

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Djilali Bounaama Khemis Miliana



Faculté des Sciences et de la Technologie

Département de Technologie

Mémoire du Projet de Fin d'Etudes

Pour l'obtention du diplôme de

Master

En « Télécommunications »

Option :

« Systèmes des Télécommunications »

Titre :

Etude des performances d'un protocole de sécurité pour les réseaux

AD-HOC

Réalisé par :

KOUIDER-AKIL Khawla

AISSAOUI Hanane

Encadré par :

Dr. KADDACHE Mourad

Année Universitaire: 2022/2023

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dédicace

Ma carrière universitaire s'est terminée après les efforts et sacrifices... et me voici en train de terminer mes recherches de fin d'études avec détermination et énergie. Je dédie cet humble travail à ma mère et à mon père qui se sont sacrifiés pour que je puisse continuer mes études.

Grâce à eux, j'ai atteint ce niveau, surtout ma mère qui me soutient depuis mon enfance. Je te dis que tu es ma couronne. Je remercie mes sœurs pour Soutien moral.

Et je dis à mes amis que je n'oublierai jamais les jours que nous avons Nous le passons ensemble. Khawla, Mona, Fatiha, Wiam, Najat, Kawthar et Fatima.

Vous êtes comme mes sœurs. Dieu bénisse notre amitié

Hanane

Dédicace

Dont je porte le nom avec fierté... mon cher père

Au symbole de l'amour, mon ciel, ma mère bien-aimée

Cœurs purs et vents de mon cœur mes frères (Yazid et Yusuf...

Marwan) mes sœurs (Kenza, Afaf, Hasna, Bushra, Noura).

Mes amis (Hanan, Sofia, Sarah, Kawthar et wiam)

A tous ceux qui nous ont aidés dans cet humble travail

Khawla

Remerciements

Nous remercions tout d'abord le grand Dieu pour l'achèvement de ce mémoire.

Nous exprimons nos gratitude à Monsieur le président de jury d'avoir accepté examiné ce mémoire.

Nous remercions Messieurs les membres de jury, d'avoir accepté de prendre part à ce jury ainsi que pour l'intérêt qu'ils l'ont portés à ce travail.

Nous remercions Monsieur Dr.KADDECHE Mourad, notre encadreur, pour ses conseils et suggestions avisés qui nous aidés à mener à bien ce travail, et d'avoir rapporté à ce mémoire ces remarques et conseils.

Résumé

Dans ce travail, nous nous intéressons aux problèmes de sécurité affectant les réseaux sans fil (AD-HOC), et nous visons à développer un protocole de routage QoS pour les réseaux AD-HOC qui est DSDV. Nous étudierons également l'impact des attaques WormHole sur ce protocole et présenterons des solutions de sécurité proposées à l'aide de l'outil de simulation Network Simulator 2 (NS2). Nous analyserons et interpréterons également les résultats de simulation à l'aide d'outils linguistiques et graphiques.

Mots clés: AD-HOC, DSDV, NS-2, IPS, wormhole, sécurité

Abstract

In this work, we are interested in security issues affecting wireless networks (AD-HOC), and we aim to develop a QoS routing protocol for AD-HOC networks that is DSDV. We will also study the impact of WormHole attacks on this protocol and present proposed security solutions using the Network Simulator 2 (NS2) simulation tool. We will also analyze and interpret simulation results using language and graphical tools.

Keywords: AD-HOC, DSDV, NS-2, IPS, wormhole, security

ملخص

في هذا العمل، نهتم بقضايا الأمان التي تؤثر على الشبكات اللاسلكية (AD-HOC) نهدف إلى تطوير بروتوكول توجيه بجودة الخدمة لشبكات (AD-HOC) هي DSDV كما سندرس تأثير هجمات WormHole على هذا البروتوكول ونقدم الحلول الأمنية المقترحة باستخدام أداة المحاكاة (Network Simulator 2 (NS2) وسنقوم أيضاً بتحليل نتائج المحاكاة وتفسيرها باستخدام اللغوية والأدوات الرسومية

الكلمات المفتاحية

هجمات WormHole, أمان الشبكات اللاسلكية, بروتوكول توجيه بجودة الخدمة, الحلول الأمنية

Liste des abréviations

• WLAN	Wireless Local Area Networks
• WMAN	Wireless Metropolitan Area Network
• WPAN	Wireless Personal Area Networks
• WWAN	Wireless Wide Area Network
• GSM	Global System for Mobile Communication.
• Wi-Fi	Wireless Fidelity
• DSDV	Dynamic Destination –Seconced Distance-Vector
• AODV	Ad -hoc On demand Distance Vector
• OLSR	Optimized Link State Routing Protocol
• ZRP	Zone Routing Protocol
• NS-2	Network Simulator version-2
• NAM	Network Animator
• RREQ	Route Request
• RREP	Route Reply
• IPS	Intrusion Prevention System
• DOS	Denial Of Service
• DSR	Dynamic source routing
• IETF	Internet Engineering Task Force
• WANET	Wireless Ad Hoc Network
• MANET	Mobile Ad Hoc Network
• WSN	Wireless Sensor Network
• IEEE	Institute of Electrical and Electronics Engineers
• ISM	Industrial, Scientific, and Medical
• MSC	Multiple things depending on the context
• BSC	Balanced Scorecard
• VLR	Véhicule Léger de Remplacement
• HLR	home Location Register
• RERR	Resource Extraction Regulatory Review
• PSTN	Public Switched Telephone Network
• TCP	Transmission Control Protocol
• UDP	User Datagram Protocol
• CBR	Constant Bit Rate
• VBR	Variable Bit Rate
• REER	Régime Enregistre D'épargne-Retraite

Liste des figures

Figure I.1 : Catégories des réseaux sans fil.....	3
Figure I.2 : Exemple d'un réseau ad-hoc (sans infrastructure)	6
Figure I.3 : réseaux sans fil sans infrastructure (réseau ad-hoc.....	7
Figure I.4 : une communication unicast.....	11
Figure I.5 : Communication dans les réseaux ad- hoc.....	12
Figure I.6 : Le modèle des réseaux mobiles avec infrastructure.....	16
Figure I.7 : Classification des protocoles de routage ad-hoc.....	18
Figure I.8 : classifications des attaques dans les réseaux Ad-hoc.....	22
Figure II.1 : Les étapes de l'analyse de risque.....	27
Figure II.2 : Découverte de route initiée par le protocole de routage	32
Figure II.3: Wormhole par encapsulation.....	33
Figure II.4 : différentes classes de protocole de routage ad-hoc.....	34
Figure II.5 : Exemple d'un réseau Ad-hoc.....	35
Figure II.6 : Inondation de RREQ et le renvoi du RREP.....	42
Figure II.7 : Exemple de réparation locale d'une route perdu.....	43
Figure II.8 : Solutions de sécurité.....	46
Figure II.9 : Authentification de messages avec TESLA. Les messages Mi sont authentifiés.....	48
Figure III.1 : Simulateur de réseau 2eme génération.....	53
Figure III.2 :L'architecture simulation du NS2.....	55
Figure III.3 : attaque wormhole dans DSDV.....	59
Figure III.4 : fichier dépendants de DSDV.tcl.....	60
Figure III.5 : DSDV simulation on NS-2.35 avec nombre du	64
Figure III.6 : le protocole DSDV avec deux sources et deux destinataires.....	64
Figure III.7 : Recherche du nœud source en envoyant des paquets au nœud récepteur.....	65
Figure III.8 : nœuds avec le wormhole	66
Figure III.9 : Le protocole IPSDSDV au début des travaux.....	68
Figure III.10 : détecter et alerter le système de la menace d'une attaque par trou de ver.....	68
Figure III.11 : Réponse de L'IPS immédiate et élimine les paquets malveillants.....	69

Figure III.12 : Élimination complète du trou de ver et restauration de la communication sécurisée entre les nœuds.....	70
Figure III.13 : L'effet du WormHole-DSDV.....	70
Figure III.14 : L'effet du IPSDSDV	71
Figure III.15 : Le débit des 30 nœuds (bits/ms)	72
Figure III.16 : Taux de livraison de paquets (%).....	73
Figure III.17 : Le taux de pertes de paquets (%).....	74

Liste des tableaux

Tableau II.1 : Table de routage du nœud M1 du graphe... ..	36
Tableau III.1 : Le tableau de routage de Protocol DSDV.....	63

Table de Matière

Dédicace

Remerciement

Résumé

Introduction générale..... 1

Chapitre 1 : Générales sur les réseaux ad hoc

I.1. Introduction..... 3

I.2. les réseaux sans fil.....3

I.2.1. Historique du réseau ad-hoc 4

I.2.2. Définition de réseau ad-hoc.....5

I.2.3. les caractéristiques des réseaux ad-hoc 7

I.2.4. Les types de réseaux ad-hoc..... 9

I.2.5. Modes de communications dans les réseaux ad-hoc 10

I.2.6. Domaines d'applications des réseaux ad hoc 12

I.2.7. Les avantage de réseau ad-hoc 13

I.2.8. Les inconvénients de réseau ad-hoc 13

I.2.9. Les réseaux ad-hoc et les réseaux cellulaires 14

I.3. La difficulté du routage dans les réseaux ad-hoc.....16

I.3.1. Classification des protocoles de routage 17

I.3.2 classification des attaques 21

I.4. La sécurité 23

I.5. Conclusion 24

Chapitre II : Le routage et la sécurité dans les réseaux ad hoc

II.1. Introduction	25
II.2. Routage dans les réseaux Ad Hoc	25
II.3. Les risque liés à la sécurité.....	26
II.4. Exigence de la sécurité dans les réseaux ad hoc.....	28
II.4.1. Contraintes de la sécurité.....	28
II.4.2. Les besoins de sécurité	28
II.5. Les attaques contre les réseaux ad hoc	30
II.5.1. Attaques d'identité.....	30
II.5.2. Modification, suppression et insertion des messages	31
II.5.3. Replay ou rejeu	32
II.5.4.Dénis de services (Dos).....	33
II.6. Protection du protocole de routage dans les réseaux ad hoc	34
II.6.1. Les type de protocole	34
II.6.2. Etude de quelques protocoles de routages.....	34
II.6.2.1. Le protocole DSDV (Dynamic Destination-Sequenced Distance-Vector).....	34
II.6.2.2. OLSR (Optimized Link State Routing Protocol).....	38
II.6.2.3. Le protocole AODV (Ad hoc On demand Distance Vector).....	39
II.6.3. Comparaison entre les protocoles (DSDV, AODV, DSR)	44
II.7. Etat de l'art des solutions pour la sécurité.....	45
II.8. Conclusion	50

Chapitre III : Tests et résultats de simulation

III.1. Introduction.....	51
III.2. L'attaque de WormHole	51
III.3. le protocole de routage DSDV (Destination-Sequenced Distance Vector).....	51
III.4. Identification du problème	51
III.5. Présentation de NS2	52
III.5.1. Les différences outils de NS2.....	53
III.5.2. Choix du simulateur ns-2.....	54

III.5.3. Modèle de simulation.....	54
III.5.4. Installation du simulateur NS2	55
III.6. La configuration des nœuds.....	56
III.7. Spécification de l'attaque par trou ver dans DSDV	58
III.7.1. L'implémentation d'un nœud malicieux	59
III.7.2. Modifications du fichier DSDV.tcl	60
III.7.3. Les modifications pour la sécurité.....	61
III.8. Les Scènes de simulation.....	62
III.8.1. Les paramètres de simulation	62
III.8.2. Les simulations	63
III.8.2.1. DSDV on action.....	63
III.8.2.2. WormHole action.....	65
III.8.2.3. Traitement de l'IPS sur le WormHole.....	66
III.8.2.4. IPS (Intrusion Prevention System).....	67
III.9. Les résultats de la simulation.....	70
III.9.1 Effets de WormHole.....	70
III.9.2 Effets de l'IPS	71
III.10. Métriques d'évaluation des performances	71
III.10.1. Débit (throughput).....	71
III.10.2. Taux de livraison de paquets (%)	72
III.10.3. Le taux de pertes de paquets (%).....	73
III.11. Conclusion	75
Conclusion générale	76

Bibliographie

Introduction générale

Les derniers développements de la technologie des réseaux sans fil permettent aux utilisateurs d'accéder à l'information à tout moment et en tout lieu avec une grande souplesse d'utilisation, les utilisateurs peuvent se déplacer librement tout en continuant à communiquer. Les réseaux sans fil mobiles peuvent être divisés en deux catégories : ceux dotés d'une infrastructure utilisant généralement un modèle de communication cellulaire et ceux sans infrastructure appelés réseaux Ad-Hoc. Un réseau ad hoc est un groupe de nœuds mobiles autonomes et coopératifs qui se déplacent et communiquent via des transmissions sans fil sans nécessiter d'infrastructure préexistante. Les réseaux Ad-Hoc se forment spontanément et temporairement tant que quelques nœuds mobiles sont à portée radio. En fonction de la distance entre les nœuds, les nœuds communiquent via deux modes de communication :

Soit les nœuds mobiles peuvent communiquer directement (dans des transmissions temporaires) parce qu'ils sont à portée de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme relais pour acheminer les paquets vers leurs destinations. Par conséquent, en raison de la couverture limitée du champ radio disponible pour chaque nœud, chaque nœud agit à la fois comme un utilisateur final et un routeur, relayant les paquets vers leur destination finale. Dans un réseau sans fil décentralisé, les nœuds mobiles constituent le réseau, car ils doivent coopérer pour fournir les fonctionnalités normalement fournies par un réseau filaire (ex : routeurs, serveurs, commutateurs, passerelles, ponts, etc.)

Quoi le rendant très vulnérable et confronté à des problèmes de sécurité fondamentaux cela pose à son tour l'un des plus grands défis.

Nous étions intéressés par un problème de sécurité affectant ces réseaux, l'attaque par trou noir, autre dans le cadre de ce travail, nous allons mettre en place une solution préventive problèmes causés par les attaques de trous noirs affectant les réseaux sans fil dispersé.

dans ce travail, nous nous intéressons aux problèmes de sécurité des protocoles de routage dans le réseau temporaire. Pour cela, nous divisons le mémoire en trois chapitres.

Le chapitre premier donne un aperçu général des réseaux ad hoc tels que leurs domaines d'application et leurs caractéristiques, de leurs concepts et de leurs propriétés

Le deuxième chapitre se focalise sur les protocoles de routage dans les réseaux Ad hoc ,nous aborderons problématique de la sécurité dans les réseaux ad hoc en expliquant les différents types d'attaques qui peuvent menacer le réseau ainsi que les services de base de sécurité existants et proposés pour faire face à ces menaces et à la fin de chapitre nous faisons une étude comparative des protocoles **AODV** et **DSDV** et **DSR** et **OLSR**

Introduction générale

Dans le troisième chapitre nous décrirons l'outil de simulation NS2 et les éléments qui l'accompagnent pour la mise en œuvre de notre application ainsi nous appliquons le protocole **DSDV** et la nature de l'effet d'attaque du **WormHole** sur celui-ci, et enfin nous sécurisons le réseau à l'aide de la fonctionnalité **IPS**, avec une description et une discussion de la simulation. Enfin, nous terminerons notre travail par une conclusion générale.

Chapitre I

Générales sur les réseaux ad hoc

I.1. Introduction

Un réseau Ad-Hoc est un réseau sans fil dans lequel les nœuds sont et interconnectés sans infrastructure centralisée. Dans ce réseau, chaque nœud est à la fois émetteur et récepteur, et les nœuds peuvent communiquer directement ou via des nœuds, ils sont utilisés dans de nombreuses applications.

Les réseaux Ad-Hoc présentent des défis de conception et de mise en œuvre uniques en raison de la nature dynamique de leur topologie et de la mobilité des nœuds. Les protocoles de routage pour les réseaux Ad-Hoc doivent pouvoir s'adapter rapidement aux modifications de la topologie du réseau et de la mobilité des nœuds. Aussi ils peuvent être divisés en deux catégories : le réseau ad hoc mobile (MANET) et le réseau ad hoc de capteurs sans fil (WSN). Les réseaux Ad-Hoc offrent des avantages tels que la flexibilité, l'indépendance par rapport à l'infrastructure centralisée et la capacité de fournir une communication dans des environnements difficiles. Cependant, ils posent également des défis tels que la sécurité, la gestion de l'alimentation et la résilience aux pannes de nœuds.

I.2. les réseaux sans fil

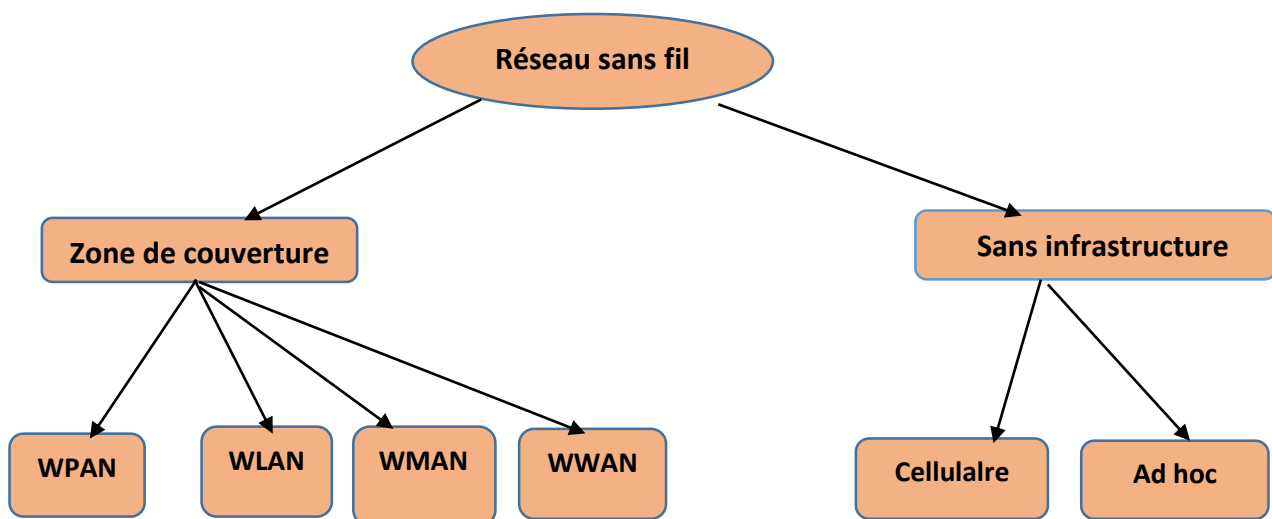


Figure I.1 : Catégories des réseaux sans fil [1]

I.2.1. Historique du réseau AD-HOC

Le réseau traditionnel, avec son infrastructure fixe, présente différents défis dans son déploiement. On peut citer, par exemple, les pannes imprévisibles des stations de base pouvant engendrer une interruption de service dans le réseau. Dans le milieu militaire, un tel cas rendrait le réseau vulnérable et non robuste. En 1972, après un premier projet par Defense Advanced Research Projects Agency (DARPA), la première génération du réseau ad hoc est apparue et a été nommée Packet Radio Network (PRNET). PRNET a été associé avec un autre projet Areal Locations of Hazardous Atmosphères (ALOHA). Ces deux projets ont abouti à des approches d'accès au médium et de routage de type vecteur de distance, testées dans un environnement militaire.

La deuxième génération du réseau ad hoc est apparue dans les années 1980. En 1983, le projet Sur viable Radio Networks (SURAN) a été mis en place. Il visait à fournir une connectivité ad hoc en se servant des équipements avec un coût réduit et une faible énergie consommée. Également, le nombre de nœuds dans le réseau a été augmenté afin de vérifier et d'améliorer le facteur de mise à l'échelle. Ainsi, la technologie nommée Low Cost Packet Radio (LPR) a été mise en place, en 1987.

Dans les années 1990, la croissance du nombre d'ordinateurs et la disponibilité des équipements sans fil ont poussé les communautés scientifiques et industrielles à créer le concept de la commercialisation de la technologie AD-HOC. L'accès du public à cette technologie est ainsi devenu une réalité. Les grandes sociétés informatiques et de télécommunication (Ericsson, IBM, Intel,...) ont formé le groupe Special Interest Group (SIG), ayant pour but de fournir des solutions pour le déploiement de la connectivité ad hoc entre des équipements avec des caractéristiques hétérogènes. S'ajoute à cela la poursuite de l'effort de DARPA qui a mis en place : Global Mobile Information Systems (GloMo) et Near Term Digital Radio (NTDR). Ces deux projets visaient à offrir un milieu de connexions multimédia entre des équipements portables (Leiner et al. 1996); (Redi, 2002).

Le comité d'IEEE 802.11 a adopté le terme AD-HOC et les chercheurs ont commencé à voir la possibilité de déploiement de réseaux AD-HOC avec des nouvelles applications. En plus en 1998, le groupe de travail Mobile ad hoc Network (MANET) a été créé au sein d'Internet

engineering Task Force (IETF) afin de fournir des standards valides de protocoles de routage basés sur la technologie IP dans le réseau AD-HOC [2].

I.2.2.Définition d'un réseau AD-HOC

Un réseau sans fil ad-hoc ou WANET ou MANET (du nom du groupe de travail qui a créé ce protocole) est un type de réseau sans fil décentralisé.

Le réseau est ad-hoc car il ne s'appuie pas sur une infrastructure préexistante, comme des routeurs dans les réseaux filaires ou des points d'accès dans les réseaux sans fil administrés. Au lieu de cela, chaque nœud participe au routage en retransmettant les données aux autres nœuds, de façon que le choix du nœud qui va transmettre les données est opéré dynamiquement sur la base de la connectivité du réseau et de l'algorithme de routage utilisé. Dans le système d'exploitation Windows, l'AD-HOC est un mode de communication (paramètre) qui permet aux ordinateurs de communiquer directement entre eux sans routeur.

Les réseaux sans fil AD-HOC sont des réseaux auto-configurant et dynamiques dans lesquels les nœuds sont libres de se déplacer. Les réseaux sans fil ne souffrent pas des complexités liées à la configuration et à l'administration d'infrastructures, permettant ainsi aux appareils de créer et joindre des réseaux à la volée – n'importe où, n'importe quand [3].

Figure I.2 représente exemple d'un réseau ad-hoc [4].

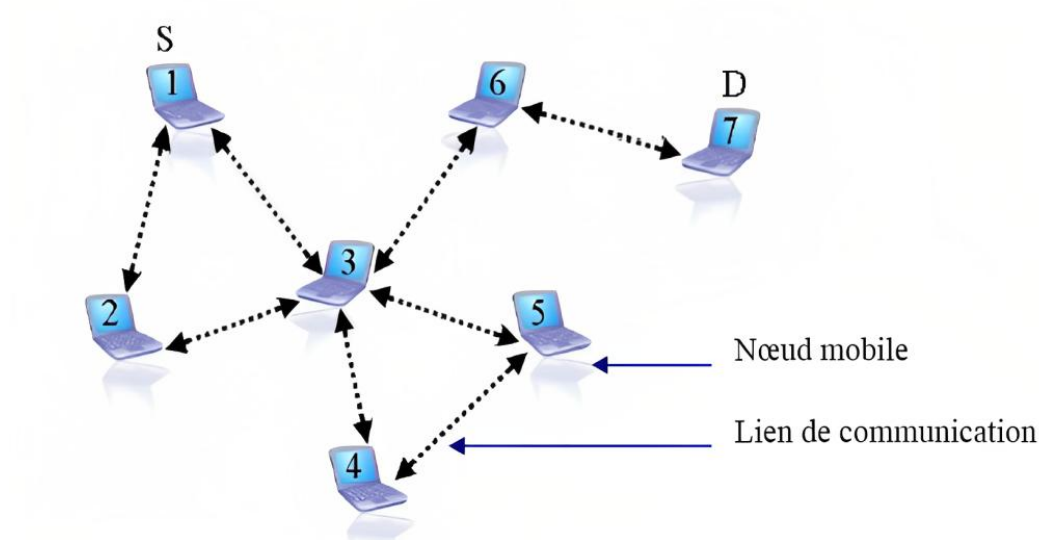


Figure I.2 : Exemple d'un réseau AD-HOC

L'IETF a créé une entité spécifique pour les réseaux mobiles ad hoc, le groupe de travail MANET les membres de ce groupe soumettent régulièrement des propositions de protocoles de routage adaptés aux réseaux mobiles ad hoc.

Les réseaux sans fil ad hoc s'appuient sur les technologies sans fil conçues à l'origine pour des réseaux locaux et domestiques :

- Les technologies IEEE 802.11a, 802.11b (Wireless Fidelity, WiFi), 802.11g, HiperLan/1 (remplace par Hyperlan/2), HomeRF (SWAP) sont propres aux réseaux WLAN
- La technologie Bluetooth, pour les réseaux WPAN
Bluetooth fonctionne en mode point à point ou point à multipoint.
- Les technologies infrarouges (IrDA, Infrared Data Association), utilisées dans les télécommandes par exemple, peuvent aussi être considérées comme support des réseaux ad hoc. Mais ces technologies se limitent à des communications point à point.
- Les technologies WiFi, IEEE 802.11g, HiperLan, HomeRF et Bluetooth opèrent dans la bande ISM 2.4 GHz alors que 802.11a opère dans la région des 5 GHz.

