L'attaque déni de service dans les réseaux sans fil

Kamel Saddiki

Thèse de Doctorat
3ème *Cycle*

Domaine : LMD Mathématiques informatique
Filière : Informatique
Spécialité : Technologies des réseaux sans fil

Par

Mr Kamel SADDIKI

Denial of service attack in wireless networks

Soutenue le 13-01-2019 devant le jury :

Pr.	Ghalem BELALEM	Université Oran 1	Rapporteur
Pr.	Djelloul BOUCHIHA	C. U. de Naama	Rapporteur
Pr.	Jalel BEN OTHMAN	Université Paris 13	Examinateur
Pr.	Ahmed SERHROUCHNI	Université ParisTech	Examinateur
Pr.	Pascal LORENZ	UHA	Directeur de thèse
Dr.	Sofiane BOUKLI-HACENE	UDL SBA	Co-Directeur de thèse

Année Universitaire : 2018 - 2019

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

Remerciement

Je tiens tout d'abord à remercier Allah le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

Je tiens à exprimer mes sincère remerciement à mes directeurs de thèse Dr. BOUKLI-HACENE Sofiane, Pr. Pascal LORENZ pour l'encadrement de qualité et les précieux conseils durant toute la période du travail.

Enfin, Je tiens également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail, notamment les membres de ma famille, mes amis, qui n'ont eu de cesse de m'épauler durant mon parcours.

Table des matières

Table des matières **iv**

Liste des figures **v**

Liste des tableaux **vi**

Préface **1**

1 Les réseaux sans fil **4**
- 1.1 Les réseaux sans fil . . . 5
- 1.2 Classification des réseaux sans fil . . . 5
  - 1.2.1 Selon la zone de couverture . . . 5
  - 1.2.2 En mode opératoire . . . 8
- 1.3 Les réseaux Ad hoc : . . . 9
  - 1.3.1 Definition : . . . 9
  - 1.3.2 Les caractéristiques des réseaux ad hoc : . . . 10
  - 1.3.3 Domaines d'utilisation des réseaux ad hoc . . . 11
  - 1.3.4 Routage dans les réseaux ad hoc . . . 11
  - 1.3.5 La sécurité dans les réseaux ad hoc . . . 16
  - 1.3.6 Les attaques dans Les réseaux ad hoc . . . 17
  - 1.3.7 Le déni de service . . . 22
- Conclusion . . . 23

2 Le protocole OLSR **24**
- 2.1 OLSR (Optimized Link State Routing Protocol) . . . 25
- 2.2 Les paquets de contrôle du protocole OLSR . . . 27
  - 2.2.1 HELLO . . . 27
  - 2.2.2 TC (Topology Control) . . . 29
  - 2.2.3 Multiple Interface Declaration (MID) . . . 30
  - 2.2.4 Host and Network Association (HNA) . . . 30
- 2.3 La selection des MPRs . . . 31
- 2.4 Construction de la table de routage . . . 33
- 2.5 la sécurité dans OLSR . . . 34
  - 2.5.1 Les attaques contre le protocole OLSR . . . 36
- 2.6 Conclusion . . . 40

3 Contribution I : Mécanisme de sécurité contre l'attaque BlackHole **41**
- 3.1 Etat de l'art . . . 42
- 3.2 Modèle de l'attaque blackhole contre le protocole OLSR . . . 48

3.3 Intérêt de la simulation : 50
3.3.1 Network Simulator 2 (NS2) 50
3.3.2 La mesure de performance 52
3.4 Simulation de l'attaque 53
3.5 Mécanisme de sécurité 55
3.5.1 Phase I 55
3.5.2 Phase II 57
3.6 Simulation et analyse 61
Conclusion 64

4 Contribution II : Mécanisme de sécurité contre l'attaque Blackhole coopérative **65**
4.1 Etat de l'art 66
4.2 Modèle de l'attaque Blackhole coopérative 69
4.3 Simulation de l'attaque Coopérative 73
4.4 Mécanisme proposé 76
4.5 Simulation et discussions des résultats 83
Conclusion 86

