans ce cas, le nœud intermédiaire ne propage plus la RREQ. Sinon, le nœud rediffuse la copie de RREQ s'il n'a jamais transmis aucune autre copie de cette RREQ et cette copie abouti à la formation / mise à jour d'un chemin inverse.

Lorsque la destination reçoit des copies RREQ, elle crée également des chemins inversés de la même manière que les nœuds intermédiaires. Cependant, la destination génère une RREP en réponse à chaque copie RREQ qui arrive à la source via un chemin sans boucle, même si elle crée des chemins inversés en utilisant uniquement les copies RREQ qui arrivent par des chemins alternatifs sans boucle et disjoints vers la source. Par conséquent, la destination renvoyait une RREP le long de chaque chemin inverse sans boucle, même si elle n'est pas disjointe des chemins inverses précédemment établis.

Lorsqu'un nœud intermédiaire reçoit une RREP, il suit les règles de mise à jour de la route de l'algorithme1 pour former un chemin de transfert sans boucle et disjoint vers la destination, si possible ; sinon, la RREP est abandonnée. En supposant que le nœud intermédiaire forme le chemin de transfert et possède un ou plusieurs chemins inverses valides vers la source, il vérifie si l'un de ces chemins inverses n'a pas déjà été utilisé pour envoyer une RREP pour cette découverte de routes. Si tel est le cas, il choisit l'un de ces chemins inversés inutilisés pour transmettre la RREP actuelle ; sinon, la RREP est simplement abandonnée.

Maintenance de routes

La maintenance de routes dans AOMDV est une simple extension de la maintenance de route AODV. Comme AODV, AOMDV utilise également des paquets RERR (Route Error). Un nœud génère ou transmet un RERR pour une destination lorsque le dernier chemin à la destination est rompu. AOMDV inclut également une optimisation pour récupérer les paquets transmis sur les liaisons défaillantes en les retransmettant sur des chemins alternatifs. Ceci est similaire au mécanisme de récupération de paquet dans DSR (Johnson 1994).

Le mécanisme de délai d'attente "timeout" s'étend de manière similaire

d'un chemin unique à plusieurs chemins (tableaux 2.1 et 2.2), bien que le problème de définition de valeurs de délai appropriés soit plus difficile pour AOMDV que pour AODV. Avec plusieurs chemins, la possibilité que les chemins deviennent périmés est plus probable. Toutefois, l'utilisation de valeurs de délai d'attente très faibles pour éviter les chemins vides peut limiter les avantages liés à l'utilisation de plusieurs chemins. Dans leurs expériences, les auteurs de AOMDV ont utilisé un réglage modéré des valeurs de délai d'attente, en outre, ont utilisé les messages HELLO pour supprimer de manière proactive les itinéraires périmés.

Transmission de paquets de données

Pour le transfert de paquets de données sur un nœud comportant plusieurs chemins vers une destination, les auteurs d'AOMDV adoptent une approche simple consistant à utiliser un chemin jusqu'à ce qu'il échoue, puis à basculer sur un autre chemin ; les chemins sont utilisés dans l'ordre de leur création.

Le protocole de routage AODVM

AODVM (Ye *et al.* 2003) est un protocole de routage multi-chemins établit à partir des modifications au protocole AODV. Ce protocole de routage peut chercher et trouver plusieurs chemins à nœuds-disjoints pour chaque destination afin de transmettre les paquets de données émis par une source.

Dans AODV, les paquets RREQ en double sont ignorés par les nœuds intermédiaires, il est probable que certains des chemins à nœuds-disjoints possibles vers la destination ne sont jamais suivis pendant le processus de requête. Sur la figure 2.3, les liaisons indiquées par les lignes en pointillés ne sont jamais signalées à la destination si les nœuds intermédiaires abandonnent les paquets RREQ reçus sur ces liaisons. Bien qu'il existe trois chemins possibles à nœuds-disjoints de la source à la destination, l'AODV ne peut en trouver qu'un.

Au lieu d'ignorer les paquets RREQ en double comme dans AODV, les nœuds intermédiaires dans AODVM doivent enregistrer les informations contenues dans ces paquets dans une table appelée «RREQ table». Pour chaque copie reçue d'un paquet RREQ, le nœud intermédiaire enregistre l'identité de la source qui a généré la RREQ, l'identité de la destination à laquelle la RREQ est destinée, l'identité du voisin qui a transmis la RREQ et le nombre de sauts (Figure 2.4(a)) dans la table «RREQ table». De plus, les nœuds intermédiaires ne sont pas capables d'envoyer le paquet RREP directement à la source, afin d'obtenir autant de chemins possibles.

Lorsque la destination reçoit le premier paquet RREQ d'un de ses voisins, elle met à jour son numéro de séquence et génère un paquet RREP. Le paquet RREP est modifié pour contenir un champ supplémentaire appelé «ROUTE_ID». Chaque chemin découvert lors d'une instance de découverte de routes assigner un «ROUTE_ID» unique par la destination. Le paquet RREP avec un «ROUTE_ID» particulier est renvoyé à la source via le voisin qui transmet le paquet RREQ. Lorsque la destination reçoit des copies dupliquées du paquet RREQ provenant d'autres voisins, elle génère

des paquets RREP pour chacun d'eux et chacun de ces paquets contient un «ROUTE_ID» unique.

Lorsqu'un nœud intermédiaire reçoit un paquet RREP de l'un de ses voisins, il supprime l'entrée correspondant à ce voisin de sa table «RREQ table» et ajoute une entrée de routage à sa table de routage (figure 2.4(b)) pour indexer la découverte de la route vers l'expéditeur du paquet RREP (la destination). Le nœud identifié ensuite le voisin dans la table «RREQ table» via lequel, le chemin d'accès à la source est le plus court, et transmet le paquet RREP à ce voisin. L'entrée correspondant à ce voisin est alors supprimée de la table «RREQ table». Afin de s'assurer qu'un nœud ne participe pas à plusieurs chemins, lorsque les nœuds entendent un nœud diffusant un paquet RREP, ils suppriment l'entrée correspondant au nœud émetteur de leurs tables «RREQ table».

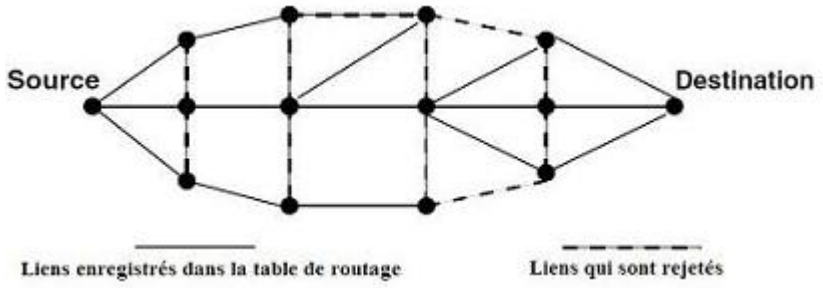

FIGURE 2.3 – *La procédure de diffusion de RREQ dans AODV.*

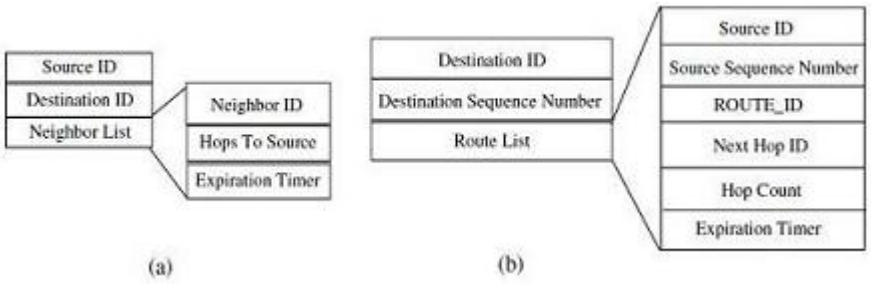

FIGURE 2.4 – *(a) Structure de chaque entrée de table «RREQ table» dans AODVM. (b) Structure de chaque entrée de la table de routage dans AODVM.*

Lorsqu'un nœud intermédiaire qui reçoit un paquet RREP ne peut plus le transmettre (sa table «RREQ table» est maintenant vide), il génère un paquet RDER (Route Discovery ERror) et envoie ce paquet au voisin qui a effectivement transmis la RREP à ce nœud. Le voisin, après avoir reçu le paquet RDER, va maintenant tenter de transmettre la RREP à un voisin différent qui peut potentiellement le transférer vers la source. Le nombre de RDER qu'un paquet RREP peut rencontrer est limité afin d'empêcher la génération et l'échange d'un grand nombre de tels paquets.

Ainsi, il est nécessaire que la source confirme chaque paquet RREP reçu au moyen d'un paquet de réponse de route RRCM (Route Reply ConfirMation). En réalité, le paquet RRCM peut être ajouté au premier paquet de données envoyé sur la route correspondante et contiendra éga-

lement des informations concernant le «ROUTE_ID» et le nombre de sauts de la route.

Comme dans le protocole AODV, des numéros de séquence sont utilisés pour empêcher les boucles. Lorsqu'un nœud source lance une requête RREQ, il augmente son numéro de séquence seq^{src}_{src} (seq^{i}_{j} représente le dernier numéro de séquence du noeud i connu du noeud j) et le numéro de séquence de la destination seq^{dst}_{src} de un. Ces deux numéros de séquence sont indiqués dans le paquet RREQ et notés respectivement seq^{src}_{RREQ} et seq^{dst}_{RREQ}. Chaque fois que le nœud de destination reçoit un nouveau paquet RREQ, il calcule un nouveau numéro de séquence :

$$seq^{dst}_{dst} = MAX(seq^{dst}_{RREQ}, seq^{dst}_{dst}) + 1.$$

La destination génère ensuite un paquet RREP contenant un numéro de séquence seq^{dst}_{RREP}, défini à seq^{dst}_{dst}.

Le protocole de routage AODV-BR

AODV-BR (Lee & Gerla 2000) est une extension améliorée du protocole de routage à la demande AODV. Le schéma du routage proposé dans AODV-BR s'inspire du schéma de routage des conduits (Shacham *et al.* 1983) proposé au début des années 1980. Le routage des conduits souffre toutefois de certaines limitations. Les paquets de données sont propagés en double par de multiples routes dans toutes les instances, créant ainsi une redondance excessive qui engendre des encombrements et des collisions. Dans l'algorithme adopté dans AODV-BR, au contraire, plusieurs chemins alternatifs ne sont utilisés que lorsque le chemin principal est déconnecté. (Wang & Crowcroft 1990) ont également proposé un protocole utilisant un chemin alternatif uniquement lorsque les paquets de données ne sont pas livrables via le chemin principal. L'algorithme proposé dans AODV-BR vise à créer un maillage et de fournir plusieurs chemins alternatifs. Cet algorithme établit le maillage et les chemins multiples sans transmettre aucun message de contrôle supplémentaire, contrairement aux algorithmes utilisés dans les protocoles de routage utilisant plusieurs chemins dans les réseaux ad hoc tels que : les schémas de (Nasipuri *et al.* 2000), (Nasipuri & Das 1999), le protocole Temporally-Ordered Routing Algorithm TORA (Park & Corson 1997), et le protocole Routing On-demand Acyclic Multipath ROAM (Raju & Garcia-Luna-Aceves 1999), qui nécessitent un message de contrôle supplémentaire pour la construction et la maintenance des chemins alternatifs.

Fonctionnement du protocole AODV-BR

Le protocole AODV-BR utilise le processus de découverte de route d'AODV, il n'apporte aucune modification au processus de demande de route RREQ de l'AODV. Tandis que dans le processus de réponse à la demande de route RREP du protocole AODV-BR, les chemins alternatifs (chemins de secours) sont créés en écoutant les messages RREPs.

Construction de route

Lorsqu'un nœud source veut établir une route pour transmettre les données vers une destination mais ne dispose d'aucun chemin, il recherche une route en inondant un paquet RREQ sur le réseau. Chaque paquet RREQ a un identifiant unique afin que les nœuds puissent détecter et supprimer les paquets en double. Lorsqu'il reçoit un message RREQ non dupliqué, un nœud intermédiaire enregistre les informations relatives au saut précédent et au nœud source dans sa table de routage (c'est-à-dire, l'apprentissage en arrière). Il diffuse ensuite le paquet ou renvoie un paquet RREP à la source s'il dispose d'une route vers la destination. Le nœud de destination envoie un RREP via la route sélectionnée lorsqu'il reçoit le premier RREQ ou les RREQ suivants qui ont emprunté un meilleur chemin (au format AODV, par exemple, un chemin plus récent ou plus court) que le chemin précédemment répondu.

La structure de maillage et les chemins alternatifs sont établis pendant la phase de réponse à la demande de route. Le protocole AODV est modifié légèrement dans cette procédure. Tirant parti de la qualité de diffusion des communications sans fil, un nœud «surprend» à l'aveuglette les paquets transmis par les nœuds voisins. À partir de ces paquets, un nœud obtient des informations de chemin alternatif et devient une partie du maillage comme suit. Lorsqu'un nœud qui ne fait pas partie de la route surprend un paquet RREP qui ne lui est pas transmis par un voisin (sur la route principale), il enregistre ce voisin en tant que prochain saut vers la destination dans sa table de routage alternative. Un nœud peut recevoir de nombreux RREP pour la même route s'il se situe dans la plage de propagation radio de plus d'un nœud intermédiaire de la route principale. Dans cette situation, le nœud choisit le meilleur chemin parmi ceux-ci et l'insère dans la table de routage alternative. Lorsque le paquet RREP atteint la source de la route, la route principale entre la source et la destination est établie et prête à être utilisée. Les nœuds ayant une entrée vers la destination dans leur table de routage alternative font partie du maillage. La route principale et les chemins alternatifs établissent ensemble une structure en mailles ressemblant à un os de poisson (figure 2.5).

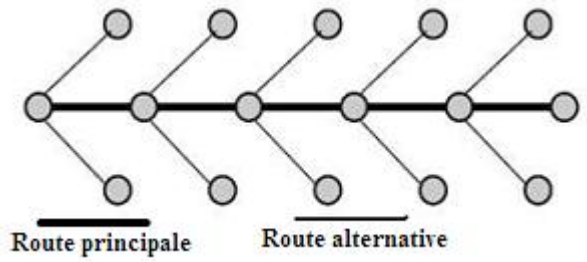

FIGURE 2.5 – *Chemins multiples formant une structure en os de poisson*

Maintenance de routes et distribution du trafic

Les paquets de données sont acheminés via la route principale, sauf en cas de déconnexion de la route. Lorsqu'un nœud détecte une rupture

de liaison, il effectue une diffusion de données d'un saut vers ses voisins immédiats. Le nœud spécifie dans l'en-tête de données que le lien est déconnecté et que le paquet est donc candidat à un «routage alternatif». Lors de la réception de ce paquet, les nœuds voisins possédant une entrée pour la destination dans leur table de routage alternative envoient le paquet en diffusion individuelle à leur nœud de saut suivant. Les paquets de données peuvent donc être acheminés via un ou plusieurs autres chemins et ne sont pas abandonnés en cas de rupture de route. Pour empêcher les paquets de tracer une boucle, ces nœuds de maille transmettent le paquet de données uniquement si le paquet n'est pas reçu de leur saut suivant vers la destination et n'est pas dupliqué. Lorsqu'un nœud de la route principale reçoit le paquet de données en provenance d'autres routes, il fonctionne normalement et transmet le paquet à son prochain saut lorsque le paquet n'est pas dupliqué. Le nœud qui a détecté la rupture de la liaison envoie également un paquet RERR à la source pour lancer une redécouverte de route. La raison pour laquelle on reconstruit un nouveau chemin au lieu d'utiliser en continu les autres chemins est de créer un nouveau chemin optimal qui reflète la situation et la topologie du réseau actuel.

Le mécanisme d'utilisation des chemins alternatifs utilisé dans le protocole AODV-BR est similaire à celui de DSR (Dynamic Source Routing), mais présente les différences suivantes. Dans AODV-BR, le système utilise le maillage uniquement pour «contourner» la partie interrompue du chemin. En revanche, dans le DSR, le nœud qui détecte une déconnexion de route peut récupérer les données en remplaçant dans l'en-tête de source l'intégralité de la route restante jusqu'à la destination par une route de secours stockée dans son cache de route. Le schéma de secours DSR nécessite une surcharge de stockage en cache considérable. Une autre différence est que le nœud de DSR envoie un paquet RERR à la source uniquement lorsqu'il n'a pas d'autre route et ne peut pas récupérer les données. Par conséquent, les chemins dans DSR sont actualisés moins souvent que dans AODV-BR.

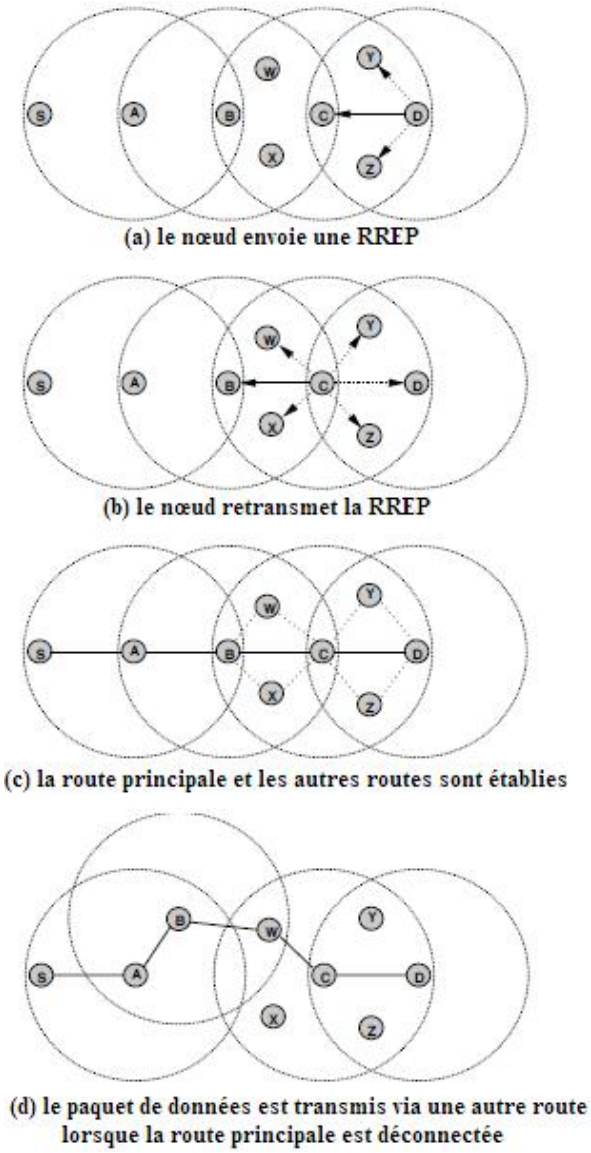

FIGURE 2.6 – *Construction de routes multiples et leurs utilisation»*

La figure 2.6 est un exemple montrant comment le maillage et les autres chemins sont construits et utilisés dans la délivrance de données. Lorsque le RREQ atteint le nœud de destination D, la route principale <S-A-B-C-D> est sélectionnée. La destination D envoie un RREP au nœud C. Les nœuds Y et Z, qui se trouvent dans la plage de propagation de D, surprennent le paquet et insèrent une entrée dans leur table de routage alternative. Ce processus est illustré à la Figure 2.6 (a). Après réception de cette RREP, seul le nœud C relaie le paquet au nœud B car il fait partie de la route. De nouveau, les nœuds voisins d'un saut peuvent entendre le paquet. Les nœuds W et X enregistrent le nœud C comme saut suivant vers la destination D dans leur table de routage alternative. Les nœuds Y et Z, au contraire, ne mettent pas à jour leur table car ils ont déjà un chemin vers le nœud D. De même, le nœud D ne réagit pas à la transmission du RREP par le nœud C puisqu'il s'agit de la destination (et d'une partie de la route). La figure 2.6 (c) montre l'état lorsque la RREP atteint

le nœud source et crée la route principale et les multiples chemins alternatifs. La figure 2.6 (d) illustre l'utilisation d'un chemin alternatif lorsque le chemin principal est déconnecté. Le nœud B a quitté la plage radio de son nœud de saut suivant C. Après avoir reçu le paquet de données du nœud A, le nœud B le transmet au nœud C. Le paquet ne sera pas livré car le nœud n'est pas accessible. Le nœud B diffuse ensuite le paquet à ses voisins pour que des chemins alternatifs récupèrent les données. Les nœuds A et W reçoivent le paquet, mais le nœud A le supprime lors de la détection dupliquée. Le nœud W, en revanche, reconnaît la déconnexion de la route principale en lisant l'en-tête du paquet. Il recherche dans sa table de routage alternative et trouve C comme prochain saut vers la destination. Il transfère le paquet au nœud C et finalement, le paquet atteint la destination.

En AODV, un chemin est expiré lorsqu'il n'est pas utilisé et mis à jour pendant un certain temps. Dans AODV-BR la même technique est utilisée pour chronométrer les chemins alternatifs. Les nœuds qui fournissent des chemins alternatifs entendent les paquets de données et si le paquet a été transmis par le saut suivant à la destination, comme indiqué dans leur table des chemins alternatifs, ils mettent à jour le chemin. Si un autre chemin n'est pas mis à jour pendant le délai «timeout», le nœud supprime le chemin de la table.