I.2.3.les caractéristiques des réseaux AD-HOC

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

D'autres caractéristiques spécifiques aux réseaux ad-hoc conduisent à une complexité et des contraintes supplémentaires, qui doivent être prises en compte lors de la conception des algorithmes et des protocoles réseaux [5] à savoir :

I.2.3.1. L'absence d'infrastructure centralisée

Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistantes et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [6]

L'absence d'infrastructure fixe de communication rend le déploiement des réseaux ad hoc très facile, c'est un des premiers avantages de ces réseaux [7].

Figure I.3 représente réseaux sans fil sans infrastructure (réseau AD-HOC)

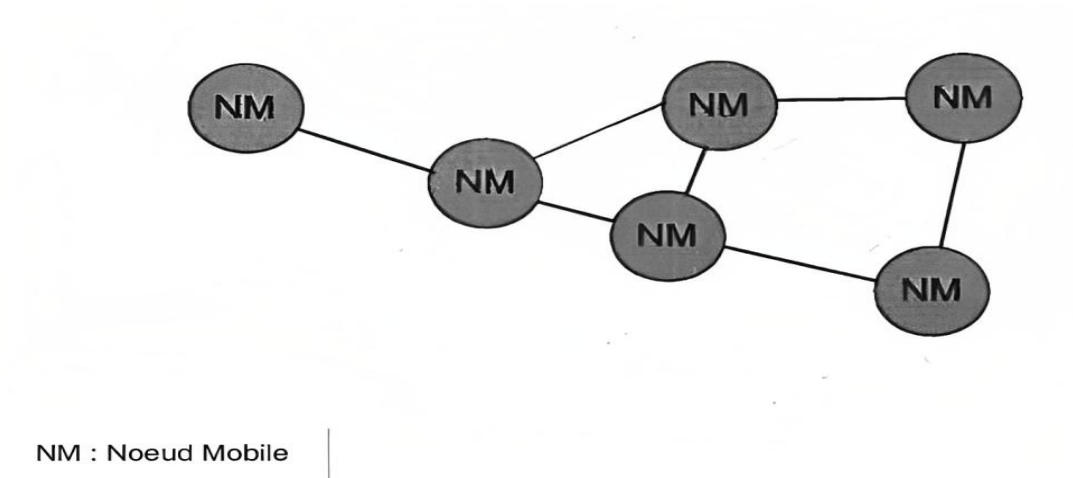


Figure I.3 : réseaux sans fil sans infrastructure (réseau AD-HOC)

I.2.3.2. Problème d'allocation des fréquences

Dans les réseaux sans fil cellulaire, caractérisés par les utilisations des stations de base, on cherche à attribuer des fréquences différentes aux stations voisines, de telle façon à éviter les interférences entre les cellules ainsi créées. Pour garantir la connectivité, au sein d'un réseau

AD-HOC, comme il n'y a pas d'infrastructures fixes et que tous les nœuds sont susceptibles de bouger ou de disparaître, il est plus simple et moins coûteux de travailler avec une seule fréquence et un multiplexage TDD (time division duplex) [8].

I.2.3.3. La mobilité des nœuds et maintenance des routes

La mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un nœud peut rejoindre un réseau, changer de position, quitter le réseau.

Cette mobilité aura un impact direct sur la morphologie du réseau, elle peut engendrer une modification du comportement du canal de communication et en général provoque des influences significatives sur les performances du réseau. Les algorithmes de routage doivent donc être capables de résoudre ces problèmes, supporter la maintenance des routes et prendre en charge un temps limité leurs constructions tout en minimisant l'over-Head généré par les messages de contrôle [8].

I.2.3.4. L'auto-configuration

L'auto- a permis aux nœuds de s'intégrer facilement dans le réseau .Elle facilite la gestion du réseau car l'interconnexion des éléments ne nécessite qu'un minimum d'intervention technique externe .Cette fonctionnalité est de plus en plus nécessaire pour un déploiement à grande échelle des réseaux sans fil ad-hoc [9].

I.2.3.5. Une topologie dynamique

Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels [10].

I.2.3.6. Sécurité et vulnérabilité

Dans les réseaux ad hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'intrusions [10].

I.2.3.7. Largeur et qualité de bande limitée

Les liens sans fil ont la capacité en largeur de bande sensiblement inférieure à leurs contreparties câblées. Ils sont également moins fiables dus à la nature de la propagation du signal [11].

I.2.3.8. Contrainte d'énergie

Les dispositifs dans un réseau mobile se fondent sur des batteries ou d'autres moyens épuisables en tant que leur source d'énergie. La conservation et l'utilisation efficace de l'énergie peuvent être le critère le plus important dans la conception de système pour ce type de réseau [11].

I.2.4. Les types de réseaux ad-hoc

Les types des réseaux ad-hoc sont divers, nous pouvons en citer quelques-uns [12]:

I.2.4.1. Les réseaux personnels PAN (Personal Area Network)

Désigne un réseau restreint d'équipement informatique habituellement utilisées dans le cadre d'une utilisation personnelle. Parmi les technologies sans fil utilisées par les réseaux PAN, nous pouvons citer le Bluetooth, l'infrarouge (IR), ou le zigbee (la technologie 802.15.4).

I.2.4.2. Les réseaux Peer to Peer

Sont des réseaux, dont le fonctionnement est décentralisé entre les différents utilisateurs du réseau, dont les machines sont simultanément, client et serveurs (routeur) des autres machines.

I.2.4.3. Les réseaux de capteurs

Sont des réseaux composés de nœuds, intégrant une unité de mesure de capter des grandeurs physiques (chaleur, humidité, vibration) et de le transformée grandeurs numériques, une unité de traitement informatique de stockage de données et un module de transmission sans fil (Wireless).

I.2.4.4. Les réseaux véhiculaires

Les voitures de nos jours embarquent de plus en plus de technologie, et ont de plus en plus, besoin de communiquer avec l'extérieur. Les voitures équipées par des capteurs sur les toits et/ou, les pare-chocs sont capables de créer des plateformes des réseaux mobiles ad-hoc et de relier en réseau les automobiles passant à proximité les uns des autres. Des prototypes ont déjà été développés pour les véhicules d'urgence (les ambulances, les voitures des pompiers, etc.).

I.2.5. Modes de communications dans les réseaux ad-hoc

Avant de parler des protocoles de routage proprement dit, nous allons rappeler quels sont les principaux modes de communication [13] dans les réseaux, et particulièrement dans les réseaux ad-hoc

I.2.5.1. La communication point à point ou unicast

Lorsque vous passez un coup de fil, vous composez le numéro de téléphone d'une personne en particulier avec laquelle vous voulez parler. Il ne vous viendrait pas à l'idée de prononcer le nom de votre interlocuteur dans l'écouteur, dans l'espoir qu'il vous entende et vous réponde. C'est d'ailleurs un des éléments qui permet à l'unicast de se distinguer du broadcast, où tous les participants du réseau vont recevoir le message.

L'unicast est une forme de connexion qui permet de relier strictement deux participants. Il n'est d'ailleurs pas très important de savoir si le transfert fonctionne dans les deux sens. De ce fait, savoir si le destinataire devient occasionnellement émetteur, si des données sont échangées dans les deux sens (bidirectionnel), ou si la connexion respecte un seul sens (unidirectionnel) n'a aucune importance. On parle d'unicast à partir du moment où l'on a un flux d'informations limité à deux participants.

L'essentiel des échanges de données sur Internet repose sur le principe de l'unicast. Chaque fois qu'un utilisateur consulte un site Web, il établit une connexion directe entre un

client et un serveur. L'envoi d'emails fonctionne généralement aussi par unicast. Un autre exemple est le transfert direct de données : lorsque vous téléchargez ou transférez un fichier sur un serveur, c'est, encore une fois, sur le principe de l'unicast. Dans certaines situations particulières, comme par exemple lors d'un streaming, on a recours à d'autres méthodes, comme le multicast [14].

Dans une connexion unicast, on a toujours deux points précis qui participent à la communication.

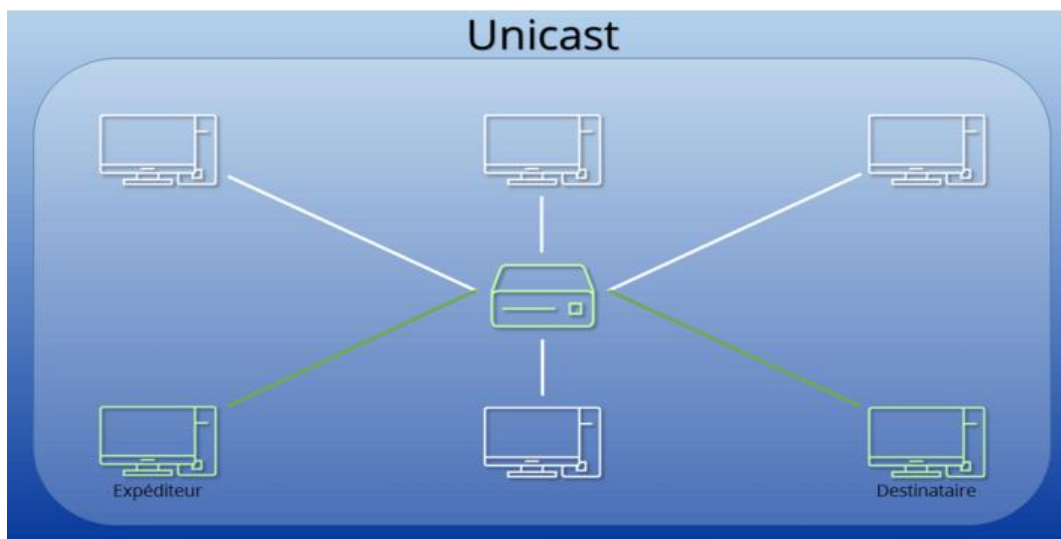


Figure I. 4 : une communication unicast

I.2.5.2. La communication multipoints ou multicast

La communication point à multipoint (PMP) fait référence à une communication qui est accomplie via une forme distincte et spécifique de connexions un-à-plusieurs, offrant plusieurs chemins d'un emplacement unique à différents emplacements. Point à multipoint est généralement abrégé en PTMP, P2MP ou PMP. La communication PMP est couramment utilisée dans les télécommunications.

PMP est généralement utilisé pour établir une connectivité d'entreprise privée aux bureaux dans des sites distants, des solutions de liaison sans fil à longue portée pour divers sites et un accès à large bande au dernier kilomètre. En tant que tel, il est largement utilisé dans la téléphonie IP et l'Internet sans fil au moyen de radio fréquences gigahertz. Ces réseaux PMP sont utilisés dans des équipements de distribution, d'immenses campus d'entreprise, des districts scolaires, des applications de sécurité publique, etc. [15].

1.2.5.3 La diffusion ou broadcast

C'est une communication issue d'un émetteur vers tous les équipements d'un même réseau. Tous les équipements de ce réseau traiteront les données reçues. On utilise pour cela une adresse spécifique dite 'adresse de broadcast'. Par exemple si l'on considère le réseau 192.168.1.0/24 alors l'adresse de diffusion sera 192.168.1.255. Au niveau d'un commutateur, les données émises arrivant sur un port connecté à l'hôte émetteur seront dupliquées sur tous les autres ports. Il faut noter qu'un routeur ne diffuse pas les données émises en broadcast. [16]

Ces trois modes de communication sont schématisés par la figure suivante [8]:

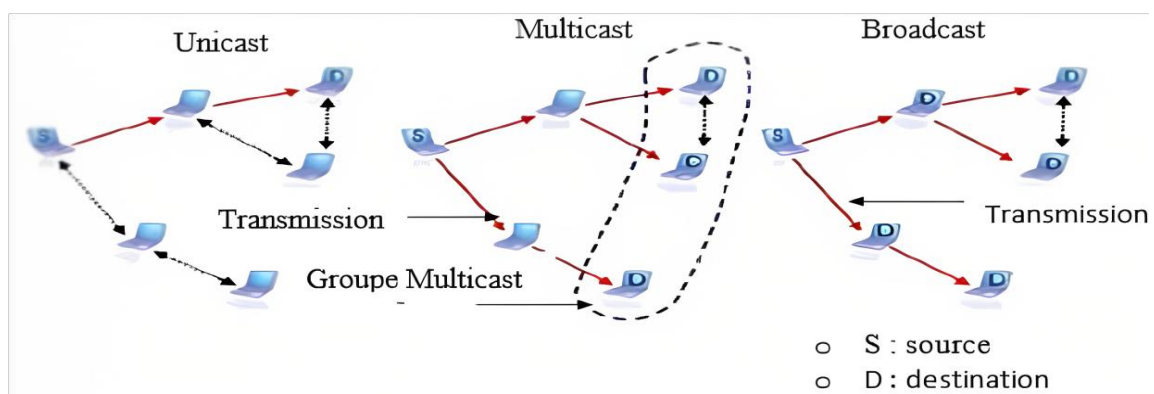


Figure I.5 : Communication dans les réseaux ad-hoc

1.2.6. Domaines d'applications des réseaux Ad-Hoc

Les réseaux ad hoc ont été développés en premier par la défense américaine au début des années 70, leurs premières applications étaient militaires, le but était de les utiliser là où les infrastructures de communication n'existaient pas ou étaient détruites, tels que les champs de bataille.

Dans les applications civiles, ces réseaux sont d'une grande utilité dans les opérations de secours où les infrastructures de communication sont endommagées par les catastrophes naturelles (tremblements de terre, ...).

D'autres applications sont envisageables pour les réseaux ad hoc tel que les réseaux spontanés (conférence, business, ...).

Pour l'usage personnel (PAN) ou ce qu'on appelle réseau personnel, les réseaux ad hoc permettent de connecter plusieurs équipements tels l'ordinateur de bureau, l'ordinateur portable

et l'ordinateur de poche. Ceci permet le transfert d'informations entre différents équipements sans aucun branchement filaire [8].

I.2.7. Avantages d'un réseau Ad-Hoc

Les réseaux ad-hoc présentent plusieurs avantages, les plus importants sont [17] :

- Déploiement facile : rapide et économique fastidieuse du déploiement des stations de base (câblage, installation, etc.) n'est plus nécessaire. En conséquence, le déploiement est aussi plus rapide et se fait avec un faible coût cela est dû à la rapidité de mise en place.
- La liaison sans fil permet aux nœuds de se déplacer dans le réseau.
- Un coût faible.
- L'indépendance technique et commerciale, vis-à-vis de point d'accès.
- La robustesse : un réseau évolutif et dynamique [4].

I.2.8. Inconvénients d'une grille ad hoc Ad-Hoc

Il existe beaucoup de problèmes techniques dans les réseaux ad hoc [18] :

I.2.8.1. Problèmes de transmission radio

Plusieurs problèmes liés à la transmission radio :

- Augmentation de nombre d'erreurs sur la transmission.
- Faible performance de la liaison sans fi
- Réduisez la vitesse de liaison

I.2.8.2. La mobilité des nœuds

- Modification de la topologie de réseau dû à la densité des nœuds.
- Transformation du tracé des routes lors des échanges des paquets.

I.2.8.3. Consommation d'énergie

La durée de vie d'un équipement dépend de la durée de vie de la batterie, pour cela la consommation d'énergie doit obligatoirement diminuée.

I.2.8.4. Les problèmes liés au routage

le problème de routage est l'un des problèmes majeurs dans les réseaux ad hoc, il se pose sur l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modeste capacité de calcul, de sauvegarde et de changements rapides de topologies .

I.2.8.5. Problème de sécurité

La sécurité dans les réseaux ad hoc constitue l'une des préoccupations durant la planification, la mise en place ainsi la gestion du réseau. Cette dernière dépend de plusieurs paramètres tel que : authentification, confidentialité, intégrité et disponibilité ; elle concerne deux points, la sécurité des données transitant sur le réseau est limité étant donné que le média de transmission est partagé par tous les nœuds de réseau. et la sécurité du routage. Ces deux aspects comportent quelques vulnérabilités et sont exposés à plusieurs attaques.

I.2.9. Les réseaux ad-hoc et les réseaux cellulaires

Un réseau cellulaire est un réseau radio distribué sur terre à travers des cellules où chaque cellule comprend un émetteur-récepteur à emplacement fixe appelé station de base. Ensemble, ces cellules assurent une couverture radio sur de plus grandes zones géographiques. L'équipement utilisateur (UE), tel que les téléphones mobiles, est donc en mesure de communiquer même si l'équipement se déplace à travers les cellules pendant la transmission. Les réseaux cellulaires offrent aux abonnés des fonctionnalités avancées par rapport aux solutions alternatives, notamment une capacité accrue, une faible consommation d'énergie de la batterie, une zone de couverture géographique plus large et une interférence réduite avec d'autres signaux. Les technologies cellulaires populaires comprennent le système mondial de communication mobile, le service général de radio par paquets, le 3 GSM et l'accès multiple par division de code [19].

Le BTS permet aux appareils cellulaires d'établir une communication directe avec les téléphones mobiles. L'unité agit comme une station de base pour acheminer les appels vers le

contrôleur central de la base de destination. Le contrôleur de station de base (BSC) se coordonne avec le MSC pour s'interfacer avec le PSTN fixe, le registre de localisation des visiteurs (VLR) et le registre de localisation du domicile (HLR) pour acheminer les appels vers différents contrôleurs du centre de base. Les réseaux cellulaires conservent des informations pour suivre l'emplacement des appareils mobiles de leurs abonnés. En réponse, les appareils cellulaires sont également équipés des détails des canaux appropriés pour les signaux des systèmes de réseau cellulaire. Ces canaux sont classés en deux domaines: Canal de contrôle dédié puissant: utilisé pour transmettre des informations numériques à un téléphone mobile cellulaire depuis la station de base et vice versa. Strong Paging Channel: utilisé pour suivre le téléphone mobile par MSC lorsqu'un appel lui est acheminé. Un site cellulaire typique offre une couverture géographique comprise entre neuf et 21 miles. La station de base est chargée de surveiller le niveau des signaux lorsqu'un appel est effectué à partir d'un téléphone mobile. Lorsque l'utilisateur s'éloigne de la zone de couverture géographique de la station de base, le niveau du signal peut baisser. Cela peut amener une station de base à demander au MSC de transférer la commande à une autre station de base qui reçoit les signaux les plus forts sans en informer l'abonné; ce phénomène est appelé transfert. Les réseaux cellulaires rencontrent souvent des interruptions environnementales comme une grue à tour mobile, des câbles électriques aériens ou les fréquences d'autres appareils.

Ce modèle est composé de deux ensembles d'entités distinctes [4].

- Les "sites fixes" du réseau filaire qui ne se trouvent pas dans ad-hoc
- Les "sites mobiles"
- Les stations de base sont interconnectées entre eux via une liaison filaire, et chaque station de base peut communiquer directement avec les sites mobiles en utilisant une interface sans fil.

L'ensemble formé par le point d'accès et les stations situées dans sa zone s'appelle ensemble des services de base (BSS) et constitué une cellule, Il dispose donc d'une infrastructure fixe contrairement les réseaux ad-hoc [20].

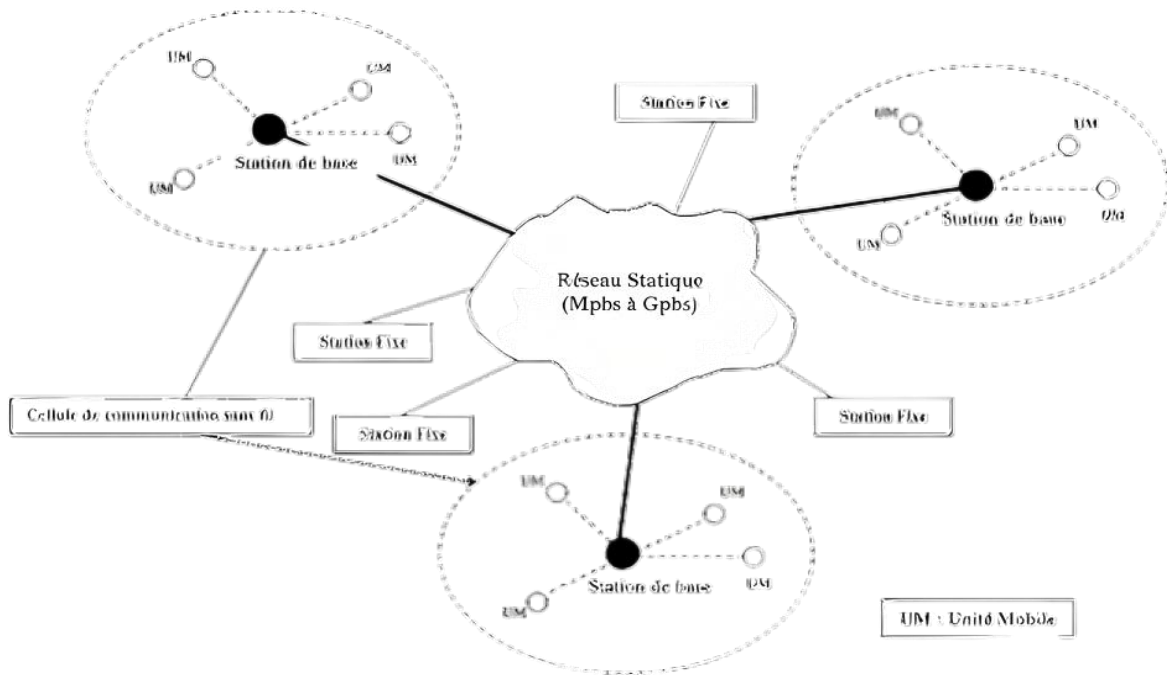


Figure I.6 : Modèle de réseaux mobiles d'infrastructure

I.3. La difficulté du routage dans les réseaux Ad-Hoc

Comme nous avons déjà vu, l'architecture d'un réseau mobile ad-hoc est caractérisée par une absence d'infrastructure fixe préexistante, à l'inverse des réseaux de télécommunication classiques. Un réseau ad hoc doit s'organiser automatiquement de façon à être déployable rapidement et pouvoir s'adapter aux conditions de propagation, au trafic et aux différents mouvements pouvant intervenir au sein des unités mobiles. Dans le but d'assurer la connectivité du réseau, malgré l'absence d'infrastructure fixe et la mobilité des stations, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination : tout nœud joue ainsi le rôle de station et de routeur. Chaque nœud participe donc à un protocole de routage qui lui permet de découvrir les chemins existants, afin d'atteindre les autres nœuds du réseau. Le fait que la taille d'un réseau ad hoc peut être énorme, souligne que la gestion de routage de l'environnement doit être complètement différente des approches utilisées dans le routage classique. Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement

utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde. Dans la pratique, il est impossible qu'un hôte puisse garder les informations de routage concernant tous les autres nœuds, dans le cas où le réseau serait volumineux. Certains protocoles, comme le DSR et l'AODV, utilisent la

sauvegarde des données de routage concernant une destination donnée (dans le cas où la source ne possède pas déjà de telles informations). Cependant, ces protocoles ne spécifient pas les destinations que les nœuds doivent garder leurs données de routage. Le problème ne se pose pas dans le cas de réseaux de petites tailles, car l'inondation (la diffusion pure) faite dans ces réseaux n'est pas coûteuse. Par contre, dans un réseau volumineux, le manque de données de routage concernant les destinations peut impliquer une diffusion énorme dans le réseau, et cela si on considère seulement la phase de découverte de routes. Le trafic causé par la diffusion, dans ce cas, est rajouté au trafic déjà existant dans le réseau ce qui peut dégrader considérablement les performances de transmission du système caractérisé principalement par une faible bande passante. Dans le cas où le nœud destination se trouve dans la portée de communication du nœud source le routage devient évident et aucun protocole de routage n'est initié. Malheureusement, ce cas est généralement rare dans les réseaux ad hoc. Une station source peut avoir besoin de transférer des données à une autre station qui ne se trouve pas dans sa portée de communication. Par exemple dans le réseau illustré par la figure 2.4 l'unité mobile W n'est pas dans la portée de communication de l'unité U (indiquée par le cercle d'origine U) et vice versa. Dans le cas où l'unité U veut transférer des paquets à W, elle doit utiliser les services de l'unité V dans l'envoi des paquets, puisque l'unité V contient dans sa portée de communication les unités U et W. Dans la pratique, le problème de routage est plus compliqué à cause de la non-uniformité de la transmission sans fil et de la possibilité du déplacement imprévisible de tous les nœuds concernés par le routage [21].