5 Conclusion et perspective **87**
5.1 Conclusion 88
5.2 Perspective 89

Liste des publications **90**

Bibliographie **91**

Notations **97**

Liste des figures

1.1 les réseaux sans fil selon la zone de couverture 5
1.2 Architecture avec infrastructure 8
1.3 Architecture en mode Ad hoc 9
1.4 Le problème des noeuds cachés 11
1.5 routage en cluster 15
1.6 Déni de service 23

2.1 Optimisation de l'inondation en utilisant les MPRs 25
2.2 Optimisation de l'inondation en utilisant les MPRs 26
2.3 Structure du paquet HELLO 28
2.4 Structure du paquet TC 29
2.5 Structure du paquet MID 30
2.6 La sélection des MPRs 32
2.7 usurpation d'identité 36

2.8 usurpation de liens 1 . . . 37
2.9 usurpation de liens 2 . . . 37
2.10 usurpation de liens 3 . . . 38
2.11 l'attaque Wormhole . . . 39

3.1 Schéma d'authentification . . . 42
3.2 Topologie de l'attaque . . . 48
3.3 Informations via les messages HELLO . . . 49
3.4 Informations via les messages TC . . . 49
3.5 Modèle de l'attaque blackhole . . . 50
3.6 Flot de simulation . . . 51
3.7 Taux de délivrance . . . 54
3.8 paquets perdus . . . 54
3.9 la surcharge . . . 55
3.10 graphe biparti . . . 59
3.11 Taux de delivrance . . . 62
3.12 Paquets perdus . . . 63
3.13 Surcharge . . . 63

4.1 l'attaque Blackhole coopérative 1 . . . 70
4.2 l'attaque Blackhole coopérative 2 . . . 71
4.3 l'attaque coopérative contre OLSR . . . 72
4.4 taux des paquets transmis (PDR) . . . 74
4.5 Nombre des paquets perdu . . . 75
4.6 La surcharge du réseau . . . 75
4.7 Usurpation des liens . . . 76
4.8 structure du paquet HELLO . . . 78
4.9 le mécanisme de sécurité . . . 82
4.10 Taux des paquets transmis avec succès (PDR) . . . 84
4.11 Nombre des paquets perdu . . . 85
4.12 La surcharge dans le réseau . . . 85

Liste des tableaux

1.1 Les réseaux sans fil selon la porté . . . 7
1.2 comparaison entre les protocoles réactifs et poactifs . . . 14
1.3 les attaque par couche . . . 19

3.1 Paramètre de simulation . . . 53
3.2 Paramètre de simulation . . . 61

4.1 Paramètre de simulation . . . 73
4.2 le champ 'reserved' . . . 78
4.3 Paramètre de simulation . . . 83

Introduction Général

Le développement technologique qu'a vu le monde d'aujourd'hui à toucher tous les domaines, particulièrement le secteur de la communication qui connait une évolution considérable par l'apparition des technologies de réseau sans fil.

Les réseaux sans fil est une alternative au réseau câblés quand ces derniers posent problèmes de Réalisation tels les réseaux temporaire, difficulté du terrain, mobilité, etc.

Le développement actuel des moyens de la communication sans fil a permis la manipulation de l'information à travers des équipements de calcul portables caractérisés par une source d'énergie autonome et une faible capacité de stockage accédant au réseau statique à travers une interface de communication sans fil. L'ensemble des équipements portable a créé un environnement mobile ou chaque unité de calcul a une mobilité libre et sans restriction sur la localisation des usages. L'extension des technologies sans fil est propulsée aujourd'hui par de nouvelles approches dans le domaine des télécommunications. Cet environnement mobile possède les caractéristiques suivantes :

— Une topologie d'interconnexion dynamique et éphémère.
— Une bande passante limitée
— Une autonomie limitée des sources d'énergie.

Ces réseaux sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent donnent un accès à une large palette d'applications dont : les applications militaires, les opérations de secours, l'utilisation à des fins éducatives.