Le protocole de routage SMR

L'objectif principal de SMR (Lee & Gerla 2001) est de créer des chemins multiples disjoints au maximum. La construction des routes disjointes au maximum permet d'éviter l'encombrement de certains nœuds et d'utiliser efficacement les ressources réseau disponibles. Pour atteindre cet objectif dans les schémas de routage à la demande, la destination doit connaître l'intégralité du chemin de toutes les routes disponibles afin de pouvoir sélectionner les routes. Par conséquent, l'utilisation de l'approche du routage source où les informations des nœuds constituant la route sont incluses dans le paquet RREQ. De plus, les nœuds intermédiaires ne sont pas autorisés à renvoyer des RREP à la source même lorsqu'ils disposent d'informations de routage vers la destination.

Le processus du routage dans le protocole SMR se compose de trois phases principales, à savoir, la découverte de route, la réponse de route et la maintenance de route.

Découverte de routes

Le protocole de routage SMR (Split Multipath Routing) est un protocole de routage à la demande qui crée plusieurs routes à l'aide de cycles de demande/réponse. Lorsque la source a besoin d'une route pour se rendre à la destination mais qu'aucune information de route n'est connue, le message RREQ est inondé dans l'ensemble du réseau. Comme ce paquet est inondé, plusieurs duplications de ce paquet ayant traversé différentes routes atteignent la destination. Le nœud de destination sélectionne plusieurs routes disjointes et renvoie les paquets RREP à la source via les routes choisies.

Lorsqu'un nœud autre que la destination reçoit un RREQ qui n'est pas dupliqué, il ajoute son ID et rediffuse le paquet. Le fait de supprimer tous les RREQ dupliqués ne générait que plusieurs chemins, qui étaient pour la plupart superposés. La figure 2.7(a) montre les chemins pris par les RREQ du nœud source au nœud destinataire, et la figure 2.7(b) décrit les routes disponibles et montre les cinq routes partagent les deux premiers liens.

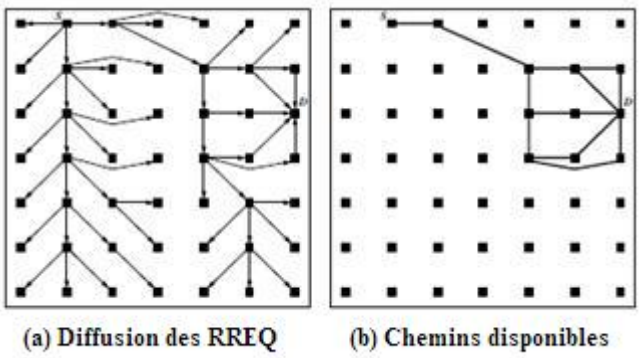

FIGURE 2.7 – *Chevauchement de plusieurs routes.»*

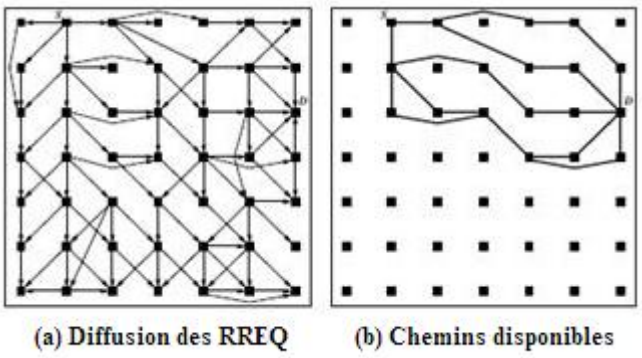

FIGURE 2.8 – *Plusieurs routes avec des chemins au maximum disjoints.»*

Afin d'éviter le problème de chevauchement des routes, l'approche de transmission de paquet différente est introduis. Au lieu de supprimer chaque RREQ dupliqué, les nœuds intermédiaires transmettent les paquets dupliqués qui ont traversé un lien entrant différent de celui par lequel le premier RREQ est reçu et dont le nombre de sauts n'est pas supérieur à celui du premier RREQ reçu. Figure 2.8(a) montre les chemins pris par les RREQ utilisant cette technique. Cette technique permet de sélectionner plus de chemins disjoints parmi les routes disponibles dans la figure 2.8(b) que ceux de la figure 2.7(b). L'approche utilisée dans SMR présente l'inconvénient de transmettre plus de paquets RREQ, mais elle permet de découvrir des routes disjointes au maximum.

Dans SMR, la destination sélectionne deux routes qui sont au maximum disjointes. L'une des deux routes est la route à retard le plus court, c'est-à-dire le chemin pris par le premier RREQ reçu par la destination. L'utilisation du chemin du retard le plus court comme l'une des deux routes à pour but de minimiser la durée d'acquisition de la route requise

par les protocoles de routage à la demande. Lors de la réception du premier RREQ, la destination enregistre l'intégralité du chemin et envoie une RREP à la source via cette route. Les identifiants des nœuds de l'ensemble du chemin sont enregistrés dans la RREP et, par conséquent, les nœuds intermédiaires peuvent transmettre ce paquet en utilisant ces informations. Après ce processus, la destination attend une certaine durée pour recevoir plus de RREQ et apprendre tous les routes possibles. Elle sélectionne ensuite la route la plus disjointe par rapport à la route déjà répondue. La route disjointe au maximum peut être sélectionnée car la destination connaît toutes les informations de la première route et de tous les autres routes candidate. S'il y a plus d'une route qui sont au maximum disjointes de la première route, celle avec la distance de saut le plus court est choisi. S'il reste encore plusieurs routes satisfaisant la condition, le chemin qui a livré le RREQ à la destination le plus rapide entre eux est sélectionné. La destination envoie ensuite une autre RREP à la source via la deuxième route sélectionnée.

Maintenance de routes

Lorsqu'un nœud ne parvient pas à transmettre le paquet de données au saut suivant de la route, il considère que le lien est déconnecté et envoie un paquet RERR à la direction amont de la route. Le message RERR contient la route vers la source et les nœuds immédiatement en amont et en aval du lien rompu. À la réception de ce paquet RERR, la source supprime chaque entrée de sa table de routage qui utilise le lien rompu (quelle que soit la destination). Si une seule des deux routes de la session est invalidée, la source utilise la route valide restante pour délivrer des paquets de données. Lorsque la source est informée de la déconnexion d'une route et que la session est toujours active, elle peut utiliser l'une des deux stratégies pour redécouvrir les routes : lance le processus de récupération de route lorsque l'une des routes de la session est interrompu, ou initie le processus de récupération de route uniquement lorsque les deux routes de la session sont rompues.

Granularité de l'allocation

Dès la réception du premier RREP par le nœud source, la première route découverte est utilisée pour envoyer les paquets de données vers le nœud de destination. Quand le deuxième RREP est reçu, le nœud source peut utiliser deux routes pour envoyer les paquets de données vers le nœud de destination, il peut ainsi répartir le trafic à l'aide d'un schéma d'allocation par paquet. Mais, avec cette technique d'allocation, les paquets de données peuvent arriver en désordre au nœud de destination. Dans ce cas, offrir une technique de ré-ordonnancement peut remédier cet inconvénient.

Le protocole de routage SMORT

Le protocole SMORT (Reddy & Raghavan 2007) est basé principalement sur le protocole de routage à un seul chemin AODV. L'objectif principal de SMORT est de réduire la surcharge de routage induite par la reprise

après ruptures de route, en utilisant des chemins alternatifs. SMORT fournit à la plupart des nœuds intermédiaires situés sur le chemin principal plusieurs chemins vers la destination, de même que le nœud source. Le chemin principal est le premier chemin reçu par le nœud source après le lancement de la découverte de route, qui est généralement le chemin le plus court. SMORT n'impose pas la contrainte de disjonction sur l'ensemble des chemins multiples qu'il génère.

SMORT utilise l'idée de plusieurs chemins dit «fail-safe». Un chemin entre la source et la destination est dit «fail-safe» pour le chemin principal s'il contourne au moins un nœud intermédiaire sur le chemin principal. En d'autres termes, le chemin «fail-safe» peut être utilisé pour envoyer des paquets de données au cas où le ou les nœuds contournés sur le chemin principal s'éloigneraient. Par exemple, sur la figure 2.9, les chemins S – A – H – C – E – D et S – A – B – C – L – D sont des chemins «fail-safe» menant au chemin principal S – A – B – C – E – D. La session de données entre S et D n'est pas modifiée même si les nœuds B et E s'éloignent en même temps, car les paquets peuvent être redirigés via les chemins «fail-safe». La figure 2.9 montre un ensemble de tels chemins qui contournent tous les nœuds du chemin principal et fournissent à la plupart des nœuds intermédiaires des chemins alternatifs vers la destination. Les chemins multiples «fail-safe» sont différents des chemins multiples à nœuds disjoints et à liens disjoints, en ce sens que les chemins «fail-safe» peuvent avoir des nœuds et des liaisons en commun. Cette contrainte moins restrictive permet de calculer plus de chemins «fail-safe» que les chemins multiples à nœuds disjoints ou à liens disjoints. A référé au segment du chemin «fail-safe» qui contourne le ou les nœuds du chemin principal en tant que segment «fail-safe», et aux autres chemins des nœuds en tant que chemins secondaires. Par exemple, B – K – E sur la figure 2.9 est un segment «fail-safe» qui contourne le nœud C sur le chemin principal et le chemin situé au nœud B via le nœud K est un chemin secondaire.

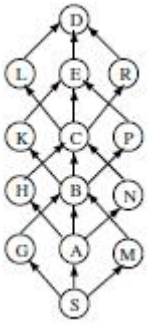

FIGURE 2.9 – *Exemples des chemins multiples «Fail-safe»*

Le processus du routage dans le protocole SMORT se compose de trois phases principales, à savoir, la découverte de route, la réponse de route et la maintenance de route.

Découverte de routes

Un nœud initie un processus de découverte de route lorsqu'il souhaite communiquer avec une destination pour laquelle il n'a pas de route va-

lide. Une route valide est une route vers la destination, dont la durée de vie «lifetime» n'a pas expirée, c'est-à-dire que la valeur de «lifetime» de l'entrée de route doit être supérieure à l'heure actuelle sur le nœud. Le nœud source insère l'adresse de la destination dans un paquet «route-request» et le diffuse. La structure du paquet «route-request» de SMORT est identique à celle d'AODV, sauf que SMORT n'utilise aucun numéro de séquence de destination.

Un nœud intermédiaire recevant «route-request» répond en envoyant un paquet «route-reply» s'il a une route vers la destination. Sinon, il rediffuse simplement «route-request». Bien que les nœuds acceptent plusieurs copies de «route-request», seule la première copie de «route-request» est rediffusée. Les nœuds stockent toutes les copies de «route-request» dans une table appelée table «request-rcvd». Les informations de «route-request» sont stockées dans la table «request-rcvd», au lieu d'établir une route inverse vers la source, comme dans l'AODV, car la route inverse peut contenir des boucles en raison de l'acceptation de plusieurs demandes. Chaque entrée de la table «request-rcvd» contient l'adresse du nœud précédent qui lui a relayé la «route-request» (appelée last-hop) et le nombre de sauts que la «route-request» a parcourus à partir du nœud source. Les nœuds utilisent ces informations pour relayer les paquets «route-reply» vers le nœud source. Si aucun des nœuds intermédiaires ne possède de nouvelle route vers la destination, la destination répond elle-même à la demande «route-request», si elle reçoit une copie de «route-request».

Réponse de route

Les réponses «route-reply» suivent les chemins inverses stockés dans la table «request-rcvd» pour atteindre le nœud source. Le paquet «route-reply» utilisé par SMORT contient trois champs supplémentaires, à l'exception de certains champs du paquet de réponse d'AODV. Ces champs supplémentaires représentés sur la figure 2.10 (reply–gen, mul–reply, node–list) sont nécessaires pour éliminer les boucles de routage et pour calculer plusieurs chemins «fail-safe». Le champ «node-list» contient la liste de tous les nœuds que le paquet de réponse a traversés jusqu'à présent. Le champ «reply-gen» sert à stocker l'adresse du nœud d'où provient cette copie particulière du paquet «route-reply», et «mul-reply» est une variable booléenne.

Avant d'envoyer «route-reply», le nœud de destination initialise les champs de «node-list» et «reply-gen» à son adresse. Le champ «mul-reply» est défini sur TRUE pour la première réponse. Pour les réponses supplémentaires générées par la destination, la valeur de «mul-reply» est définie sur FALSE. Les nœuds recevant «route-reply» l'acceptent, s'il s'agit de la première réponse pour cette destination, et stockent les informations de route qui y sont transportées dans la table de routage, ainsi que le chemin complet. La structure de l'entrée de routage typique est illustrée à la Figure 2.11. Plusieurs routes vers la destination sont stockées dans «route-list» de l'entrée de routage. Chaque route individuelle routei à «$nexthop_i$» comme adresse du voisin par lequel la route va à destination, «$hopcount_i$» comme distance à destination (en nombre de sauts) et «$fullpath_i$» comme chemin complet de destination. «precur-list» est la liste des lasthops par

lesquels le paquet «route-reply» est relayé à la source. «$lifetime_i$» est expliquée dans la phase de maintenance de route.

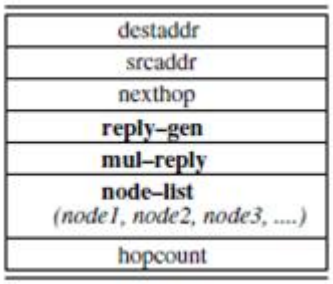

FIGURE 2.10 – *Structure du paquet de réponse de SMORT.*

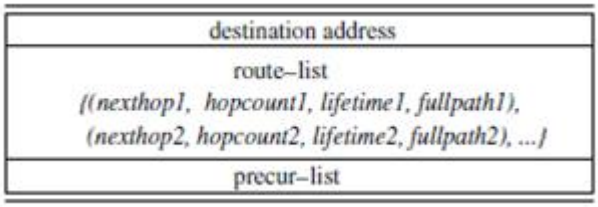

FIGURE 2.11 – *Structure d'entrée de route de SMORT.*

Après avoir stocké les informations de routage, les nœuds intermédiaires transmettant le paquet «route-reply» par des chemins inverses au nœud source. Ils ajoutent leurs adresses à la liste «node-list» avant de relayer le paquet de réponse. Les nœuds relaient les paquets «route-reply» via plusieurs chemins inverses, chacun via un lasthop différent, si le champ «mul-reply» de «route-reply» reçue est VRAI. Le nombre de réponses multiples qu'un nœud peut relayer est limité à «MAX-REPLY», afin d'éviter une tempête de «route-reply». La liste des lasthops, par laquelle les réponses sont envoyées, est stockée dans la liste «precur-list» de l'entrée de routage. Cette liste est requise pour envoyer le paquet d'erreur de route au nœud source, au cas où le nœud détecte une rupture de route et qu'aucun chemin secondaire vers la destination n'est disponible sur ce nœud. Les nœuds envoient la première copie de la réponse sans modifier les valeurs des champs «mul-reply» et «reply-gen». Dans le reste des copies, «mul-reply» est défini sur FALSE afin que les nœuds situés sur le chemin secondaire n'envoient pas plusieurs réponses. En effet, les nœuds situés sur les chemins secondaires n'ont pas besoin de plusieurs chemins. Cette disposition limite également le nombre de transmissions de paquets «route-reply». En outre, le champ «reply-gen» est remplacé par l'adresse du nœud, car il s'agit du nœud à l'origine de cette copie particulière de «route-reply».

Si la valeur «mul-reply» de «route-reply» reçue par un nœud est FALSE, le nœud se trouve sur un segment «fail-safe». Par conséquent, il ne transmet qu'une copie de «route-reply» sans modifier les valeurs «mul-reply» et «reply-gen». Par exemple, sur la figure 2.12, le nœud E reçoit «route-reply» avec la valeur de «mul-reply» est TRUE de la desti-

nation D. Il relaie trois copies du paquet de réponse par les nœuds C, H et M. Mais seule la «route-reply» envoyée par C a la valeur «mul-reply» comme TRUE, car C est sur le chemin principal.

Ainsi, seuls les nœuds du chemin principal peuvent relayer plusieurs réponses. Les réponses envoyées par H et M contiennent la valeur «mul-reply» comme FALSE et elles ne transmettent pas plusieurs réponses, même si elles ont reçu plusieurs copies de «route-request». Les valeurs «reply-gen» des paquets «route-reply» relayés par les nœuds H et M sont remplacées par E. De manière similaire, le nœud D répond aux paquets supplémentaires «route-request» via J et N avec la valeur «mul-reply» est FALSE.

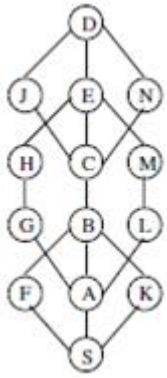

FIGURE 2.12 – *Multi Chemins «Fail-safe» entre les nœuds S et D.*

Lorsque le nœud reçoit une réponse supplémentaire «route-reply», il accepte la réponse «route-reply» uniquement si la liste «node-list» de «route-reply» ne contient pas son adresse et si cette copie de «route-reply» a été créée par l'un des nœuds situés sur le chemin principal. Sinon, «route-reply» est rejetée par le nœud. Le nœud peut vérifier si la réponse «route-reply» a été générée par l'un des nœuds sur son chemin principal ou non, en utilisant le champ «reply-gen» de «route-reply» et le champ «fullpath» du chemin principal. Les nœuds ne transmettent pas les paquets supplémentaires «route-reply» au nœud source, ils sont supprimés une fois que le nœud a stocké les informations de routage qu'ils transportent dans la table de routage. Lorsque le nœud C de la figure 2.12 reçoit des réponses supplémentaires via J et N, il ne les transmet pas davantage puisqu'il a déjà transmet la réponse «route-reply» reçue de E. À tout moment, les nœuds utilisent le plus court des chemins multiples pour transférer les paquets de données vers la destination.

Dans le cas où un nœud intermédiaire recevant la demande «route-request» a une route vers la destination, il lance le processus de réponse en copiant son chemin complet vers la destination dans le champ «node-list» du paquet «route-reply». La valeur «reply-gen» est définie sur l'adresse de ce nœud et "mul-reply" sur TRUE.

Maintenance de routes

La phase de maintenance de la route conserve les routes établies pendant la phase de réponse de la route pendant la durée de la session. La

durée «lifetime» des entrées de routage est utilisée à cette fin. La durée «$lifetime_i$» de la $route_i$ représente le temps jusqu'à ce que la route passant par «$nexthop_i$» soit valide. Les nœuds situés sur le chemin principal actualisent la durée «lifetime» de leurs entrées dans la table de routage, chaque fois qu'un paquet de données destiné à la destination correspondante est transmis. La durée «lifetime» des routes aux nœuds du chemin secondaire est initialisée à une valeur suffisamment grande. Cette valeur peut être décidée en fonction de la fréquence des ruptures de chemin dues à la mobilité et de la probabilité de défaillance des nœuds. Ce paramètre est appelé SEC_ROUTE_LIFETIME. Si un besoin pour la route secondaire arrive avant ce moment, la route secondaire est utilisée pour la transmission de données, puis sa durée «lifetime» est mise à jour tant que la transmission de données passe par elle. Sinon, les routes secondaires sont supprimées des tables de routage une fois que leur durée «lifetime» initiale a expiré.

La durée «$lifetime_i$» de la $route_i$ est mise à jour à CURRENT-TIME + ACTIVE-ROUTE-TIMEOUT, chaque fois qu'un paquet de données est transmis avec succès par le biais de «$nexthop_i$». Cela signifie que la route est valide et nécessaire jusqu'à la prochaine seconde ACTIVE-ROUTE-TIMEOUT. CURRENT-TIME est l'heure de l'horloge absolue du nœud effectuant cette mise à jour. Si une route vers la destination expire, c'est-à-dire si la durée «lifetime» existante de la route est inférieure à CURRENT-TIME, la route est invalidée et ne peut plus être utilisée pour l'envoi de paquets de données. Plus tard, lorsqu'un paquet de données arrive pour cette destination, le nœud vérifié si un chemin secondaire valide vers la destination est disponible dans la liste «route-list» de l'entrée de routage. Si une seconde route valide existe, le chemin principal est remplacé par ce chemin et les paquets sont acheminés par ce dernier. S'il n'existe pas de route secondaire valide, un paquet «route-error» est envoyé à tous les nœuds sources par l'intermédiaire des nœuds de la liste «precur-list» de l'entrée de route de la destination.

Lorsqu'un nœud reçoit le paquet «route-error», il invalide les routes via le voisin qui a envoyé le paquet «route-error», à toutes les destinations mentionnées dans la liste «dest-list». Si le nœud ne dispose pas de telles routes, il supprime simplement le paquet «route-error».

Au cas où des routes vers l'une des destinations sont invalidées, le nœud remplace la route invalidée par une route secondaire, s'il en existe un. Il supprime cette destination de la liste «dest-list» du paquet «route-error». Si la liste «dest-list» devient vide, le nœud supprime le paquet «route-error», car les routes vers toutes les destinations sont rétablies avec les routes secondaires. Si certaines destinations restent dans la liste «dest-list», le nœud relaie le paquet «route-error» via les précurseurs des destinations restantes dans la liste «dest-list». Enfin, si les nœuds sources des sessions reçoivent le paquet «route-error», ils lancent un nouveau processus de découverte de route afin de rétablir les routes vers des destinations déconnectées, s'ils ne disposent pas non plus de chemins secondaires valides.

Alors que la plupart des déconnexions de route sont rétablies au niveau des nœuds intermédiaires avec des chemins secondaires, le nombre

d'erreurs de route communiquées dans le réseau diminue considérablement.

Le diagramme état-espace de la figure 2.13 illustre l'action de SMORT. Les nœuds S et D sont des nœuds source et destination, communiquant l'un avec l'autre. Les nœuds N1 et N2 sont des nœuds intermédiaires qui transmettent les paquets à la destination.