I.3.1. Classification des protocoles de routage

Le routage dans les réseaux ad hoc est devenu une matière populaire de recherche. Au début des années 80, un grand nombre de protocoles de routage sont conçus et proposés pour les réseaux Ad-Hoc. Ces protocoles couvrent un éventail de choix et des approches de conception, des modifications simples des protocoles d'Internet à des protocoles hiérarchiques à multi niveaux plus complexes.

Les protocoles de routage qui ont été conçus, sont basés sur les ensembles semblables de suppositions. Par exemple, la plupart des protocoles de routage ne supposent que tous les nœuds ont des ressources et des possibilités homogènes. Ceci inclut les gammes de transmission des nœuds et les liens bidirectionnels qui sont souvent assumés. Dans ce dernier cas, les protocoles éliminent alors des liens unidirectionnels de la considération [22].

Ce chapitre décrit les classifications des approches de routage les plus connues et leurs caractéristiques. Les protocoles de routage mentionnés comme exemples de classes, sont

choisis pour un certain nombre de raisons. Ils peuvent être des choix populaires pour la recherche parmi la communauté ad hoc. Ils peuvent, à l'heure de cette écriture de ce mémoire, mis à l'étude par le groupe de travail ad hoc mobile des réseaux (MANET) de l'IETF pour la standardisation ou ils peuvent simplement être de bons exemples de protocoles d'illustration de leurs classes.

Dans les classifications citées par la suite, les classes de protocoles n'ont pas de structure sous forme d'arbre, bien que certaines caractéristiques, soient en général communes entre les classes.

Quelques classes sont d'une nature d'opposition par exemple : réactive et proactive. D'autres n'auront pas des contreparties avec des caractéristiques intéressantes à préciser (comme le routage hiérarchique, puisque les protocoles non hiérarchiques ne partagent pas des caractéristiques distinguées, à part qu'ils ne sont pas hiérarchiques) [23].

La figure I.7 classification des protocoles de routage Ad-Hoc [8].

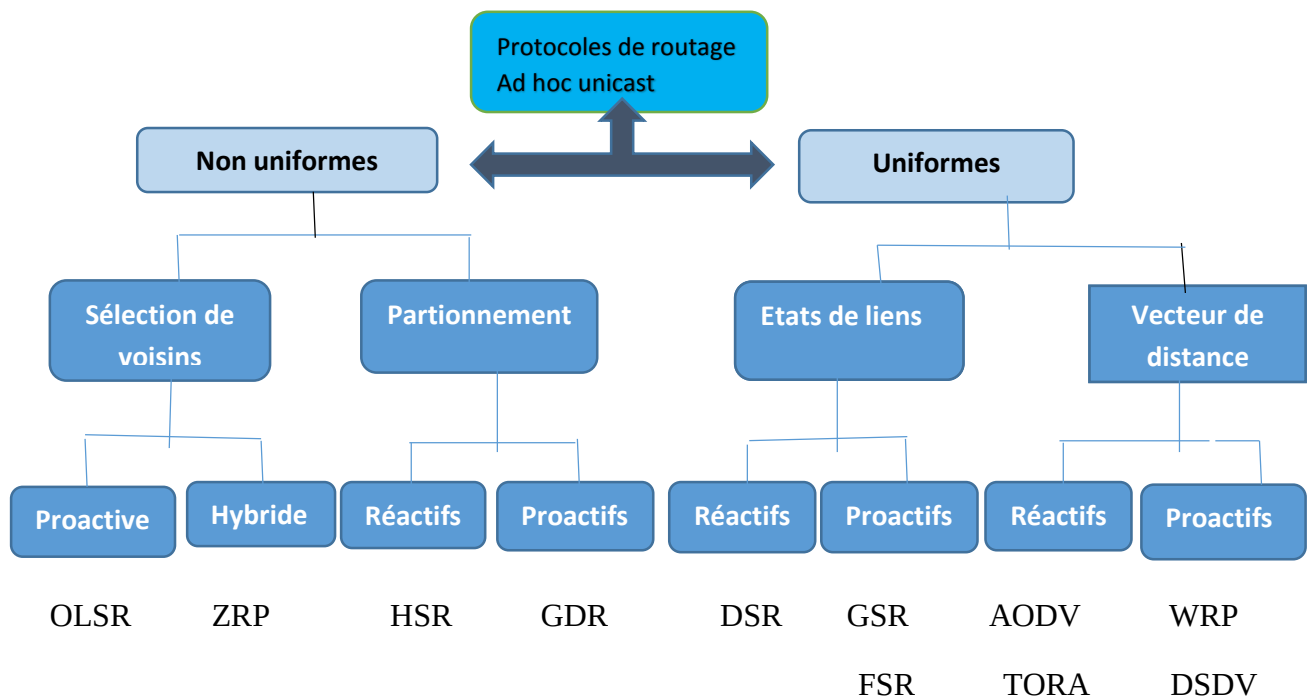


Figure I.7 : Classification des protocoles de routage Ad-Hoc

I.3.1.1. Protocoles de routage proactifs

Les approches proactives de routage, conçues pour les réseaux ad hoc, sont dérivées des protocoles traditionnels du vecteur d'état et à vecteur de distance développés pour l'usage dans les réseaux filaires. La caractéristique primaire des approches proactives est que chaque nœud dans le réseau maintient un itinéraire à tous les autres nœuds dans le réseau à tout moment. La création et l'entretien d'itinéraire sont accomplis par une combinaison des mises à jour périodiques et par le déclenchement des événements : Les mises à jour périodiques se font par

des échanges d'informations de routage entre les nœuds dans des intervalles de temps prédéfinis, indépendamment des caractéristiques de mobilité et du trafic du réseau.

Les mises à jour par le déclenchement d'événements, se font par des échanges d'informations de routage toutes les fois qu'un certain événement est produit, tel qu'une addition de liens ou un déplacement d'un nœud. Dans ce cas, le taux de mobilité affecte directement la fréquence des mises à jour parce que les changements de lien se produisent à mesure que la mobilité augmente.

Les approches proactives ont l'avantage que les itinéraires sont disponibles à tous moments. Cependant, l'inconvénient majeur de ces protocoles est que les frais généraux de contrôle peuvent être importants surtout dans de grands réseaux ou dans les réseaux de forte mobilité.

De plus, la quantité d'état de routage maintenue dans chaque nœud est de $O(n)$, où n est le nombre de nœuds dans le réseau.

Les protocoles proactifs tendent à être performants dans les réseaux où il y a un nombre significatif de sessions de données actives. Dans ces derniers, les frais généraux sont justifiés parce que la majorité de ces chemins sont utilisés [11].

I.3.1.2. Protocoles de routage réactifs

Le routage réactif fonctionne à la demande. Aucune information n'est stockée dans les routeurs sur des destinations vers lesquelles le nœud concerne n'a pas de route active. Lorsqu'une application désire contacter un correspondant, et seulement à cet instant, une route est recherchée. Ce type de protocoles présente l'avantage de ne pas surcharger le réseau en trafic de contrôle et de ne requérir des routeurs qu'une capacité de stockage minimale. Toutefois, le délai d'établissement des communications peut être élevé lorsque le réseau est chargé ou lorsque le correspondant est à une distance importante de l'émetteur.

Le protocole Ad Hoc On Demand Distance Vector (AODV) est un protocole réactif de type vecteur de distance. Lorsqu'un mobile désire envoyer un flux de paquets à destination d'un autre mobile et qu'il ne dispose d'aucune route pour joindre son correspondant, il diffuse un paquet de requête de route (RREQ). Ce paquet se propage par inondation à travers tout le réseau. Lorsque la destination est atteinte, elle envoie un paquet de réponse (RREP) qui traversera le chemin inverse de la requête correspondante, provoquant l'activation de la route dans les nœuds intermédiaires. Lorsque ce paquet arrive à la source du trafic, le transfert peut commencer. Pour pallier la mobilité des nœuds intermédiaires, un mécanisme de reconstruction locale des routes est mis en place.

Le protocole Dynamic Source Routing (DSR) effectue, quant à lui un routage par la source.

La recherche de routes est effectuée de la même manière qu'avec AODV, par inondation du réseau.

Cependant, aucune information n'est stockée dans les routeurs intermédiaires. Les paquets de requête sont, quant à eux modifiés de saut en saut et contiennent la liste intégrale des routeurs qu'ils ont traversés.

Pour chaque requête de route reçue, la destination envoie une réponse. Ces réponses décrivent l'intégralité du chemin emprunté par la requête correspondante. Lors de la communication, la route que chaque paquet de données doit emprunter est contenue dans l'en-tête du paquet, ce qui permet à la source disposant d'autant de routes qu'elle a reçu de réponses d'effectuer un équilibrage de charge ou de disposer de routes de secours pour palier la mobilité [24].

I.3.1.3. Protocoles de routage Hybrides

Ces protocoles, qui mêlent généralement les modes proactif et réactif, fonctionnent dans l'un ou l'autre mode suivant des conditions prédéfinies.

Dans ce système, on peut garder la connaissance locale de la topologie jusqu'à un nombre prédéfini – a priori petit – de saut par un échange périodique de trames de contrôle, autrement dit par une technique proactive. Les routes vers des nœuds plus lointains sont obtenues par schéma réactif, c'est-à-dire par l'utilisation de paquets de requête en diffusion [25].

Les protocoles hybrides combinent les deux approches proactive et réactive. Le principe proactif est utilisé pour le proche voisinage de chaque nœud (2 à 3 sauts). Et le principe réactif est utilisé au-delà, optimisé par ce regroupement de nœuds de proches voisins [26].

Les protocoles de routage hybrides sont une combinaison des protocoles de routage proactifs et réactifs. Ils utilisent un protocole proactif pour apprendre le voisinage de chaque nœud jusqu'à un, deux ou trois sauts, etc. Ainsi, ces protocoles disposent immédiatement de routes dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride utilise les techniques des protocoles réactifs pour chercher des routes. Grâce à cette segmentation en zones, le réseau est divisé en plusieurs parties, ce qui améliore la recherche de routes en mode réactif, à la réception d'une requête de recherche réactive, un nœud peut indiquer immédiatement si la destination est dans le voisinage ou non, et par conséquent savoir s'il faut aiguiller la dite requête vers les autres zones sans déranger le reste de sa zone. Ce type de protocole s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs.

Les protocoles les plus connus sont OLSR (Optimised Link State Routing) pour les proactifs et AODV pour les réactifs. OLSR a été optimisé en matière de qualité de service pour réduire la taille des messages de contrôle et limiter le trafic de contrôle par l'utilisation de relais multipoints (MPR). En effet, les MPR sont des nœuds, parmi les proches voisins d'un nœud, qui sont les seuls autorisés à diffuser les messages de contrôle de ce nœud [27], entre autres, ces protocoles permettent l'exploitation des réseaux ad-hoc pour des applications concrètes.

I.4. Classification de l'attaque Une intrusion peut être définie comme tout ensemble d'actions qui essaient d'exploiter une ou plusieurs failles du système à travers une ou plusieurs menaces détectées. La taxonomie des attaques contre les réseaux ad-hoc proposée dans les attaques peuvent être conduites pour les raisons suivantes [28].

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

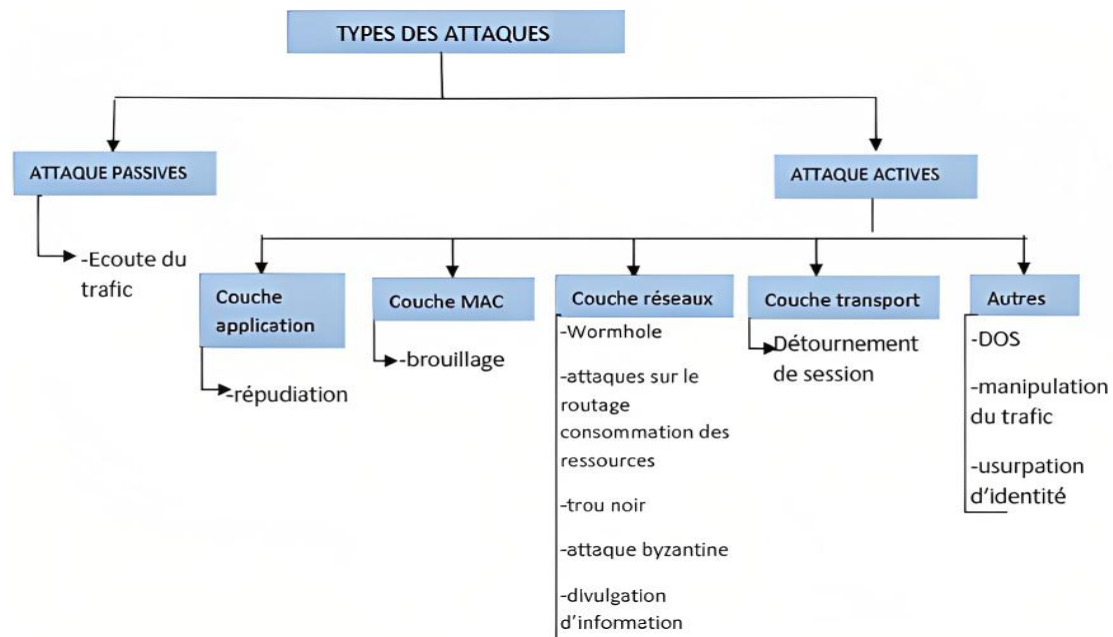


Figure I.8 : Classifications des attaques dans les réseaux Ad-Hoc

Les attaques passives, telles que l'écoute indiscrète ("eavesdropping"), se limitent à surveiller et analyser le trafic échangé. Ces attaques sont relativement faciles à réaliser car l'attaquant a juste besoin d'un récepteur approprié. De plus, elles sont difficiles à détecter car l'attaquant n'altère pas les informations échangées. L'objectif de l'attaquant peut être de recueillir des informations confidentielles ou d'identifier des nœuds importants dans le réseau, comme les "Chef de groupe" (cluster head). En analysant les informations de routage, l'attaquant se prépare à mener ultérieurement une action spécifique.

D'un autre côté, les attaques actives consistent en des tentatives de suppression ou de modification des messages transmis sur le réseau. L'attaquant peut également injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service. Ces attaques sont plus complexes à exécuter que les attaques passives, mais elles peuvent avoir un impact plus direct et immédiat sur le fonctionnement du réseau [29].

I.5. La sécurité

La sécurité est un défi majeur dans les réseaux Ad-Hoc en raison de la nature ouverte et la dynamique de leur environnement. Les réseaux Ad-Hoc sont plus vulnérables aux attaques malveillantes car ils manquent d'une infrastructure centralisée et sont plus difficiles à sécuriser communication entre nœuds.

Les attaques courantes dans les réseaux ad hoc comprennent l'usurpation d'identité, le brouillage, la modification ou la suppression de données, l'écoute passive et active, et les attaques par déni de service.

Pour garantir la sécurité dans les réseaux Ad-Hoc, il est nécessaire de mettre en œuvre des mesures de sécurité robustes telles que l'authentification des nœuds, le chiffrement des données, le contrôle d'accès, la détection d'intrusion et la protection contre les attaques par déni de service.

Les protocoles de sécurité pour les réseaux Ad-Hoc doivent être conçus pour prendre en compte la mobilité des nœuds et les changements fréquents de la topologie du réseau. Des approches telles que le partage de clés, la segmentation de données et l'utilisation de certificats numériques peuvent être utilisées pour renforcer la sécurité des réseaux ad hoc.

En fin de compte, la sécurité des réseaux ad hoc dépend de la mise en œuvre efficace de mesures de sécurité robustes et de la sensibilisation des utilisateurs à l'importance de la sécurité dans les réseaux ad hoc. Les recherches continuent de se concentrer sur le développement de protocoles de sécurité innovants et efficaces pour les réseaux ad hoc afin de garantir des communications sécurisées et fiables dans ces environnements complexes.

I.6. Conclusion

Les réseaux Ad-Hoc sont des réseaux sans fil dynamiques et flexibles qui ne dépendent pas d'une infrastructure centralisée. Ils peuvent être utilisés dans de nombreuses applications, notamment les réseaux de capteurs sans fil, les réseaux de communication militaires, les réseaux de communication d'urgence et les réseaux de communication pour véhicules autonomes. Cependant, les réseaux Ad-Hoc présentent des défis de conception et de mise en œuvre, notamment en termes de gestion de l'énergie, de sécurité et de résistance aux pannes de nœuds. Les protocoles de routage pour les réseaux Ad-Hoc doivent pouvoir s'adapter rapidement aux modifications de la topologie du réseau et de la mobilité des nœuds.

Malgré ces défis, les réseaux Ad-Hoc continuent de susciter un grand intérêt de la part de la communauté des chercheurs et constituent un domaine actif de développement technologique. Avec l'avènement des nouvelles technologies de communication et de détection, les réseaux auto-organisés sont susceptibles de se généraliser et de jouer un rôle de plus en plus important dans notre vie quotidienne, et à la fin nous avons parlé en général sur le routage et la sécurité dans les réseaux mobile Ad-Hoc comme point de départ pour la deuxième chapitre.

Chapitre II :

Le routage et la sécurité dans les
réseaux Ad-Hoc

II.1. Introduction

Les réseaux Ad-Hoc sont des réseaux sans fil où les dispositifs mobiles communiquent directement entre eux sans passer par une infrastructure centralisée telle qu'un routeur ou un point d'accès. Cela les rend extrêmement utiles dans les environnements où une infrastructure réseau fixe n'est pas disponible ou pratique, tels que les zones de catastrophe, les événements en plein air, ou les réseaux militaires sur le terrain.

Cependant, les réseaux Ad-Hoc sont également vulnérables aux attaques, car ils sont souvent déployés dans des environnements non sécurisés et les nœuds du réseau ont des ressources limitées pour gérer la sécurité. Les attaquants peuvent compromettre le fonctionnement du réseau, accéder à des informations confidentielles, ou encore lancer des attaques par déni de service. Pour remédier à ces problèmes de sécurité, plusieurs mécanismes de routage et de sécurité ont été développés pour les réseaux ad hoc. Les protocoles de routage adaptatifs permettent aux nœuds de trouver des chemins de communication efficaces et résistants aux pannes. Les protocoles de sécurité utilisent des techniques telles que le chiffrement, l'authentification et la gestion des clés pour protéger les communications et les données stockées.

II.2. Routage dans les réseaux Ad Hoc

II.2.1. Définition du routage

Le routage est une méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœud appartenant au réseau, ce qui assure l'échange des messages d'une manière continue.

Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante. Son intérêt consiste à trouver le chemin optimal au sens d'un certain critère de performance (bande passante, délai, etc.).

Il doit aussi être capable de s'adapter aux événements venant perturber le réseau (panne, congestion, etc.). Son problème réside dans l'effet de trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa serviabilité en cas de n'importe quelle panne d'arc ou de nœud [30].

II.2.2. Le routage dans les réseaux ad hoc

Le routage est la tâche d'acheminement de flux des données à partir des nœuds sources vers les nœuds destinations. Si une seule destination est impliquée dans la communication, alors il s'agit d'un "routage unicast", si encore tous les nœuds du réseau ou juste un sous ensemble sont concernés par la réception des données alors on parle du "broadcast" et du "routage multicast".

L'objectif principal des protocoles de routage est l'établissement et la maintenance des chemins, pour que les données soient correctement délivrées dans le réseau. La conception des protocoles de routage pour les réseaux Ad hoc est loin d'être un problème simple. Des nouvelles approches de routage sont nécessaires pour effectuer un routage de données sûr et efficace. L'instabilité du médium de communication sans fil, la limitation d'énergie et de la bande passante, ainsi que la mobilité des nœuds introduisent plus de difficulté et de complexité à la conception des protocoles de routage pour les réseaux Ad hoc [31] [32].

II.3. Les risques liés à la sécurité

Le risque est un concept informatique - c'est la probabilité de perte de la sécurité du système, qu'elle soit élevée, moyenne, faible ou nulle, trois facteurs entrent en ligne de compte dans la détermination du risque : la nature de la menace, la vulnérabilité du système et l'importance de l'actif qui pourrait être endommagé ou rendu indisponible.

Le risque peut donc être défini de la manière suivante [33]:

$$\text{Risque} = \text{Menace} \times \text{Vulnérabilité} \times \text{Actif}$$

Quand vous souhaitez évaluer le risque associé à une menace de piratage qui compromettrait un système particulier. Si votre réseau est très vulnérable, et que l'actif est critique, votre risque est élevé. Mais si vous avez de bonnes défenses périmétriques et que votre vulnérabilité est faible, même si l'actif est critique, votre risque est moyen [34].

II.3.1. Analyse de risque en sécurité

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire donc de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions et les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. Afin de bien appréhender

la problématique de la sécurité dans les réseaux mobiles ad hoc, les éléments suivant pouvant servir de base à une étude de risque :

1. Détermination des fonctions et données sensibles des réseaux sans fil Ad Hoc.
2. Recherche des exigences de sécurité fondées sur les propriétés de la sécurité.
3. Etude des vulnérabilités.
4. Etude des menaces et quantification de leur probabilité d'occurrence ou de leur faisabilité.
5. Mesure du risque encouru en fonction des vulnérabilités mises en lumière et des menaces associées [4].

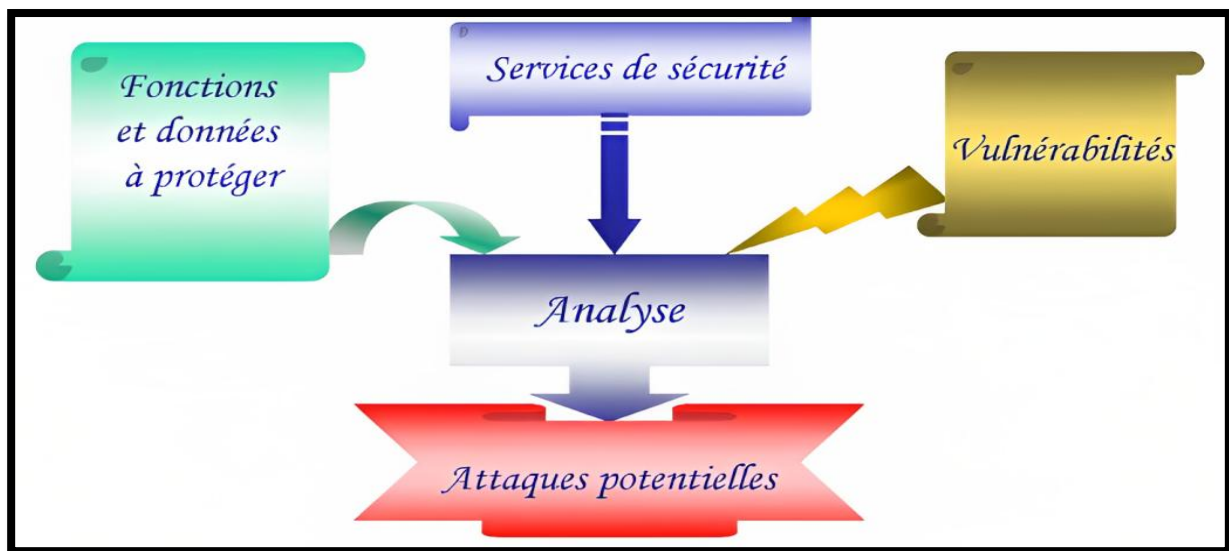


Figure II.1 : étapes de l'analyse des risques

II.4. Exigence de la sécurité dans les réseaux ad hoc

Déterminer les exigences de sécurité de tout système nécessite de comprendre toutes les limitations qui pèsent sur ce système. Cette étape permet de mesurer les paramètres de sécurité [33].

II.4.1. Contraintes de la sécurité

Les contraintes de sécurité ad hoc sont multiples. On peut les répartir en six grands thèmes traitant :

II.4.1.1. Caractéristiques des nœuds

Les nœuds eux-mêmes sont des points de vulnérabilité du réseau car un attaquant peut compromettre un élément laissé sans surveillance. De plus, certains éléments peuvent avoir de faibles capacités de calculs.

II.4.1.2. Gestion de l'énergie

L'énergie doit être conservée au maximum pour cela les nœuds chercheront le plus souvent à se mettre en veille, ce qui provoque donc une minimisation de l'activité de l'ensemble du réseau.

II.4.1.3. L'absence d'infrastructure centralisée

Cette caractéristique du réseau ad hoc qui pénalise la gestion des accès aux ressources du réseau.

II.4.1.4. La technologie sans fil

Les perturbations dues à l'environnement radio peuvent entraîner des diminutions de débit et bande passante.

II.4.1.5. Mobilité

Les éléments étant fortement mobiles, leur sécurité physique est moins assurée.