Les réseaux Ad hoc ne peuvent pas être utiles sans l'utilisation des protocoles de routage fiable pour acheminer les paquets de la source à la destination et qui respectent les caractéristiques des réseaux ad hoc. Le groupe de travail MANET à définie trois types de protocoles de routage : les protocoles proactifs (OLSR, DSDV), les protocoles réactifs (AODV, DSR) et les protocoles hybrides (ZRP), cependant le grand problème de ces réseaux est la sécurité. Les travaux de recherche indiquent que les réseaux sans fil sont plus vulnérable que les réseaux filaires en raison de leur caractéristiques. L'utilisation des liaisons sans fil rend ces réseau sujets à plusieurs menaces de sécurité physique allant de l'écoute passive à l'interférence active. Ces réseaux sont encore vulnérable au attaques tel que Le sniffing, Le wardriving, Le warchalking et Le Deni de service.

Dans notre thèse nous nous sommes intéressés à l'aspect sécuritaire des MANET (Mobil Ad Hoc Network) au niveau de la couche réseau, et l'étude de l'effet des attaques de type déni de service qui perturbent le bon fonctionnement de ces réseaux, pour enfin proposer un mécanisme de sécurité efficace contre ces menaces.

Contribution

L'objectif principal de la thèse est de proposer un schéma de sécurité pour assurer la détection des nœuds malveillants dans un réseau MANET. Dans cette étude, nous avons sélectionné l'attaque déni de service (DOS), déni de service distribué (DDOS) et l'attaque de trou noir (Black Hole) pour évaluer le mechanisme de sécurité proposé.

Nous avons proposé en premier lieu une solution en utilisant des techniques basées sur des aspects sémantiques et logiques au niveau des liens entre les nœuds, ainsi que la confiance collaborative entre les voisins pour détecter les nœuds malveillants dans le réseau. Afin d'assurer le fonctionnement de notre mécanisme, nous avons calculé un seuil en fonction du nombre de liens à ne pas dépasser dans chaque zone, en cas de franchisse par un nœud, il est considéré comme un suspect. Enfin, pour confirmer la présence d'un nœud malveillant, une procédure de vérification optimisée est déclenché et les nœuds malicieux sont placés dans une liste noire.

Dans la deuxième partie de notre contribution, nous nous sommes intéressés à l'attaque collaborative par deux ou plusieurs nœuds contre le protocole OLSR. Pour faire face à l'attaque collaborative nous avons présenté une solution collaborative entre les nœuds voisins. Le mécanisme proposé est appelé Trust-Neighbors-Based. Le principe du protocole est d'échanger des informations pour calculer le degré de confiance (TV : Trusted value) de chaque nouveau MPR par les nœuds voisins en utilisant seulement les champs réservés du paquet HELLO. À partir de cette information calculée et échangé (TV) nous pouvons distinguer entre les nœuds avec un rôle important dans le réseau et les nœuds malicieux qui tentent de découper le réseau.

Organisation de la thèse

Ce mémoire de thèse est composé de cinq chapitres. Dans le premier chapitre nous présentons les réseau sans fil en général, et les réseau mobile ad hoc en particulier (caractéristique, domaine d'application, routage) avant d'entamer l'aspect sécuritaire des réseau mobile ad hoc et les vulnérabilité aux attaques dans le même chapitre. Nous détaillerons dans le deuxième chapitre le protocole OLSR commençant par ces caractéristiques, ces différent message de contrôle pour avoir la topologie du réseau ainsi que l'algorithme de sélection des MPRs, enfin nous discuterons sur l'aspect sécuritaire du protocole OLSR et les vulnérabilité aux attaques. les deux chapitres suivants (troisième et quatrièmes) sont consacrés à la partie contribution de notre thèse. Afin de sécuriser le protocole OLSR, nous commençons par l'état de l'art approfondi des solutions proposées contre

les différentes attaques qui peuvent nuir au fonctionnement du protocole. Après cela, nous présenterons un schéma sécurisé pour faire face à l'attaque simple et coopérative contre le protocole OLSR avec des simulations détaillés avec le fameux simulateur de réseau NS-2 en se basant sur les métriques de performance. Le dernier chapitre concluera notre travail et présentera quelques perspectives de recherche dans la sécurité des réseau ad hoc.