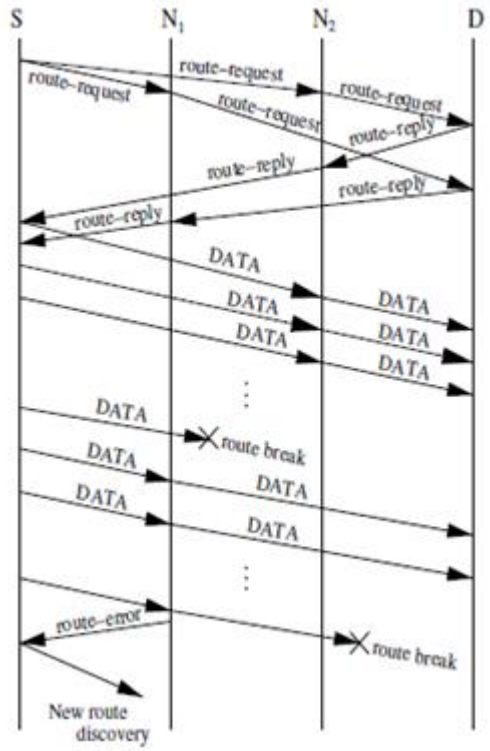

FIGURE 2.13 – *Diagramme d'état-espace de SMORT.*

Le protocole de routage CHAMP

CHAMP (Valera *et al.* 2003) est un protocole de routage qui utilise la mise en cache coopérative des paquets et l'acheminement le plus court par les chemins multiples pour réduire les pertes de paquets dues aux pannes fréquentes de routes. Une technique exploitant la localité temporelle dans les paquets perdus, visant à réduire la perte de paquets due à la rupture de route. Chaque nœud maintient une petite mémoire-tampon pour la mise en cache des paquets de données qui le traversent. Lorsqu'un nœud en aval rencontre une erreur de transmission, un nœud en amont avec les données pertinentes dans sa mémoire-tampon et sa route alternative peut retransmettre les données. Pour que cette stratégie soit efficace, les nœuds doivent stocker plusieurs routes vers chaque destination active.

Fonctionnement du protocole CHAMP

Un réseau ad hoc est représenté sous la forme d'un graphe G = (N, L), où N est l'ensemble des nœuds et L, l'ensemble des arêtes ou des liens. Tout nœud $i \in N$ peut servir à la fois de routeur et de source de données.

Soit Ni l'ensemble des voisins de i défini comme l'ensemble des nœuds où i a une connectivité bidirectionnelle directe.

Le successeur défini au nœud i pour chaque destination active j, noté par $S_j^i \in N^i$, est défini comme l'ensemble des nœuds pouvant être utilisés par i comme saut suivant pour les paquets destinés à j. La longueur de toute route allant de $k \in S_j^i$ à j est S_j^k. Une propriété unique de CHAMP est qu'il ne comporte un nœud k dans S_j^i que si la longueur de la route de k à j est égale au plus court chemin.

Structures de données

Chaque nœud conserve deux structures de données : une mémoire cache de route pour contenir des informations de transfert ; et une mémoire cache de demandes de route pour stocker les demandes de route récemment reçues et traitées.

Le cache de route au nœud i est une liste contenant une entrée pour chaque destination active j. Chaque entrée contient les éléments suivants : identificateur de destination (j), distance par rapport à la destination (D_j^i), ensemble de noeuds successeurs ou de sauts suivants par rapport à la destination (S_j^i), heure à laquelle chaque noeud successeur k a été utilisé pour la dernière fois ($ltu_{jk}^i, \forall k \in S_j^i$), et le nombre de fois où chaque nœud successeur k est utilisé ($use_{jk}^i, \forall k \in S_j^i$). Une entrée de route qui n'a pas été utilisée pendant plus de *RouteLifeTime* (secondes) est supprimée.

Le cache de demandes de route au nœud i est une liste contenant une entrée pour chaque demande de route unique reçue et traitée. Chaque entrée contient les éléments suivants : identificateur de la source de la demande de route (h), identificateur du nœud recherché (j), numéro de séquence de la demande (sn), nombre de transferts minimal ($minfc_{ji}^h(sn)$), l'ensemble des nœuds qui ont transmis la même demande avec $fc = minfc_{ji}^h(sn)(P_{ji}^h(sn))$ et l'état de la demande de route ($status_{ji}^h(sn)$), qui peut être soit «*Replied*», soit «*NotReplied*».

Outre les deux structures de données, chaque nœud conserve également deux mémoires-tampon (premier entré, premier sorti) : une mémoire tampon d'envoi pour stocker les paquets en attente de routes ; et une mémoire cache de données pour stocker les paquets de données récemment transférés.

Découverte de routes

CHAMP fonctionne à la demande, c'est-à-dire que le nœud i ne maintient S_j^i que s'il existe des paquets de données à envoyer à j. Sa découverte de route est similaire aux "calculs par diffusion" : à partir d'un DAG (Graphe Acyclique Direct), chaque nœud calcule sa distance en fonction de la distance rapportée par les nœuds en aval et rend sa distance à ses nœuds en amont (Garcia-Lunes-Aceves 1993).

Un nœud source h lance la découverte de route lorsqu'il a des données à envoyer à j mais qu'il n'a pas de route disponible. Le nœud h inonde le réseau avec un RREQ pour j. Ceci établit un DAG enraciné à h. Quand

j reçoit un RREQ, il renvoie un RREP à i par l'intermédiaire de certains nœuds constituant un sous-ensemble du DAG enraciné à h.

Chaque RREQ de h à j a un champ de compte de transfert *fc*, qui est initialisé à zéro par la source et incrémenté de un chaque fois que le message est retransmis. La première fois que i reçoit un RREQ de h à j, il initialise $minfc_{ji}^{h}$ à *fc* et P_{ji}^{h} au saut précédent du message. Chaque fois que i reçoit une demande avec $fc = minfc_{ji}^{h}$ (ce qui signifie que la demande a parcouru un chemin de même longueur de h à ce nœud), il inclut le saut précédent du message dans P_{ji}^{h}. Si i reçoit une demande avec $fc < minfc_{ji}^{h}$ (ce qui signifie que la demande a parcouru un chemin plus court de h à ce nœud), il réinitialise $minfc_{ji}^{h}$ à *fc* et P_{ji}^{h} au saut précédent du message. L'ensemble P_{ji}^{h} contient les identifiants des nœuds pouvant recevoir un RREP correspondant de i, si i en envoie un.

Lorsqu'un nœud destination j reçoit un RREQ, il renvoie immédiatement un RREP si $fc < minfc_{ji}^{h}$. Chaque RREP spécifie explicitement l'ensemble des nœuds P pouvant l'accepter. Le nœud destination j initialise ce champ au saut précédent du RREQ, indiquant ainsi que le RREP n'est destiné qu'à ce nœud. Chaque RREP possède également un champ de nombre de sauts hc initialisé à zéro par la destination.

Un nœud i traite une RREP si $i \in P$. Le nœud i accepte alors la route dans RREP si $hc \leq D_j^i$ ou ses routes existantes vers j n'ont pas été utilisées pendant plus que *RouteFreshTime* et à condition que le nombre de routes vers j soit inférieur à ou égal à *MaxRoutes*. Si la route reçue est plus courte ($hc < D_j^i$) ou si les routes existantes vers j n'ont pas été utilisées pendant plus que *RouteFreshTime*, S_j^i est réinitialisé pour contenir le saut précédent de RREP. Le nœud i calcule ensuite sa distance $D_j^i \leftarrow hc$ et transmet le message à ses nœuds en amont en définissant $P \leftarrow P_{ji}^{h}$ et en incrémentant *hc* de un si la demande correspondante n'a pas encore été répondue. Ce processus est répété jusqu'à ce que le RREP atteigne la source h.

Transmission de paquets de données

Dans CHAMP, les paquets de données sont identifiés par l'identifiant de source et un numéro de séquence fixé par la source. Ils incluent également leur saut précédent respectif dans leur en-tête, servant de «pointeur» au nœud amont qui a mis en cache les mêmes données.

Lors de la transmission d'un paquet de données, un nœud i choisit le voisin du saut suivant le moins utilisé k. Cela répartit les paquets sur toutes les routes de manière alternée. Le nœud i enregistre ensuite une copie du paquet dans son cache de données, définit le champ du saut précédent sur son adresse, puis transmet le paquet de données au saut suivant choisi. Si i n'a pas de route vers j et qu'il est la source du paquet, il enregistre le paquet dans son tampon d'envoi et effectue une découverte de route. Toutefois, si i n'est pas la source, il supprime simplement le paquet et diffuse un RERR contenant les informations d'en-tête (source, destination, numéro de séquence et saut précédent) du paquet supprimé.

Maintenance de routes

Les nœuds s'appuient sur l'accusé de réception de paquet de données fourni par la couche liaison pour déterminer l'état d'un lien. Comme les paquets sont expédiés en mode «round-robin» (une technique de répartition des paquets selon un algorithme d'ordonnancement), tous les liens sont actualisés périodiquement. La maintenance de la route ne se produit que lorsqu'un nœud i perd toutes ses routes actives vers une destination j après un échec de transfert de données.

Un lien (i, k) est déclaré comme "en panne" lorsque le nœud i ne reçoit pas d'accusé de réception du nœud de saut suivant k après avoir transmis un paquet de données à k. Lorsque cela se produit, k est supprimé de S_j^i. Si i a une autre route vers j, il transfère tous les paquets non distribuables via cette route. Si i n'a pas d'autre route vers j, i diffuse un RERR contenant les informations d'en-tête de tous les paquets de données (à l'exception des paquets provenant de ce nœud) qui ne peuvent pas être distribuées à la suite de la défaillance de la liaison. S'il existe des paquets non distribuables en provenance de ce nœud, i effectue une découverte de route.

Récupération de paquets à partir du cache de données

Il est possible que le RERR contienne des informations d'en-tête d'un ou plusieurs paquets de données. Avant d'analyser le RERR reçu de k, i crée un nouveau message RERR qu'il se propagera en amont s'il ne parvient pas à récupérer un paquet. Pour chaque paquet référencé dans le message, le nœud i effectue les opérations suivantes : le nœud i supprime k de S_j^i, où j est la destination du paquet. Si i est à l'origine du paquet référé et qu'il n'a pas d'autre route j, il lance une nouvelle découverte de route s'il n'y en a pas en cours. Si i à d'autres routes pour accéder à j et qu'il a une copie du paquet de données dans son cache de données, il transfère le paquet de données conformément à la règle de transfert de données. Si i n'a pas d'autre route vers j et qu'il possède une copie des données auxquelles il est fait référence dans son cache de données, il supprime le paquet de données référencé de son cache de données et ajoute les informations d'en-tête de paquet de données dans le RERR qu'il a créé. Si i n'a pas le paquet dans son cache de données et que c'est le saut précédent du paquet, i ajoute les informations d'en-tête de paquet de données dans le RERR qu'il a créé. Si, après analyse du RERR, i ne parvient pas à récupérer un ou plusieurs paquets de données, il diffuse le RERR qu'il a créé.

Conclusion

Le présent chapitre a pour objectif de présenter les protocoles de routage multi-chemins dans les MANETs. Dans le but d'éclairer les étapes d'acheminement des paquets de données entre les nœuds communiquant dans le réseau, nous avons exposé les trois principaux composants des protocoles de routage multi-chemins à savoir : la découverte de routes, la maintenance de routes et l'allocation du trafic. Nous avons détaillé les

principaux avantages du routage multi-chemins tels que : la tolérance aux pannes, l'agrégation de la bande passante, la réduction du délai de découverte de route, l'équilibrage de la charge, et la sécurité, avec l'intention de montrer l'évolution des protocoles de routage multi-chemins en comparant leurs performances avec les protocoles de routage à un seul chemin. Nous avons présenté certains protocoles de routage multi-chemins les plus connus, afin d'expliquer leurs fonctionnalités et leurs caractéristiques fondamentales. Dans le chapitre suivant, nous considérons la sécurité du routage dans les protocoles de routage multi-chemins, nous examinons l'effet des attaques trou noir auxquelles le routage est apprécié et proposons un nouveau mécanisme pour sécuriser la communication et les paquets de données transmis par ce type de routage.

3 Détection et prévention de l'attaque trou noir dans le protocole de routage AOMDV

Sommaire

Introduction

Le réseau ad hoc mobile est un ensemble de nœuds mobiles autonomes connectés par des connexions sans fil (Johnson 1994). Sans l'aide d'une infrastructure ou d'une administration centralisée, les nœuds se déplacent librement et forment une topologie dynamique. Dans ce type de réseau, les nœuds ont une interface sans fil pour communiquer entre eux où chaque nœud peut agir en tant qu'hôte ou routeur. La communication entre nœuds est établie selon certaines règles communes sous la forme d'un protocole de routage qui permet la découverte, l'établissement et le choix de la route de transmission des paquets de données entre la source et la destination via des nœuds intermédiaires. Cependant, en raison de ses caractéristiques, les réseaux mobiles ad hoc sont exposés à différents types d'attaques et leur sécurité est une tâche difficile (Yang *et al.* 2004). Dans notre travail de recherche, nous concentrons notre étude sur les protocoles de routage multi-chemins, en particulier le protocole de routage AOMDV (Marina & Das 2001; Marina & Das 2006). Ce protocole peut rechercher plusieurs chemins et choisir la bonne route pour envoyer des paquets de données. Cependant, ce protocole ne dispose d'aucun mécanisme de protection contre tout type d'attaque. L'attaque trou noir est l'un des problèmes les plus dangereux qui perturbent la communication entre les nœuds d'un réseau. Dans cette attaque, le nœud malveillant s'annonce comme ayant le chemin le plus récent vers le nœud de destination ; il envoie un faux paquet de réponse au nœud source. Ainsi, le nœud source, dès qu'il reçoit cette fausse réponse, commence le transfert des paquets de données via le nœud malveillant vers le nœud de destination. Cependant, le nœud malveillant ne transmet pas les paquets de données vers le nœud de destination et absorbe tous ces paquets. Les attaques trou noir peuvent dégrader les performances des protocoles de routage de manière très sérieuse, en falsifiant la manière de gérer les communications entre les nœuds d'un réseau ad hoc. Pour cela, la sécurisation du routage devient une tâche primordiale pour lutter contre ce type d'attaque. Dans ce chapitre, nous proposons une technique efficace et efficiente pour détecter et isoler les nœuds qui se comportent mal, ainsi que pour assurer la découverte des chemins les plus fiables et sécurisés entre les nœuds communicants dans le protocole de routage AOMDV.

Le reste de ce chapitre est organisé comme ceci. La section suivante présente un état de l'art, nous détaillons les mécanismes existants dans la littérature pour détecter et isoler les nœuds malveillants. Ensuite, nous expliquons notre mécanisme de sécurité, nous discutons ainsi les résultats obtenus, puis une étude détaillée de comparaison des performances de notre approche proposée avec d'autres approches existantes, nous présentons ensuite une synthèse sur cette étude de comparaison. Enfin, nous concluons ce chapitre.

3.1 Etat de l'art

Nous présentons dans cette section les travaux liés à cette thèse. Le problème des attaques trou noir a été étudié dans plusieurs travaux de recherche. Cependant, certains travaux visent à trouver et sécuriser le pro-

tocole de routage contre un seul nœud malveillant ; ainsi, d'autres travaux s'intéressent au problème de plusieurs nœuds malveillants coopératifs. Il existe un certain nombre de solutions pour surmonter ces problèmes liés à la sécurité. D'une part, des propositions qui traitent le problème de la sécurité du routage en termes de comportement utilisant les messages de contrôle (RREP, RERR et RREQ) par rapport à leur contenu, comme le nombre de sauts et le numéro de séquence de destination. D'autre part, des études utilisent la cryptographie pour ce genre de problème. Dans ce qui suit, nous examinons quelques travaux connexes.

La solution proposée dans (Raj & Swadas 2009), Effectue une vérification supplémentaire pour décider si RREP_seq_no est supérieur à une valeur seuil. A chaque intervalle de temps, la valeur seuil est mise à jour dynamiquement. Si la valeur de RREP_seq_no est supérieure à la valeur seuil, le nœud est suspecté d'être malveillant et sera ajouté à la liste noire. Ainsi, envoyer un paquet de contrôle ALARM à ses voisins afin que les RREP provenant du nœud malveillant soient ignorés. La valeur de seuil est la moyenne de la différence dans chaque intervalle de temps entre le numéro de séquence de la table de routage et le numéro de séquence dans le paquet RREP. La valeur de seuil est mise à jour chaque fois qu'un nouveau nœud reçoit un paquet RREP. Cette solution augmente le taux de livraison de paquets (PDR) avec une augmentation minimale du délai moyen de bout en bout et de la surcharge de routage normalisée. Le principal avantage de cette technique est que le nœud source proclame le nœud malveillant à ses nœuds voisins afin d'être ignoré, mais cette méthode peut également se tromper lorsque le nœud non malveillant peut être inscrit dans la liste bloquée en fonction de son numéro de séquence plus élevé. D'autre part, cette méthode peut détecter et supprimer des attaques trou noir simples et multiples, mais elle sera trop complexe pour les attaques trou noir coopératives. De plus, le surdébit d'acheminement est considérablement augmenté du fait de la mise à jour du seuil à chaque fois avec la transmission du paquet de contrôle ALARM.

Pour isoler les nœuds malveillants et protéger les nœuds normaux des attaques trou noir dans le réseau, (Mistry *et al.* 2010) ont proposé une amélioration du protocole AODV contre les attaques trou noir. L'avantage de cette solution réside dans l'utilisation d'une fonction supplémentaire Pre_ReceiveReply (Packet P), l'ajout d'une nouvelle table Cmg_RREP_Tab, d'un timer MOS_WAIT_TIME, et d'une variable (Mali_node) aux structures de données dans le protocole de routage AODV. Dans la fonction Pre_ReceiveReply (Packet P), il conserve tous les RREP dans le Cmg_RREP_Tab jusqu'au moment de MOS_WAIT_TIME. Le MOS_WAIT_TIME est initialisé par la moitié du RREP_WAIT_TIME (pendant où le nœud source attend le RREP) avant de régénérer le RREQ. Cependant, le nœud source après avoir reçu le premier RREP attend MOS_WAIT_TIME et pendant lequel il enregistrera tous les futurs RREP dans le Cmg_RREP_Tab. Par la suite, le nœud source analyse tous les RREP stockés dans le Cmg_RREP_Tab et ignore le RREP du nœud dont le numéro de séquence de destination est probablement très élevé (ce nœud est suspecté d'être malveillant) et maintient l'identité du nœud malveillant, d'où d'ignorer tous les RREP provenant de ce nœud dans le futur. Ensuite, la sélection de RREP avec le numéro de séquence de destination le

plus élevé dans le Cmg_RREP_Tab qui sera utilisé dans la fonction recvReply (Packet P) de l'AODV à utiliser pour envoyer des paquets de données. De plus, pour maintenir la fraîcheur du Cmg_RREP_Tab, il est vidé dès qu'un RREP est choisi. Cependant, cette solution n'ajoute aucun message de contrôle à l'AODV. Le risque d'augmenter la surcharge de routage normalisé est minime. Le PDR est augmenté avec un délai de bout en bout acceptable. Ainsi, cette solution peut être utilisée pour détecter et éviter des attaques trou noir simples et multiples, mais introduit une augmentation de la mémoire due à l'utilisation de Cmg_RREP_Tab.

(Mahmoud *et al.* 2015) ont proposé un protocole de routage AODV modifié pour éviter l'attaque trou noir dans les MANETs. Le système d'évitement d'intrusion proposé (IASAODV) détecte et évite les nœuds trou noir en deux étapes. La première étape est basée sur le comptage des messages de contrôle RREQ et RREP pendant la découverte d'itinéraire. La deuxième étape est basée sur le numéro de séquence de destination (DSN) du message RREP, le nombre de messages RREP calculé dans la première étape et l'heure d'arrivée de RREP à la source. Cependant, dans la première étape, une table de réponse d'itinéraire est créée pour stocker tous les messages RREP du nœud de destination. Le temps d'attente avant l'envoi des données est considéré comme deux fois la valeur de RREP_WAIT_TIME. Dès que le temporisateur RREP_WAIT_TIME expire, le nombre de messages RREP dans la table de réponse d'itinéraire (RRT) est vérifié dans la deuxième étape. L'existence de plus d'un message RREP dans la table RRT signifie une menace d'attaque de trou noir. Dans le cas de la réception d'un seul message RREP, le nœud de destination est considéré comme un nœud de confiance et toutes les données lui seront envoyées. Les résultats obtenus avec ce mécanisme donnent de meilleures valeurs pour le PDR, le débit et la charge de routage normalisée (NRL). Cette solution peut détecter et éviter des attaques trou noir simples et multiples, mais introduit une augmentation du temps d'attente et de la mémoire en raison de l'attente doublée de RREP_WAIT_TIME et de l'utilisation de RRT.