II.4.1.6. Les mécanismes de routage

Sont d'autant plus critiques dans les réseaux Ad-Hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

II.4.2. Les besoins de sécurité

Le réseau a besoin de sécurité contre les attaquants et les pirates. Le premier est la sécurité des informations de données, c'est-à-dire pour protéger les informations contre tout accès non autorisé et toute perte. Et le second est la sécurité informatique c'est-à-dire protéger les données et déjouer les pirates. Ici, la sécurité du réseau ne signifie pas seulement la sécurité dans un seul réseau, mais plutôt dans n'importe quel réseau ou réseau de réseaux.

Maintenant, notre besoin de sécurité réseau s'est divisé en deux besoins. L'un est le besoin de sécurité de l'information et l'autre est le besoin de sécurité informatique.

Sur internet ou n'importe quel réseau d'une organisation, des milliers d'informations importantes sont échangées quotidiennement. Ces informations peuvent être utilisées à mauvais escient par des attaquants. La sécurité de l'information est nécessaire pour les raisons suivantes.

- Pour protéger les informations secrètes des utilisateurs sur le net uniquement.
Aucune autre personne ne doit le voir ou y accéder.

- Pour protéger les informations contre toute modification indésirable, accidentelle ou intentionnelle par des utilisateurs non autorisés.
- Pour protéger les informations contre la perte et les faire parvenir correctement à leur destination.
- Pour gérer l'accusé de réception du message reçu par n'importe quel nœud afin de se protéger contre le refus de l'expéditeur dans des situations spécifiques

Les réseaux ad hoc doivent satisfaire les services de sécurité suivants : [35] [36].

II.4.2.1. Contrôle d'accès

Empêcher les nœuds étrangers d'accéder au réseau. Le contrôle d'accès donne aux nœuds légitimes un moyen de détecter les messages provenant de sources externes au réseau

II.4.2.2. Authentification

S'assurer de l'identité des entités en cours de communication. Avec l'authentification, le destinataire sera sûr que le message provient de la source prétendue.

II.4.2.3. Confidentialité des données

Assuré que l'information ne peut pas être interprétée par des tiers non autorisés. Les informations de routage doivent aussi, dans certains cas, rester secrètes.

II.4.2.4. Intégrité

Assuré que la modification des données transmises sera détectée. On utilise souvent les fonctions de hachage pour assurer l'intégrité.

II.4.2.5. Non-répudiation

Empêcher un nœud de nier l'envoi ou bien la réception d'un message.

II.4.2.6. Fraîcheur

Garantir que les données présentes échangées sur le réseau sont viables.

Ce service permet de lutter contre la réinjection d'anciens messages interceptés par un attaquant

II.4.2.7. Disponibilité :

Assuré la présence des services du réseau même en présence d'attaques de déni de service. Ces attaques peuvent se présenter au niveau de différentes couches d'un réseau ad hoc. La disponibilité donne aussi une assurance sur la réactivité et le temps de réponse du réseau

II.4.3. Vulnérabilité des réseaux Ad- Hoc

Les réseaux ad hoc présentent quelques faiblesses. Certaines faiblesses sont liées à la technologie sans fil, d'autres aux caractéristiques de ces réseaux.

La première vulnérabilité de ces réseaux est liée à la technologie sans fil sous-jacente. En effet l'utilisation d'un canal radio favorise l'écoute et la perturbation des messages échangés par tout

nœud possédant le récepteur adéquat même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges.

Les nœuds sont aussi des points de vulnérabilité du réseau. En effet, un attaquant peut compromettre un terminal laissé sans surveillance. L'absence d'infrastructure fixe est une autre faiblesse des réseaux ad hoc car elle rend impossible l'utilisation d'une entité centrale pour la gestion des accès aux ressources du réseau [37].

II.5. Les attaques contre les réseaux Ad- Hoc

II.5.1. Attaques d'identité

Dans cette classe d'attaque, un intrus usurpe l'identité d'un autre nœud, afin de l'utiliser pour mener des attaques contre les autres nœuds du réseau. Un nœud peut usurper facilement l'identité d'un autre nœud, ceci peut être fait en changeant sa propre adresse IP, MAC ou toutes autres identités définies dans la couche application avec celle d'un autre nœud légitime. Certaines procédures fortes d'authentification peuvent être employées pour empêcher cette attaque. Cette classe d'attaque inclut : [38] [39].

II.5.1.1. Sybil attack

Dans cette attaque, le nœud présente des identités multiples aux autres nœuds du réseau, créant ainsi des inconsistances dans les tables de routage des nœuds voisins. Ce qui permet de créer plusieurs routes, passant par le nœud malicieux, qui ne sont en réalité qu'un seul chemin.

II.5.1.2. Usurpation d'identité (Spoofing)

Un nœud malveillant peut altérer son adresse IP ou son adresse MAC dans le but de se faire passer pour un autre nœud légitime du réseau. En utilisant l'identité de ce nœud, l'intrus peut ensuite lancer ses attaques de manière trompeuse et potentiellement causer des dommages au réseau.

II.5.1.3. Man in the middle attack

L'attaquant peut personifier le récepteur pour l'expéditeur, et vice versa, sans que l'un ou l'autre se rendent compte qu'ils ont été attaqués. De cette façon, l'attaquant se positionne entre le récepteur et l'émetteur et en conséquence, il peut mener facilement son attaque dans le réseau.

II.5.2. Modification, suppression et insertion des messages

Dans un réseau ad hoc, un nœud malicieux peut modifier ou supprimer les messages passant par lui, comme il peut insérer de nouveaux messages dans le but, de perturber le bon fonctionnement du réseau. Cette classe d'attaque inclut [37] :

II.5.2.1. Blackhole attack

Un nœud qui falsifie les informations de routage peut manipuler le flux de données afin de forcer leur passage par lui-même. Une fois que les données sont redirigées vers ce nœud malveillant, celui-ci ne transfère rien et agit comme un "trou noir" dans le réseau, absorbant les données sans les transmettre à leur destination légitime. Cela peut entraîner une perte de données, des retards ou des interruptions de communication pour les autres nœuds du réseau. Si aucun contrôle n'est fait sur la provenance et l'intégrité des messages de routage du réseau Ad hoc, un nœud malicieux pourra facilement causer des perturbations au réseau. Cela lui sera d'autant plus facile que les réseaux sans fil Ad hoc n'ont pas de barrière physique pour se protéger et que tous les éléments peuvent potentiellement participer au mécanisme de routage. Si un nœud malicieux a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut lors du mécanisme de découverte de route répondre au nœud initiateur avec un message de type route replay en annonçant un chemin avec un cout minimal, vers le nœud demandé. Le nœud émetteur mettra alors sa table de routage à jour avec cette fausse route. Les paquets de données du nœud émetteur vers le nœud destinataire transiteront par le nœud malicieux qui pourra tout simplement les ignorer. Cette attaque est appelée trou noir, (black hole) Les paquets sont captés et absorbés par le nœud malicieux.

La figure II.2 illustre cette attaque [33].

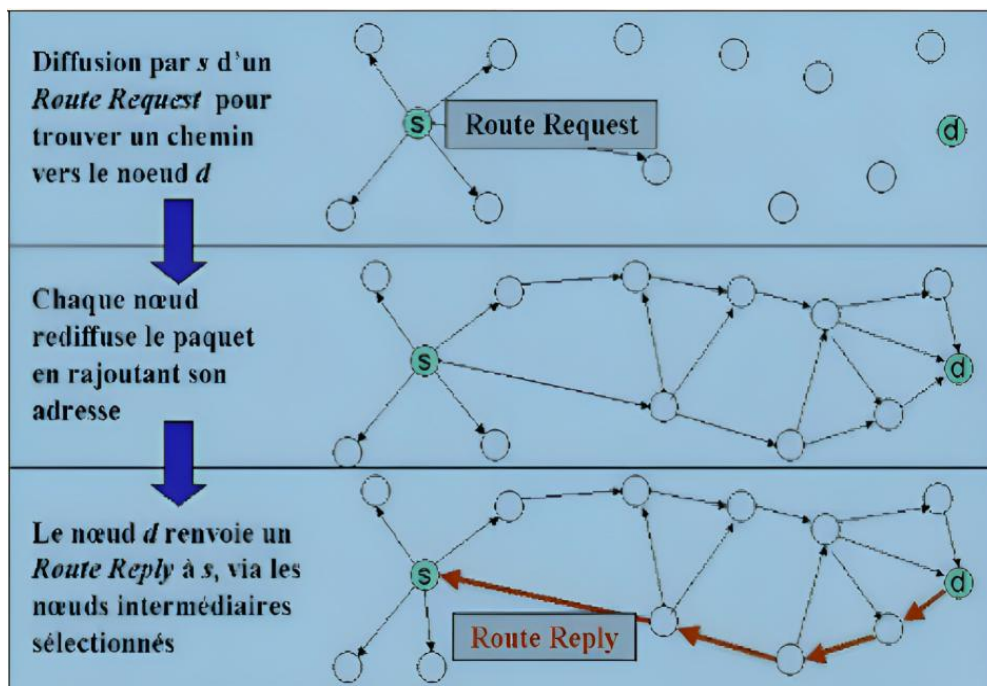


Figure II.2 : Découverte de route initiée par le protocole de routage

II.5.2.2. Attaque Grayhole

C'est une variante de l'attaque Blackhole qui consiste à éliminer seulement les paquets de données de certaines applications qui sont vulnérables à la perte de paquets

II.5.2.3. Attaque Rushing

Le rush concerne les protocoles de routage réactifs que l'attaquant n'utilise pas les règles d'accès aux canaux ne sont pas respectées, imposées par la couche MAC pour se précipiter les paquets RREQ qui le traversent ; Par conséquent, ces colis se propagent plus rapidement vers la destination et il est donc tout à fait possible de rejeter tous les autres paquets. Car dans la plupart des protocoles de routage interactifs, les auteurs proposent des mécanismes pour contrôle pour réduire le coût de la découverte d'itinéraire, sous lequel les nœuds intermédiaires rediffuser uniquement les paquets de contrôle (paquets RREQ) qui arrivent en premier, et Jeter toutes les autres copies de ce paquet qui arrivent plus tard

II.5.3. Replay ou rejeu

Un nœud malicieux réinjecte des messages dans le réseau. Des anciens messages continuent à circuler ce qui occupe de la bande passante et peut même affecter la justesse de la topologie [40].

II.5.3.1. Wormhole attack

Dans une attaque trou ver, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant, pour les réintroduire dans le réseau. Dans ce genre d'attaque, les adversaires coopèrent pour fournir un canal à basse latence, pour la communication, en utilisant une radio pour communiquer avec une puissance plus élevée et des liens à longue portée. Ceci favorise les nœuds voisins à acheminer leurs données à travers l'attaquant.

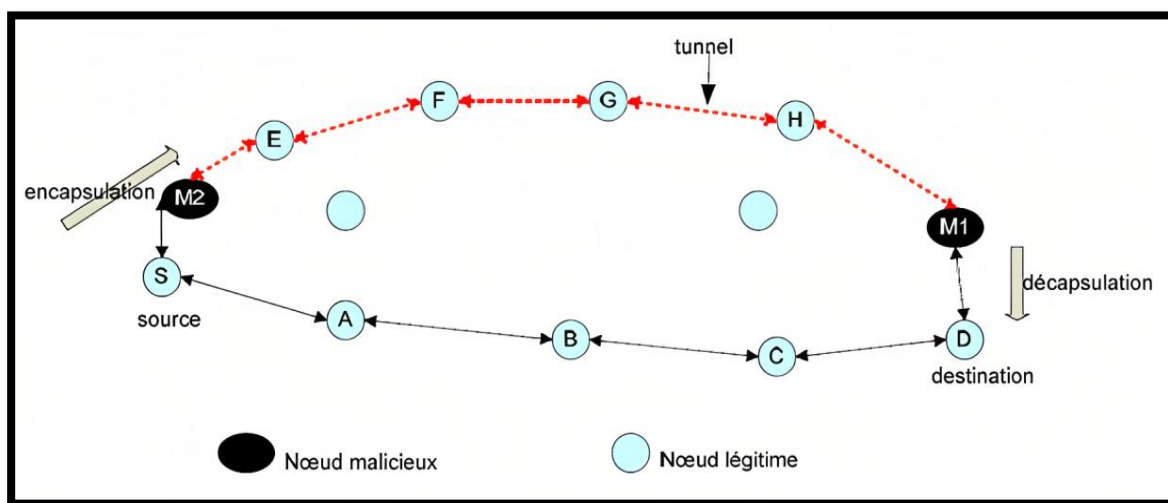


Figure II.3: Wormhole par encapsulation

II.5.4. Dénis de services (DoS)

Cette classe d'attaque inclut toutes attaques touchant à la disponibilité du réseau. On cite à titre d'exemple [37] :

II.5.4.1. Consommation des ressources

L'attaquant consomme les ressources du réseau (bande passante, mémoire, énergie) de sorte que le réseau devient indisponible aux utilisateurs.

II.5.4.2. Destruction ou changement d'information

Dans cette attaque de DoS, un attaquant essaye de changer ou détruire l'information de configuration, de ce fait empêchant les utilisateurs légitimes d'employer le réseau. Un réseau incorrectement configuré peut ne pas bien travailler ou ne pas fonctionner du tout.

II.6. Protection du protocole de routage dans les réseaux ad hoc

Lorsque nous parlons d'obtenir des conseils, nous voulons garantir l'intégrité, la non-répudiation et disponibilité du service. Le routage des messages et les informations sont protégés à l'aide des protocoles de sécurité suivants :

II.6.1. Types de protocoles

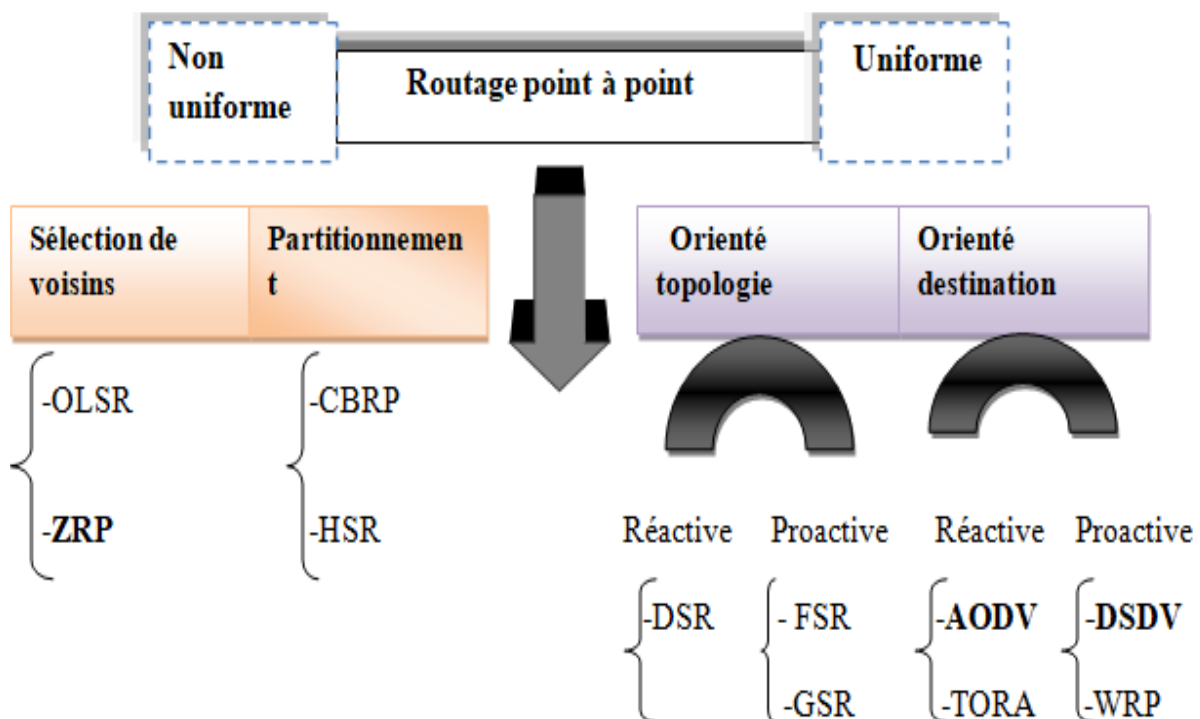


Figure II.4 : différentes classes de protocole de routage ad-hoc [41]

II.6.2. Etude de quelques protocoles de routages

Chaque protocole présente des caractéristiques distinctes en termes de fonctionnalités, de performances et d'adaptabilité, et le choix dépend des besoins spécifiques du réseau.

II.6.2.1. Le protocole DSDV

II.6.2.1.1. Définition

Est un protocole proactif, uniforme et orienté destination. Chaque nœud possède en permanence dans sa table de routage le chemin le plus récent découvert vers chaque nœud du réseau. Parmi plusieurs chemins possibles, DSDV privilégie le chemin le plus court il est principalement inspiré de l'algorithme distribué de Bellman Ford (DBF Distributed

Bellman-Ford) Toute fois, chaque station mobile se voit maintenir une table de routage contenant :

- Toutes les destinations possibles dans le réseau.
- Le nombre de nœuds (ou de sauts) nécessaire pour atteindre chacune de ces destinations.
- Le numéro de séquences (SN : Séquence Number) qui correspond à un nœud destination afin de conserver la consistance des tables de routages dans un réseau, souvent connue par la forte variation de la topologie, à chaque nœud est attribué un numéro de séquence NS qui permet de distinguer les nouvelles routes des anciennes. Ce qui permette remédier au problème de boucle de routage.

II.6.2.1.2. Principales fonctionnalités

Chaque nœud transmet à son voisin direct sa table de routage périodiquement ou en cas de changement imprévu de la table. Donc, la mise à jour se fait selon deux facteurs les événements qui peuvent surgir (déplacement de nœuds, apparition d'un nouveau voisin ...etc.), vu ces deux facteurs, on peut distinguer deux types de mise à jour.

- **Mise à jour complète**

Qui n'est rien autre que la mise à jour périodique, c'est-à-dire que le nœud transmet la totalité de sa table de routage vers ses voisins.

- **Mise à jour incrémentale**

"Cette mise à jour est réalisée uniquement lorsqu'il y a des événements (tels que l'arrivée d'un nouveau voisin, la disparition d'un nœud, etc.). Dans ce cas, seule l'entrée concernant le nœud spécifique dans la table de routage est modifiée. Cette mise à jour est également désignée comme une mise à jour partielle. À noter que la mise à jour est effectuée en transmettant généralement un paquet contenant :"

- Le nouveau numéro de séquence, incrémenté, du nœud émetteur.
- L'adresse de la destination.
- Le nombre de sauts séparant le nœud de la destination.
- Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination. [42]

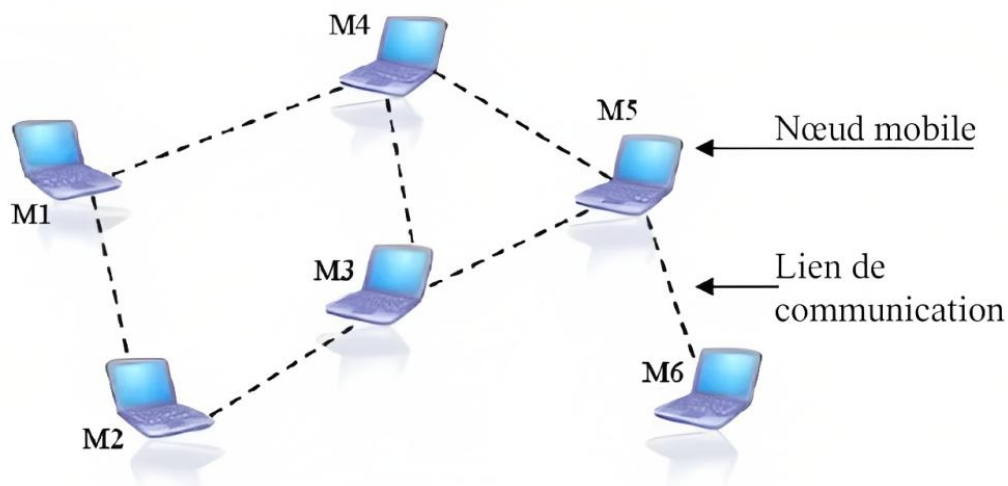


Figure II.5 : Exemple d'un réseau Ad-hoc

Si l'on considère que le DSDV est le protocole de routage utilisé dans la table II.1 de routage correspondante au nœud M1 ressemblera à la suivante [42] [4] :

destination	Nombre de sauts	Prochain nœud	Numéro de séquence
M1	0	M1	NS1

M2	1	M2	NS2
M3	2	M2	NS3
M4	1	M4	NS4
M5	2	M4	NS5
M6	3	M4	NS6

Tableau II.1 : Table de routage du nœud M1 du graphe

Ainsi tout nœud, qui a subi une mise à jour, compare les données de routage reçus avec pour lui, et la route la plus récente (celle avec la plus grande valeur du numéro de séquence) sera utilisée. Si deux routes ont le même numéro de séquence, alors la route qui possède la meilleure métrique est celle qui sera utilisée. La métrique utilisée dans le calcul des plus courts chemins est, tout simplement, le nombre de nœuds intermédiaires existants sur ce chemin. Un lien rompu est matérialisé par une valeur infinie de sa métrique, i.e. une valeur plus grande que la valeur maximale permise par la métrique.

Parmi les inconvénients du protocole DSDV, est qu'il est très lent, du fait qu'il doit attendre la mise à jour transmise par le destinataire pour modifier l'entrée adéquate dans la table de distance. Bien qu'il remédie au problème de boucle de routage « a Routing Loop » et du Counting to Infinity (du DBF) [42]

II.6.2.1.3. Avantages et inconvénients

Extension de la couverture de la station de base les ordinateurs mobiles seront fréquemment utilisés en conjonction avec des stations de base, qui leur permettent d'échanger des données avec d'autres ordinateurs connectés au réseau filaire réseau.

En participant au protocole DSDV, les stations de base peuvent étendre leur couverture au-delà de la portée imposée par leurs émetteurs sans fil. Lorsqu'une base station participe au DSDV, elle est indiquée comme route par défaut dans les tables transmises par une station mobile. De cette façon, les stations mobiles à portée d'une station de base peuvent coopérer pour étendre efficacement la portée de la station de base afin de desservir d'autres stations en dehors de la portée de la station de base, tant que ces autres stations mobiles sont proches vers une autre station mobile à portée. Il était parfait pour les réseaux ad hoc avec quelques nœuds.

Étant donné que cet algorithme ne présente pas les spécifications formelles, est donc pas utilisé à des fins commerciales, malgré de nombreuses améliorations ont été apportées.

D'autre part, il à ses inconvénients DSDV nécessite des mises à jour régulières des tables de routage qui nécessitent un gaspillage de ressources (batterie et bande passante) même lorsque le réseau est inactif. En outre, Parce que les nœuds sont capables de se reconnaître, DSDV il y a « utilisation de balise-message et « bonjour paquet ». Pour chaque mise à jour à envoyer, vous aurez un nouveau numéro de séquence. Le pire des cas se produit lorsqu'il y a un chemin de rupture: pour chaque individu sûr (porté en MANET compte tenu de la mobilité de l'hôte), les nœuds sont contraints d'échanger NPDU (avec un nombre impair de séquence) dans

L'inondation, la génération de tête sur la consommation de bande passante. Par conséquent, DSDV ne convient pas à des réseaux très dynamiques [43] [44].

II.6.2.2. OLSR

II.6.2.2.1. Définition

L'autre proposition retenue par l'IETF pour le routage dans les réseaux Ad-Hoc. Est un protocole proactif qui repose sur l'échange régulier d'informations sur la topologie du réseau. L'algorithme est optimisé par la réduction de la taille et du nombre des messages échangés: seuls des nœuds particuliers, les MPR, Multipoint Relay, diffusent des messages de contrôle sur la totalité du réseau.

II.6.2.2.2. Principales fonctionnalités

Les définitions suivantes sont utilisées dans la description du protocole:

Nœud: hôte d'un réseau ad hoc implémentant le protocole OLSR.

Interface: point d'accès au réseau ad hoc. Un nœud peut avoir plusieurs interfaces, chacune ayant une adresse IP propre.

Voisin immédiat: le nœud X est un voisin immédiat du nœud Y si Y est à portée du nœud X

MPR (MultiPoint Relay): nœud sélectionné par un de ses voisins immédiats (appelé MS, MPR Selector) pour retransmettre ses messages de mise à jour. L'ensemble des MPR d'un nœud est choisi parmi les voisins immédiats, de manière à permettre d'atteindre tous les nœuds situés exactement à 2 sauts.

Lien: couple d'interfaces capables de communiquer (i.e. recevoir des messages). L'état d'un lien peut être :

Symétrique SYM si les deux interfaces peuvent s'entendre.

Asymétrique ASYM ou HEARD, si les nœuds ont des puissances d'émission différentes.