Les réseaux sans fil

1

Sommaire

1.1 Les réseaux sans fil 5
1.2 Classification des réseaux sans fil 5
1.2.1 Selon la zone de couverture 5
1.2.2 En mode opératoire 8
1.3 Les réseaux Ad hoc : 9
1.3.1 Definition : 9
1.3.2 Les caractéristiques des réseaux ad hoc : 10
1.3.3 Domaines d'utilisation des réseaux ad hoc 11
1.3.4 Routage dans les réseaux ad hoc 11
1.3.5 La sécurité dans les réseaux ad hoc 16
1.3.6 Les attaques dans Les réseaux ad hoc 17
1.3.7 Le déni de service 22
Conclusion 23

Les réseaux sans-fil connaissent une évolution extrêmement rapide dans la dernière décennie et un succès très important au sein des entreprises et du grand public. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires, en s'affranchissant notamment des problèmes de câblage et de mobilité des équipements. Il existe plusieurs familles de réseaux sans fil, chacune étant développée par des organismes différents et donc incompatibles entre elles. Dans ce chapitre nous allons définir les réseaux sans fil, classifier les réseaux, présenter les architectures avec infrastructure et ad hoc où on va donner leurs définitions et les principaux caractéristiques et leur domaine d'application pour enfin entamer l'aspect sécuritaire dans ce type de réseaux.

1.1 Les réseaux sans fil

Un réseau sans fil (Wireless Network en anglais) (Alagha *et al.* 2001; Geier 1999) est un réseau de machines qui n'utilisent pas de câbles . C'est une technique qui permet aux utilisateurs de rester connectés tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité". Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio , infrarouges ou acoustiques) au lieu des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée , ainsi que le débit et la portée des transmissions.

1.2 Classification des réseaux sans fil

1.2.1 Selon la zone de couverture

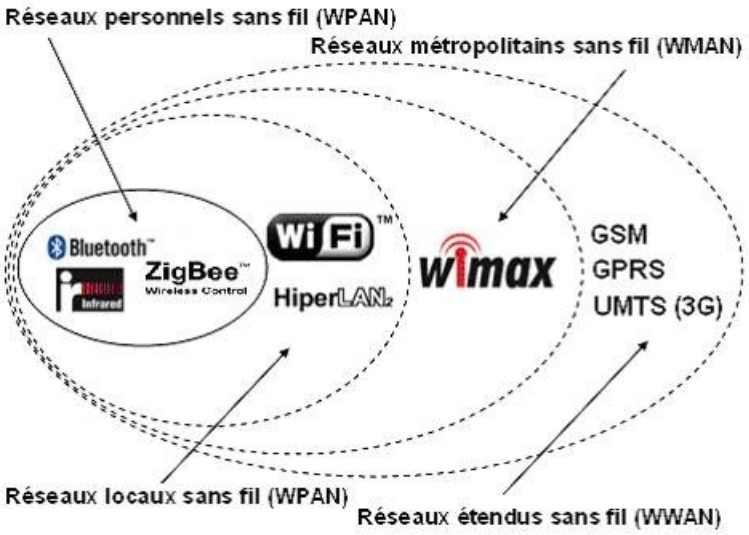

Figure 1.1 – *les réseaux sans fil selon la zone de couverture*

Les WPAN (Wireless Personal Area Networks)

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN).Dans cette catégorie, on retrouve les réseaux sans fil à l'échelle humaine dont la portée maximale est limitée à quelques dizaines de mètres autour de l'usager (bureaux, salles de conférence...). On y trouve les standards tels que le Bluetooth (Hauspie 2001) connu aussi sous la nom de la norme IEEE802.15.1 son débit théorique supérieur a 24 Mbits/s pour une portée de 100 mètres (Gupta 2016), ZIGBEE (Farahani 2008) permet la communication machine à machine, avec une très faible consommation électrique et des coûts très bas (Alagha *et al.* 2001), ce qui le rend particulièrement facile a intégré dans de petits appareil, et HomeRF (Stojmenovic 2002) avec une vitesse était d'environ 10 Mbits/s avec une portée avoisinant les 100 mètres.