Le protocole de routage AOMDV a également capté l'intérêt des chercheurs afin de détecter et d'éviter les nœuds trou noir. Dans (Bhardwaj & Singh 2014), les auteurs ont proposé un mécanisme de détection de l'AOMDV. La méthode proposée consiste à envoyer des paquets de données sur toutes les routes possibles après l'envoi d'un nombre aléatoire de paquets. Dans cette solution, le nœud de destination est modifié pour recevoir et comparer les paquets. Si un nœud malveillant provoque une attaque, la destination le connaît car le paquet de données ne sera pas reçu par elle de la route active, puis la destination envoyez le paquet FINISH par une autre route au nœud source. Le nœud source après avoir reçu le paquet FINISH, il arrête d'envoyer des données via la route actuelle en purgeant l'entrée actuelle de la table de routage et commence à envoyer des paquets via une autre route présente dans la table de routage. Cette procédure sera répétée après l'envoi de paquets de données qui sont exponentiellement plus grandes que le précédent jusqu'à ce que toute la transmission soit terminée. Ce mécanisme utilise un compteur qui sera augmenté de façon exponentielle et il est possible de réduire la surcharge d'envoi de paquets sur toutes les routes. L'approche proposée a un

taux de fausse détection négligeable et peut détecter des attaques trou noir uniques, multiples et coopératives. Il ne nécessite même pas de mémoire supplémentaire et a une surcharge de routage nominale.

Dans (Sultana & Ahmed 2018), les auteurs ont proposé une solution de transmission de données basé sur la cryptographie à courbe elliptique contre l'attaque de trou noir dans le MANET. Dans leur solution, ils ont implémenté la cryptographie à courbe elliptique (ECC) avec le protocole de routage AOMDV. Dans ECC, un mécanisme de cryptographie à clé publique qui s'exécute sur un problème de logarithme discret avec une taille de clé plus petite a été utilisé pour crypter les paquets de données vers le nœud source avant la transmission. Ils ont créé un agent sécurisé qui génère le paquet crypté, puis ce paquet atteint la destination par l'un des multiples chemins sélectionnés. En fait, le nœud source génère une paire de clés privée / publique. Au début, le nœud source choisit une clé privée aléatoire et génère une clé secrète à partir de sa propre clé privée et de la clé publique du destinataire. Il crypte le paquet avec la clé secrète nouvellement générée et annonce la clé publique. Après cela, le paquet crypté est envoyé via l'AOMDV. A la réception du paquet chiffré par le nœud de destination, il génère la même clé secrète en utilisant sa propre clé privée et la nouvelle clé publique du nœud source. Le nœud de destination peut décrypter le paquet en utilisant sa clé secrète partagée et sa paire de clés privée / publique pour obtenir les données d'origine. Dans ce cas, il sera difficile pour le nœud malveillant d'extraire la clé privée d'une clé secrète et la clé publique. Le mécanisme proposé garantit l'authentification et la confidentialité pour une transmission sécurisée des données. Cependant, le principal avantage de l'utilisation d'ECC est qu'il prend moins de mémoire et offre une grande sécurité. Ainsi, ce mécanisme a atteint un haut niveau de sécurité. L'un des enjeux de cette solution est la gestion et la distribution des clés car les nœuds mobiles ne disposent pas d'une administration centralisée.

Les auteurs de (Elmahdi *et al.* 2020) ont proposé une solution pour la transmission de données sécurisée et fiable utilisant un cryptage homomorphe contre les attaques trou noir dans les réseaux mobiles ad hoc, dans laquelle ils ont modifié la version antérieure (Elmahdi *et al.* 2018) intitulée "Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks". Ils ont étendu le schéma AOMDV pour rendre la transmission de données fiable et sécurisée en présence de nœuds malveillants dans les MANETs en distribuant les parties du message entier dans plusieurs chemins et en utilisant une méthode de cryptage homomorphique pour la cryptographie. L'idée de ce schéma est d'assigner un ensemble de chemins disjoints dans un ensemble de groupes et plusieurs chemins disjoints actifs sont attribués à chaque groupe, où tous les chemins disjoints sont connectés entre un émetteur et un récepteur. Ils divisent un message en plusieurs parties avant que le message ne soit transmis et chiffre chaque partie en fonction d'une méthode de cryptage homomorphique. Ensuite, la partie du message est transmise à chaque groupe afin qu'une seule partie chiffrée du message puisse atteindre chaque groupe. Chaque nœud de chaque groupe peut recevoir la même partie du message. Ensuite, même si un nœud intermédiaire se comporte mal (abandonnant la partie), la partie du message peut être livrée à la destination via un autre chemin.

Ainsi, le récepteur est capable de recevoir toutes les parties cryptées du message, de décrypter toutes les parties, de les combiner et de récupérer l'ensemble du message. Les résultats de la simulation montrent que le schéma proposé fournit un taux de livraison de paquets et un débit plus élevés, qui sont de bonnes caractéristiques pour les applications d'urgence dans les MANETs. De plus, le taux de réussite du schéma proposé pour assurer et garantir la livraison du paquet à la cible est très élevé avec de nombreux chemins actifs dans chaque groupe du réseau. Ce mécanisme a atteint un haut niveau de sécurité. L'un des inconvénients de cette solution est l'augmentation du délai de bout en bout dû au fractionnement et au chiffrement des messages.

Le tableau 3.1 montre les limites des approches existantes.

Table 3.1 – Limites des Approches Existantes

Métrique de comparaison	**Limites**
Détection de différents types d'attaques trou noir	Les approches (Mahmoud *et al.* 2015), (Bhardwaj & Singh 2014), (Mistry *et al.* 2010) et (Raj & Swadas 2009) peuvent détecter et éviter des attaques trou noir simples et multiples. De plus, l'approche (Bhardwaj & Singh 2014) peut détecter les attaques trou noir coopératives, mais elle sera trop complexe pour l'approche (Raj & Swadas 2009) de détecter les attaques trou noir coopératives.
Augmentation / diminution des mesures de performance	Dans (Elmahdi *et al.* 2020), le délai de bout en bout est plus élevé dans le schéma proposé que dans le schéma AOMDV original lorsque le nombre de nœuds malveillants augmente au fur et à mesure que le temps est pris par la division et le cryptage des messages. L'impact est présent avec une perte de données plus élevée dans le schéma proposé en augmentant les nœuds malveillants. Dans (Elmahdi *et al.* 2018), le taux de livraison de paquets reste au même niveau (100%) dans le schéma proposé en présence de nœuds malveillants. Le schéma proposé prend plus de temps pour livrer le paquet, le débit est plus élevé dans le schéma proposé par rapport au schéma d'origine pour la transmission de paquets. Il y a un impact de plusieurs attaquants dans le protocole proposé parce que le schéma utilise plusieurs chemins simultanément. L'impact est présent avec une perte de données plus élevée dans le schéma proposé en augmentant les nœuds malveillants. Le délai est plus élevé pour le schéma proposé que pour le schéma AOMDV d'origine lorsque le nombre de nœuds malveillants est augmenté en raison de ses procédures et fonctionnalités de sécurité.

	Dans (Sultana & Ahmed 2018), le taux de livraison de paquets est certainement le plus élevé sans nœud malveillant dans l'environnement. Il diminue lentement avec le nombre croissant de nœuds malveillants. Le délai moyen de bout en bout augmente progressivement avec les nœuds malveillants incrémentés au fur et à mesure que le processus de chiffrement avec ECC prend du temps. Dans (Mahmoud *et al.* 2015), le délai moyen de bout en bout du protocole AODV est inférieur au protocole IA-SAODV proposé en raison du temps d'attente doublé.
Besoin de mémoire / base de données supplémentaire	L'approche (Mahmoud *et al.* 2015) introduit une augmentation du temps d'attente et de la mémoire en raison de la double attente de RREP_WAIT_TIME et de l'utilisation de la table de réponse d'itinéraire (RRT). L'approche (Bhardwaj & Singh 2014) ne nécessite même pas de mémoire supplémentaire. L'approche (Mistry *et al.* 2010) introduit une augmentation de la mémoire due à l'utilisation de Cmg_RREP_Tab.
Charge sur les nœuds intermédiaires	Dans (Bhardwaj & Singh 2014), aucune implication des nœuds intermédiaires n'est requise pour le bon fonctionnement du schéma évitant ainsi une charge supplémentaire sur les nœuds intermédiaires mobiles. Seuls l'expéditeur et le nœud de destination sont responsables du bon fonctionnement de l'approche. Mais, dans (Raj & Swadas 2009), une charge supplémentaire sur l'énergie des nœuds mobiles, due à la transmission de messages ALARM aux nœuds voisins. De plus, dans (Elmahdi *et al.* 2020) et (Elmahdi *et al.* 2018), chaque message est divisé en plusieurs parties, la consommation d'énergie peut alors augmenter en raison de l'augmentation de la taille totale des messages transmis.
Faux rapport de détection.	Le taux de fausse détection de l'approche (Raj & Swadas 2009) est élevé, mais il est négligeable dans l'approche (Bhardwaj & Singh 2014) car il ne fonctionne pas sur la supposition.
Frais généraux de communication / routage	Dans (Sultana & Ahmed 2018), la charge de routage normalisée augmente avec le nombre de nœuds trou noir attaquants présents dans la situation, bien que la charge de routage normalisée puisse varier en fonction du nombre de transmissions de paquets. Dans (Bhardwaj & Singh 2014), un surdébit de communication nominal est présent car le schéma n'implique pas de paquets de contrôle supplémentaires sauf celui qui n'est envoyé qu'une seule fois. Dans (Raj & Swadas 2009), le surdébit d'acheminement est considérablement augmenté en raison de la mise à jour du seuil à chaque intervalle de temps avec la transmission du paquet de contrôle ALARM.

3.2 Mécanisme proposé

3.2.1 Principe de fonctionnement du mécanisme proposé

L'objectif principal de notre IDSAOMDV est de détecter, isoler et éliminer les attaques de nombreux nœuds malveillants. Dans l'AOMDV, au cours du processus de découverte d'itinéraire, plusieurs chemins peuvent être découverts afin d'en choisir un comme chemin principal pour la transmission des paquets de données au nœud de destination. Cependant, les critères de sélection pour ce chemin sont basés sur le numéro de séquence et le nombre de sauts afin d'obtenir le chemin le plus court et le plus récent. Ce critère conduit à des menaces qui sont utilisées dans les attaques trou noir. Pour surmonter ce problème, nous avons créé une nouvelle fonction qui renvoie deux valeurs, la première valeur (sum) est la somme des différences entre le numéro de séquence dans les paquets RREQ et RREP et la seconde (nrep) qui est le nombre des paquets RREP reçus. Cette fonction sera appelée à partir de la fonction standard recvRepp (p) du protocole AOMDV. Les deux valeurs sum et nrep permettent de calculer un seuil (TH) comme barrière contre les numéros de séquence annoncés par les noeuds trou noir attaquants et sécuriseront le processus de sélection des routes principales pour transmettre les paquets de données. On rappelle que le protocole AOMDV peut choisir un chemin principal parmi plusieurs chemins après avoir vérifié le critère : $if(rt- > rt\_seqno < rp- > rp\_dst\_seqno)$. Cependant, dans notre technique, nous avons changé ce critère comme suit : $if((TH > rp- > rp\_dst\_seqno)\&\&(rt- > rt\_seqno < rp- > rp\_dst\_seqno))$. Cette condition permet uniquement de conserver les routes avec une valeur de numéro de séquence de destination inférieure à TH et en même temps supérieure au numéro de séquence défini dans la table de routage. Cependant, le protocole de routage peut choisir la route appropriée pour la transmission de données. Ainsi, les autres valeurs de numéro de séquence ne seront jamais prises en compte par le noeud source pour éviter les nœuds malveillants. Ainsi, cette idée permettra de trouver des routes sécurisées et d'isoler les nœuds trou noir du réseau. Une nouvelle table supplémentaire nommée ADDTABLE pour stocker les réponses RREP et les fonctions qui y traitent sont implémentées. La première fonction nommée (allrrep (p)) qui enregistre les RREP dans ADDTABLE et elle est appelée par la deuxième fonction (prerrep (p)) qui retourne sum et nrep afin de calculer le TH. La fonction (prerrep (p)) est appelée dans la fonction recvReply (p) avant que le nœud source choisit l'itinéraire de transfert.

La figure 3.1 montre l'organigramme de notre mécanisme proposé.

3.2.2 Algorithme proposé

Les notations suivantes sont utilisées pour exprimer l'algorithme proposé :

SN : Source Node ;
DN : Destination Node ;
RREQ : Route Request ;
RREP : Route Reply ;
TH : Threshold ;

dif : Difference between sequence number of RREP and of RREQ ;
sum : Summation of dif ;
nrep : Replies number.
L'algorithme de détection et de prévention proposé est le suivant :

Algorithme 2 : Algorithme décrivant le mécanisme de détection et de prévention

Démarrez le processus de découverte d'itinéraire avec SN et DN à l'aide des paquets RREQ et RREP;
Stockez tous les paquets RREP dans ADDTABLE;
while *ADDTABLE is not emty* **do**
  if $rp->rp\_dst\_seqno > rq->rq\_src\_seqno$ **then**
    dif = $((rp->rp\_dst\_seqno) - (rq->rq\_src\_seqno))$;
    sum= sum + dif;
    nrep++ ;
TH=sum/nrep ;
For all RREP responses;
if $(TH > rp->rp\_dst\_seqno)\&\&(rt->rt\_seqno < rp->rp\_dst\_seqno)$ **then**
  Legitimate node detection ;
  Continue with normal routing process;
else
  Malicious node detection ;
  Discard RREP;

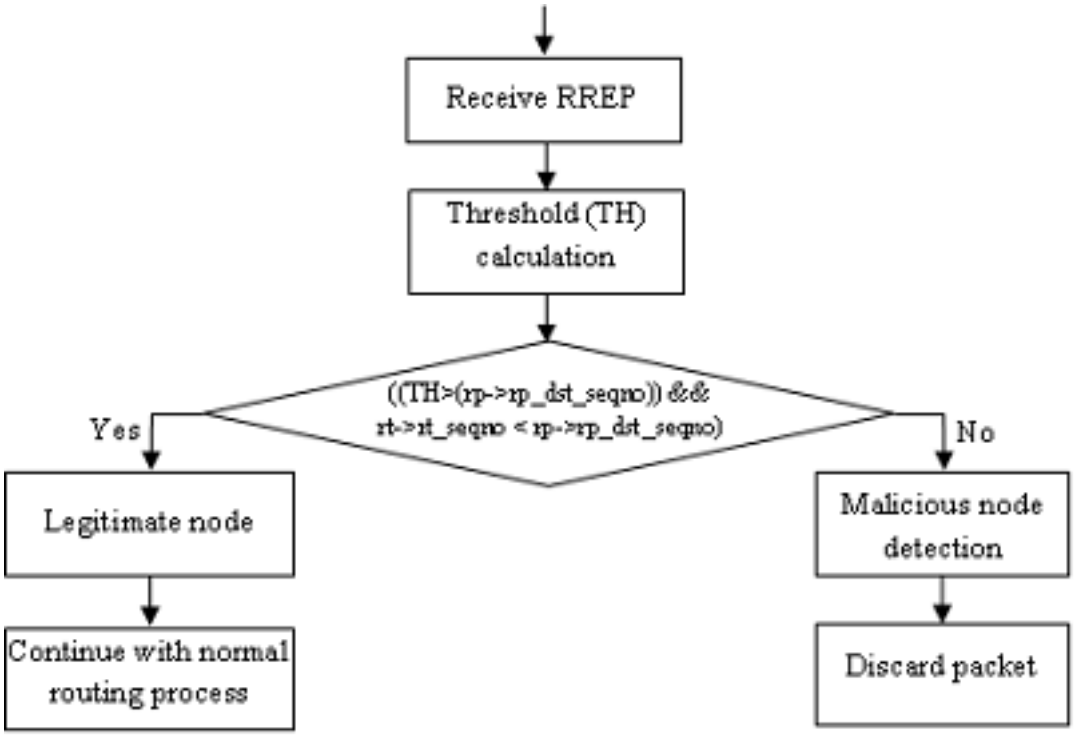

FIGURE 3.1 – *Organigramme du mécanisme proposé*

3.3 Évaluation des performances et discussions sur les résultats

Pour évaluer les performances de notre mécanisme, nous avons réalisé une étude de simulation détaillée sous le simulateur bien connu ns 2.35. Nous avons implémenté trois protocoles AOMDV, BHAOMDV sous les attaques trou noir, et notre proposition de solution IDSAOMDV.

3.3.1 Paramètres de simulation

Nous utilisons un modèle aléatoire de mobilité des nœuds, où chaque nœud se déplace de manière aléatoire dans une zone de $1500m \times 300m$. Le temps de simulation est de 900 secondes, le temps de pause variait comme $(0s, 30s, 60s, 120s, 300s, 600s, 900s)$, le nombre de nœuds communicants variait comme $(10, 20, 30, 40)$ sur 50 nœuds du réseau avec 4 paquets/seconde. La vitesse maximale est de $20m/s$, la taille du paquet est de $512octets$. Le nombre de nœuds attaquants variait de 1 à 5. Nous avons étudié quatre scénarios, et la version 5.2 de Gnuplot représente des graphiques. Le tableau 3.2 présente les principaux paramètres de simulation.

Table 3.2 – Paramètres de simulation

Paramètre	Valeur
Zone de simulation ($m \times m$)	1500×300
Nombre de nœuds	50
Temps de simulation (s)	900
Modèle de mobilité	Random way point
Vitesse maximale (m/s)	20
Temps de pause (s)	$0, 30, 60, 120, 300, 600, 900$
Nombre de nœuds communicants	$10, 20, 30, 40$
Couche d'application	Constant Bit Rate (CBR)
Taille du paquet	512 bytes
Taux de paquets	4 packet/second
Protocoles de routage	AOMDV-BHAOMDV-IDSAOMDV
Nombre de nœuds attaquants	$1, 2, 3, 4, 5$

3.3.2 Mesures de performance

- Taux de livraison de paquets -Packet Delivery Ratio- (PDR) :
  Représente le rapport entre le nombre de paquets reçus par le nœud de destination et le nombre de paquets envoyés par le nœud source ;
- Délai moyen de bout en bout -Average End to End Delay- (AEED) :
  Représente le délai moyen de bout en bout d'envoi de paquets par la source et de réception par la destination ;
- Paquets perdus -Drop Packets- (DP) :
  Représente le nombre de paquets perdus lors de la simulation ;

— Paquets transmis -Forwarded Packets- (FP) :
Représente le nombre de paquets transmis pendant la simulation.

3.3.3 Résultats de la simulation

Taux de livraison des paquets

Les figures 3.2, 3.3, 3.4, et 3.5 et tables 3.4, 3.5, 3.6 et 3.7 (voir annexe) présentent respectivement l'évolution du PDR pour l'AOMDV, BHAOMDV et IDSAOMDV avec variation des nœuds communicants de 10 à 40 nœuds, variation du temps de pause de 0 à 900 secondes, et variation du nombre de nœuds malveillants de 1 à 5. Dans le premier scénario où le nombre de nœuds communicants est de 10 et avec présence d'un seul nœud malveillant, le PDR variait de 98,72% à 99,99% pour AOMDV et de 61,57% à 96,56% pour BHAOMDV. Ainsi, la dégradation de PDR dans BHAOMDV variait de 3,16% à 37,39% par rapport à l'AOMDV. L'AOMDV et l'IDSAOMDV ont presque la même valeur que le PDR.