MPR, si l'émetteur a sélectionné le nœud comme MPR, dans ce cas le lien doit être symétrique.

Lost, quand le lien est perdu tous les nœuds envoient périodiquement des messages HELLO à leurs voisins immédiats sur chacune de leurs interfaces. Ces messages ne sont pas relayés vers d'autres nœuds.

II.6.2.2.3. Avantages et inconvénients

D'après la présentation ci-dessus du protocole de routage OLSR, nous remarquons qu'il offre des fonctionnalités très intéressantes tout en recherchant des routes optimales en termes de nombre de sauts, il diminue au maximum le nombre de messages de contrôle transmis sur le réseau, en utilisant la technique de sélection des MPR. OLSR gère convenablement la topologie du réseau, en expédiant périodiquement des messages TC et il peut contrôler l'utilisation multiple des interfaces (messages MID) ainsi qu'OLSR offre la possibilité de communication entre un réseau MANET et un réseau filaire (messages HNA)

Tous ces avantages du protocole OLSR ne veut pas dire qu'il n'a pas d'inconvénients, or que le problème actuel d'OLSR est celui de la sécurité, Malgré que ces dernières années beaucoup de recherches ont été faites pour améliorer sa protection contre les attaques, mais OLSR reste toujours vulnérable à certaines attaques[45].

II.6.2.3. Le protocole AODV

II.6.2.3.1. définition

Un des protocoles les plus connus dans cette catégorie est le protocole AODV qui n'est en réalité qu'une combinaison entre les deux protocoles DSDV et DSR. En effet, c'est une combinaison de la demande de base de la découverte et le maintien de route de DSR et le routage de saut par saut et des numéros de séquence de DSDV. La route retenue est bidirectionnelle et correspond au plus court chemin (en nombre de sauts) entre la source et la destination. Chaque nœud maintient une table de routage dont les entrées mémorisent,

Quand un nœud source S veut atteindre la destination D pour laquelle il ne possède pas de route, il inonde le message de demande de route RREQ à ses voisins. Le paquet RREQ contient le numéro de séquence pour cette destination, si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut, il contient aussi la valeur du numéro de séquence du nœud

source. Le RREQ sera propagé jusqu'à ce que le paquet atteigne un nœud qui a une route à la destination. Chaque nœud intermédiaire expédie la demande et crée une route inversée vers S (mémoire une route vers la source).

Quand un nœud intermédiaire a une route vers D, il produit une réponse RREP qui contient le nombre de saut et le numéro de séquence pour D (le plus récent). Les nœuds qui portent la réponse vers S créent une route vers D mais seulement avec le prochain saut et non pas la route toute entière. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud de transit appartenant au chemin recherché.

Pour la mise à jour des routes, le protocole AODV exige des messages HELLO toutes les quelques secondes. Un lien est considéré invalide si trois messages HELLO consécutifs ne sont pas reçus (à travers ce même lien).

Quand un nœud intermédiaire a une route vers D, il produit une réponse RREP qui contient le nombre de saut et le numéro de séquence pour D (le plus récent). Les nœuds qui portent la réponse vers S créent une route vers D mais seulement avec le prochain saut et non pas la route toute entière. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud de transit appartenant au chemin recherché.

Pour la mise à jour des routes, le protocole AODV exige des messages HELLO toutes les quelques secondes, un lien est considéré invalide si trois messages HELLO consécutifs ne sont pas reçus (à travers ce même lien).

II.6.2.3.2. Le principe de numéro de séquence

La circulation inutile des paquets de messages, qui peut arriver avec le DBF (Distribution de Bellman Ford), est intolérable dans les réseaux mobiles ad hoc, caractérisés par une bande passante limitée et des ressources modestes.

L'AODV utilise les principes de numéro de séquence afin d'éviter le problème des boucles infinies et des transmissions inutiles de messages sur le réseau, en plus il permet de maintenir la consistance des informations de routage. A cause de la mobilité des nœuds dans le réseau ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraîches (fresh routes), un nœud les met à jour chaque fois qu'une nouvelle information provenant d'un message RREQ, RREP ou RERR, il incrémente son propre numéro de séquence dans les circonstances suivantes :

- Il est lui-même le nœud de la destination et offre une nouvelle façon de l'atteindre.
- Il reçoit un message AODV (RREQ, RREP, RERR) contenant de nouvelles informations sur le numéro de séquence d'un nœud destination.
- Le chemin vers une destination n'est plus valide.

II.6.2.3.3. Principales fonctionnalités

Dans cette partie nous détaillerons le fonctionnement de protocole AODV, en commençant d'abord par la manière dont il découvre les routes, nous parlerons par la suite sur la façon dont il maintient ces routes, une fois valides.

Découverte de route : Lorsqu'un nœud veut émettre un message, il cherche dans sa table de routage si une route valide existe pour la destination qu'il souhaite atteindre, s'il n'en existe aucune, il se met à la recherche d'une route.

Cette tâche est réalisée par la diffusion de message RREQ sur une adresse de type broadcast au travers du réseau. Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence associé au nœud destination. Cette valeur est copiée de la table de routage, si le numéro de séquence n'est pas connu, la valeur nulle ne sera prise par défaut. Avant l'envoi du paquet RREQ, le nœud origine sauvegarde l'identificateur du message et l'adresse IP de façon à ne pas traiter le message dans le cas où un voisin le lui renverrait, une fois la demande de route effectuée, le nœud demandeur se met en attente de réponses.

Quand un nœud de transit (intermédiaire) reçoit le paquet de la requête, il vérifie dans sa table historique si cette requête a déjà été vue et traitée. Si le paquet est doublon, le nœud doit l'ignorer et arrêter le traitement. Dans le cas contraire le couple (@ source, ID de requête) sera inscrit dans la table historique pour rejeter les futurs doublons, et le nœud continue le traitement en cherchant la destination dans sa table de routage : s'il possède une route récente, à noter qu'une route est récente si le numéro de séquence de la destination dans la table est supérieure ou égale au numéro de séquence dans le paquet RREQ. Dans ce cas, le nœud envoie un paquet de réponse (RREP) à la source lui indiquant comment atteindre la destination.

Autrement le nœud ne connaît pas la route vers la destination : il incrémente le nombre de sauts et rediffuse le paquet (figII.6) [45].

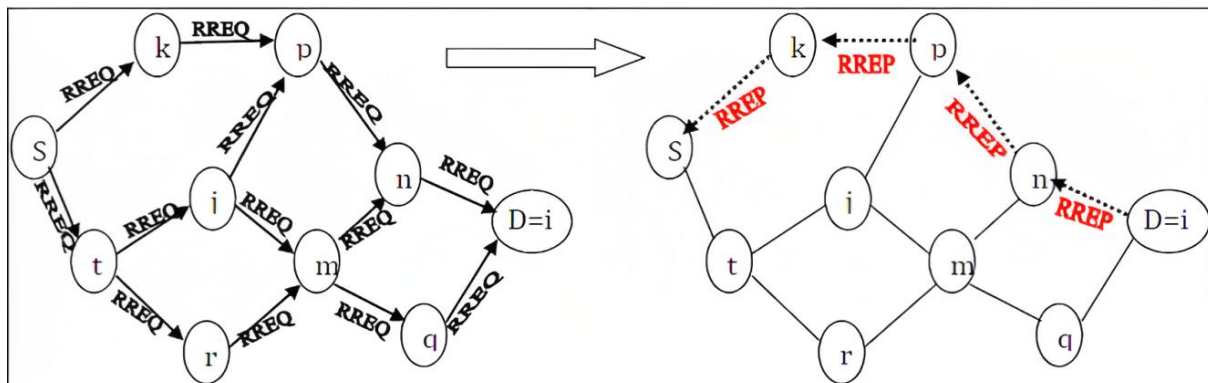


Figure II.6 : Inondation du RREQ et retour du RREP

Avant de l'envoi de paquet, le nœud intermédiaire sauvegarde l'adresse du nœud précédant et celle du nœud source à partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse, qui sera traversé par le paquet réponse de la route de manière unicast (cela veut dire qu'AODV supporte seulement les liens symétriques).

Si la requête atteint le nœud destination, un paquet RREP est construit avec le nouveau numéro de séquence de la destination est suit la route inverse notée dans les tables (voir la Figure II.6). Le champ hop count de message route RREP est incrémenté à chaque nœud traversé, une fois le nœud origine atteint, la valeur du champ hop count représente la distance en nombre de sauts pour aller du nœud source vers le nœud destination. Quand le nœud reçoit une réponse de route, le paquet est examiné, et une entrée pour la route vers la destination est inscrite dans la table de routage si au moins une de ces conditions est satisfaite :

- aucune route vers la destination n'est connue.
- le numéro de séquence pour la destination dans le paquet de réponse est supérieure a la valeur présente dans la table de routage.
- les numéros de séquences sont égaux mais la nouvelle route est plus courte.

Afin de limiter le coût dans le réseau, AODV propose d'étendre la recherche progressivement, initialement, la requête RREQ est diffusée à un nombre de sauts limité. Si la source ne reçoit

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

A chaque nouvelle diffusion, le champ Broadcast ID du paquet RREQ est incrémenté pour identifier une requête de route particulière associée à une adresse source. Si la requête RREQ est rediffusée un certain nombre de fois (RREQ.RETRIES) sans réception de réponse, un message d'erreur est délivré à l'application [46].

II.6.2.3.4. Maintenance des routes

AODV maintient les routes aussi longtemps que celles-ci sont actives, une route est considérée active tant que des paquets des données transitent périodiquement de la source a la destination selon ce chemin. Lorsque la source stoppe d'émettre des paquets des données, le lien expirera et sera effacé des tables de routage des nœuds intermédiaires. Si un lien se rompt lorsqu'une route est active, le lien est considéré défaillant. Les défaillances des liens sont, généralement, dues à la mobilité du réseau ad hoc.

Afin de détecter cette défaillance, AODV utilise les messages de contrôle «HELLO» qui permettent de vérifier la connectivité ou plutôt l'activité des routes. Un nœud détermine l'activité d'une route en écoutant périodiquement les messages « HELLO » transmis par ses voisins. Si pendant un laps de temps, trois messages « HELLO » ne sont pas reçus consécutivement, le nœud considère que le lien -vers ce voisin est cassé. Il envoie un message d'erreur (RERR) à la source et la route devient invalide [45].

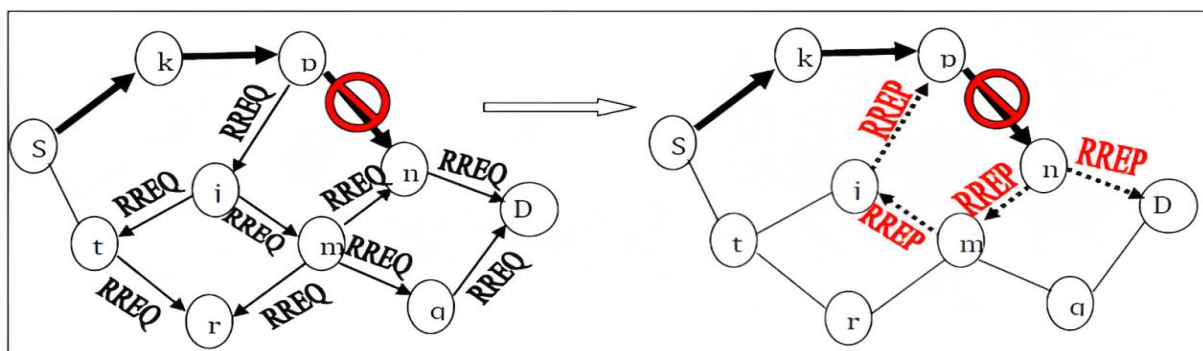


Figure II.7 : Exemple de réparation locale d'une route perdu

II.6.2.3.5. Gestion de la connectivité locale

En fait, lors de la rupture d'un lien d'une route active, AODV tente de réparer la connectivité localement en diffusant une requête de recherche de route dans le voisinage. Si cette tentative échoue, alors la route est supprimée, et nouvelle recherche de route est lancée par la source. [46]

II.6.2.3.5.1. Avantages et inconvénients :

Comme tout autre protocole, AODV a des avantages ainsi qu'il souffre de quelques inconvénients parmi eux on cite quelques-uns :

Avantages

- L'utilisation de numéro de séquence dans les messages qui permet d'éviter les problèmes de boucles innées qui est essentiels au processus de mise à jour de la table de routage
- Rappel sur l'adresse IP du nœud origine dans chaque message qui permet de garder la trace du nœud à l'origine de l'envoi du message

Inconvénients

- Il n'existe pas de format générique des messages. Chaque message a son propre format RREQ, RREP, RERR (surcharge de paquet de contrôle).

II.6.3. Comparaison entre les protocoles (DSDV, AODV, DSR)

DSDV, AODV et DSR sont tous des protocoles de routage utilisés dans les réseaux sans fil Ad Hoc. Voici une brève comparaison de ces protocoles :

- **DSDV**
 - Protocole proactif : établit et maintient les itinéraires à l'avance.
 - Basé sur l'algorithme de vecteur de distance.
 - Utilise des numéros de séquence pour assurer la fraîcheur des routes.
 - Nécessite des mises à jour périodiques pour maintenir les tables de routage.
 - Convient aux réseaux statiques ou à faible mobilité.
 - Enclin aux boucles de routage et à une surcharge de contrôle accrue.

- **AODV**

- Protocole réactif : établit des routes à la demande selon les besoins.
- Utilise des mécanismes de découverte et de maintenance des routes.
- Prend en charge le routage unicast et multicast.
- Utilise des numéros de séquence pour éviter les boucles de routage.
- Convient aux réseaux dynamiques et hautement mobiles.
- Réduction des frais généraux de contrôle par rapport au DSDV.

- **DSR**

- Protocole réactif : découvre et maintient les itinéraires à la demande.
- Utilise le routage source, où la totalité de la route est incluse dans l'en-tête du paquet.
- Favorise la mise en cache des itinéraires pour une réutilisation efficace des itinéraires.
- Prend en charge le routage unicast et multicast.
- Convient aux réseaux hautement dynamiques et mobiles.
- Augmentation de la surcharge due à des tailles de paquets plus importantes.

En résumé, DSDV est proactif, AODV est réactif et DSR est réactif avec le routage source. DSDV convient aux réseaux statiques, tandis qu'AODV et DSR conviennent mieux aux réseaux dynamiques et mobiles. AODV a une surcharge de contrôle inférieure à DSDV, et DSR utilise le routage source avec des tailles de paquet accrues. Le choix du protocole dépend des exigences de mobilité, d'évolutivité et de surcharge du réseau.

II.7. Etat de l'art des solutions pour la sécurité

Plusieurs solutions ont été proposées dans la littérature pour remédier aux problèmes de sécurité et surtout d'assurer les objectifs de la sécurité dans le réseau ad hoc. Une classification des solutions de sécurité proposées est illustrée dans la figure (Fig. II.8) ci-dessous. Pour chaque classe de solutions, nous allons expliquer le principe de base et présenter quelque solution représentative qui récapitule les services de sécurité assurés par les solutions de sécurité présentes. [47]

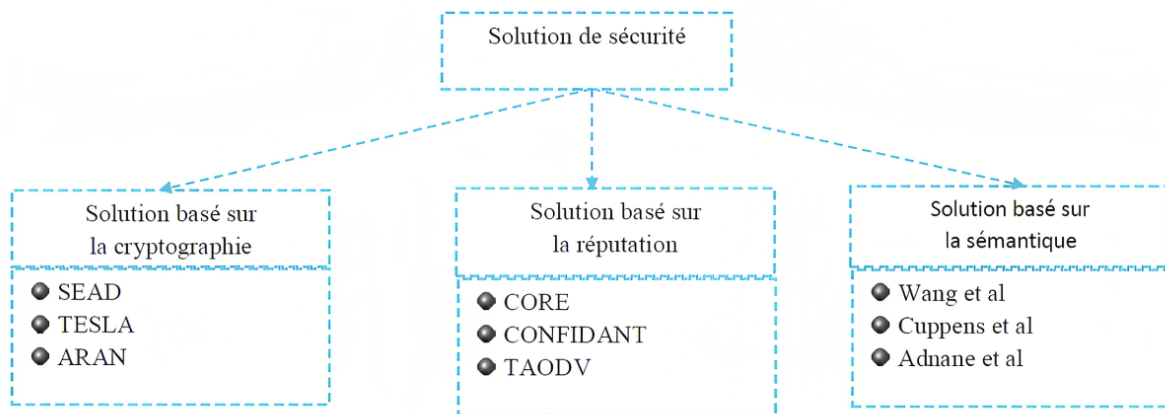


Figure II.8 : Solutions de sécurité

II.7.1. Solution pour l'authentification

Le problème d'authentification dans les réseaux ad hoc est très compliqué à cause de l'absence d'une infrastructure centralisée, d'où la nécessité de concevoir des schémas ou des protocoles qui s'adaptent à ce changement de topologie dans les MANETs. Une première ligne de défense pour contrecarrer ces attaques consiste à assurer les services d'authenticité et d'intégrité des informations qui sont échangées à l'aide de primitives cryptographiques. Plusieurs solutions ont été proposées pour l'authentification, l'inconvénient commun à cette solution est l'utilisation des algorithmes cryptographiques asymétriques (à clé publique) [4]

- **Cryptage symétrique (clé secrète)**

La cryptographie symétrique se base sur l'usage d'une même clé pour chiffrer et déchiffrer des données, ces clés sont appelées des clés symétriques (secrètes) ; très efficace et assez économe en ressources CPU. Cependant la complexité réside dans la mise en place de la même clé entre l'émetteur et le récepteur.

II.7.2. Solution pour la sécurisation du routage

Le mécanisme de cryptographie tel que les cryptographies à clé symétrique, clé publique ou chaîne de hachage sont les plus employés pour assurer un routage sécurisé. Plusieurs objectifs sont mis en œuvre pour sécuriser le routage : [4]

La disponibilité : les routes peuvent être trouvées si elles existent.

L'exactitude : une route en fonction doit au moins exister.

La sureté : la route en fonction ne contient pas d'attaquant.

Efficacité de ressource : les mécanismes de la sécurité de routage doivent être légers.

II.7.3. Solution pour l'intégrité et l'authentification des messages

Les moyens classiques pour assurer l'intégrité et l'authentification des messages échangés par les nœuds d'un réseau sont l'utilisation de signatures numériques ou de MACs (Message Authentication Code). Les signatures numériques s'appuient sur la cryptographie à clé publique. Un nœud possède une clé publique qui sert à ses correspondants pour chiffrer des messages lui étant destinés et le nœud déchiffre les messages qu'il reçoit avec sa clé privée. Dans le cas de la signature, le nœud utilise une clé privée (dédiée à la signature) pour signer un message. Le destinataire du message déchiffre la signature avec la clé publique de l'émetteur et est convaincu que ce dernier est bien l'auteur du message car lui seul connaît sa clé privée. De plus, le message est bien intègre car ne connaissant pas la clé privée de l'émetteur un attaquant ne pourra pas modifier le message original. L'utilisation de la cryptographie asymétrique n'est pas une solution préférée dans les réseaux ad hoc car certains nœuds peuvent avoir des capacités de calcul réduites. Or, la cryptographie asymétrique demande plus de temps de calcul que la cryptographie symétrique.

Une autre solution consiste à utiliser des MACs. Il s'agit de fonctions mathématiques à sens uniques dépendant d'une clé secrète qui, à partir du message original, produisent un condensé de ce message. Ces fonctions mathématiques sont telles qu'il est difficile de retrouver un message à partir de son condensé ou de produire deux messages ayant le même condensé. De plus, la moindre modification du message original entraîne un changement dans le condensé. L'inconvénient de cette solution est qu'il est nécessaire au préalable d'établir autant de clés secrètes que de paires de nœuds susceptibles de vouloir communiquer ensemble. D'autres solutions doivent donc être envisagées pour les réseaux ad hoc.

TESLA (Time Efficient Stream Loss-tolerant Authentication) a été proposé par Perret al. Il s'agit d'une extension au protocole décrit en dit 'Guy Fawkes' protocol. TESLA permet d'authentifier les messages avec un MAC dépendant d'une clé secrète qui n'est divulguée par l'émetteur du message qu'après un délai d'attente. La valeur est calculée de manière à ce qu'on soit sûr que le destinataire a reçu le message avant la divulgation de la clé, cette condition garantit l'intégrité du message. Le temps ne doit pas être trop important pour limiter les latences dans le réseau, en effet un destinataire doit attendre la divulgation de la clé secrète avant de pouvoir électivement traiter un message. [33]

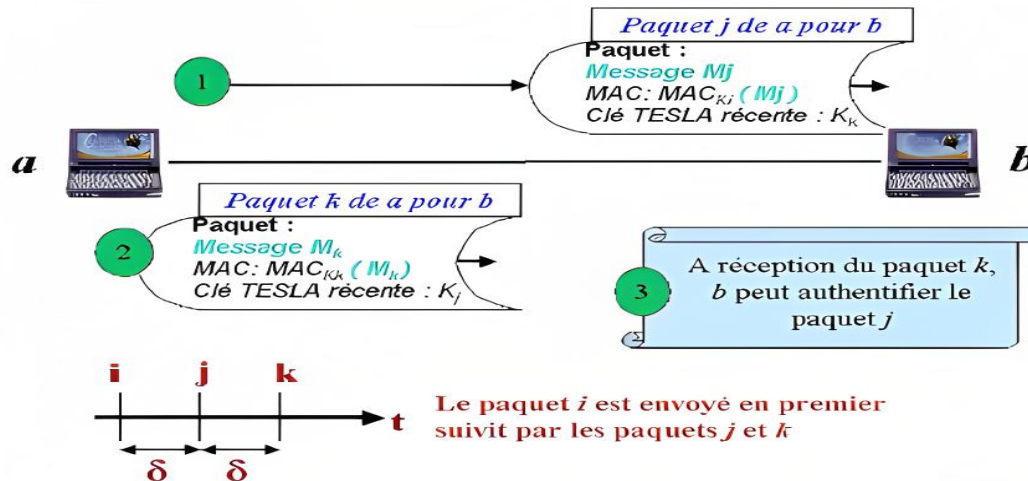


Figure II.9 : Authentification de messages avec TESLA

II.7.4. Solution pour la confidentialité

La confidentialité dans les réseaux ad hoc est d'abord traitée par l'utilisation de transmission par saut de fréquence, frequency hopping. Les données sont transmises sur une séquence de fréquence définie pseudo-aléatoirement. L'attaquant doit connaître cette séquence pour pouvoir se synchroniser en réception. Une fois l'authentification des participants clairement établie, les outils cryptographiques permettent de rendre les communications confidentielles. Toutefois, étant donné qu'une des contraintes des réseaux ad hoc est de devoir être adaptable à des nœuds ayant de faibles capacités de calcul, la cryptographie symétrique sera préférée à la cryptographie à clé publique, cette dernière nécessitant beaucoup plus de puissance de calcul. [4]

II.7.5. Solution pour l'intégrité physique des nœuds

L'intégrité des nœuds du réseau dépend fortement des capacités physiques de ce nœud à résister à des attaques qui permettraient à un attaquant de modifier le fonctionnement du nœud au lieu de le corrompre. Avoir la possibilité de booter sur la disquette ou le CD-ROM d'un PC en libre-service dans un réseau ouvert corrompt fortement l'intégrité de ce nœud. En effet, l'OS (Operating System) du nœud peut alors être échangé par un OS corrompu. L'intégrité physique d'un système informatique, sa résistance, est une propriété très difficile à mettre en œuvre par les fabricants. Un moyen de contourner ce problème peut se faire en mettant en place des fonctions permettant de mettre en évidence une attaque physique sur un élément. Une telle

fonction peut être comparée à un sceau assurant l'inviolabilité d'un courrier. Elle met en œuvre des notions de traçabilité de l'attaque. [33]

II.7.6. Solution pour la disponibilité

Il n'existe aucun moyen de contrer un déni de service sur le canal radio provoqué par un attaquant puissant ayant les moyens de brouiller efficacement la totalité du spectre radio. Néanmoins, des techniques comme le saut de fréquence permettent de se prémunir contre des attaquants ayant des capacités plus réduites.

En émet, ces techniques permettent une transmission des données sur un large spectre de fréquence. Pour être efficace un attaquant doit donc être capable de brouiller l'étendue des fréquences utilisées. [4]

II.8. Conclusion

Le routage et la sécurité sont des éléments clés pour assurer le bon fonctionnement des réseaux Ad-hoc et pour protéger les données sensibles qui y circulent. Les attaquants cherchent toujours à exploiter les vulnérabilités des réseaux Ad-Hoc pour perturber les communications, voler des informations confidentielles ou causer des dommages. Les mécanismes de routage adaptatifs et les protocoles de sécurité sont des moyens importants pour renforcer la sécurité des réseaux ad hoc. Cependant, il est important de continuer à améliorer ces mécanismes pour rester à jour avec les nouvelles menaces et vulnérabilités.