Les WLAN (Wireless Local Area Networks)

C'est la catégorie des réseaux locaux sans fil dont la portée va jusqu'à 500 m, pour les applications couvrant un campus, un bâtiment, un aéroport, un hôpital, etc. On y trouve les standards tels que IEEE802.11 (Labiod 2002)(Wi-Fi pour Wireless Fidelity) permet de relier des ordinateurs portables, des assistants personnels (PDA : Personal Digital Assistant.), des objets communicants ou même des périphériques à une liaison haut débit (de 11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b à à 54 Mbit/s théoriques jusqu'a 1 Gb dans la norme 802.11ac (Siddiqui *et al.* 2015)) sur un rayon de plusieurs dizaines de mètres, HIPERLAN (Paolo 2005) qui offre un débit de 20 Mbits/s, mais la version Hiperlan2 permet d'atteindre 54 Mbits/s sur une bande de fréquence de 5GHz.

Les WMAN (Wireless Metropolitan Area Networks)

Plus connus sous le nom de Boucle Locale Radio (BLR) (Alagha *et al.* 2001), ce type de réseau utilise le même matériel que celui qui est nécessaire pour constituer un WLAN mais peut couvrir une plus grande zone de la taille d'une ville tout en économisant le cout élevé de la pose du câblage fibre ou cuivre. Les WMAN sont basés sur la norme IEEE 802.16 (Nuaymi 2007). La norme 802.16 est généralement appelée Wimax, Il exploite une bande de fréquence de 2 à 11Ghz. La porté peut atteindre jusqu'a 122 km dans la normal 802.11e (Soin *et al.* 2009), offrant un débit débits jusqu'à 1 Gbit/s stationnaire et 100 Mbit/s en mobile grande vitesse dans la norme 802.16m (Ahmadi 2010).

Les WWAN (Wireless Wide Area Networks)

Le réseau étendu sans fil est la catégorie de réseaux cellulaires mobiles dont la zone de couverture est très large, à l'échelle mondiale. WWAN sont des réseaux basés sur des infrastructures comme MSC et les stations de base BTS pour permettre à l'utilisateur mobile des connexions sans fil sur le réseau public ou privé distants (Alagha *et al.* 2001). Dans cette catégorie, on peut citer le GSM(Global System for Mobile Communications) (De Aguiar *et al.* 2009) et ses évolutions GPRS (Lindemann & Thummler 2001) (General Packet Radio Service), EDGE (Enhanced Data GSM Environment), l'UMTS (Richardson 2000) (Universal Mobile Telecommunication System), ainsi que la technologie LTE (Long Term Evolution) et LTE-Advanced. Le debit dans cette derniere peut atteindre ou dépasser 1 Gbit/s (Dahlman *et al.* 2013).

Cat	Portée max	Débit	Usages	Normes
WPAN	Jusqu'a 100 m	Réseau particulier	Réseau particulier	I EEE 802.15 (bluetooth) NFC, HyperPan
WLAN	500 m	Réseaux internes,propres à un bâtiment(soit comme réseau d'entreprise, soit comme réseau domestique).	Réseaux internes,propres à un bâtiment(soit comme réseau d'entreprise, soit comme réseau domestique).	Ville, Compus,...,Interconnect plusieurs WLAN
WMAN	50 à 122 Km	de 100 Mbit/s a 1Gbit/s	Ville, Compus, Interconnect plusieurs WLAN	Régional, National Interconnecte plusieurs villes
WWAN	Plusieurs centaine de Kms	1 Gbit/s	Régional, National Interconnecte plusieurs villes	Basé sur des technologies cellulaires