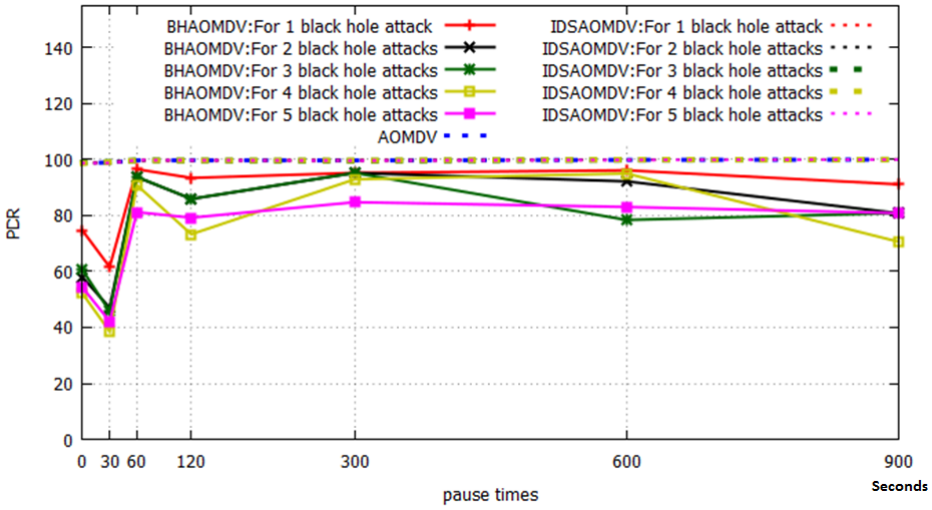

FIGURE 3.2 – *Taux de livraison des paquets pour* 10 *nœuds communicants*

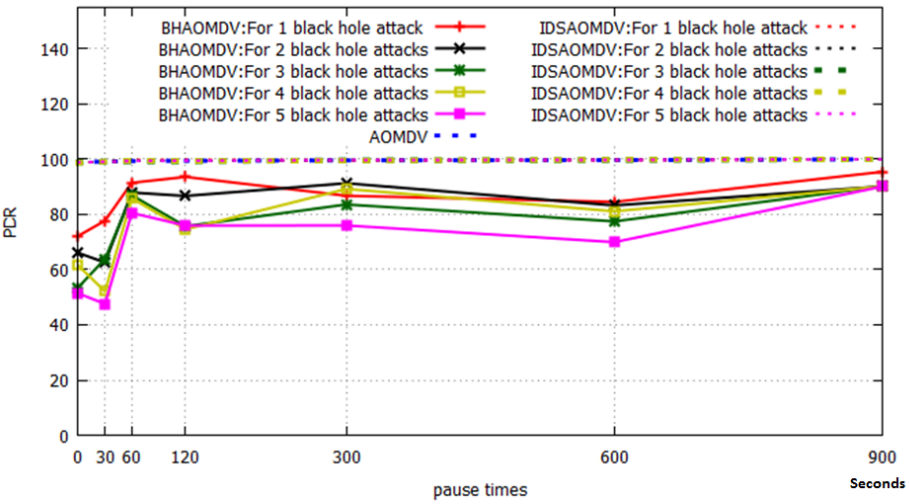

FIGURE 3.3 – *Taux de livraison des paquets pour* 20 *nœuds communicants*

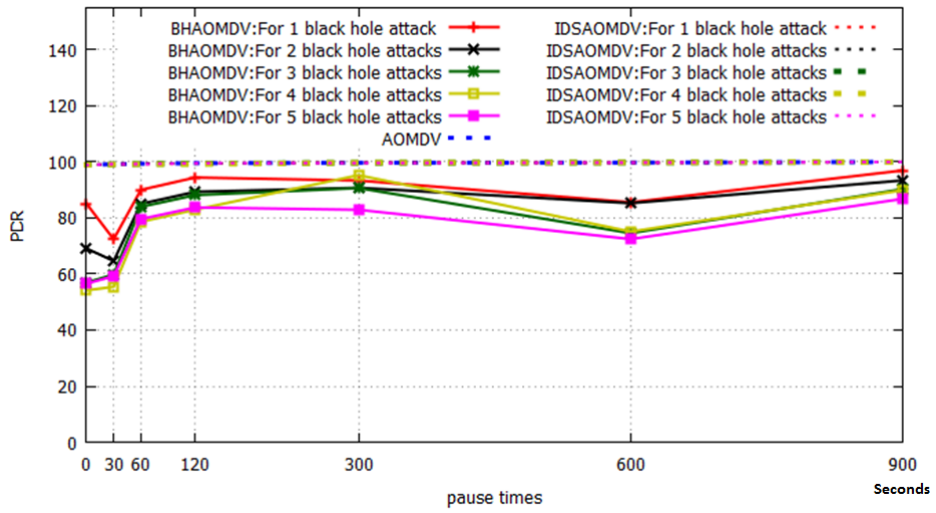

FIGURE 3.4 – *Taux de livraison des paquets pour* 30 *nœuds communicants*

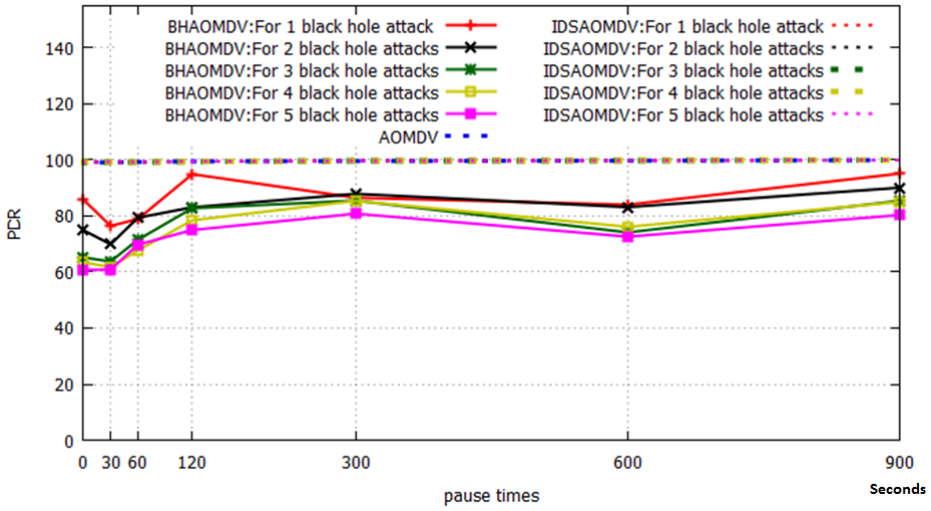

FIGURE 3.5 – *Taux de livraison des paquets pour* 40 *nœuds communicants*

Par la suite, les performances de BHAOMDV se dégradent progressivement en fonction de la variation du nombre de nœuds malveillants. Cependant, d'autres scénarios se comportent de la même manière. Par conséquent, les quatre scénarios montrent une dégradation des performances du BHAOMDV et montrent également que l'IDSAOMDV proposé donne des résultats similaires à ceux de l'AOMDV, ce qui indique que notre mécanisme proposé détecte parfaitement tous les nœuds malveillants.

Délai moyen de bout en bout

Nous avons également étudié le délai de bout en bout entre les nœuds source et de destination. Les graphiques suivants illustrés sur les figures 3.6, 3.7, 3.8, et 3.9 et tables 3.8, 3.9, 3.10 et 3.11 (voir annexe) montrent respectivement les performances d'AOMDV, BHAOMDV et IDSAOMDV en termes de retard de bout en bout. Les figures 3.6, 3.7, 3.8, et 3.9 montrent clairement qu'AOMDV et IDSAOMDV donnent moins de retard de bout en bout sans et avec les attaques trou noir. Avec la présence d'un seul

nœud malveillant et avec 10 nœuds communicants, le délai moyen de bout en bout atteint jusqu'à $0,0011ms$ pour AOMDV, $0,0011ms$ pour IDSAOMDV et $0,0095ms$ pour BHAOMDV. Dans ce cas, presque tous les graphiques sont similaires, à l'exception du temps de pause 0, où il existe une variation de la valeur du délai moyen de bout en bout en raison de l'instabilité des nœuds dans la communication à ce moment. Mais dans les scénarios où le nombre de nœuds variait de 20 à 40 (figures 3.7, 3.8, et 3.9), le délai moyen de bout en bout augmente progressivement en fonction de la variation du nombre de nœuds en communication et simultanément de la variation du nombre de nœuds malveillants pour BHAOMDV. Par conséquent, les valeurs moyennes de la mesure des performances de retard de bout en bout sont importantes et instables pour BHAOMDV. Cependant, ces valeurs sont très proches et faibles pour AOMDV et IDSAOMDV, ce qui indique que notre mécanisme est léger.

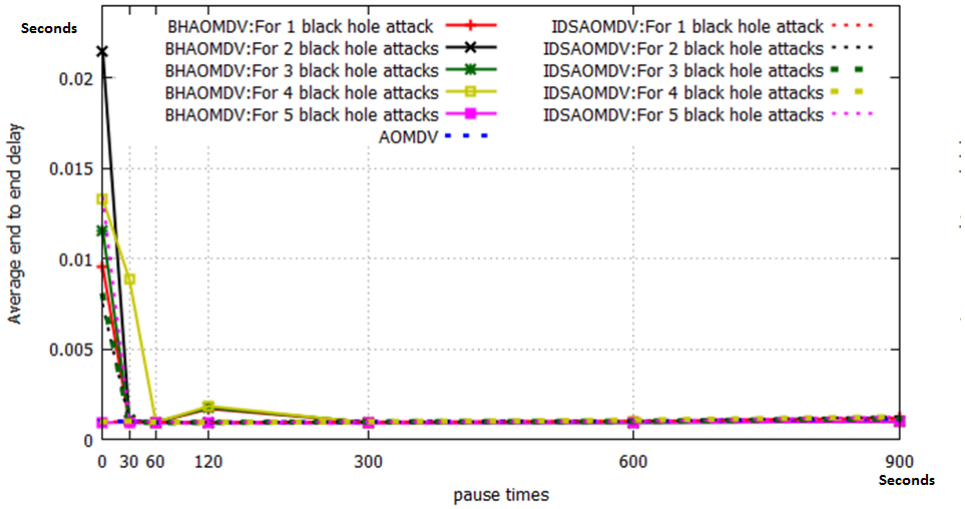

FIGURE 3.6 – *Délai moyen de bout en bout pour* 10 *nœuds communicants*

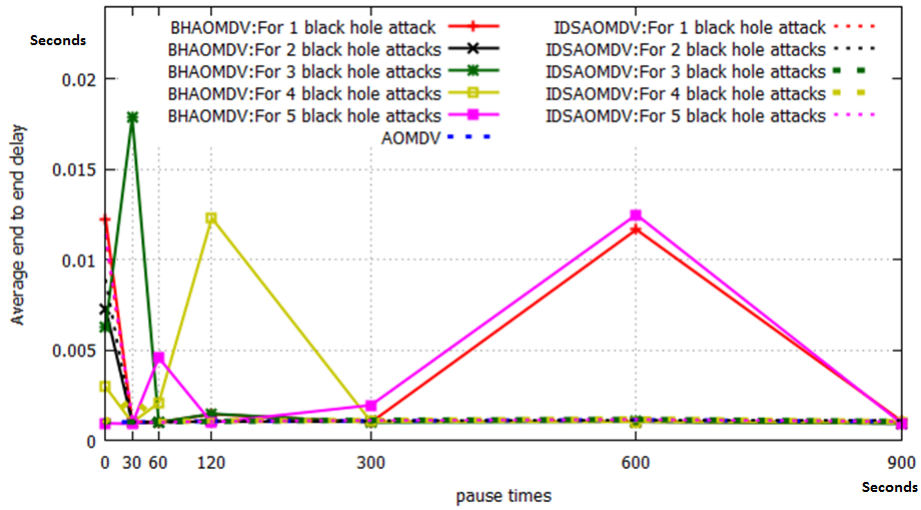

FIGURE 3.7 – *Délai moyen de bout en bout pour* 20 *nœuds communicants*

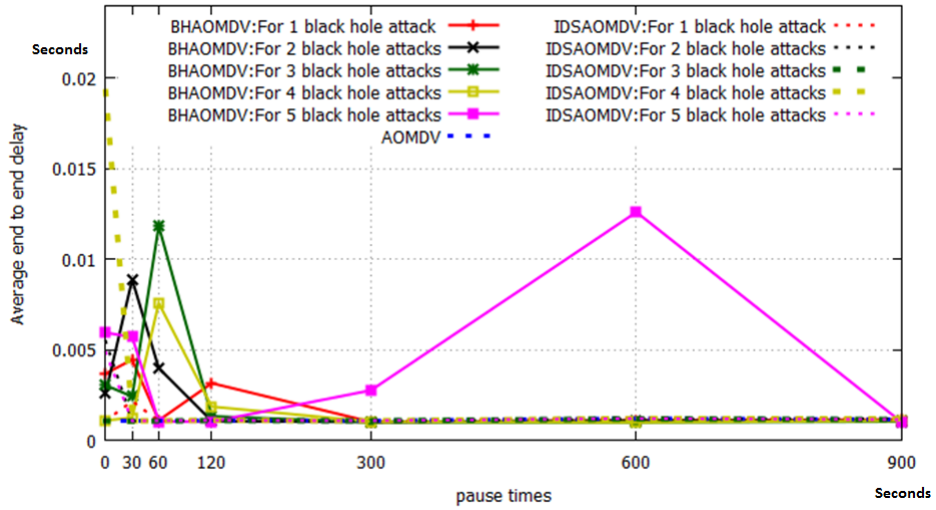

FIGURE 3.8 – *Délai moyen de bout en bout pour* 30 *nœuds communicants*

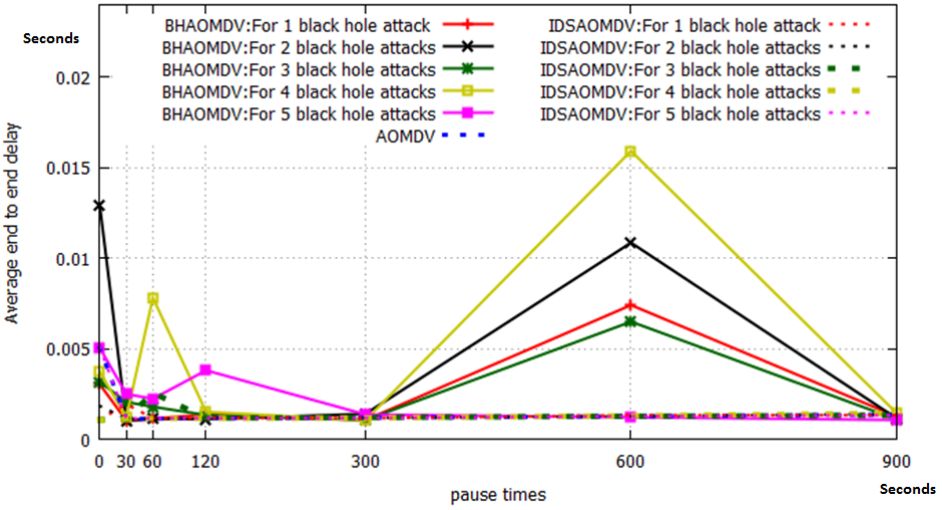

FIGURE 3.9 – *Délai moyen de bout en bout pour* 40 *nœuds communicants*

Paquets perdus

Les figures 3.10, 3.11, 3.12, et 3.13 et tables 3.12, 3.13, 3.14 et 3.15 (voir annexe) illustrent respectivement le nombre de paquets perdus pour AOMDV, BHAOMDV et IDSAOMDV. Les résultats montrent que IDSAOMDV basé sur notre technique a moins de paquets perdus que dans BHAOMDV, car des nœuds malveillants ont été identifiés et évités dans notre solution, ce qui réduit le nombre de paquets perdus. Selon la figure 3.10, le nombre de paquets perdus pour AOMDV est de 2 à 432, donc la technique appliquée dans notre solution avec la présence d'un seul nœud malveillant génère des résultats comme 3 à 425 paquets perdus pour IDSAOMDV, par contre en BHAOMDV avec la présence d'un seul nœud malveillant entraîne la perte de 1168 à 13082 paquets. Ainsi, le nombre de paquets perdus est plus grand dans BHAOMDV par rapport à AOMDV ou IDSAOMDV. Sur la même figure (Fig. 3.10), et lorsqu'il y a augmentation du nombre de nœuds malveillants, le nombre de paquets perdus augmente en BHAOMDV.

On remarque que les résultats se comportent de la même manière que

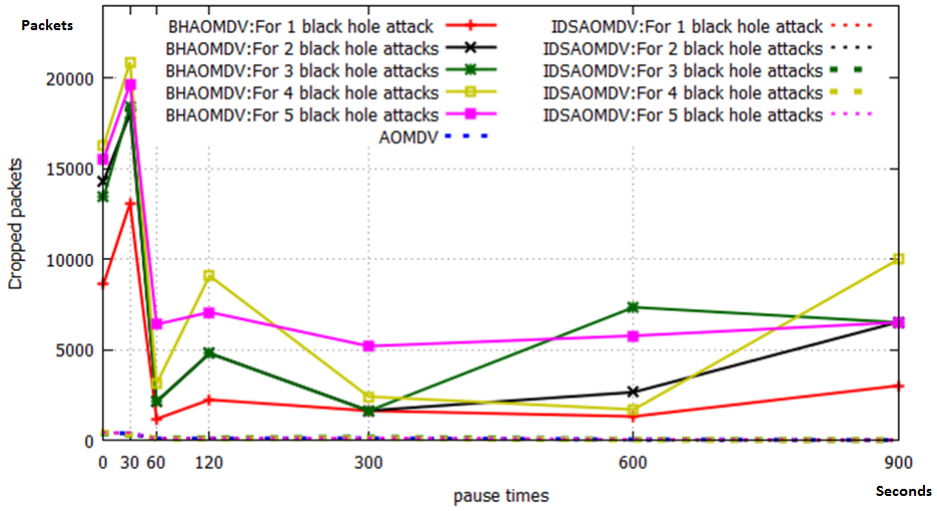

FIGURE 3.10 – *Paquets perdus pour* 10 *nœuds communicants*

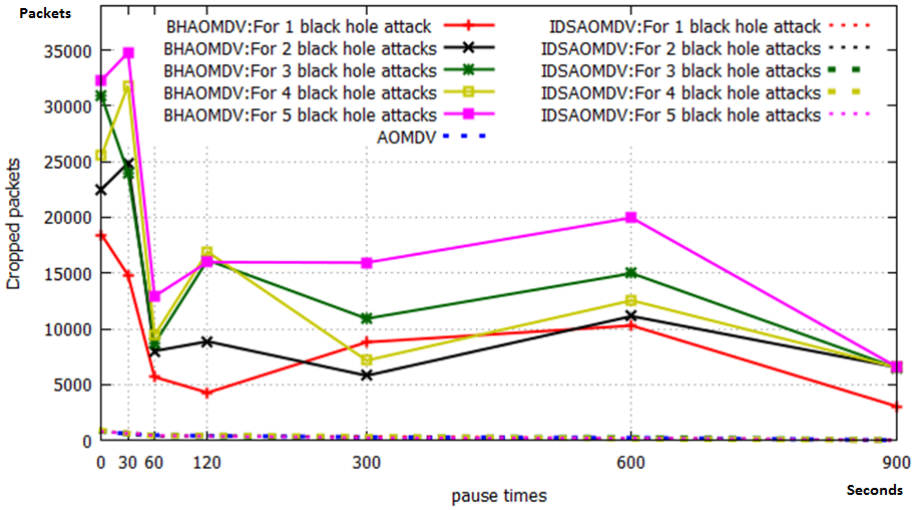

FIGURE 3.11 – *Paquets perdus pour* 20 *nœuds communicants*

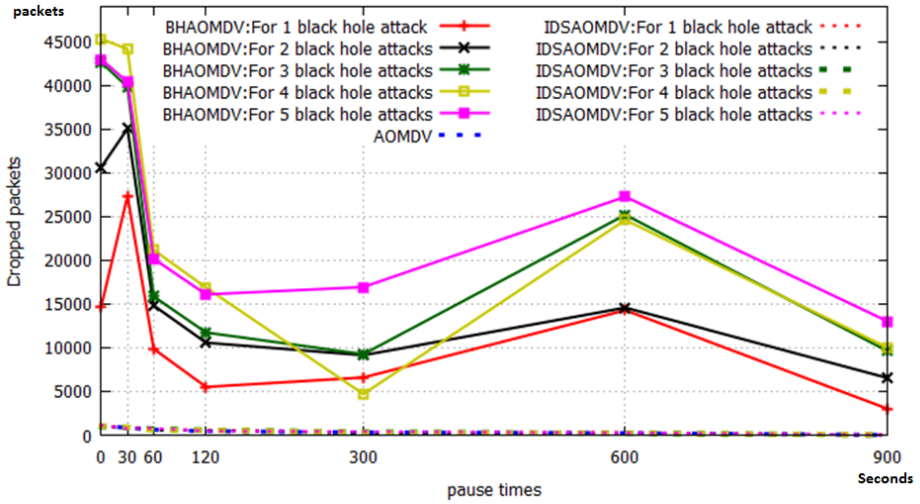

FIGURE 3.12 – *Paquets perdus pour* 30 *nœuds communicants*

pour 10 nœuds communicants en faisant varier le nombre de nœuds com-

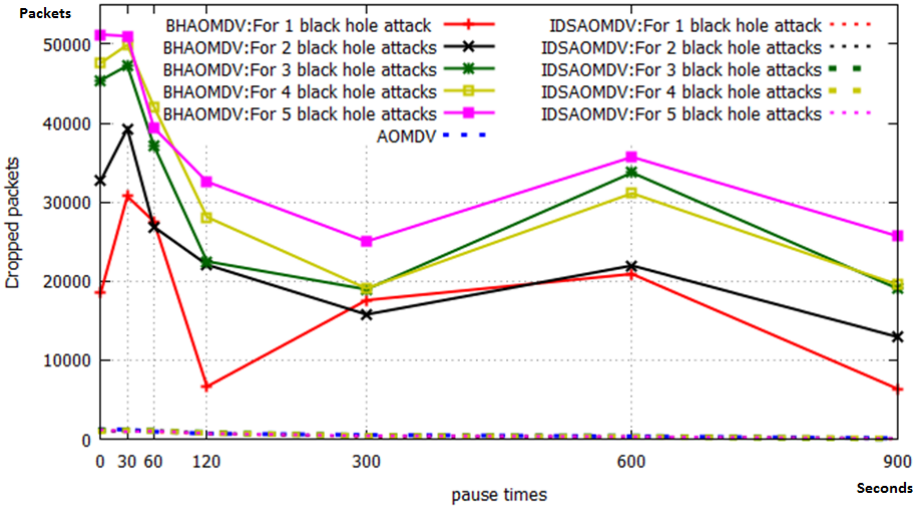

FIGURE 3.13 – *Paquets perdus pour* 40 *nœuds communicants*

municants de 20 à 40 nœuds (figures 3.11, 3.12, et 3.13), aussi, l'augmentation du nombre de nœuds communicants provoque l'augmentation progressive de paquets perdus pour BHAOMDV. De plus, c'est une indication de meilleures garanties de performances lors de l'utilisation de notre technique proposée.