En somme, les réseaux Ad-Hoc sont de plus en plus utilisés dans des environnements divers et variés, et la sécurité de ces réseaux doit être prise en compte pour assurer leur fiabilité et leur utilité. Il est donc essentiel de poursuivre la recherche et le développement pour renforcer la sécurité de ces réseaux et permettre leur utilisation en toute confiance dans de nombreux contextes.

Chapitre III

Tests et résultats de simulation

III.1. Introduction

Nous intéressons dans ce chapitre au protocole de routage DSDV et à son comportement face à une attaque de type "Wormhole".

L'attaque de trou ver "Wormhole" constitue une menace sérieuse dans les réseaux "Wormhole" où les attaquants capturent et transmettent rapidement les paquets entre deux points distants du réseau, créant ainsi un raccourci artificiel. Cette attaque peut induire en erreur les protocoles de routage, y compris DSDV, en manipulant les informations de routage et entraînant des résultats indésirables ce qui nous permet de mieux comprendre les vulnérabilités potentielles et les contre-mesures à prendre pour renforcer la sécurité du protocole DSDV dans des environnements Ad- Hoc confrontés à l'attaque de trou ver "Wormhole".

III.2. Attaque de WormHole

Une attaque de type "Wormhole" est un type d'attaque de sécurité qui peut affecter les protocoles de réseau sans fil (les réseaux Ad- Hoc) avec exploite la vulnérabilité de l'infrastructure de communication du réseau, où les nœuds malveillants créent un tunnel direct entre deux points distants dans le réseau, contournant ainsi les nœuds intermédiaires. Cette attaque permet aux attaquants de tromper les autres nœuds en faisant croire qu'ils sont à proximité, ce qui peut perturber le routage et causer des problèmes de sécurité.

III.3. Protocole de routage DSDV

Le protocole DSDV est un protocole de routage utilisé dans les réseaux ad hoc. Il utilise des vecteurs de distance pour déterminer les itinéraires les plus courts vers les destinations et met à jour ces itinéraires en fonction des informations de séquence.

III.4. Identification du problème

Le protocole DSDV est un protocole de routage utilisé dans les réseaux ad hoc. Il utilise des vecteurs de distance pour déterminer les itinéraires les plus courts vers les destinations et met à jour ces itinéraires en fonction des informations de séquence. Une attaque de type wormhole est une forme d'attaque dans les réseaux ad hoc où les nœuds malveillants créent un tunnel direct entre deux points distants dans le réseau, contournant ainsi les nœuds intermédiaires. Cette attaque permet aux attaquants de tromper les autres nœuds en faisant croire qu'ils sont à proximité, ce qui peut perturber le routage et causer des problèmes de sécurité dans le cas du protocole DSDV, une attaque wormhole peut compromettre le routage

en créant un raccourci artificiel entre deux nœuds éloignés. Les nœuds du réseau pourraient alors choisir cette route plus courte, même si elle n'est pas la meilleure option en termes de distance réelle ou de performance. Ceci conduit à entraîner des problèmes tels que des boucles de routage, des retards de transmission ou une dégradation globale des performances.

En résumé, la principale problématique entre le protocole DSDV et une attaque wormhole est que cette attaque peut fausser les informations de routage et conduire à des décisions de routage inefficaces ou inappropriées, affectant ainsi la fiabilité et les performances globales du réseau ad-hoc.

III.5. Présentation de NS2

Network simulateur version 2 est un logiciel de simulateur de réseaux orienté objet à événements à temps discrets, et qu'il est totalement open source. NS-2 permet à l'utilisateur de définir un réseau et de simuler les communications entre les nœuds. Le simulateur utilise le langage orienté objet OTcl2 pour la description des conditions de simulation sous forme de script.

L'application NS se compose de deux éléments fonctionnels: un interpréteur et un moteur de simulation. Au moyen de l'interpréteur l'utilisateur est capable de créer le modèle de simulation ce qui revient à assembler les différents composants nécessaires à l'étude. Les composants du modèle de simulation sont appelés objets ou encore instances de classe. Le moteur de simulation effectue les calculs applicables au modèle préalablement construit par l'utilisateur via l'interpréteur [48]

III.5.1. Les différences outils de NS2

NS est un outil logiciel de simulation de réseaux informatiques. Il est principalement bâti avec les idées de la conception par objets, de réutilisation du code et de modularité. Il est devenu aujourd'hui un standard de référence en ce domaine. C'est un logiciel dans le domaine public disponible sur l'Internet. Son utilisation est gratuite. Le logiciel est exécutable tant sous Unix que sous Windows. Ce logiciel permet la description et la simulation de réseaux IP. Le réseau est représenté (modélisé) par ses sources de trafic (applications), ses protocoles (UDP, TCP), ses routeurs (avec leurs files d'attente) et les liens qui les relient. Le réseau est ensuite simulé, ce qui produit des traces et des statistiques. Des outils périphériques permettent l'animation (Nam) ou la conversion vers d'autres outils (xgraph). L'utilisateur décrit le modèle de son réseau, c'est-à-dire les éléments qui le constituent, dans le langage Otcl (une extension objet du langage tcl). Ce fichier est ensuite passé au simulateur

proprement dit. A travers ce langage, l'utilisateur décrit les conditions de la simulation : la topologie du réseau, les caractéristiques des liens physique, les protocoles utilisés, les communications qui ont lieu. La simulation doit d'abord être saisie sous forme de fichier texte que NS va utiliser pour produire un fichier trace contenant les résultats. Ensuite, on utilise le programme NAM pour interpréter ces données et en donner un rendu graphique. Mais l'utilisation de l'OTcl permet aussi à l'utilisateur de créer ses propres procédures (par exemple s'il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps). L'outil final que nous avons utilisé est xgraph, un programme de traçage pour le but de créer la représentation graphique du résultat de simulation. Dans nos expériences nous avons trace les performances des réseaux fils et sans fil [49]

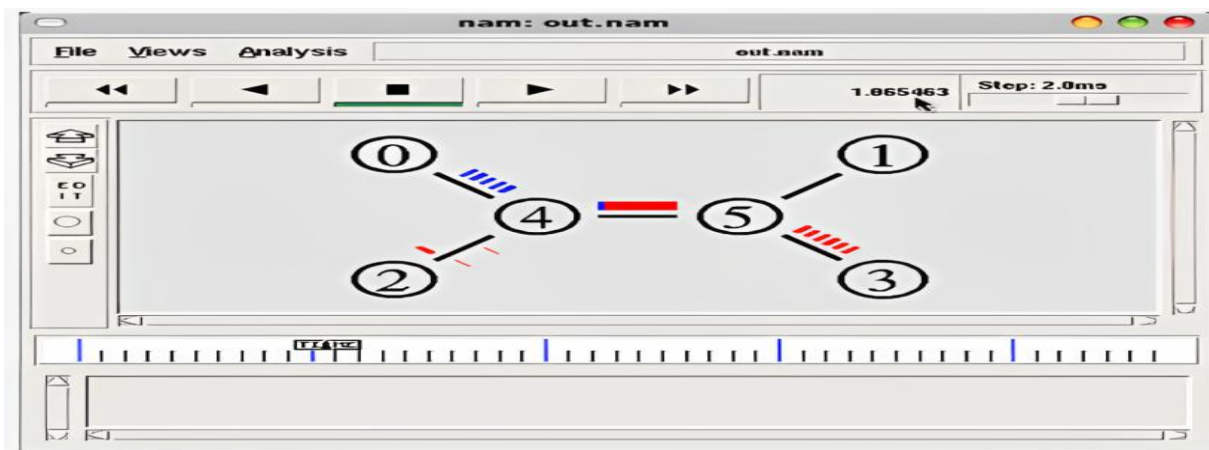


Figure III.1 : un simulateur de réseau de 2 générations

III.5.2. Choix du simulateur ns-2

- **Avantage**
 - Ne nécessite pas d'équipement coûteux
 - Les résultats peuvent être obtenus rapidement - plus d'idées peuvent être testées dans un laps de temps plus court.
 - Protocoles pris en charge
 - Plateformes supportées
 - Modularité
 - Populaire

- **Inconvénients**
 - Les bogues ne sont pas fiables
 - Scénario de trafic pour réseau filaire et sans fil [50]

III.5.3. Modèle de simulation

Un réseau modèle sous NS comprend les éléments suivants :

Des nœuds de réseau : des endroits où le trafic est généré, ou des nœuds de routage.

Des liaisons de communication entre les réseaux.

Des agents de communication représentant les protocoles de niveau transport tels que TCP et UDP. Ces agents sont attachés aux nœuds et sont interconnectés pour permettre l'échange de données (connexion TCP, flux UDP).

Des applications qui génèrent le trafic de données selon certaines lois (CBR, VBR) et qui utilisent les agents de transport. [51] [52]

La figure III.2 illustre l'architecture simulation du NS2 :

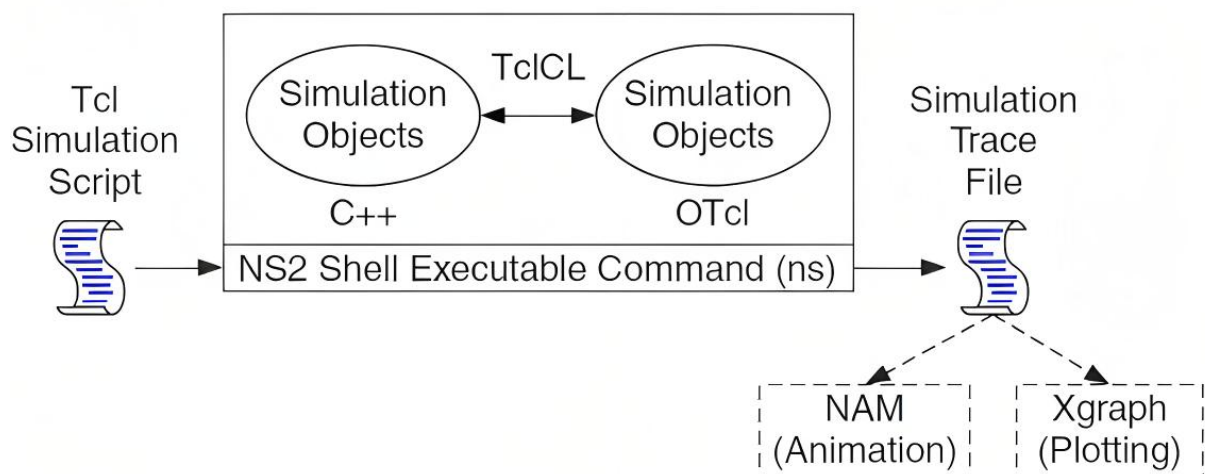


Figure III.2 :L'architecture simulation du NS2

III.5.4. Installation du simulateur NS2

Pour installer le logiciel NS-2.35 nous il devrait d'abord installer UBUNTU-16.04.7-desktop-amd64 et virtualbox-6.1.14-140239-win, Après nous pouvons suivre les prochaines étapes :

Téléchargement de NS-2.35 : nous pouvons télécharger les fichiers d'installation de NS-2.35 à partir du site officiel ou d'un dépôt fiable. Assurez-vous de télécharger les fichiers correspondant à notre système d'exploitation.

- Prérequis : NS-2.35 nécessite quelques dépendances et bibliothèques pour fonctionner correctement. Assurez-vous d'installer les prérequis nécessaires. Les prérequis courants incluent Tcl/Tk, Xgraph, et les compilateurs C++.
- Extraction des fichiers : Une fois le téléchargement terminé, extrayez les fichiers du package NS-2.35 dans un répertoire de votre choix.
- Configuration : Accédez au répertoire NS-2.35 dans le terminal ou l'invite de commande et exécutez la commande « ./config ». Cela configurera NS-2.35 en fonction de votre système.
- Compiler : après une configuration réussie, exécutez la commande "make" pour l'Assemblage du NS-2.35. Cette étape peut prendre un certain temps.
- Installer : Une fois la compilation terminée, lancez la commande 'make install' pour installer NS-2.35 sur votre système.
- Vérifier l'installation : Pour vérifier que NS-2.35 est correctement installé, exécutez la commande "ns" dans le terminal ou l'invite de commande. Cela devrait exécuter le traducteur Tcl/Tk avec NS-2.35.
- Ces étapes nous permettront d'installer NS-2.35 sur votre système. Notez que NS-2.35 est une version assez ancienne, et il peut être intéressant de parcourir les anciennes versions dernières alternatives ou alternatives selon vos besoins..

III.6. La configuration des nœuds

configure the nodes

```
$ns node-config -adhocRouting $Val (rp) \  
-llType $Val (ll) \  
-macType $Val (mac) \  
-ifqType $Val (ifq) \  
-ifqLen $Val (ifqlen) \  
-antType $Val (ant) \  
-propType $Val (prop) \  
-phyType $Val (netif) \  
-channelType $Val (chan) \  
-topoInstance $topo \  
-agentTrace ON \  

```

```
-routerTrace ON \
-macTrace OFF \
-movement Trace ON
```

```
For {set i 0} {$i < $Val (nn)} {incr i} {
```

```
Set node_ ($i) [$ns node]
```

- **Création du fichier de traces NS-2**

```
Set tracefd [open simple-dsdv.tr w]
```

```
Set windowVsTime2 [open win.tr w]
```

```
Set namtrace [open simwrls.nam w]
```

- **Coloration des classes**

```
#node 0 is give GREEN color and a label- acts as a source node
```

```
$node_ (0) color green
```

```
$ns at 0.0 "$node_ (0) color green"
```

```
$ns at 0.0 "$node_ (0) label source"
```

```
#node 1 is give GREEN color and a label- acts as a Destination node
```

```
$node_ (1) color green
```

```
$ns at 0.0 "$node_ (1) color green"
```

```
$ns at 0.0 "$node_(1) label Destination"
```

- **Procédure de fin de simulation**

```
# ending nam and the simulation
```

```
$ns at $Val (stop) "$ns nam-end-wireless $Val (stop)"
```

```
$ns at $Val (stop) "stop"
```

```
$ns at 150.01 "puts \"end simulation\>>"; $ns halt"
```

```
Proc stop {} {
```

```
Global ns tracefd namtrace
```

```
$ns flush-trace
```

```
Close $tracefd
```

```
Close $namtrace
```

```
Exec nam simwrls.nam &
```

```
}
```

- **Création des nœuds**

```
# Provide initial location of mobilenodes
```

```
$node_ (0) set X_ 36.0
```

```
$node_ (0) set Y_ 204.0
```

```
$node_ (0) set Z_ 0.0
```

```
$node_ (1) set X_ 476.0
```

```
$node_ (1) set Y_ 120.0
```

```
$node_ (1) set Z_ 0.0
```

```
$node_ (2) set X_ 241.0
```

```
$node_ (2) set Y_ 328.0
```

```
$node_ (2) set Z_ 0.0
```

```
:::: :: ::
```

```
:::: :: ::
```

```
$node_ (29) set X_ 268.0
```

```
$node_ (29) set Y_ 60.0
```

```
$node_ (29) set Z_ 0.0
```

III.7. Spécification de l'attaque par trou de ver dans DSDV

Une attaque par trou de ver (wormhole attack) dans le protocole DSDV implique la création d'un tunnel virtuel entre deux nœuds malveillants, contournant ainsi les nœuds intermédiaires. Voici les spécifications générales de cette attaque :

Capture des paquets : Les nœuds malveillants dans l'attaque par trou de ver captent les paquets échangés entre deux nœuds légitimes de manière rapide et efficace. Ils transmettent ensuite ces paquets à travers le tunnel virtuel vers un autre nœud malveillant, créant ainsi une communication directe entre les deux extrémités du tunnel.

Temps de propagation réduit : Le tunnel créé par les nœuds malveillants dans l'attaque par trou de ver a un temps de propagation extrêmement court, ce qui donne l'impression aux autres nœuds du réseau qu'il s'agit d'une connexion directe et courte. Les nœuds légitimes peuvent donc être trompés en utilisant ce tunnel comme route préférentielle pour acheminer leurs paquets.

Annonce trompeuse des routes : Les nœuds malveillants diffusent des informations de routage trompeuses dans le réseau, indiquant que le tunnel du trou de ver est la route la plus courte ou la plus efficace vers certaines destinations. Cela incite les nœuds légitimes à sélectionner cette route altérée au lieu de suivre les mécanismes de routage normaux du protocole DSDV.

Altération des séquences de destination : Les nœuds malveillants peuvent également altérer les numéros de séquence de destination dans les paquets capturés et transmis à travers le tunnel du trou de ver. Cela peut fausser davantage les informations de routage et provoquer des incohérences dans les tables de routage des nœuds légitimes.

En combinant ces techniques, les attaquants peuvent tromper les nœuds légitimes en leur faisant croire qu'ils ont une route plus courte ou plus fiable, ce qui peut entraîner des boucles de routage, des retards de transmission et une dégradation des performances globales du réseau dans le protocole DSDV. [53]

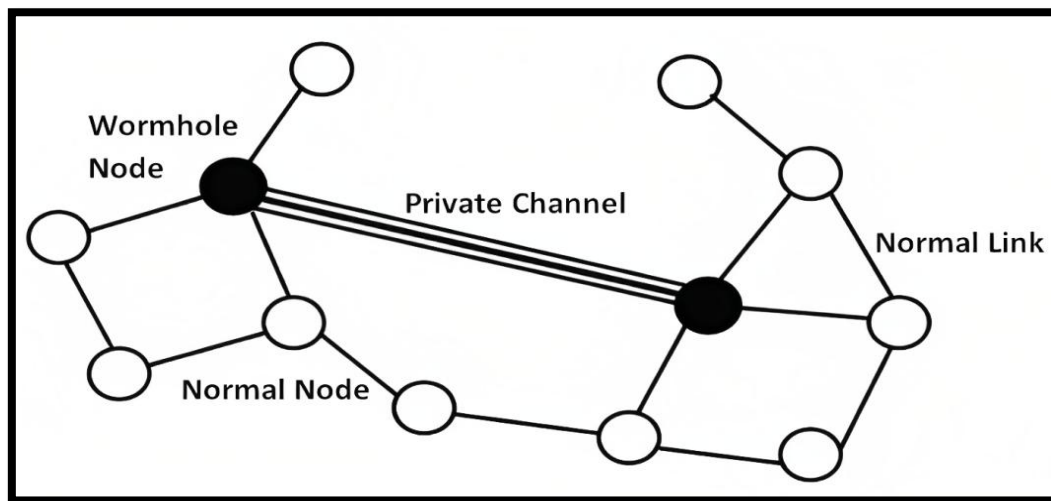


Figure III.3 : attaque wormhole dans DSDV

III.7.1. L'implémentation d'un nœud malicieux

L'implémentation d'un nœud malveillant dans le protocole DSDV attaqué par un wormhole peut être réalisée de la manière suivante :

- Capture de paquets : Le nœud malveillant doit être capable de capturer les paquets échangés entre les nœuds légitimes du réseau. Cela peut être réalisé à l'aide de dispositifs de capture de paquets ou en modifiant le firmware du nœud pour intercepter les paquets.
- Création d'un tunnel virtuel : Une fois les paquets capturés, le nœud malveillant doit créer un tunnel virtuel avec un autre nœud malveillant distant. Cela peut être réalisé en utilisant des techniques telles que l'injection directe des paquets capturés dans le canal

de communication entre les nœuds malveillants ou en utilisant des dispositifs de transmission sans fil à haute puissance pour établir une communication directe.

- Transmission des paquets : Les paquets capturés doivent être transmis rapidement à travers le tunnel virtuel vers le nœud malveillant distant. Cela peut être effectué en utilisant des dispositifs de transmission à haute vitesse ou en utilisant des protocoles de communication spécifiques pour garantir une transmission rapide et fiable des paquets
- Annonce trompeuse de routes : Les nœuds malveillants doivent diffuser des informations de routage trompeuses dans le réseau afin d'inciter les nœuds légitimes à sélectionner le tunnel du wormhole comme route préférentielle. Cela peut être réalisé en modifiant les métriques de coût des routes annoncées, en falsifiant les numéros de séquence ou en utilisant d'autres techniques de manipulation des informations de routage.
- Dissimulation du nœud malveillant : Le nœud malveillant doit également essayer de se dissimuler et d'éviter d'être détecté par les autres nœuds du réseau. Cela peut être réalisé en utilisant des techniques de camouflage d'adresse IP, en évitant de répondre aux requêtes de découverte de voisins ou en utilisant des méthodes d'atténuation des contre-mesures de sécurité mises en place dans le protocole DSDV. [54]

La figure III.4 fichier dépendants de DSDV.tcl [55]

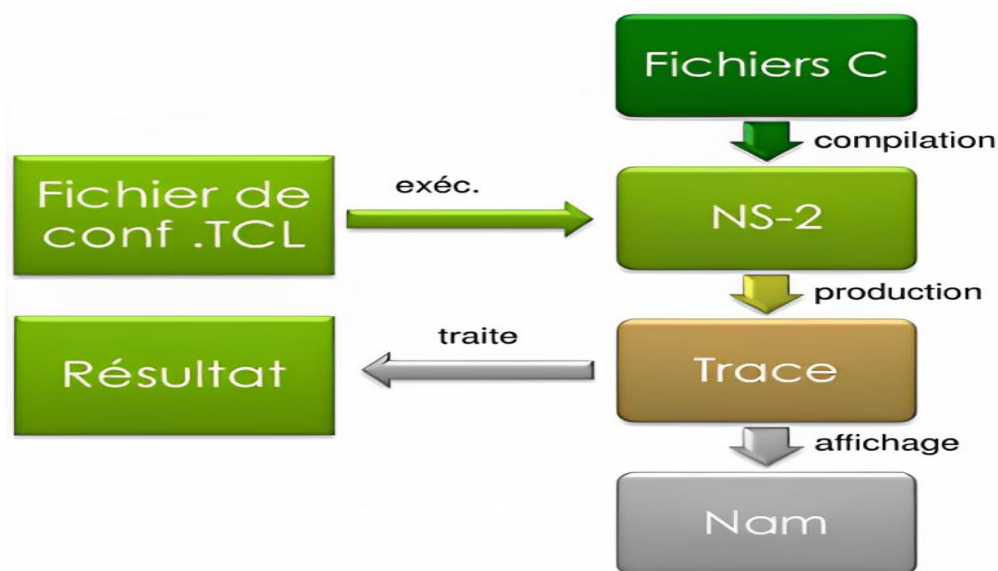


Figure III.4 : fichier dépendants de DSDV.tcl

III.7.2. Modifications du fichier DSDV.tcl

Dans notre cas, nous devons ajouter un nœud malveillant appartenant à trou ver attaque dans le protocole DSDV et le marquer pour remarquer les changements qui se sont produits, et c'est en modifiant le fichier < **DSDV.tcl** > et nous passons ainsi au fichier <**wormhole.tcl**>.

```
# [$node_ (12) set ll_ (0)] wormhole-peer [$node_ (12) set ll_ (0)]
# [$node_ (16) set ll_ (0)] wormhole-peer [$node_ (16) set ll_ (0)]

# set a TCP connection between node_ (12) and node_ (16)
Set tcp [new Agent/TCP/Newreno]
$tcp set class_ 2
Set sink [new Agent/TCPSink]
$ns attach-agent $node_ (12) $tcp
$ns attach-agent $node_ (16) $sink
$ns connect $tcp $sink
Set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns at 19.0 "$ftp start"
```

III.7.3. Les modifications pour la sécurité

Dans l'étape de sécurité, nous apportons les modifications suivantes au fichier wormhole.tcl, et nous passons ainsi au fichier < **ips.tcl** >.

```
# set the packet loss threshold for the alert

Set lossThreshold 0.1

# Function to check for packet loss and raise alert if threshold exceeded

Proc checkPacketLoss {

{Global ns lossMonitor lossThreshold

Set packetsSent [$lossMonitor set packets_sent_]

Set packetsLost [$lossMonitor set packets_lost_]


```

```

    Set lossPercentage [expr {$packetsLost / $packetsSent}] if {$lossPercentage >
$lossThreshold} {

    Puts "ALERT: Packet loss exceeded the threshold! Loss Percentage: $lossPercentage"

# Additional actions to be taken when the alert is triggered

# ...

}

}

#node 12 and 16 is grive RED color and a label- acts as a malicious node
$node_ (12) color red
$ns at 40.0 "$node_ (12) color red"
$ns at 40.0 "$node_ (12) label malicious"
$node_ (16) color red
$ns at 40.0 "$node_ (16) color red"
$ns at 40.0 "$node_ (16) label malicious"

#Remove malicious nodes from the simulation
$ns at 67.0 "$node_ (12) reset" ; #Remove node_ (12) from the simulation
$ns at 67.0 "$node_ (16) reset" ; #Remove node_ (16) from the simulation

```

III.8. Les Scènes de simulation

- **Scénario 1** : Ce scénario vise à simuler le protocole de bus de distance série de destination sans présence de nœud d'attaque de trou de ver.
- **Scénario 2** : Dans ce cas, deux nœuds d'attaque de trou de ver sont insérés entre des nœuds du réseau ad-hoc utilisant le protocole DSDV. Nous étudierons leur comportement en observant leur influence sur le réseau.
- **Scénario 3** : est un scénario de test de la sécurité (solution de problème) pour le montrer que l'IPS élimine l'effet du wormhole.