TABLE 1.1 – *Les réseaux sans fil selon la porté*

1.2.2 En mode opératoire

Avec infrastructure (cellulaire)

Dans le mode avec infrastructure, toutes les communications entre les stations mobiles ou entre les stations et le réseau extérieur passent à travers un point d'accès (AP : Access Point) ou station de Base (BS : Base station) qui prend alors le rôle de relais. L'ensemble des points d'accés et tous les terminaux mobiles se trouvant dans sa zone de couverture est appelé un BSS ou Basic Service Set (ensemble de services de base). Les ponits d'accés peuvent être reliés ensemble par un system de distribution (DS) pour permettre l'extension de la couverture du réseau. Les DS gère aussi l'itinérance (roaming) des stations. Le standard ne donnera pas des spécifications particulières sur la nature de cette interconnexion mais il s'agit en général d'un réseau filaire. La figure ci-dessous illustre l'architecture d'un ESS (Extended Service Set) constitue par un ensemble de BSS relies par un réseau filaire (DS).

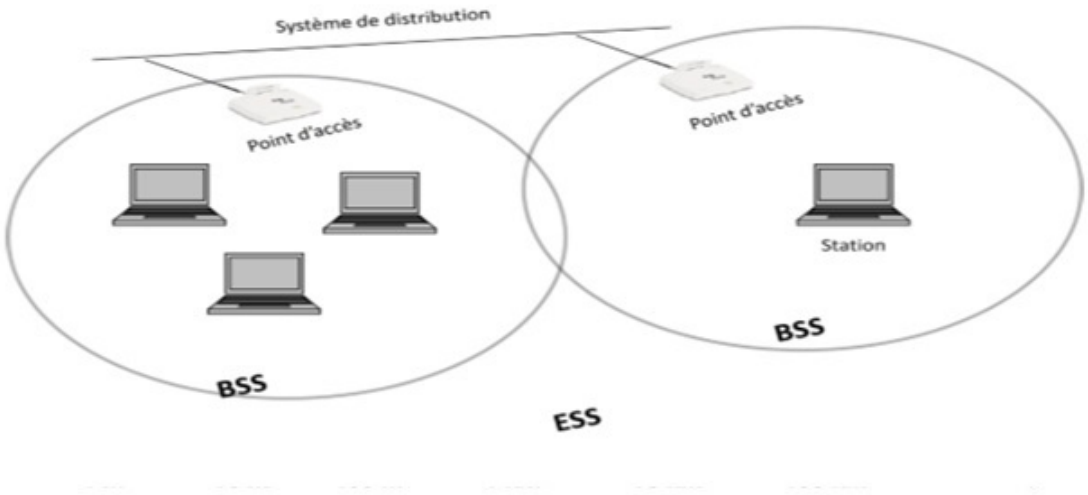

FIGURE 1.2 – *Architecture avec infrastructure*

Dans ce mode de fonctionnement le réseau est obligatoirement composé d'un point d'accès appelé station de Base (SB) muni d'une interface de communication sans fil pour la communication directe avec les unités mobiles (UM). Une station de base couvre une zone géographique limitée. La station de Base représente un pont réseau filaire et réseau sans fil permettant de relier une UM à une autre UM connecté à un site fixe. La station de base est aussi le point de passage de la transmission d'une UM à une autre UM.

Sans infrastructure (Ad Hoc)

Les systèmes de communication cellulaires sont basés essentiellement sur l'utilisation des réseaux filaires et la présence des stations de base qui couvrent les différentes unités mobiles du système. Les réseaux mobiles "ad hoc" sont à l'inverse, des réseaux formés de façon dynamique grâce à la coopération d'un ensemble arbitraire de noeud indépendant qui s'organise automatiquement de façon à être déployables rapidement, et qui doivent pouvoir s'adapter aux conditions de propagation, aux trafics et aux différents mouvements pouvant intervenir au sein des noeuds mobiles (Tanenbaum 2003).