Paquets transmis

Sur les figures 3.14, 3.15, 3.16, et 3.17 et tables 3.16, 3.17, 3.18 et 3.19 (voir annexe) respectivement, nous avons illustré le nombre de paquets transmis dans le cas de AOMDV, BHAOMDV et IDSAOMDV. Dans AOMDV, la probabilité de transmettre des paquets de données augmente en présence de chemins alternatifs dans le réseau si le premier chemin échoue. Dans BHAOMDV, la présence de nœuds malveillants dans le réseau provoque la perte de paquets en raison du mauvais comportement des nœuds malveillants, ainsi le nombre de paquets transmis est inférieur à celui d'AOMDV. En appliquant notre technique dans IDSAOMDV, le nombre de paquets transmis est plus grand que dans BHAOMDV car notre technique évite les nœuds malveillants pour construire les chemins de transmission des paquets de données. Dans le cas de la figure 3.14, le nombre de paquets transmis est de 2847 à 10011 pour AOMDV, de 1420 à 10576 pour BHAOMDV avec présence d'un seul nœud malveillant et de 2956 à 9967 pour IDSAOMDV avec la présence d'un seul nœud malveillant. Ainsi, le nombre de paquets transmis représente 94,35% à 157,68% de plus pour AOMDV que pour BHAOMDV. À mesure que le nombre de nœuds malveillants augmente, le nombre de paquets transmis est considérablement réduit pour BHAOMDV. Le nombre de paquets transmis dans le cas d'IDSAOMDV est très grand par rapport à BHAOMDV. Cela montre que le nombre de paquets transmis de la source à la destination a augmenté pour IDSAOMDV, la raison en est que si un nœud malveillant se présente dans le réseau il provoque la perte de paquets dans le cas de BHAOMDV, mais nous appliquons notre technique dans IDSAOMDV, le noeud malveillant est évité avant que le protocole

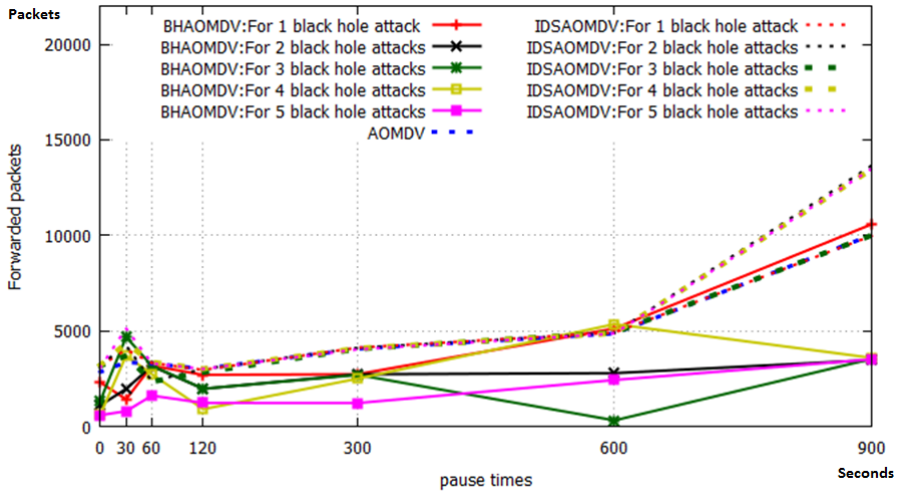

FIGURE 3.14 – *Paquets transmis pour* 10 *nœuds communicants*

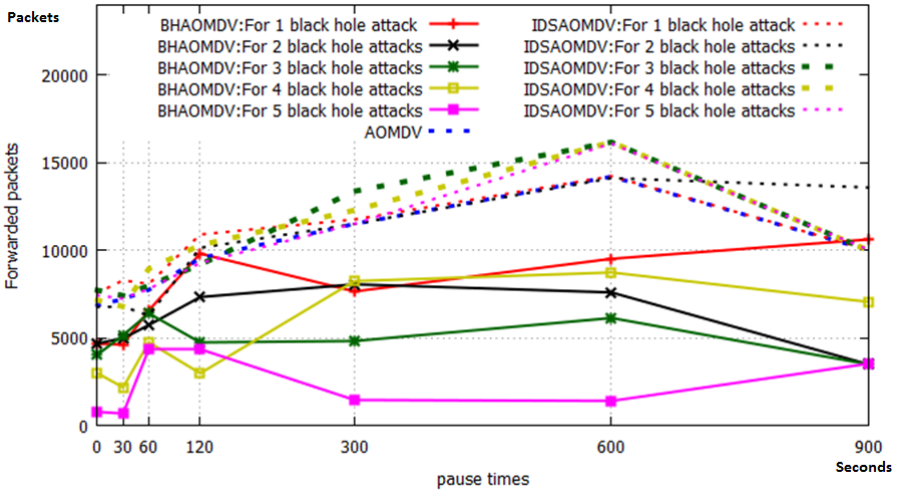

FIGURE 3.15 – *Paquets transmis pour* 20 *nœuds communicants*

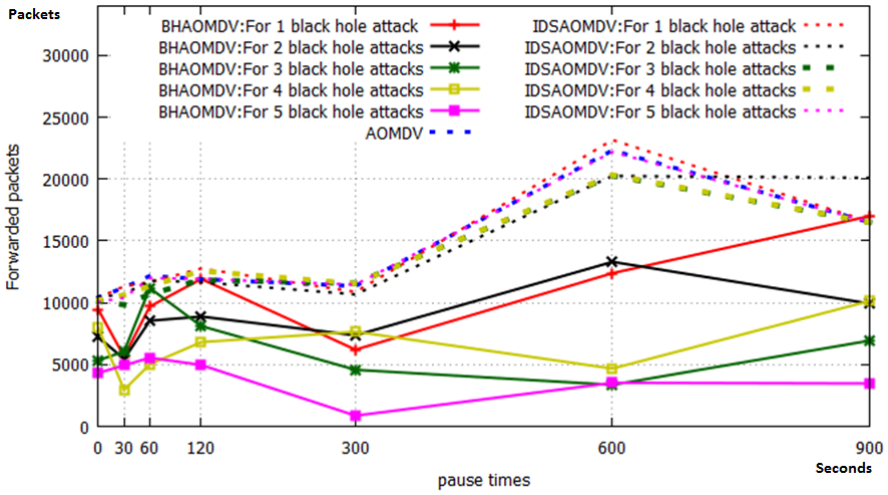

FIGURE 3.16 – *Paquets transmis pour* 30 *nœuds communicants*

n'établisse les chemins de transmission de paquets de données qui maintiennent la fiabilité des chemins construits du noeud source au noeud

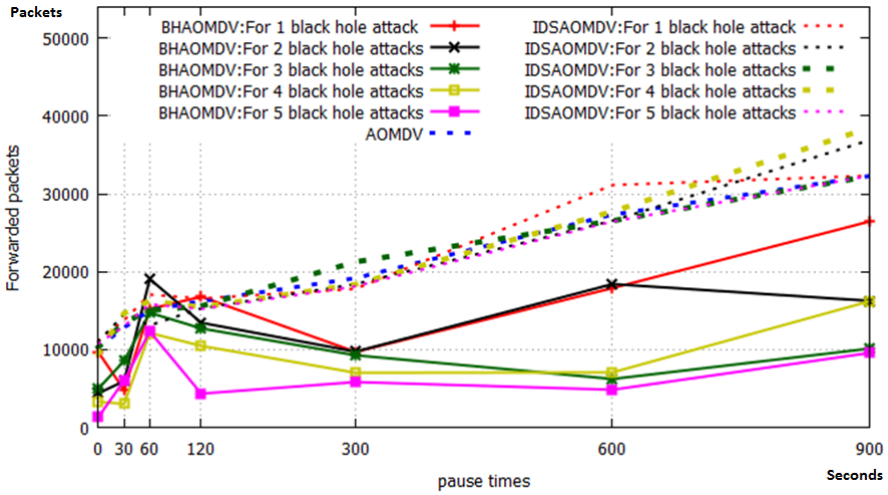

FIGURE 3.17 – *Paquets transmis pour* 40 *nœuds communicants*

de destination et améliore le nombre de paquets transmis. Les résultats présentés sur les figures 3.15, 3.16, et 3.17 se comportent de la même manière que pour 10 nœuds communicants, de plus, l'augmentation du nombre de nœuds communicants entraîne l'augmentation progressive des paquets transmis pour AOMDV, BHAOMDV et IDSAOMDV, en raison de l'utilisation des chemins alternatifs. Ainsi que, plus le nombre de nœuds malveillants est moins, plus le nombre de paquets transmis est plus gros pour BHAOMDV. Les résultats obtenus prouvent l'efficacité de notre technique proposée.

3.3.4 Comparaison avec d'autres approches

Dans cette section, nous comparons notre approche proposée (Tami *et al.* 2021) en termes de performances avec d'autres approches proposées dans la littérature qui sont décrits dans la section 4.2 ((Bhardwaj & Singh 2014), (Sultana & Ahmed 2018), (Elmahdi *et al.* 2018) et (Elmahdi *et al.* 2020)) qui présentent des similitudes avec notre approche proposée. Cette comparaison, a pour but de positionner notre approche par rapport aux autres approches et montrer ces avantages et ces inconvénients.

Dans (Bhardwaj & Singh 2014), lorsque leur approche est mise en œuvre, malgré la présence de nœuds malveillants, le taux de livraison de paquets s'est considérablement amélioré et il atteint 94% lorsque trois nœuds malveillants étaient présents et avec une croissance moyenne supérieure à 60%. Dans (Sultana & Ahmed 2018), le taux de livraison de paquets est certainement le plus élevé sans nœud malveillant dans l'environnement, il atteint 99, 86%. Il diminue lentement avec le nombre croissant de nœuds malveillants, il est de 32% pour un nœud malveillant et de 6% pour trois nœuds malveillants. Dans (Elmahdi *et al.* 2018), le taux de livraison de paquets reste au même niveau (100%) dans le schéma proposé en présence de noeuds malveillants. Dans (Elmahdi *et al.* 2020), le taux de livraison de paquets est proche de plus de 70% pour un seul nœud malveillant, et il n'est pas inférieur à 45% pour 5 nœuds malveillants, mais il est proche de 90% sans nœuds malveillants. Dans notre solution, comme

indiqué dans la section 4.4.3, dans tous les scénarios, le PDR pour IDSAOMDV n'est pas inférieur à 98%.

Dans (Sultana & Ahmed 2018), le délai moyen de bout en bout augmente progressivement avec les nœuds malveillants incrémentés au fur et à mesure que le processus de cryptage avec ECC prend du temps. Le délai moyen de bout en bout est de $85655,8ms$ en présence d'un seul nœud malveillant et de $85658,6ms$ en présence de 3 nœuds malveillants, mais il est de $85652,4ms$ sans nœud malveillant. Dans (Elmahdi *et al.* 2018) et (Elmahdi *et al.* 2020), le délai de bout en bout est plus élevé dans ses schémas que le schéma AOMDV d'origine lorsque le nombre de noeuds malveillants est augmenté en raison de ses procédures et de ses fonctionnalités de sécurité. Dans ces solutions, le message est divisé et chiffré pour atteindre leur fonction. Pour cette raison, la livraison prend plus de temps. Dans notre solution, comme indiqué dans la section 4.4.3, dans tous les scénarios, les délais de bout en bout sont très proches pour IDSAOMDV par rapport à AOMDV.

Dans (Elmahdi *et al.* 2018) et (Elmahdi *et al.* 2020), il y a un impact de plusieurs attaquants parce que le schéma utilise plusieurs chemins simultanément. Même si l'impact est présent avec une perte de données plus élevée dans ce schéma en augmentant le nombre de noeuds malveillants, il délivre presque tout le paquet à la destination en le distribuant dans plusieurs chemins pour assurer la livraison entière via des chemins sûrs. Dans notre solution, comme indiqué dans la section 4.4.3, dans tous les scénarios, les valeurs des paquets abandonnés sont très proches pour IDSAOMDV par rapport à AOMDV.

En résumé, la comparaison couvre la plupart des scénarios tels que le taux de livraison de paquets, le délai moyen de bout en bout et les paquets abandonnés en présence d'attaques trou noir. Sur la base des comparaisons de performances ci-dessus, la solution proposée est très efficace dans la plupart des scénarios que nous avons testés. Le tableau 3.3 résume la comparaison du protocole de routage sécurisé proposé avec certaines approches existantes récentes.

Table 3.3 – Comparaison des approches de routage sécurisées

Approches	Avantages	Désavantages
Notre approche (Tami *et al.* 2021)	-Simple. -Pas de problème de consommation d'énergie. -L'opération de comparaison du numéro de séquence de destination avec une valeur de seuil sur la réponse d'itinéraire n'augmente pas le délai de communication. -Les évaluations comparatives des performances prouvent qu'en détectant et en rejetant les nœuds trou noir dans le réseau, le taux de livraison augmente sans causer trop de retard supplémentaire.	-Impossible de détecter le nœud malveillant s'il n'utilise pas de numéro de séquence de destination élevé. -Problème de zone de stockage en raison de la table supplémentaire. -l'attaque coopérative des nœuds malveillants n'est pas traitée dans ce mécanisme.
(Elmahdi *et al.* 2020)	-La sécurité est élevée en raison de l'utilisation des algorithmes de cryptage / décryptage. -La méthode proposée augmente le taux de livraison et le débit.	-Complexe. -Problème de consommation d'énergie. -Problème de zone de stockage et de puissance de calcul. -Ajoute une charge de calcul importante en raison de la méthode de cryptage homomorphique. -Les opérations de division et de combinaison des messages augmente le délai total de bout en bout dans le réseau.
(Elmahdi *et al.* 2018)	-La sécurité est élevée en raison de l'utilisation d'algorithmes de cryptage / décryptage. -Tous les paquets de données transmis sont reçus avec succès par les nœuds de destination. Le taux de livraison est de 100%. -La méthode proposée augmente le débit.	- Complexe. -Problème de consommation d'énergie. -Problème de zone de stockage et de puissance de calcul. -Ajoute une charge de calcul importante en raison de la méthode de cryptage homomorphique. -Les opérations de division et de combinaison des messages augmente le délai total de bout en bout dans le réseau.
(Sultana & Ahmed 2018)	-Ce mécanisme garantit l'authentification et la confidentialité, dans ce cas la sécurité est élevée en raison de l'utilisation la cryptographie à courbe elliptique (ECC). -Ce protocole prend moins de mémoire avec l'utilisation de ce type de cryptographie.	-A mesure que le processus de chiffrement avec ECC prend du temps avec les nœuds malveillants incrémentés, le délai moyen de bout en bout augmente aussi. -Un grand nombre de nœuds attaquants diminuer gravement le taux de livraison de paquets.

Conclusion

Les réseaux mobiles ad hoc souffrent de plusieurs types d'attaques, en particulier l'attaque trou noir. Il s'agit d'une attaque dans laquelle le nœud malveillant peut falsifier le message de réponse du protocole en prétendant qu'il a le chemin le plus court pour atteindre le nœud de destination. Les mécanismes présentés dans le protocole de routage AOMDV ne tiennent pas compte de la sécurité. Cependant, nous avons proposé une amélioration de l'AOMDV pour détecter et isoler les attaques trou noir. Dans ce chapitre, nous avons étudié les attaques trou noir pour prouver notre technique contre ces attaques. Afin d'analyser ses impacts sur l'AOMDV, nous avons implémenté BHAOMDV avec plusieurs attaques trou noir, et pour détecter et isoler les nœuds malveillants, nous avons également implémenté IDSAOMDV comme solution contre les attaques trou noir. Notre technique proposée fonctionne bien même lorsque plusieurs nœuds malveillants attaquent. Les résultats montrent que les performances des deux protocoles AOMDV et IDSAOMDV sont presque égales. Les résultats prouvent également l'impact des attaques trou noir sur les performances de l'AOMDV et montrent la validité de notre technique proposée dans l'IDSAOMDV comme solution contre les attaques trou noir.

Conclusion générale et perspectives

Ce chapitre présente une conclusion de notre travail de recherche, il comporte une synthèse du travail abordé et il donne un aperçu général sur le travail achevé dans cette thèse. Effectivement diverses perspectives envisageables sont à accomplir dans des futures recherches.

Conclusion générale

Durant les deux dernières décennies, les réseaux mobiles ad hoc ont connu un succès sans cesse progressif au sein des recherches scientifiques et aux développements technologiques. Dus à ses avantages, différents domaines ont été influencés par la technique des réseaux mobiles ad hoc. Afin d'exploiter les meilleures performances des techniques sans fil, il est nécessaire de recouvrir les problèmes de sécurité du routage dans les réseaux mobiles ad hoc.

En raison des caractéristiques des ondes radio qui sont la base fondamentale des transmissions dans les réseaux mobiles ad hoc, ces réseaux sont vulnérables à plusieurs types d'attaques, en effet, les ondes radio peuvent être interceptées à l'écoute ou à d'autres opérations non autorisées. Toutefois, due aux caractéristiques des réseaux mobiles ad hoc, à savoir la topologie dynamique, la bande passante limitée, les contraintes d'énergie, l'absence d'infrastructure fixe, l'absence d'administration centralisée et la sécurité physique limitée, plusieurs types d'attaques ont la possibilité de causer plusieurs problèmes au niveau du routage. Dans certains cas, il est difficile de maintenir des méthodes de protection puissante contre les différentes attaques provoquées par des nœuds malveillants dans leurs buts est de perturber le bon fonctionnement du routage ou de détruire la fonctionnalité de la transmission des paquets dans le réseau.

Le routage est une opération fondamentale dans la composition des routes et l'acheminement des paquets communiqués entre les nœuds dans le réseau. Malheureusement, dans les réseaux mobiles ad hoc cette opération ne prend pas en considération les mesures de sécurité afin de transmettre les paquets entre les nœuds du réseau. Cette situation pose plusieurs problèmes de sécurité dans ce type de réseau.

La sécurité du routage devient un élément crucial dans les protocoles de routage, il sera bénéfique de protéger les paquets communiqués dans les réseaux mobiles ad hoc. Plusieurs protocoles de routage ont été développés au sein des réseaux mobiles ad hoc. Cependant, ces protocoles de routages soufrent particulièrement d'un des principaux défis est celui de la sécurité du routage.

L'objectif de cette thèse est d'assurer le routage pour qu'il gère l'acheminement des paquets dans le réseau d'une manière plus sécurisée. Ce travail de thèse a été justifié par la grande évolution et le rôle de la technologie de communication attaché au sein des réseaux mobiles ad hoc. La sécurité des réseaux prend toujours ça place dans l'évolution de ces technologies. La sécurité des réseaux mobiles ad hoc reste un aspect crucial et un défi pour les chercheurs dans différents domaines utilisant la technologie dans ces réseaux.

Dans cette thèse, nous focalisons notre travail de recherche sur la sécurité du routage dans les protocoles de routage multi-chemins, en particulier le protocole AOMDV. Le routage dans ce protocole ne tient pas compte des comportements des nœuds communicants dans le réseau, il sert à établir les chemins optimaux afin de permet la transmission des paquets entre les nœuds communicants. Ce protocole ne possède pas de mécanismes de vérification de l'authenticité des nœuds qui participes ou qui accèdent au réseau pour communiquer les paquets entre eux, en d'autres

termes, le routage dans ce protocole est vulnérable à plusieurs types d'attaques, parmi eux l'attaque trou noir, où les nœuds attaquants peuvent injecter de faux paquets dans le réseau, dans leurs buts est de perturber le fonctionnement du réseau ou de paralyser la communication entre les nœuds ce qui provoque de graves risques dans le réseau.

L'effet de l'attaque trou noir est très dangereux dans le réseau, le nœud attaquant peut utiliser incorrectement les paquets reçus d'autres nœuds, comme il peut supprimer les paquets de données. Ce qui provoque la complication des communications entre les nœuds, la non-transmission des paquets des données et le mal fonctionnement du réseau. L'attaque trou noir peut agir profondément sur les performances du protocole de routage dans le réseau, par exemple il augmente le nombre de paquets perdus et il réduit le taux de délivrance des paquets.

Dans cette thèse, nous avons étudié et analysé plusieurs approches aperçues dans la littérature étayant la sécurité contre les attaques dans les réseaux mobiles ad hoc. Nous avons ensuite proposé une solution pour apaiser aux problèmes de la sécurité du routage contre les attaques trou noir dans le protocole AOMDV. Les chapitres antérieurs étale cet objectif.

Après avoir présenté les points essentiels de ce travail de recherche et l'objectif de cette thèse, nous allons ensuite donner un aperçu sur notre contribution.

Pour résoudre le problème de vulnérabilité du protocole AOMDV, nous avons proposé un mécanisme de détection et d'isolement des attaques trou noir dans le réseau. Cette solution est fondée essentiellement sur le message de réponse de la demande de route (RREP), et basée particulièrement sur le numéro de séquence de destination (DSN). Un seuil est calculé qui permet la sélection des nœuds légitimes ou malveillants, de sorte que seuls les nœuds légitimes peuvent participer à la communication entre les nœuds du réseau et à la transmission des paquets de données dans ce réseau. Les fonctionnalités principales du protocole AOMDV sont conservées. Cette idée est la base notre travail de recherche. Le chapitre 3 décrit cette idée.

Dans cette thèse, nous avons élaboré une solution sécurisée pour remédier au problème des attaques trou noir. Nous avons implémenté deux protocoles basés sur AOMDV. Le premier protocole BHAOMDV qui comporte le protocole AOMDV sous attaques trou noir, dédié pour étudier le comportement des attaques trou noir, et pour analyser l'impact des attaques trou noir sur les performances et le fonctionnement du protocole AOMDV. Cela nous a permis d'observer les effets des attaques trou noir, d'analyser les résultats obtenus, de comprendre le comportement de ces attaques. Cette partie du travail nous a ouvert une nouvelle voie pour proposer un protocole amélioré du protocole AOMDV d'origine. Le deuxième protocole IDSAOMDV qui inclut notre mécanisme de détection et d'isolement des attaques trou noir.