III.8.1. Les paramètres de simulation

Pour une étude de faisabilité de l'attaque wormhole, nous avons étudié un outil de simulation

NS-2 selon les critères suivants :

Paramètre	Définition
type de canal	Channel / wireless channel
Modèle de radio-propagation	Propagation / tworayground
Type d'interface réseau	Phy/wirelessphy
Type de Mac	IEEE 802.11
Type de file d'attente d'interface	Queue / DropTail
type de couche de liaison	LL
modèle d'antenne	Antenna / omniantenna
paquet max dans ifq	100
nombre de nœuds mobiles	30
protocole de routage	DSDV
dimension x de la topographie	500
dimension y de la topographie	400
heure de fin de la simulation	150
Nombre d'attaquants internes	1 ; 2
Version NS-2	NS-2.35 patché
Type de trafic	FTP

Tableau III.1 : Le tableau de routage de Protocol DSDV

III.8.2. La simulation en utilisant le logiciel NS-2

III.8.2.1. DSDV en action

Lorsqu'un nœud veut envoyer des données vers une destination, il consulte sa table de routage pour déterminer le prochain saut vers la destination. La table de routage comprend des informations sur le nombre de sauts pour atteindre la destination et le numéro de séquence, qui

est utilisé pour suivre la fraîcheur de la route. Le numéro de série est incrémenté chaque fois qu'un changement de chemin se produit.

Voici un aperçu étape par étape du fonctionnement pratique de DSDV :

III.8.2.1.1 Recherche des pistes

La photo III.5 représente une simulation du protocole DSDV dans logiciel NS-2 avec 30 nœuds :

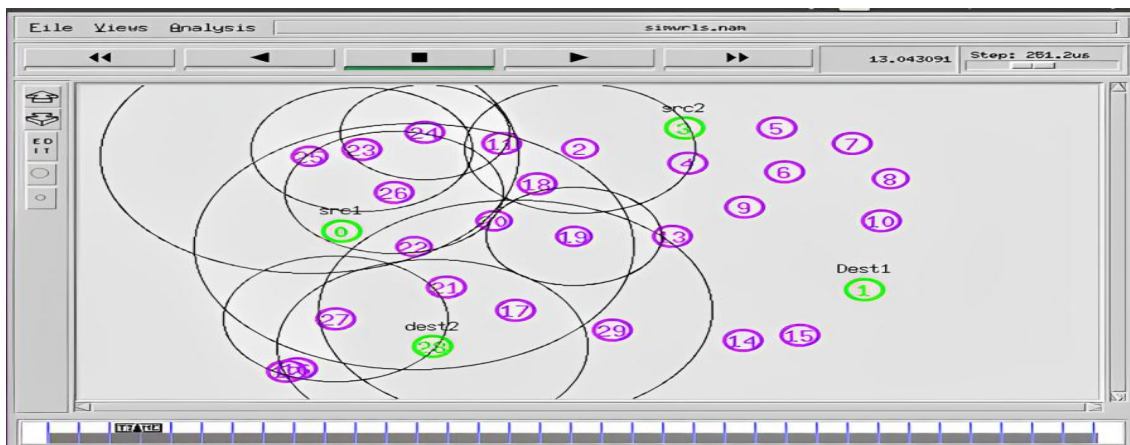


Figure III.5 : DSDV simulation on NS-2.35

II.8.2.1.2. Trouver le chemin et envoyer les paquets :

La photo III.6 représente le début de la simulation avec l'adoption de deux émetteurs et deux récepteurs :

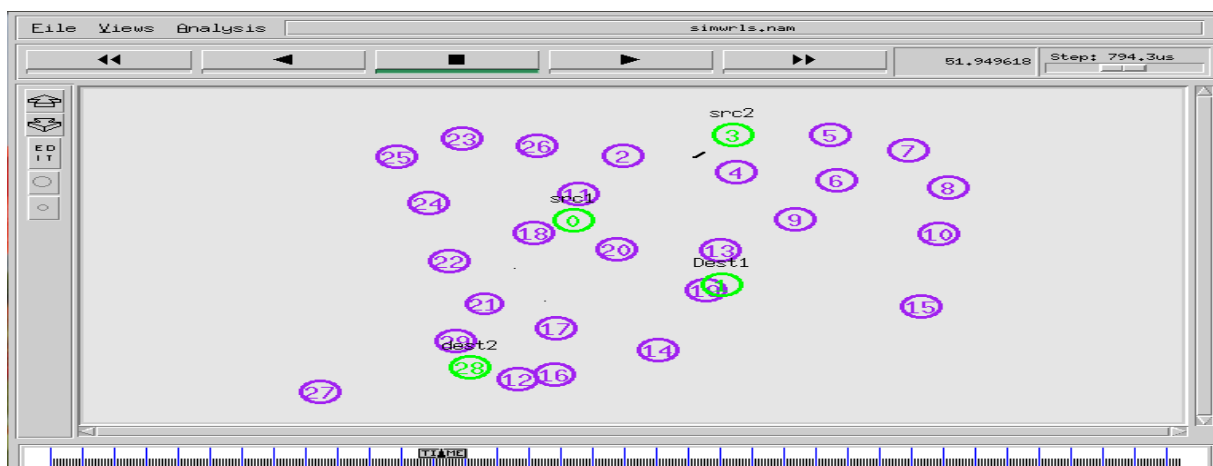


Figure III.6 : Protocole DSDV avec deux sources et deux récepteurs

Dans cette simulation simple, sans la menace d'un trou de ver, DSDV recherche les chemins les plus récents et les plus fiables en publiant des mises à jour en continu, en recherchant un

chemin de numéro de série long avec un court chemin, et tous les protocoles essaie de livrer des colis en un temps record.

III.8.2.2. WormHole action

III.8.2.2.1. Avant le début du trou de ver

Le nœud source cherche un chemin, et envoie un message RREQ sur le réseau

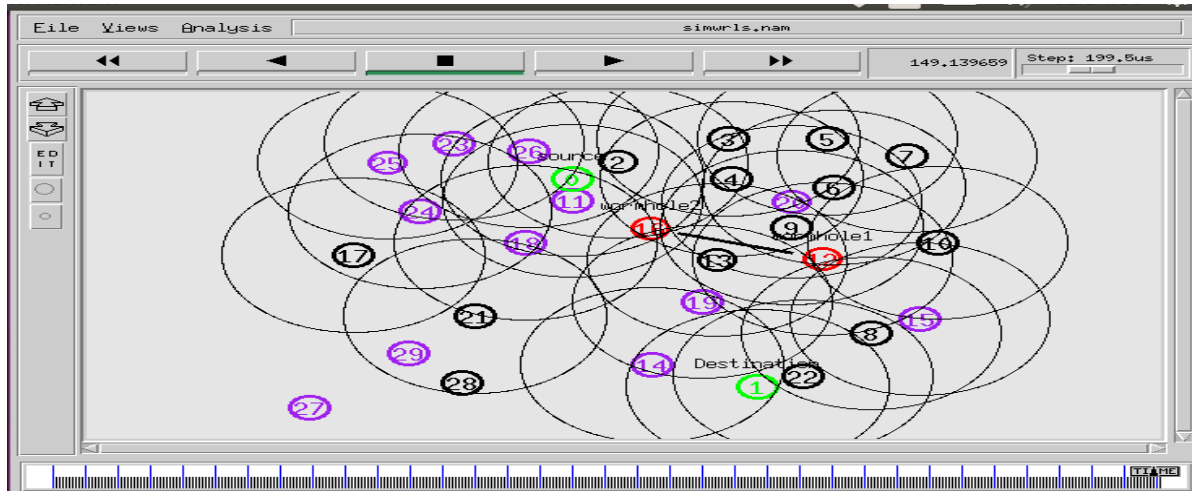


Figure III.7 : Recherche du nœud source en envoyant des paquets au nœud récepteur

III.8.2.2.1. Après le début du trou de ver

Le photo III.8 montre un nœud de trou de ver avant qu'il ne commence à fonctionner :

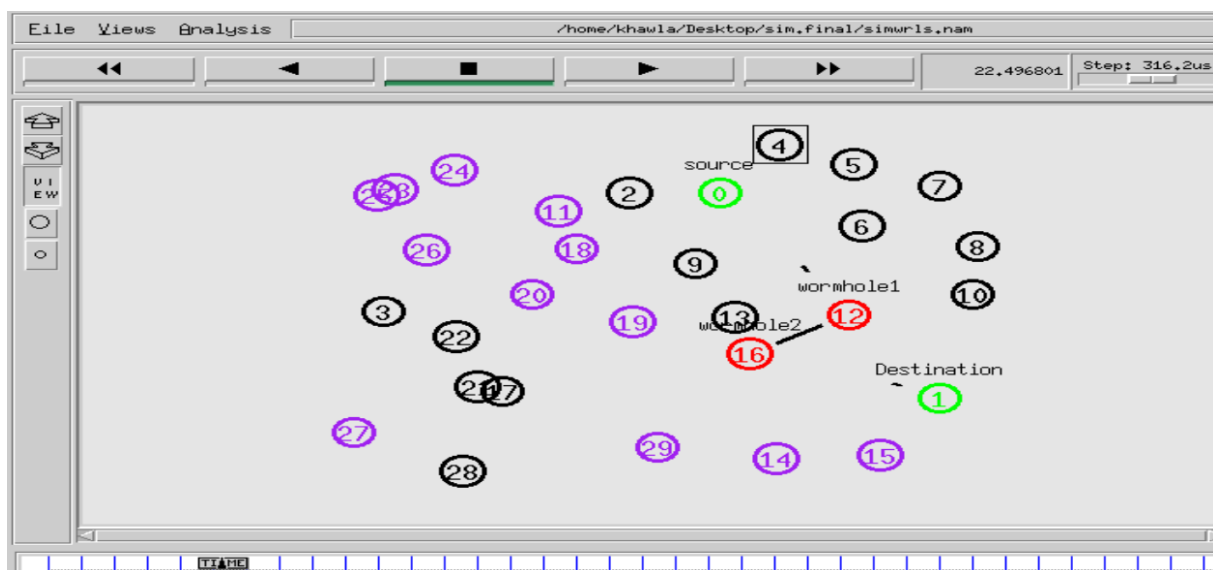


Figure III.8 : Un nœud avec un trou de ver

Lorsque le nœud source recherche un chemin, il envoie un message RREQ sur le réseau. Immédiatement, les deux nœuds de trou de ver répondent et envoient un message RREP à la source, afin que ce soit celle qui remplisse toutes les conditions requises. La source commence à envoyer des paquets au nœud de trou de ver, il les analyse, en prend une copie pour les utiliser à ses fins, puis les renvoie au récepteur. Dans ce scénario, les nœuds sont 12 et 16 les nœuds de trou de ver qui suce les paquets.

III.8.2.3. Traiter IPS sur WormHole

Nouveaux protocoles (IPSDSDV)

Le protocole IPSDSDV est un protocole de routage ad hoc sécurisé et adaptatif qui vise à fournir des communications fiables et sécurisées dans les réseaux ad hoc. Il utilise une approche de routage basée sur la source dynamique, ce qui signifie que chaque nœud du réseau peut agir en tant que routeur pour transmettre les paquets de données. Le protocole IPSDSDV intègre également des mécanismes de sécurité pour protéger les échanges de données contre les attaques malveillantes. Voici quelques fonctionnalités principales du protocole IPSDSDV :

- **Routage dynamique** : Le protocole permet aux nœuds de découvrir et de maintenir des informations sur les routes disponibles vers les destinations souhaitées. Les routes sont déterminées en fonction de la source dynamique, ce qui signifie que chaque nœud peut prendre le rôle de routeur pour transmettre les paquets de données vers leur destination.
- **Adaptabilité** : Le protocole est capable de s'adapter aux changements de topologie du réseau, tels que les mouvements des nœuds et les déconnexions temporaires. Il met à jour dynamiquement les informations de routage pour tenir compte de ces changements, assurant ainsi une connectivité continue.
- **Sécurité** : Le protocole IPSDSDV intègre des mécanismes de sécurité pour protéger les échanges de données contre les attaques malveillantes. Il peut inclure des techniques telles que le cryptage des données, l'authentification des nœuds et la détection d'intrusion pour garantir la confidentialité et l'intégrité des communications.
- Il adapte ses mécanismes de routage pour minimiser les délais de transmission et améliorer les performances globales du réseau.

III.8.2.4. IPS

Pour détecter, prévenir et bloquer les attaques de trous de ver internes au réseau, nous utilisons des solutions IPS, que le protocole DSDV n'a pas pu détecter malgré son efficacité

dans d'autres crises, mais pour les topologies d'attaques malveillantes qui ont trompé le système, Le système a besoin de plus de protection car il surveille en permanence le trafic réseau pour détecter les activités malveillantes entrant sur le réseau en fonction des paquets appartenant au réseau (wormhole) à l'aide de signatures,, de modèles de comportement et d'algorithmes d'analyse spécifiques ..

III.8.2.4.1. Surveillance routière

La photo III.9 représente le protocole IPSDSDV au début des travaux :

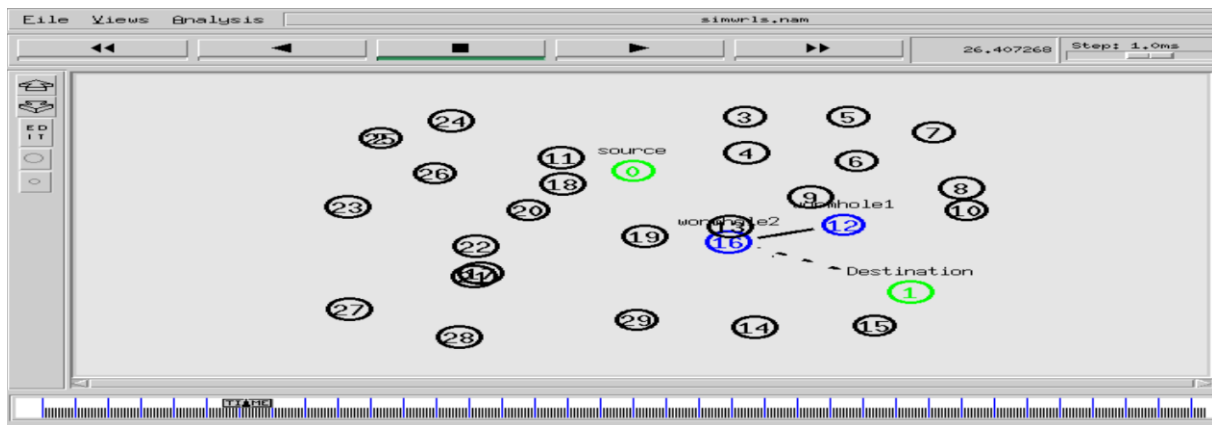


Figure III.9 : Protocole IPSDSDV en début de chantier

Au début de son travail, l'IPS surveille en permanence le trafic réseau et analyse les paquets de données au fur et à mesure qu'ils circulent pour détecter toute menace en analysant les modèles de trafic et en recherchant tout comportement anormal indiquant des attaques potentielles.

III.8.2.4.2. Alerter le système d'une menace

La photo III.10 montre l'état du système lorsqu'il est alerté par une menace Wormhole :

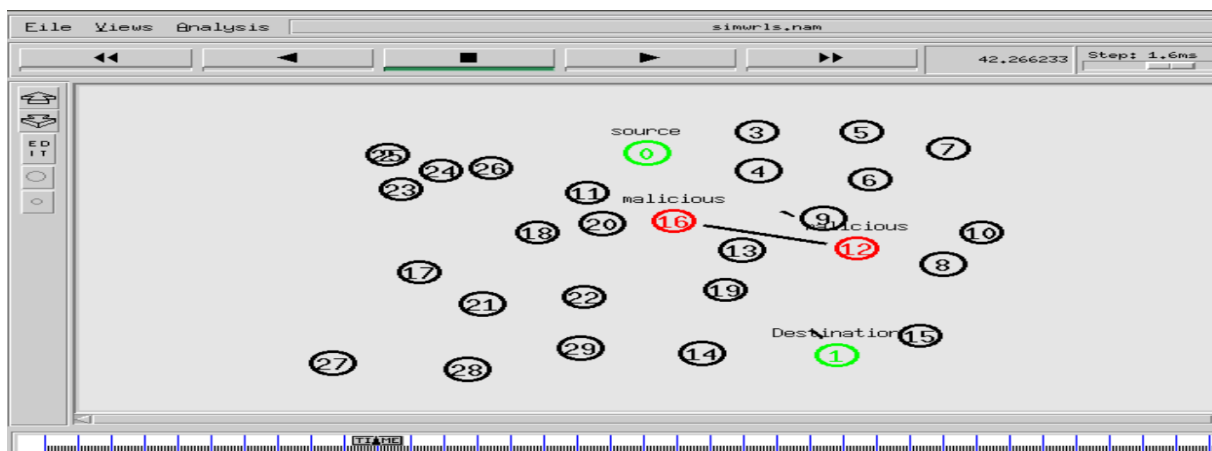


Figure III.10 : Détecte et alerte le système de la menace d'une attaque par trou de ver

Quand IPS détecte l'attaque, il effectue une inspection approfondie des paquets et une analyse comportementale pour déterminer la nature de la menace. Il génère des alertes pour informer les administrateurs réseau de l'existence de la menace de trou de ver, tout en identifiant les paquets affectés. Ainsi, le protocole DSDV change la couleur des paquets (rouge) affectés pour les distinguer les uns des autres

.III.8.2.4.3. Elimination de la menace

L'image suivante montre la réponse de L'IPS immédiate et élimine les paquets malveillants :

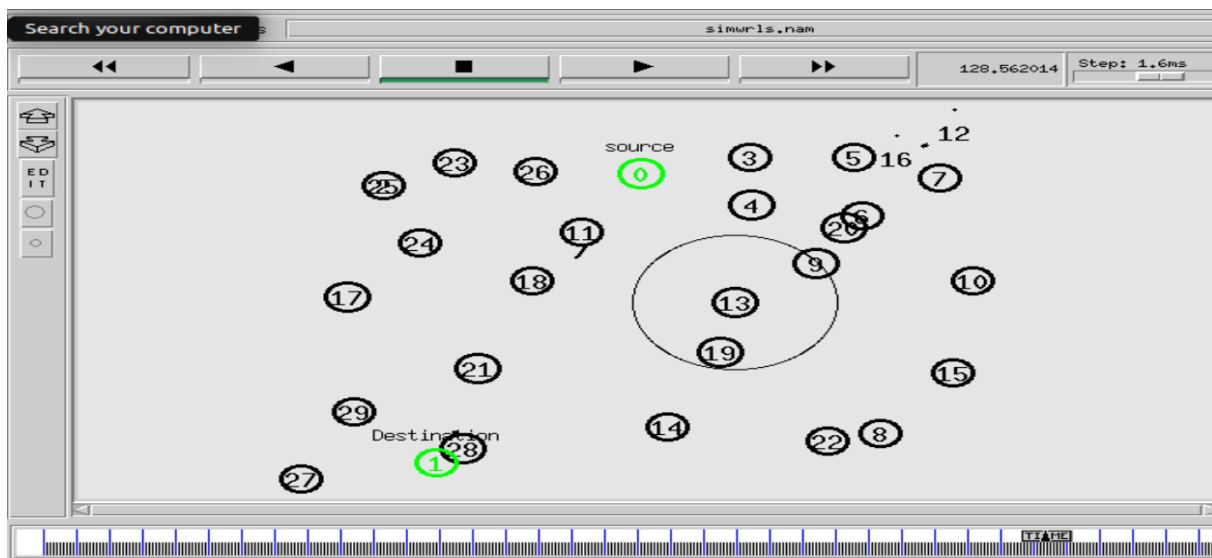


Figure III.11 : Réponse de L'IPS immédiate et élimine les paquets malveillants

IPS a réveillé le système En même temps, il active la fonction de réponse instantanée en traiter le trafic suspect et couper les connexions avec des paquets malveillants et trouver un moyen différent et rationnel de créer un chemin sûr pour terminer les paquets travail en réseau.

III.8.2.4.4. Réponse immédiate de l'IPS et l'élimination des paquets malveillants

La photo III.12 représente le moment où la menace de trou de ver est éliminée et une nouvelle connexion sécurisée est établie :

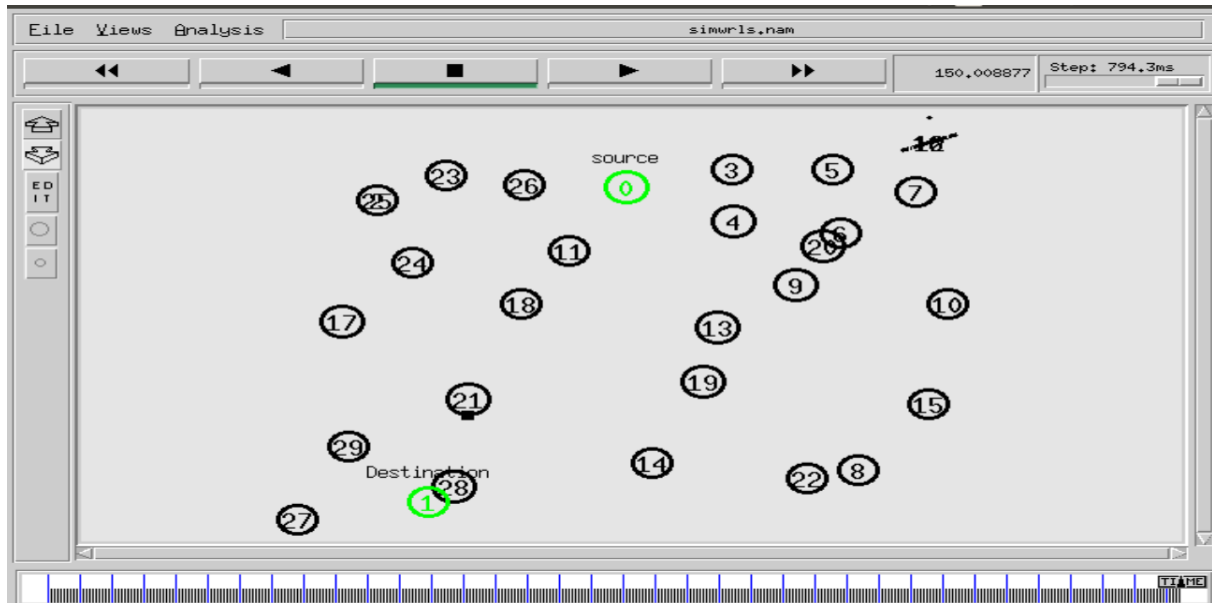


Figure III.12 : Élimination complète du trou de ver et restauration de la communication sécurisée entre les nœuds

Et enfin la disparition des nœuds nuisibles avec le retour du système à son état normal et sur (connexion de nœuds sains) grâce à la sécurité IPS.

III.9. Les résultats de la simulation

III.9.1 Effets de WormHole sur le protocole DSDV

La Figure III.13 représente l'effet du wormhole dans le protocole DSDV :

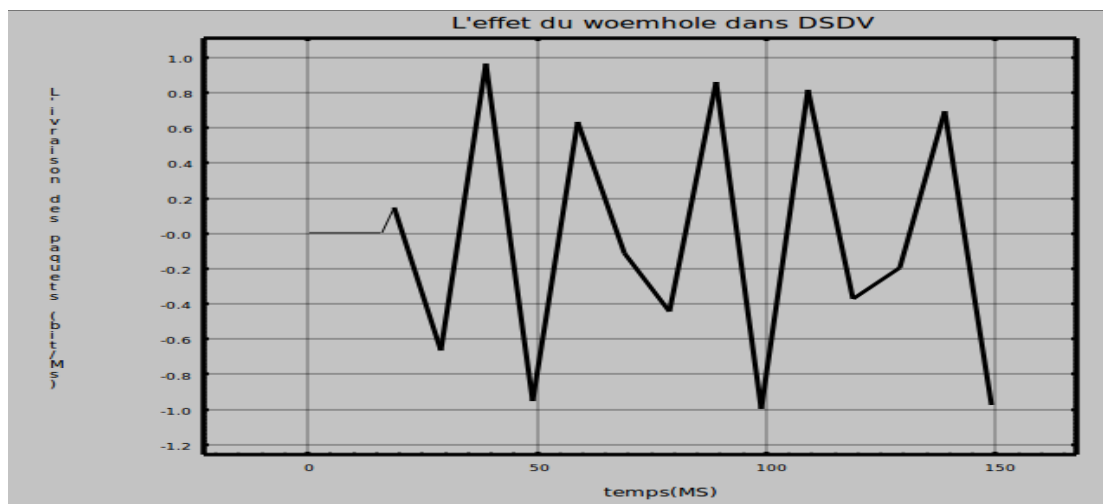


Figure III.13 : L'effet du WormHole-DSDV

Les nœuds de trou de ver trompeurs en déclarant les informations de routage requises par DSDV jusqu'à 19 ms, le trou de ver absorbe les paquets et les analyse, puis envoie des paquets vers la destination (le récepteur) tout en gardant des copies, mais d'autres paquets ont le sort d'être ignorés par le trou de ver vers le nœud de destination.

III.9.2 Effets de l'IPS sur le protocole WormHole-DSDV

La Figure III.14 représente l'effet de l'IPS-DSDV dans wormhole-DSDV protocole :

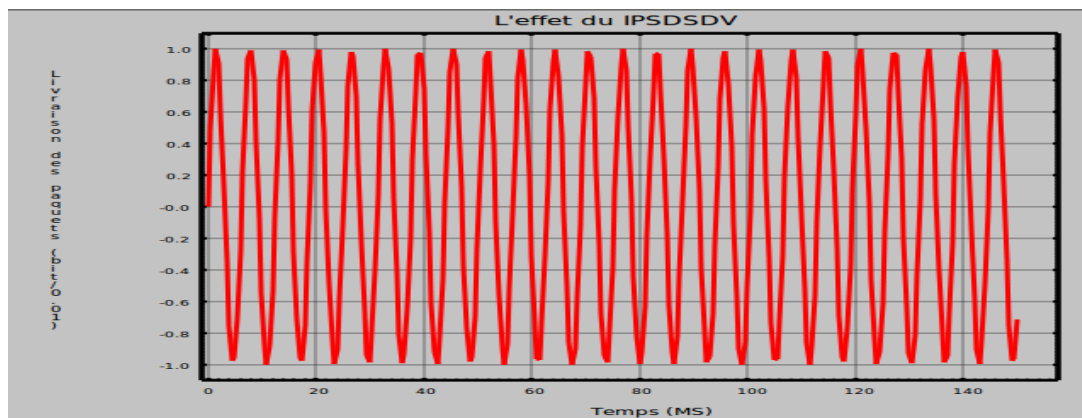


Figure III.14 : L'effet du IPSDSDV

Le paquet arrive à destination, l'IPS a éliminé l'attaque de trou de ver et rétabli la connexion à son état normal (DSDV sans WormHole).

III.10. Métriques d'évaluation des performances

III.10.1. Débit (throughput)

Dans les réseaux Ad-Hoc, le débit, ou throughput en anglais, se réfère à la quantité de données qui peut être transmise avec succès à travers le réseau par unité de temps. Le débit dans les réseaux Ad-Hoc dépend de plusieurs facteurs, tels que la capacité du canal de communication, les interférences, la distance entre les nœuds, la qualité du signal, le protocole de routage utilisé et la charge du réseau.

Le calcul du débit dans un réseau ad-hoc :

$$\text{Débit d'un nœud} = \frac{\text{Le nombre total des bits reçus}}{\text{Le temps}}$$

La figure III.15 représente le débit des 30 nœuds (bit/ms) :

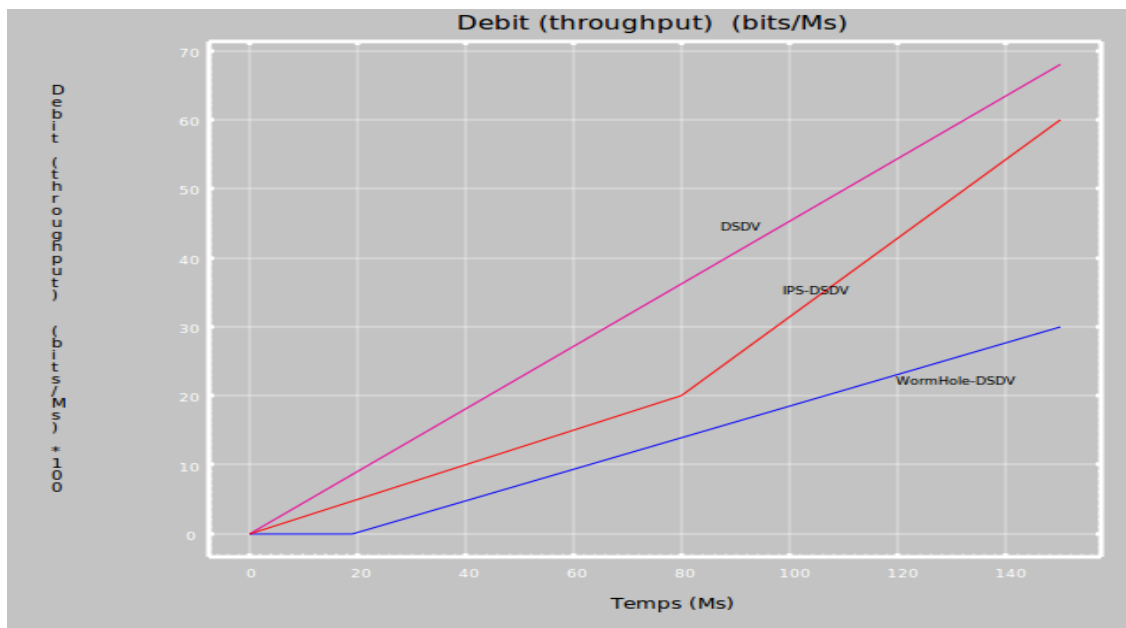


Figure III.15 : Le débit des 30 nœuds (bits/ms)

Ce nombre représente le débit du réseau en fonction du temps. La simulation montre une augmentation progressive du débit dans le temps, grâce à l'effet du protocole IPSDSDV, qui neutralise l'effet wormhole, car ce dernier stabilise le débit jusqu'à 19ms puis lui permet d'augmenter, mais à faible cadence.

III.10.2.Taux de livraison des colis (%)

Il en va de même avec le débit de livraison de paquets jusqu'au débit de livraison de paquets (%) est généralement calculé en comparant le nombre de paquets livrés avec succès avec le nombre nombre total de paquets envoyés. Voici comment vous pouvez le calculer :

$$\text{Taux de livraison} = (\text{Nombre de paquets reçus} / \text{Nombre de paquets transmis}) * 100$$

La figure III.16 représente taux de livraison de paquets (%) :

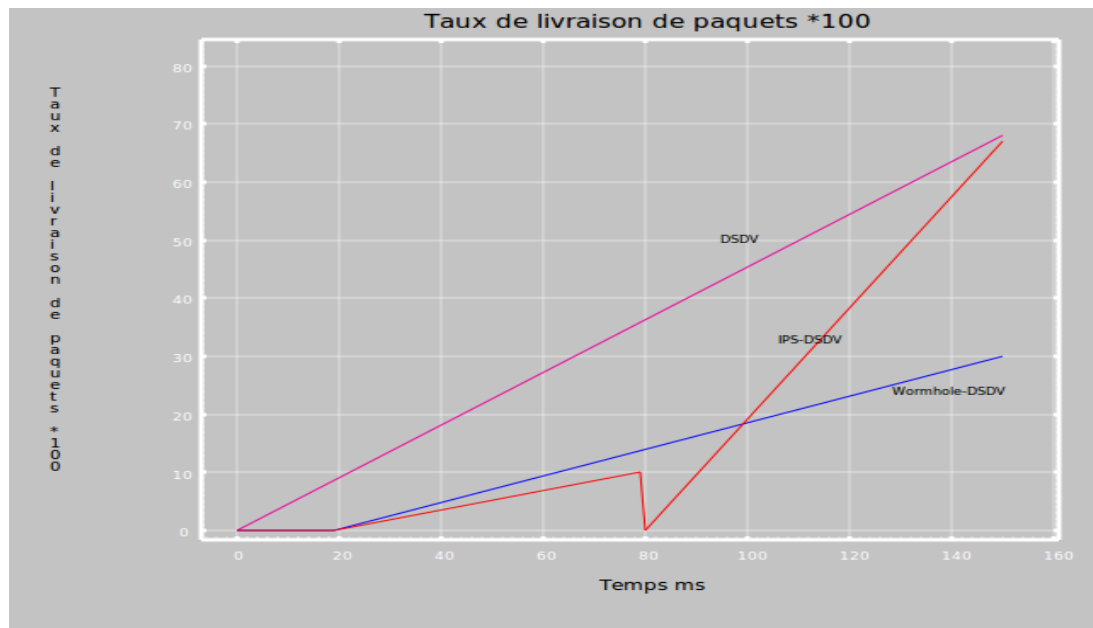


Figure III.16 : Taux de livraison des colis (%)

L'IPS-DSDV est considéré comme un facteur clé pour augmenter le taux de livraison des paquets après avoir éliminé l'attaque par trou de ver qui décourageait le processus de livraison, mais malgré cela, les paquets n'atteignent pas 100 % car il existe plusieurs facteurs tels que la densité du réseau, la présence de perturbations, soit la durée de convergence de l'algorithme.

III.10.3. Taux de perte de paquets (%)

Le taux de perte de paquets est calculé en comparant le nombre de paquets perdus au nombre total de paquets envoyés. Voici comment vous pouvez le calculer :

$$\text{Taux de pertes de paquets (\%)} = \left(\frac{\text{le nombre de paquets perdus}}{\text{le nombre total de paquets envoyés}} \right) * 100$$

La figure III.17 représente le taux de pertes de paquets (%) :

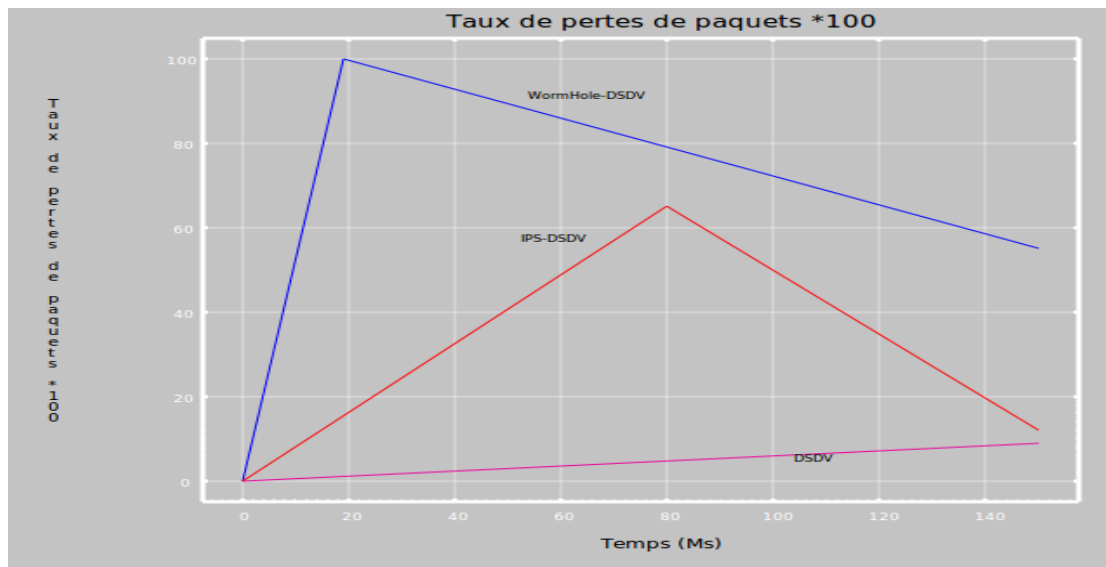


Figure III.17 :Taux de perte de paquets (%)

A cause de la mauvaise qualité de la liaison sans fil due aux effets du trou de ver sur le protocole de routage DSDV, on voit que la perte de paquets augmente jusqu'à 19ms puis diminue d'un petit pourcentage car le trou de ver envoie des paquets de 55% et aussi le mouvement des nœuds et du chargement du trafic au début fait le taux de perte les forfaits sont volumineux, mais après l'intervention d'IPS-DSDV et son élimination de la menace, le pourcentage diminue considérablement Jusqu'à ce qu'il atteigne son pourcentage dans le protocole dans sa première phase (sans aucune menace)

III.11. Conclusion

Après les résultats de simulation, nous avons évalué les performances et la sécurité du protocole de routage DSDV dans les réseaux sans fil Ad-Hoc contre les attaques de trous de ver à l'aide de NS-2. Cela nous a permis de mieux comprendre les vulnérabilités et les contre-mesures, y compris IPS, que nous avons ajoutées au protocole pour réduire l'attaque par trou de ver (wormhole).

Nous avons d'abord appliqué le protocole DSDV dans le simulateur NS-2, dont le comportement était normal sans perdre aucun paquet dans le réseau dédié, mais après application du wormhole, nous avons constaté une augmentation significative de la perte de paquets dans le réseau, et pour repousser cette attaque nous avons ajouté la sécurité IPS à notre programme, qui rompt la connexion entre les nœuds nuisibles et les nœuds sains, puis crée une nouvelle connexion sécurisée pour transférer le paquet.

Le DSDV est un protocole de routage actif couramment utilisé dans les réseaux Ad-Hoc sans fil. Il vise à fournir un routage fiable et sans boucle en maintenant des tables de routage et en échangeant périodiquement des mises à jour de routage entre les nœuds. Le protocole DSDV fonctionne bien dans les petits et moyens réseaux, mais il présente plusieurs limites.

Dans le premier chapitre, nous fournissons des informations générales sur les réseaux Dédiés, tels que leurs domaines d'application, caractéristiques, concepts et caractéristiques propriétés.

Le deuxième chapitre se concentre sur les protocoles de routage dans les réseaux Ad-hoc ; nous aborderons les problèmes de sécurité dans les réseaux ad hoc en expliquant les différents types d'attaques qui peuvent menacer le réseau, ainsi que les services de sécurité de base qui existent, et ferons des recommandations pour contrer ces menaces , et à la fin de ce chapitre, les caractéristiques et protocoles de travail AODV et DSDV ainsi que des protocoles DSR et OLSR sont comparés.

Dans le troisième chapitre, Nous allons décrire l'outil Simulateur et objets NS2 qui l'accompagnent pour implémenter notre application. Appliquons le protocole DSDV et la nature de l'attaque WormHole l'affecte, Enfin nous utiliser la fonction IPS, avec une description de simulation et une discussion. L'une des principales menaces de sécurité pour DSDV et d'autres protocoles de routage est les attaques de trous de ver. Lors d'une attaque par trou de ver, un nœud malveillant crée un tunnel entre deux points distants du réseau, les faisant apparaître comme directement connectés. En relayant les paquets via ce tunnel, un attaquant pourrait obtenir un accès non autorisé au trafic réseau, modifier ou supprimer des paquets et perturber les communications.

Pour lutter contre les attaques de trous de ver dans DSDV, une méthode appelée IPS-DSDV peut être utilisée. IPS-DSDV améliore le protocole DSDV avec des capacités de détection et de prévention des intrusions. Cela implique de surveiller le réseau pour détecter toute activité suspecte et de prendre des précautions pour détecter et atténuer les attaques de trous de ver. En combinant des techniques de détection d'intrusion avec des mises à jour de routage dans DSDV, IPS-DSDV peut identifier la présence d'attaques par trou de ver en fonction d'un comportement ou de modèles anormaux. Une fois qu'une attaque de trou de ver

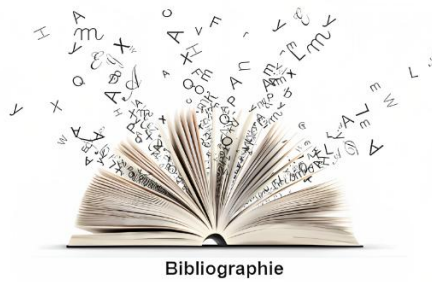
Conclusion générale

est détectée, IPS-DSDV peut prendre des contre-mesures telles que l'isolement des nœuds malveillants, le blocage des tunnels de trou de ver ou l'alerte des administrateurs réseau.

Travail futur

De nouveaux protocoles de routage peuvent être conçus qui sont résilients aux trous de ver tels que la vérification de routage sécurisée basée sur la géographie et développent également des mécanismes d'authentification forts. Tout en continuant à évaluer les performances des mécanismes de détection de wormhole et des protocoles IPS-DSDV avec la simulation de différents scénarios et bien sûr le développement de versions NS-2

D'autre part, nous voulions appliquer notre travail sur le terrain et mettre en œuvre la menace de trou de ver sur un ordinateur avec la présence d'IPS security, et nous aurions la possibilité de couper la communication avec lui ou de le tromper si nous voulions lui permettre pour recevoir de faux messages.



References

- [1] B. T. C. Amel, "Analyse par simulation des performances d'un réseau de capteurs sans fil (WSN),"2015-2016.
- [2] www.clicours.com/le-reseau-ad-hoc.
- [3] https://fr.wikipedia.org/wiki/R%C3%A9seau_ad_hoc#Premiers_travaux_sur_le_MANET..
- [4] Farida, "Sécurité et routage dans les réseaux Ad hoc," <https://www.ummo.dz/dspace/handle/ummo/6253>.
- [5] S.Carson and j.Macker,«RFC 2501 : Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration, january 1999.
- [6] F. AMEZA, Les technologies sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV) bejaia, 2007.
- [7] R. Hamza, "Protocoles de routage pour les réseaux ad hoc," Université de Montréal, 2004.
- [8] D. A. & N. MAISSOUM, "Détection d'intrusions dans les réseaux Ad Hoc," UNIVERSITÉ BADJI MOKHTAR - ANNABA, 2020-2021.
- [9] b. zouhir,"la sécurité de protocole OLSR dans les réseaux AD-HOC"2010 / 2011.
- [10] www.memoireonline.com/01/09/1878/m_Les-technologies-sans-fil-Le-routage-dans-les-reseaux-ad-hoc-OLSR-et-AODV2..
- [11] A. Mira, "Routage QoS et Prédiction de Rupture de Route dans les Réseaux Ad Hoc,"Béjaïa.
- [12] A. A. Korba, "Détection d'attaques dans les protocoles de routage pour des réseaux informatiques,"ANNABA, 2016.

- [13] A. Bessaih and S. Bouchakel, "Routage et simulation dans les réseaux mobiles ad hoc," Béjaia, 2017.
- [14] www.ionos.fr/digitalguide/serveur/know-how/unicast/.
- [15] fr.theastrologypage.com/point-multipoint-communication.
- [16] www.ac-lille.fr/daip/pole-pedagogie/fiches-techniques/glossaire-technique/diffusion-broadcast.
- [17] Lahcen, Toudjine "dspace.univ-bba.dz, Université Mohamed El Bachir El Ibrahimi de Bordj Bou Arreridj", 2020 / 2021.
- [18] H. Maouchi, "Routage avec qualité de service dans les réseaux ad hoc," Université de MOULOUD MAMMERI de TIZI OUZOU.
- [19] <https://fr.theastrologypage.com/mobile-ad-hoc-network>
- [20] A. Zebd, "DZ-MAODV : nouveau protocole de routage multicast pour les réseaux ad-hoc mobiles basé sur les zones," l'université du Québec à Trois-Rivières.
- [21] www.clicours.com/le-routage-dans-les-reseaux-mobiles-ad-hoc/ - 2002/2003.
- [22] E. Royer, "A review of current routing protocols for ad-hoc mobile wireless networks," IEEE Personal, in 46–55, April 1999..
- [23] M. Abolhasan, "A review of routing protocols for mobile ad hoc networks," Elsevier, Ad Hoc Networks 2, 2004, p. PP 1–22.
- [24] C. Chaudet, "HAL Id," 19 décembre 2004. <https://theses.hal.science/tel-00007706> Submitted.
- [25] Sebastien Loye "Protocoles de routage IP multicast" 10/05/2006
- [26] <http://igm.univ-mlv.fr>
- [27] www.univ-bouira.dz/ar/wp-content/uploads/2018/12/RAV7_adhoc_routage.pdf
- [28] R. Abdellaoui, "SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR," l'école de technologie supérieure, Montréal,, 05-05-2009.
- [29] N. Labraoui, "LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL AD HOC," tlemcen, 2012.
- [30] N. BADACHE, "Le routage dans les réseaux mobiles Ad Hoc," Université d'Alger USTHB, 2000.
- [31] Bulent Tavli "Mobile Ad Hoc Networks: Energy-Efficient Real-Time Data Communications", University of Rochester-NY-USA 2006.

- [32] M. Yassine, "Gestion de la qualité de service et contrôle de topologie dans les réseaux Ad Hoc," École nationale supérieure des télécommunications (Paris), 2004.
- [33] L. NUAYMI, "La sécurité dans les réseaux Ad hoc," université ENST Bretagne
- [34] [/blog.netwrix.fr/2019/04/03/comment-realiser-une-evaluation-des-risques-informatiques/](http://blog.netwrix.fr/2019/04/03/comment-realiser-une-evaluation-des-risques-informatiques/).
- [35] [www.indiastudychannel.com/resources/105777-Need-of-Network Ssecurity](http://www.indiastudychannel.com/resources/105777-Need-of-Network-Security) 14/02/2010
- [36] O. Cheikhrouhou, "La sécurité des réseaux Ad hoc," Ecole Sfax tunisien, 2005.
- [37] F. Imloul, "Sécurité dans les réseaux Ad Hoc Wormhole.," Université A/Mira de Béjaïa, 2012/2013.
- [38] C. Karlof, "Secure routing in wireless sensor networks : attacks and countermeasures", Ad Hoc Networks 1(2003) 293-315," 2003.
- [39] R. ARMOR "Les attaques sur le routage dans les réseaux ad hoc," 09 /02/ 2007.
- [40] A. Hu, "Rushing attacks and defense in wireless ad Hocnetwork routing protocols," San Diego,CA, USA, 2003.
- [41] a. sofia, Analyse par simulation des performances d'un réseau de capteurs sans fil (WSN), khemis meliana-ain defla, 2022/2023.
- [42] www.academia.edu/29810376/Chapitre_2_Les_R%C3%A9seaux_Mobiles_Ad_Hoc_and_les_Protocoles_de_Routage_2_1_Introduction.
- [43] S. K. sarka, "Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications," 2008. www.auerbach-publications.com.
- [44] boowiki.info/art/protocoles-de-routage/dsdv.html#Vantaggi.
- [45] m. kamel, "Mémoire de fin de cycle pour l'ob administration et sécurité des réseaux sous le thème etude comparative entre AODV et AOMDV dans le cadre des réseaux Ad Hoc"univ.A/Mira .Bejaia. 2016/2017
- [46] www.memoireonline.com/01/09/1878/Les-technologies-sans-fil-Le-routage-dans-les-reseaux-ad-hoc-OLSR-et-AODV.html.
- [47] Bouchebbah,Razika "Adaptation du simulateur multi-agents netlogo pour modeliser et simuler le routage dans un reseau mobile Ad-Hoc 17/09/2020
univ-bejaia.dz/xmlui/handle/123456789/14381
- [48] I. Sekhri, "Générateur de script Tcl pour les simulateur NS-2," univ- alarbi ben mhidi, 2012/2013.

- [49] <https://ex001slvr.wordpress.com/2011/03/10/presentation-de-ns2>.
- [50] i. Sekhri, "Performance Analysis of Wired and Wireless Network using NS2 Simulator," SRM University NCR Campus, Modinagar, JUNE 2013.
- [51] Takoia,miloudi, "Etude comparative de deux simulateurs pour les reseau ad-hoc sans fil ,"
UNIVERSITE KASDI MERBAH OUARGLA, 25/06/2018
- [52] www.researchgate.net/figure/Basic-Architecture-of-NS-2_fig3_259484464.
- [53] www.researchgate.net/figure/Working-of-Wormhole-Attack-in-MANETs_fig1_282500613.
- [54] chat.openai.com
- [55] docplayer.fr/69182750-Analyse-des-protocoles-des-reseaux-de-capteurs-sans-fil.html.
- [56] S. h. Imfeeney/, "A taxonomy for routing protocols in mobile ad hoc networks," in *A taxonomy for routing protocols in mobile ad hoc networks*, L.M. Feeney, October 1999.
- [57] "A review of current routing protocols for ad-hoc mobile wireless networks," *IEEE Personal Communications Magazine*, 46–55,, April 1999.
- [58] "A review of routing protocols for mobile ad hoc networks," *Elsevier, Ad Hoc Networks 2 (2004)*, PP 1–22., 2004.
- [59] "A comprehensive overview about selected Ad Hoc Networking RoutingProtocols," *Technical Report I0311, 2003, TU Munich*, March 2003..