Nous avons utilisé *NS*2.35 comme simulateur de notre solution proposé. NS (Network Simulator) est un logiciel libre de simulation d'événements discrets conçu pour les réseaux de communication filaires et sans fil. Pour étudier l'impact des attaques trou noir sur le protocole de routage AOMDV, et évaluer notre solution proposée, nous avons effectué plusieurs simulations selon plusieurs étapes préparées et bien déterminées,

nous avons varié le nombre de nœuds attaquants, le nombre de nœuds communiquants et le temps de pause, nous avons conçu 4 scénarios différents. Nous avons utilisé les métriques de performances, telles que le PDR, AEED, FP et DP.

Une étude comparative est effectuée entre notre protocole proposé IDSAOMDV, le protocole AOMDV, et le protocole BHAOMDV. Les résultats obtenus sont observés, représentés, analysés, et étudiés afin de donner des critiques et décisions sur l'impact des attaques trou noir sur le protocole AOMDV, l'efficacité de notre protocole proposé IDSAOMDV contre les attaques trou noir. Ainsi, notre solution proposée est comparée avec d'autres solutions existant dans la littérature qui traite la sécurité contre le même problème de l'attaque trou noir dans le même champ du travail de recherche.

Les résultats des simulations montrent clairement les mauvais comportements des nœuds malveillants, le mal fonctionnement du réseau et la dégradation des performances en présence des nœuds malveillants dans le réseau. Ces résultats montrent aussi que notre solution proposée est largement similaire au protocole de routage AOMDV en termes de performances tels que PDR, DP, FP, AEED.

Par le biais des résultats obtenus, et les comparaisons effectuées, nous avons conclu que notre solution proposée est convenable pour remédier au problème des attaques trou noir dans le protocole AOMDV. Toutefois, nous avons montré que notre technique permet d'assurer la sécurité du routage dans le protocole AOMDV, cette technique permet de détecter et d'isoler les nœuds malveillants dans le réseau, de protéger les paquets contre les attaques trou noir, de choisir les chemins sécurisés pour transmettre les paquets dans le réseau et de garantir les bonnes performances du réseau et de soutenir les fonctionnalités du protocole de routage.

Perspectives

Basant sur les analyses observées dans les chapitres antérieurs, appuyant en particulier sur la contribution et les limites de notre solution, cette thèse pose certainement quelques chemins pour les futures recherches. Après avoir entamé ce travail de recherche, nous avons inspiré plusieurs nouvelles pistes de recherches et nous avons octroyé des idées qui peuvent être considérées comme perspectives. Ci-après, nous citons quelques perspectives pour les futures recherches, à savoir :

Nous envisageons d'étudier notre solution avec modifications des paramètres de simulations, à savoir augmenter le nombre de nœuds malveillants, le nombre de nœuds communicants afin de percevoir le fonctionnement du protocole dans cette situation et discerner comment les performances du protocole vont être agies selon ces conditions. Il est préférable d'implémenter des mécanismes dans des situations déférentes que ce soit un environnement qui contient un petit nombre de nœuds ou dans un environnement vaste. Toutefois, réaliser des expérimentations dans un environnement réel avec des équipements technologiques permettre une grande validité aux résultats obtenus par les simulations effectuées sur notre mécanisme de détection et d'isolement des nœuds malveillants. Afin

d'avoir des résultats qui garantit l'opportunité de notre mécanisme proposé, il devient incontestable d'exécuter les expérimentations dans un environnement réel.

Nous avons concentré notre travail sur les attaques trou noir simples et multiples qui posent des problèmes graves au protocole de routage AOMDV, nous espérons dans un premier temps d'étendre notre solution de détection et d'isolement des nœuds malveillants par une amélioration de notre mécanisme de base ou l'ajout d'un autre mécanisme de sécurité qui détecte et défend le réseau contre les attaques trou noir coopératives. Comme ça, nous percevons d'accomplir un renforcement de notre solution contre tous types d'attaques à savoir simple, multiple ou coopérative. Cela impose plus de sécurité et détecter plus d'attaques et garantir une excellente protection des communications dans le réseau.

Il est préférable d'allonger le champ de détection et d'isolement des nœuds malveillants et qu'il intègre des mécanismes sécurisés contre plusieurs types d'attaques. Dans cette thèse, nous avons étudié, analysé et accomplir une solution de détection et d'isolement contre seulement l'attaque trou noir, dans les futurs travaux, nous envisageons et préférons améliorer notre solution proposée ou d'ajouter d'autres mécanismes afin de les appliquer pour d'autres types d'attaques à savoir l'attaque trou gris (Greyhole Attack), l'attaque trou de ver (Wormhole Attack), l'attaque précipitée (Rushing Attack) et l'attaque par déni de service (DoS attack pour Denial of Service attack). C'est très intéressé à étudier et d'évaluer des mécanismes convenables pour sécuriser le routage dans le protocole AOMDV.

Le travail effectué dans cette thèse se focalise sur les protocoles de routage multi-chemins, il s'articule sur le protocole AOMDV. Nous souhaitons arranger et étendre notre mécanisme proposé et de l'appliquer pour d'autres protocoles de routage multi-chemins ayant des principes de fonctionnement similaires au protocole AOMDV. Il est avantageux d'étudier et analyser le routage multi-chemins et les principes de sécurité afin d'apercevoir des solutions appropriées à ce type de routage.

Contributions scienfifiques

— Abdelaziz TAMI, Sofiane BOUKLI HACENE, and Moussa ALI CHERIF, "Detection and prevention of Blackhole attack in the AOMDV routing protocol", Journal of Communications Software and Systems (JCOMSS), vol. 17, no. 1, pp. 1-12, DOI : 10.24138/jcomss.v17i1.945, 2021.
— Abdelaziz TAMI, Sofiane BOUKLI HACENE, and Moussa ALI CHERIF, "Detect Black hole attacks and protect packets in Mobile Ad-hoc Network using AOMDV routing protocol", qui sera prochainement soumissionné.

Bibliographie

[Ait-Salem 2011] B. Ait-Salem. *Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques*. PhD thesis, Département de Mathématiques et Informatique, Université de Limoges, 2011.

[Aluvala *et al.* 2016] S. Aluvala, K. R. Sekhar et D. Vodnala. *An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks*. Procedia Computer Science, vol. 92, pages 554–561, 2016.

[Ayanoglu *et al.* 1993] E. Ayanoglu, I. Chih-Lin, R. D. Gitlin et J. E. Mazo. *Diversity coding for transparent self-healing and fault-tolerant communication networks*. IEEE Transactions on communications, vol. 41, no. 11, pages 1677–1686, 1993.

[Bakshi *et al.* 2013] A. Bakshi, A. K. Sharma et A. Mishra. *Significance of mobile AD-HOC networks (MANETS)*. International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 2, no. 4, pages 1–5, 2013.

[Bargaoui 2016] H. Bargaoui. *Gestion optimisée et autonome des réseaux radio maillés : garantie du niveau de service de bout en bout avec un routage basé sur la QoS*. PhD thesis, Cotutelle entre l'Université de Bourgogne et l'Université de Carthage Tunis, 2016.

[Bertsekas & Gallager 1992] D. Bertsekas et R. Gallager. Routing in Data Networks, volume 1, chapitre Chapter 5, pages 363–492. Prentice Hall, Englewood Cliffs, New Jersey 07632, second edition édition, 1 1992.

[Bhardwaj & Singh 2014] N. Bhardwaj et R. Singh. *Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs*. International Journal of Application or Innovation in Engineering and Management (IJAIEM), vol. 3, no. 5, pages 376–383, 2014.

[Bhattacharyya *et al.* 2011] A. Bhattacharyya, A. Banerjee, D. Bose, H. N. Saha et D. Bhattacharya. *Different types of attacks in Mobile ADHOC Network*. arXiv preprint arXiv :1111.4090, 11 2011.

[Burgod 2009] C. Burgod. *Contribution à la sécurisation du routage dans les réseaux ad hoc*. PhD thesis, Université de Limoges, 10 2009.

[Burmester & Van Le 2004] M. Burmester et T. Van Le. *Secure multipath communication in mobile ad hoc networks*. In International Conference on Information Technology : Coding and Computing, 2004. Proceedings. ITCC 2004., volume 2, pages 405–409. IEEE, 2004.

[Chan & Perrig 2003] H. Chan et A. Perrig. *Security and Privacy in Sensor Networks*. Computer, vol. 36, no. 10, pages 103–105, 10 2003.

[Chelius 2004] G. Chelius. *Architectures et communications dans les réseaux spontanés sans-fil*. PhD thesis, Institut National des Sciences Appliquées, Université de Lyon, 2004.

[Corson & Macker 1999] S. Corson et J. Macker. *Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations*. Rapport technique, RFC2501, 1999.

[Deng *et al.* 2002] H. Deng, W. Li et D. P. Agrawal. *Routing Security in Wireless Ad Hoc Networks*. IEEE Communications Magazine, vol. 40, no. 10, pages 70–75, 10 2002.

[Devikar *et al.* 2016] R. N. Devikar, D. V. Patil et V. Chandraprakash. *Issues in Routing Mechanism for Packets Forwarding : A Survey*. International Journal of Electrical and Computer Engineering, vol. 6, no. 1, page 421, 2016.

[Dipobagio 2009] M. Dipobagio. *An overview on ad hoc networks*. Institute of Computer Science (ICS), Freie Universität Berlin, 2009.

[Elmahdi *et al.* 2018] E. Elmahdi, S. M. Yoo et K. Sharshembiev. *Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks*. In 2018 IEEE 8th annual computing and communication workshop and conference (CCWC), pages 463–467. IEEE, 2018.

[Elmahdi *et al.* 2020] E. Elmahdi, S. M. Yoo et K. Sharshembiev. *Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks*. Journal of Information Security and Applications, vol. 51, page 102425, 2020.

[Ganjali & Keshavarzian 2004] Y. Ganjali et A. Keshavarzian. *Load balancing in ad hoc networks : single-path routing vs. multi-path routing*. In IEEE INFOCOM 2004, volume 2, pages 1120–1125. IEEE, 2004.

[Garcia-Luna-Aceves & Mosko 2005] J. J. Garcia-Luna-Aceves et M. Mosko. *Multipath routing in wireless mesh networks*. In in Proc. IEEE Workshop on Wireless Mesh Networks (WiMesh. Citeseer, 2005.

[Garcia-Lunes-Aceves 1993] J. J. Garcia-Lunes-Aceves. *Loop-free routing using diffusing computations*. IEEE/ACM transactions on networking, vol. 1, no. 1, pages 130–141, 1993.

[Gopi 2014] P. Gopi. *Multipath Routing in Wireless Sensor Networks : A Survey and Analysis*. IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 4, pages 27–34, 2014.

[Gurung & Saikia 2015] S. K. Gurung et D. K. Saikia. *A Survey of Multipath Routing Schemes of Wireless Mesh Networks*. International Journal of Computer Applications, vol. 125, no. 14, pages 12–20, 2015. Published by Foundation of Computer Science (FCS), NY, USA.

[Hu *et al.* 2003a] Y. C. Hu, A. Perrig et D. B. Johnson. *Packet leashes : A defense against wormhole attacks in wireless networks*. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), volume 3, pages 1976–1986. IEEE, 03 2003.

[Hu *et al.* 2003b] Y. C. Hu, A. Perrig et D. B. Johnson. *Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols*. In Proceedings of the 2nd ACM workshop on Wireless security, pages 30–40, 2003.

[Hu *et al.* 2005] Y. C. Hu, A. Perrig et D. B. Johnson. *Ariadne : A Secure On-Demand Routing Protocol for Ad Hoc Networks*. Wireless Networks, vol. 11, no. 1, pages 21–38, 2005.

[Jadye 2016] S. Jadye. *Survey of MANET Attacks, Security Concerns and Measures*. International Journal of Computer Science and Information Technologies (IJCSIT), vol. 7, no. 2, pages 1014–1017, 2016.

[Johnson & Maltz 1996] D. B. Johnson et D. A. Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks*. In Mobile computing, pages 153–181. Springer, 1996.

[Johnson *et al.* 2007] D. B. Johnson, Y. C. Hu et D. A. Maltz. *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*. Rapport technique, RFC 4728, 2 2007.

[Johnson 1994] D. B. Johnson. *Routing in Ad Hoc Networks of Mobile Hosts*. In 1994 First Workshop on Mobile Computing Systems and Applications, pages 158–163. IEEE, 1994.

[Kabeto 2000] M. D. Kabeto. *The Design and Simulation of Routing Protocols for Mobile Ad hoc Networks*. PhD thesis, University of Natal, Durban, 12 2000.

[Karlof & Wagner 2003] C. Karlof et D. Wagner. *Secure Routing in Wireless Sensor Networks : Attacks and Countermeasures*. Ad Hoc Networks, vol. 1, no. 2, pages 293–315, 2003.

[Kumar 2011] A. Kumar. *Security Attacks in Manet - A Review*. In IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing, 2011.

[Lee & Gerla 2000] S. J. Lee et M. Gerla. *AODV-BR : Backup Routing in Ad hoc Networks*. In 2000 IEEE Wireless Communications and Networking Conference, volume 3, pages 1311–1316. IEEE, 2000.

[Lee & Gerla 2001] S. J. Lee et M. Gerla. *Split multipath routing with maximally disjoint paths in ad hoc networks*. In IEEE International Conference on Communications, ICC 2001, June 11-14, Helsinki, Finland, volume 10, pages 3201–3205. IEEE, 2001.

[Li & Joshi 2008] W. Li et A. Joshi. *Security Issues in Mobile Ad Hoc Networks - A Survey*. White House Papers Graduate Research in Informatics at Sussex, vol. 17, 1 2008.

[Lou *et al.* 2006] W. Lou, W. Liu et Y. Zhang. *Performance Optimization using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks*. In Combinatorial Optimization in Communication Networks, pages 117–146. Springer, 2006.

[Lu 2004] H. Lu. *Wireless Ad-hoc Networks*. Wirel. Pers. Commun. J, vol. 4, 2004.

[Lundberg 2000] J. Lundberg. *Routing Security in Ad Hoc Networks*, 2000.

[Mahmoud *et al.* 2015] T. M. Mahmoud, A. A. Aly et O. Makram. *A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs*. International Journal of Computer Applications, vol. 109, no. 6, pages 27–33, 2015.

[Mansouri & Bouhlel 2014] A. Mansouri et M. S. Bouhlel. *Algorithmes dynamiques pour la communication dans le réseau ad hoc : Coloration des graphes*. CoRR, vol. abs/1406.1329, 2014.

[Marina & Das 2001] M. K. Marina et S. R. Das. *On-Demand Multipath Distance Vector Routing in Ad Hoc Networks*. In Proceedings Ninth International Conference on Network Protocols. ICNP 2001, pages 14–23. IEEE, 2001.

[Marina & Das 2006] M. K. Marina et S. R. Das. *Ad Hoc on-Demand Multipath Distance Vector Routing*. Wireless Communications and Mobile Computing, vol. 6, no. 7, pages 969–988, 2006.

[Marina 2001] S. R. Marina M. K. Das. *On-Demand Multipath Distance Vector Routing in Ad Hoc Networks*. In Proceedings Ninth International Conference on Network Protocols. ICNP 2001, pages 14–23. IEEE, 2001.

[Marina 2006] S. R. Marina M. K. Das. *Ad Hoc on-Demand Multipath Distance Vector Routing*. Wireless Communications and Mobile Computing, vol. 6, no. 7, pages 969–988, 2006.

[Mishra & Nadkarni 2003] A. Mishra et K. M. Nadkarni. Security in wireless ad hoc networks, pages 499–549. CRC Press, Inc., 2003.

[Mistry *et al.* 2010] N. Mistry, D. C. Jinwala et M. Zaveri. *Improving AODV Protocol against Blackhole Attacks*. In Proceeding of the International MultiConference of Engineers and Computer Scientists, volume 2. Citeseer, 2010.

[Monnet 2015] Q. Monnet. *Modèles et mécanismes pour la protection contre les attaques par déni de service dans les réseaux de capteurs sans fil*. PhD thesis, Université Paris-Est, 7 2015.

[Mueller *et al.* 2003] S. Mueller, R. P. Tsang et D. Ghosal. *Multipath Routing in Mobile Ad Hoc Networks : Issues and Challenges*. In Mariacarla Calzarossa et Erol Gelenbe, editeurs, Performance Tools and Applications to Networked Systems, Revised Tutorial Lectures [from MASCOTS 2003], volume 2965 of *Lecture Notes in Computer Science*, pages 209–234. Springer, 2003.

[Murshedi *et al.* 2016] T. A. Murshedi, X. Wang et H. Cheng. *On-demand Multipath Routing Protocols for Mobile Ad-Hoc Networks : A Comparative Survey*. International Journal of Future Computer and Communication, vol. 5, no. 3, pages 148–157, 2016.

[Murthy & Manoj 2004] C. S. R. Murthy et B. S. Manoj. Ad Hoc Wireless Networks : Architectures and Protocols. Prentice Hall Communications Engineering and Emerging Technologies. Pearson education, 5 2004.

[Narware *et al.* 2019] K. Narware, R. Paliwal et C. Agrwal. *Congestion Control and Multipath Routing Technique in MANET : A Survey*. International Journal of Scientific & Engineering Research, vol. 10, no. 1, pages 1332–1338, 1 2019.

[Nasipuri & Das 1999] A. Nasipuri et S. R. Das. *On-Demand Multipath Routing for Mobile Ad Hoc Networks*. In Proceedings Eight International Conference on Computer Communications and Networks (Cat. No. 99EX370), pages 64–70. IEEE, 1999.

[Nasipuri *et al.* 2000] A. Nasipuri, R. Castaneda et S. R. Das. *Performance of Multipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks*. Mobile Networks and applications, vol. 6, no. 4, pages 339–349, 2000.

[Park & Corson 1997] V. D. Park et M. S. Corson. *A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks*. In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), volume 3, pages 1405–1413. IEEE, 1997.

[Perkins & Bhagwat 1994] C. E. Perkins et P. Bhagwat. *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers*. ACM SIGCOMM computer communication review, vol. 24, no. 4, pages 234–244, 1994.

[Perkins & Royer 1999] C. E. Perkins et E. M. Royer. *Ad-hoc on-demand distance vector routing*. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100. IEEE, 2 1999.

[Perkins *et al.* 2003] C. Perkins, E. M. Royer et S. Das. *Ad hoc On-Demand Distance Vector (AODV) Routing*. Rapport technique, IETF Internet-Draft, 2003.

[Ploumidis *et al.* 2017] M. Ploumidis, N. Pappas et A. Traganitis. *Flow Allocation for Maximum Throughput and Bounded Delay on Multiple Disjoint Paths for Random Access Wireless Multihop Networks*. IEEE Transactions on Vehicular Technology, vol. 66, no. 1, pages 720–733, 2017.

[Rachedi 2008] A. Rachedi. *Contributions à la sécurité dans les réseaux mobiles ad Hoc*. PhD thesis, Université d'Avignon, 2008.

[Raj & Sumathi 2018] L. D. A. A. Raj et P. Sumathi. *A Study on Multipath Based Routing in Wireless Sensor Communication Networks*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 3, pages 210–214, 2018.

[Raj & Swadas 2009] P. N. Raj et P. B. Swadas. *DPRAODV : A dyanamic learning system against blackhole attack in aodv based manet*. International Journal of Computer Science Issue, vol. 2, pages 54–59, 2009.

[Raju & Garcia-Luna-Aceves 1999] J. Raju et J. J. Garcia-Luna-Aceves. *A New Approach to On-demand Loop-Free Multipath Routing*. In Proceedings Eight International Conference on Computer Communications and Networks (Cat. No. 99EX370), pages 522–527. IEEE, 1999.

[Reddy & Nagendra 2019] Y. V. Reddy et M. Nagendra. *Data Security through Node-Disjoint on Demand Multipath Routing in MANETs*. International Journal of Advanced Networking and Applications, vol. 10, no. 5, pages 3990–3998, 2019.

[Reddy & Raghavan 2007] L. R. Reddy et S. V. Raghavan. *SMORT : Scalable Multipath On-Demand Routing for Mobile Ad Hoc Networks*. Ad Hoc Networks, vol. 5, no. 2, pages 162–188, 2007.

[Shacham *et al.* 1983] N. Shacham, E. Craighill et A. Poggio. *Speech Transport in Packet-Radio Networks with Mobile Nodes*. IEEE Journal on Selected Areas in Communications, vol. 1, no. 6, pages 1084–1097, 1983.

[Siddiqui *et al.* 2007] M. S. Siddiqui, S. O. Amin, J. H. Kim et C. S. Hong. *Mhrp : A secure multi-path hybrid routing protocol for wireless mesh network*. In MILCOM 2007-IEEE Military Communications Conference, pages 1–7. IEEE, 2007.

[Subhankar 2005] D. Subhankar. *MANET : Applications, Issues, and Challenges for the Future*. International Journal of Business Data Communications and Networking, vol. 1, no. 2, pages 66–92, 2005.

[Sultana & Ahmed 2018] J. Sultana et T. Ahmed. *Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET*. International Journal of Electrical & Computer Engineering (2088-8708), vol. 8, no. 6, pages 4412–4422, 2018.

[Suresh *et al.* 2017] K. C. Suresh, K. Haripriya et S. R. Kruthika. *Cooperative Multipath Admission Control Protocol : A Load Balanced Multipath Admission Policy*. 2nd World Research Journals Congress 2017 at Bangkok, Thailand, vol. 2, pages 134–139, 8 2017.

[Tami *et al.* 2021] A. Tami, S. Boukli Hacene et M. Ali Cherif. *Detection and prevention of Blackhole attack in the AOMDV routing protocol*. Journal of Communications Software and Systems (JCOMSS), vol. 17, no. 1, pages 1–12, 2021.

[Tsai & Moors 2006] J. Tsai et T. Moors. *A Review of Multipath Routing Protocols : From Wireless Ad Hoc to Mesh Networks*. In ACoRN Early Career Researcher Workshop on Wireless Multihop Networking. IEEE, volume 30. Citeseer, 2006.

[Ubéda 2008] S. Ubéda. Ad hoc networks : principles and routing, volume 6, pages 7–34. ISTE Ltd and John wiley & Sons, Inc., 2008.

[Valera *et al.* 2003] A. Valera, W. K. G. Seah et S. V. Rao. *Cooperative Packet Caching and Shortest Multipath Routing in Mobile Ad hoc Networks*. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), volume 1, pages 260–269. IEEE, 2003.

[Vanhala 2000] A. Vanhala. *Security in Ad-hoc Networks*. In Research Seminar on Security in Distributed Systems. Citeseer, 2000.

[Vermeulen *et al.* 2020] K. Vermeulen, J. P. Rohrer, R. Beverly, O. Fourmaux et T. Friedman. *Diamond-Miner : Comprehensive Discovery of the Internet's Topology Diamonds*. In 17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20), pages 479–493, 2020.

[Vinod & Madhusudan 2012] D. S. Vinod et G. Madhusudan. *Novel Technique of Multipath Routing Protocol in Ad hoc Network*. International Journal of Computer Networks & Communications (IJCNC), vol. 4, no. 3, pages 109–119, 5 2012.

[Vishnu *et al.* 2010] K. Vishnu, A. J. Paul, K. Vishnu et Amos J. Paul. *Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks*. International Journal of Computer Applications, vol. 1, no. 22, pages 38–42, 2010.

[Wang & Crowcroft 1990] Z. Wang et J. Crowcroft. *Shortest Path First with Emergency Exits*. In Proceedings of the ACM symposium on Communications architectures & protocols, pages 166–176, 1990.

[Wang & Tseng 2007] Y. C. Wang et Y. C. Tseng. *Attacks and Defenses of Routing Mechanisms in Ad Hoc and Sensor Networks*. Security in Sensor Networks, pages 3–25, 2007.

[Wang *et al.* 2003] A. I. A. Wang, G. H. Kuenning et P. Reiher. *Multipath Routing in Ad Hoc Networks*. In Mobile and Wireless Internet, pages 245–262. Springer, 2003.

[Weiser 1993] M. Weiser. *Some computer sciences issues in ubiquitous computing*. Communications of the ACM, vol. 36, no. 7, pages 75–84, 1993.

[Yang & Wang 2008] Y. Yang et J. Wang. *Design guidelines for routing metrics in multihop wireless networks*. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications, pages 1615–1623. IEEE, 2008.

[Yang *et al.* 2004] H. Yang, H. Luo, F. Ye, S. Lu et L. Zhang. *Security in Mobile Ad Hoc Networks : Challenges and Solutions*. IEEE Wireless Communications, vol. 11, no. 1, pages 38–47, 2004.

[Ye *et al.* 2003] Z. Ye, S. V. Krishnamurthy et S. K. Tripathi. *A Framework for Reliable Routing in Mobile Ad Hoc Networks*. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), volume 1, pages 270–280. IEEE, 2003.

[Zhang & Zhou 2003] C. Zhang et M. Zhou. *A stochastic petri net approach to modeling and analysis of ad hoc network*. In International Conference on Information Technology : Research and Education, 2003. Proceedings. ITRE2003., pages 152–156. IEEE, 2003.

[Zhou & Haas 1999] L. Zhou et Z. J. Haas. *Securing Ad Hoc Networks*. IEEE Networks Special Issue on Network Security, 11/12 1999.

Annexe

Table 3.4 – PDR pour 10 noeuds communicants

Pause time (s)	Packet Delivery Ratio (%)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	98.72	74.64	57.96	60.51	52.10	54.30	98.75	98.65	98.89	98.69	98.73
30	98.96	61.57	47.01	45.75	38.51	42.16	98.99	98.93	99.15	99.08	98.78
60	99.73	96.56	93.73	93.80	90.85	81.19	99.73	99.69	99.74	99.73	99.77
120	99.75	93.43	85.91	85.97	73.29	79.22	99.69	99.74	99.66	99.72	99.75
300	99.71	95.23	95.22	95.25	92.93	84.75	99.73	99.69	99.55	99.69	99.63
600	99.88	96.15	92.21	78.40	95.02	83.04	99.94	99.94	99.89	99.95	99.87
900	99.99	91.15	80.81	80.88	70.61	80.86	99.99	100	99.99	99.99	99.99

Table 3.5 – PDR pour 20 noeuds communicants

Pause time (s)	Packet Delivery Ratio (%)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	98.86	72.21	66.04	53.55	61.47	51.38	98.96	98.69	98.76	98.69	98.84
30	99.13	77.73	62.56	63.87	52.10	47.56	98.92	99.23	99.12	99.11	99.10
60	99.34	91.45	87.94	86.93	85.82	80.51	99.46	99.50	99.40	99.43	99.39
120	99.42	93.59	86.67	75.69	74.57	75.96	99.46	99.38	99.42	99.35	99.46
300	99.59	86.76	91.29	83.59	89.23	76.00	99.50	99.68	99.63	99.51	99.69
600	99.69	84.53	83.26	77.48	81.11	69.94	99.74	99.75	99.68	99.83	99.74
900	99.99	95.43	90.16	90.23	90.16	90.11	99.99	99.99	99.98	99.99	99.99

Table 3.6 – PDR pour 30 noeuds communicants

Pause time (s)	Packet Delivery Ratio (%)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	98.95	85.09	69.07	56.93	54.15	56.55	98.99	98.94	99.02	98.93	98.85
30	99.16	72.38	64.64	59.79	55.42	59.21	99.09	99.18	99.12	99.09	99.24
60	99.37	90.05	85.02	83.97	78.61	79.62	99.34	99.44	99.30	99.44	99.20
120	99.54	94.43	89.32	88.15	82.95	83.73	99.42	99.45	99.42	99.44	99.53
300	99.69	93.35	90.76	90.64	95.25	82.89	99.68	99.76	99.66	99.70	99.60
600	99.77	85.57	85.28	74.55	75.12	72.44	99.69	99.75	99.79	99.78	99.73
900	99.97	96.94	93.38	90.27	89.88	86.82	99.97	99.97	99.98	99.95	99.98

Table 3.7 – PDR pour 40 noeuds communicants

Pause time (s)	Packet Delivery Ratio (%)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	99.03	85.80	74.86	65.15	63.45	60.72	99.17	99.19	99.15	99.24	99.09
30	99.08	76.43	69.90	63.74	61.72	60.85	99.23	99.29	99.13	99.16	99.30
60	99.27	78.87	79.38	71.49	67.71	69.76	99.28	99.14	99.19	99.21	99.22
120	99.47	94.90	83.06	82.74	78.45	74.99	99.49	99.42	99.39	99.41	99.46
300	99.60	86.50	87.89	85.46	85.38	80.81	99.74	99.72	99.67	99.68	99.69
600	99.73	83.98	83.16	74.11	76.12	72.61	99.76	99.76	99.75	99.80	99.75
900	99.92	95.12	90.08	85.39	84.98	80.30	99.97	99.92	99.97	99.93	99.95

Table 3.8 – AEED pour 10 noeuds communicants

Pause time (s)	Average End to End Delay ($\times 10^{-4} ms$)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	9,63	95,54	214,96	115,68	132,90	9,20	9,65	74,38	79,44	9,70	133,70
30	9,64	9,38	10,35	9,63	88,72	9,41	9,86	9,92	9,72	10,01	10,25
60	9,47	9,50	9,53	9,53	9,38	9,05	9,44	9,20	9,20	9,51	9,47
120	9,38	16,82	9,14	17,40	18,39	8,97	9,32	9,39	9,33	9,40	9,39
300	9,69	9,37	9,31	9,30	9,00	8,89	9,68	9,68	9,72	9,70	9,70
600	9,93	10,07	9,45	9,20	10,27	9,38	9,99	9,95	9,95	10,57	9,95
900	11,43	11,85	9,67	9,74	9,87	9,69	11,41	12,50	11,44	12,43	12,41

Table 3.9 – AEED pour 20 noeuds communicants

Pause time (s)	Average End to End Delay ($\times 10^{-4} ms$)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	10,25	122,54	72,92	62,98	29,50	9,42	112,45	88,45	10,48	10,26	113,16
30	10,11	9,74	9,81	178,58	9,83	9,11	10,29	10,06	10,12	23,25	10,18
60	10,18	9,97	10,05	9,99	20,68	45,72	10,18	9,94	10,27	10,47	10,18
120	10,55	14,46	10,40	14,66	123,01	9,75	10,86	10,64	10,47	10,81	10,53
300	10,79	9,95	10,30	9,85	10,34	19,43	10,92	10,74	11,09	10,97	10,92
600	11,19	116,63	10,26	10,35	10,22	124,91	11,21	11,19	11,55	11,83	11,52
900	10,39	10,57	9,33	9,36	9,96	9,37	10,35	10,91	10,43	10,33	10,40

Table 3.10 – AEED pour 30 noeuds communicants

Pause time (s)	Average End to End Delay ($\times 10^{-4} ms$)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	10,72	36,79	25,97	30,26	10,85	59,31	10,75	54,53	10,62	192,49	48,46
30	10,69	44,48	88,70	24,10	12,47	57,07	21,50	10,63	10,49	10,63	10,61
60	10,70	10,97	39,83	118,29	75,75	10,29	10,63	10,73	10,62	10,63	10,76
120	10,89	31,45	10,52	13,18	18,49	10,22	11,14	10,86	10,80	10,98	10,89
300	10,73	10,06	10,04	9,89	10,21	27,56	10,61	10,53	10,70	10,71	10,75
600	11,95	10,89	10,83	9,84	9,83	126,01	12,26	11,69	11,74	11,96	11,94
900	11,45	11,44	10,62	10,29	10,73	9,91	11,42	11,90	11,40	11,76	11,40

Table 3.11 – AEED pour 40 noeuds communicants

Pause time (s)	Average End to End Delay ($\times 10^{-4} ms$)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	50,44	30,27	129,10	31,65	37,21	50,41	10,81	18,35	10,66	10,57	50,75
30	11,07	10,29	10,26	20,48	11,98	24,90	19,28	11,25	11,20	11,30	11,20
60	11,34	11,22	11,23	17,85	78,06	22,29	11,60	11,15	25,58	11,52	11,56
120	11,56	13,61	11,04	13,26	15,08	37,97	11,69	11,60	11,62	11,51	11,55
300	11,85	10,56	13,94	10,51	10,44	13,62	11,55	11,69	12,00	11,68	11,56
600	12,60	74,05	108,54	64,89	159,20	12,04	13,17	12,66	12,66	12,89	12,67
900	13,48	12,53	11,45	10,88	14,38	10,58	13,22	13,89	13,07	14,25	13,15

Table 3.12 – DP pour 10 noeuds communicants

Pause time (s)	Dropped Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	432	8624	14304	13424	16283	15515	425	459	376	444	429
30	353	13082	18049	18438	20884	19672	343	366	289	311	418
60	90	1168	2131	2111	3109	6397	89	105	87	91	77
120	86	2232	4800	4784	9080	7071	105	88	115	93	85
300	98	1619	1627	1610	2402	5193	89	103	152	104	126
600	40	1308	2648	7340	1689	5767	19	17	35	15	44
900	2	3013	6527	6502	9992	6503	3	0	1	2	1

Table 3.13 – DP pour 20 noeuds communicants

Pause time (s)	Dropped Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	754	18444	22531	30870	25586	32314	690	870	820	875	772
30	574	14804	24871	23999	31830	34803	720	506	585	591	594
60	439	5666	8003	8676	9419	12915	361	329	396	376	402
120	383	4261	8865	16158	16904	15985	355	410	383	428	359
300	269	8794	5785	10910	7153	15935	328	208	242	324	204
600	200	10281	11129	14981	12546	19966	172	162	213	114	167
900	3	3032	6539	6491	6532	6576	3	4	8	1	1

Table 3.14 – DP pour 30 noeuds communicants

Pause time (s)	Dropped Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	1035	14741	30652	42612	45299	42975	995	1047	969	1058	1135
30	835	27341	35041	39819	44129	40352	903	805	863	895	746
60	618	9851	14816	15844	21173	20158	650	555	694	559	784
120	454	5509	10566	11725	16857	16092	576	539	570	552	458
300	303	6590	9133	9250	4700	16931	314	228	335	294	395
600	225	14275	14575	25193	24602	27259	305	247	200	209	266
900	25	3020	6535	9630	10017	13021	22	27	13	42	13

Table 3.15 – DP pour 40 noeuds communicants

Pause time (s)	Dropped Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	1262	18531	32749	45439	47621	51213	1087	1057	1113	993	1178
30	1194	30739	39282	47287	49916	51020	1004	934	1127	1097	916
60	958	27541	26867	37146	42086	39396	930	1114	1072	1024	1024
120	689	6651	22078	22493	28111	32584	657	752	793	762	706
300	526	17589	15776	18961	19071	25019	328	363	422	408	400
600	343	20909	21966	33731	31116	35713	302	304	327	260	319
900	101	6360	12931	19050	19555	25687	36	103	34	93	61

Table 3.16 – FP pour 10 noeuds communicants

Pause time (s)	Forwarded Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	2847	2294	1103	1353	629	588	3169	3229	3173	3202	3087
30	3356	1420	1965	4676	3704	796	4022	4227	3696	4352	5124
60	3284	3172	3153	3171	2728	1607	3315	2370	2337	3355	3298
120	3010	2695	1967	1968	901	1225	2956	2999	2826	3010	3005
300	4065	2729	2725	2696	2499	1219	4116	4106	4048	4082	4030
600	4860	5123	2784	311	5351	2428	4909	4892	4908	4876	4861
900	10011	10576	3472	3528	3589	3505	9967	13646	9998	13448	13472

Table 3.17 – FP pour 20 noeuds communicants

Pause time (s)	Forwarded Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	6856	4664	4680	4036	2977	772	7567	6751	7717	7146	7416
30	7208	4611	4967	5146	2167	671	8281	6782	7408	6781	7240
60	7736	6566	5729	6393	4740	4374	8072	6268	7985	8939	7789
120	9542	9806	7327	4735	2975	4377	10899	10135	9179	10288	9271
300	11505	7647	8054	4817	8236	1450	11757	11500	13370	12282	11506
600	14201	9511	7591	6129	8729	1393	14229	14118	16166	16168	16092
900	10009	10615	3479	3481	7049	3522	10023	13581	9998	9989	10026

Table 3.18 – FP pour 30 noeuds communicants

Pause time (s)	Forwarded Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	10448	9435	7217	5344	7971	4327	10404	10468	10134	10203	10086
30	11222	5641	5454	6062	2948	4937	11334	10694	9832	10616	10397
60	12172	9698	8541	11183	5018	5548	11657	11801	10691	11352	12003
120	11911	11921	8885	8112	6818	4966	12773	11651	11837	12573	11926
300	11352	6203	7365	4573	7655	867	10877	10676	11575	11550	11466
600	22321	12395	13308	3354	4673	3523	23167	20260	20277	20341	22195
900	16510	17013	9932	6935	10143	3470	16554	20106	16506	16511	16523

Table 3.19 – FP pour 40 noeuds communicants

Pause time (s)	Forwarded Packets (packet)										
	AOMDV without attack	BHAOMDV					IDSAOMDV				
		Number of attacks					Number of attacks				
		1	2	3	4	5	1	2	3	4	5
0	10293	9646	4392	4972	3294	1321	11122	11050	10317	9487	10754
30	12827	4812	5944	8545	3007	6014	13771	14483	13490	14672	13009
60	15044	15221	19052	14720	12126	12320	17055	13113	15019	16255	15834
120	16217	16786	13438	12709	10468	4334	16564	15276	15582	15440	15214
300	19170	9699	9729	9258	7018	5820	17791	18389	21260	18370	18108
600	27327	17896	18412	6213	7058	4834	31127	26542	26533	27719	26438
900	32286	26447	16254	10120	16200	9562	32332	36893	32264	38467	32305

Notations

ADDTABLE	Additional TABLE
AEED	Average End to End Delay
AODV	Ad-hoc On-Demande Distance Vector
AODV-BR	AODV Backup Routing
AODVM	AODV Modified
AOMDV	Ad-hoc On-Demand Multipath Distance Vector
BHAOMDV	Black Hole AOMDV
CBR	Constant Bit Rate
DAG	Direct Acyclic Graph
DN	Destination Node
DoS	Denial of Service
DP	Drop Packets
DSDV	Destination Sequenced Distance Vector
DSN	Destination Sequence Number
DSR	Dynamic Source Routing
ECC	Elliptic Curve Cryptography
FP	Forwarded Packets
Gbps	Gigabit per second
GPS	Global Positioning System
IASAODV	Intrusion Avoidance System for AODV
IDSAOMDV	Intrusion Detection System for AOMDV
IP	Internet Protocol
MANET	Mobile Ad hoc NETwork

Mbps	Megabits per second
NRL	Normalized Routing Load
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PDR	Packet Delivery Ratio
PDU	Protocol Data Unit
QoS	Quality of Service
RDER	Route Discovery ERror
RERR	Route Error
RFID	Radio Frequency Identification
ROAM	Routing On-demand Acyclic Multipath
ROUTE_ID	Route Identity
RRCM	Route Reply ConfirMation
RREP	Route Reply
RREQ	Route Request
RRT	Route Reply Table
SMORT	Scalable Multipath On-demand Routing
SMR	Split Multipath Routing
SN	Source Node
TH	Threshold
TORA	Temporally Ordered Routing Algorithm
WLAN	Wireless Local Area Network

الملخص

الشبكة اللاسلكية المخصصة هي مجموعة من العقد المنظمة ديناميكيًا حيث تعمل كل عقدة كمضيف وموجه. تتميز الشبكات اللاسلكية المخصصة بعدم وجود بنية تحتية موجودة مسبقًا أو إدارة مركزية. لذلك فهي عرضة لعدة أنواع من الهجمات، وخاصة هجوم الثقب الأسود. يعد هذا الهجوم من أخطر الهجمات في هذا النوع من الشبكات. في هذا النوع من الهجوم، ترسل العقدة الخبيثة إجابة خاطئة تشير إلى أن لديها أقصر مسار إلى العقدة الوجهة عن طريق زيادة رقم التسلسل وتقليل عدد القفزات. سيكون لهذا تأثير سلبي كبير على عقدة المصدر التي ترسل حزم البيانات الخاصة بها عبر العقدة الخبثة إلى الوجهة. تستقبل هذه العقدة الخبيثة حزم البيانات وتمتص كل حركة مرور في الشبكة. للتغلب على هذه المشكلة، أصبح تأمين بروتوكولات التوجيه مطلبًا مهمًا للغاية في الشبكات اللاسلكية المخصصة. تعد بروتوكولات التوجيه متعددة المسارات من بين البروتوكولات المتأثرة بهجوم الثقب الأسود. في هذا البحث، نقترح تقنية فعالة تتجنب سوء سلوك العقد السوداء وتسهل اكتشاف المسارات الأكثر موثوقية لنقل آمن لحزم البيانات بين عقد الاتصال في بروتوكول التوجيه متعدد المسارات المعروف (*AOMDV*).

Résumé

Le réseau mobile ad hoc est un ensemble de nœuds organisés dynamiquement où chaque nœud agit comme un hôte et un routeur. Les réseaux mobiles ad hoc se caractérisent par le manque d'infrastructures préexistantes ou d'administration centralisée. Ainsi, ils sont vulnérables à plusieurs types d'attaques, en particulier l'attaque trou noir. Cette attaque est l'une des attaques les plus graves dans ce type de réseaux mobiles. Dans ce type d'attaque, le nœud malveillant envoie une fausse réponse indiquant qu'il a le chemin le plus court vers le nœud de destination en augmentant le numéro de séquence et en diminuant le nombre de sauts. Cela aura un impact négatif significatif sur les nœuds sources qui envoient leurs paquets de données via le nœud malveillant vers la destination. Ce nœud malveillant abandonne les paquets de données reçus et absorbe tout le trafic du réseau. Pour surmonter ce problème, la sécurisation des protocoles de routage devient une exigence très importante dans les réseaux ad hoc mobiles. Les protocoles de routage multi-chemins font partie des protocoles affectés par l'attaque trou noir. Dans cette thèse, nous proposons une technique efficace et efficiente qui évite le mauvais comportement des nœuds trou noir et facilite la découverte des chemins les plus fiables pour la transmission sécurisée de paquets de données entre les nœuds communicants dans le célèbre protocole de routage multi-chemins (AOMDV).

Abstract

Mobile ad hoc network is a collection of dynamically organized nodes where each node acts as a host and router. Mobile ad-hoc networks are characterized by the lack of preexisting infrastructures or centralized administration. So, they are vulnerable to several types of attacks, especially the Black hole attack. This attack is one of the most serious attacks in this kind of mobile networks. In this type of attack, the malicious node sends a false answer indicating that it has the shortest path to the destination node by increasing the sequence number and decreasing the number of hops. This will have a significant negative impact on source nodes which send their data packets through the malicious node to the destination. This malicious node drop received data packets and absorbs all network traffic. In order overcome this problem, securing routing protocols become a very important requirement in mobile ad hoc networks. Multipath routing protocols are among the protocols affected by the Black hole attack. In this thesis, we propose an effective and efficient technique that avoids misbehavior of Black hole nodes and facilitates the discovery for the most reliable paths for the secure transmission of data packets between communicating nodes in the well-known multi-path routing protocol (AOMDV).