1.3 Les réseaux Ad hoc :

1.3.1 Definition :

Un réseau mobile ad hoc, appelé généralement MANET (Mobile Ad hoc NETwork), consiste en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou d'administration centralisée (Pujolle 2014; Boukhalda 2006), chaque machine joue en même temps le rôle de client et le rôle de point d'accès comme illustré dans la figure1.3.

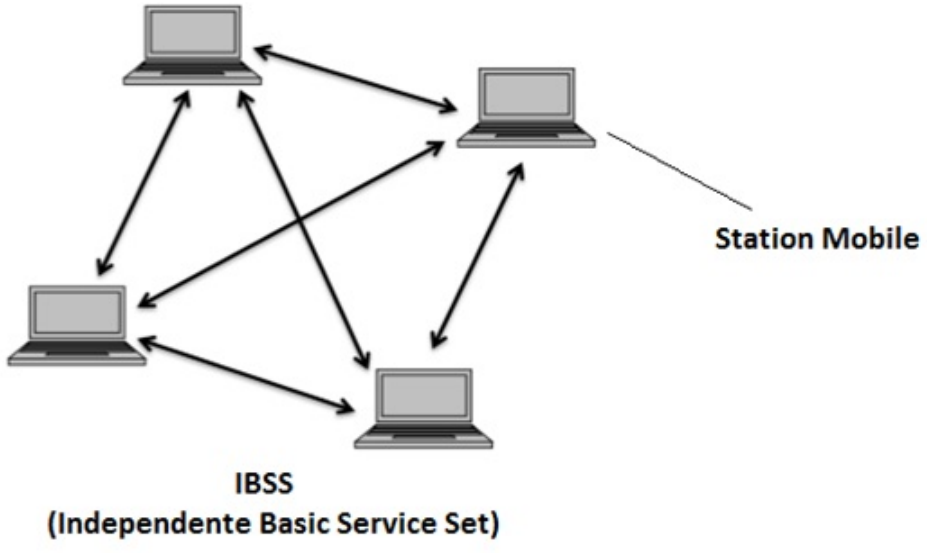

Figure 1.3 – *Architecture en mode Ad hoc*

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais Independant Basic Service Set, abrégé en IBSS). Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès (Xuan 2007). L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données.

1.3.2 Les caractéristiques des réseaux ad hoc :

Les réseaux mobiles ad hoc sont caractérisés par (Murthy & Manoj 2004) :

— 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 (Jamalipour 2003). Les liens de la topologie peuvent être uni ou bidirectionnels.

— Une bande passante limitée : Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagée. Ce partage fait que la bande passante réservée à un hôte soit modeste.

— Des contraintes d'énergie : Les stations mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.

— Erreurs de transmission : Les erreurs de transmission sont plus fréquentes que dans les réseaux filaires (Hamrioui 2014).

— Une sécurité physique limitée : Les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques (Aarti & Tyagi 2013). Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

— L'absence d'infrastructure : Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistantes et de tous genres d'administration centralisée. Les équipements mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue (Jamalipour 2003).

— La qualité de service : De nombreuses applications ont besoin de certaines garanties relatives par exemple au débit, au délai ou encore à la gigue. Dans les réseaux ad hoc ces garanties sont difficiles à obtenir. Ceci est dû à la nature du canal radio (interférence et taux d'erreur élevé) et au fait que les liens entre mobiles peuvent se partager les ressources. De ce fait, les protocoles de qualité de service habituel ne sont pas utilisables directement dans le mode ad hoc et des solutions spécifiques doivent être proposées

— problème des noeuds cachés : ce phénomène est très particulier à l'environnement sans fil. Un exemple est illustré par la figure 1.4. Dans cet exemple, les noeuds B et C ne sentent pas à cause d'un obstacle qui empêche la propagation des ondes. Les mécanismes d'accès au canal vont permettre alors à ces noeuds de commencer leur émission simultanément ce qui provoque des collisions au niveau du noeud A (Farooq *et al.* 2010).

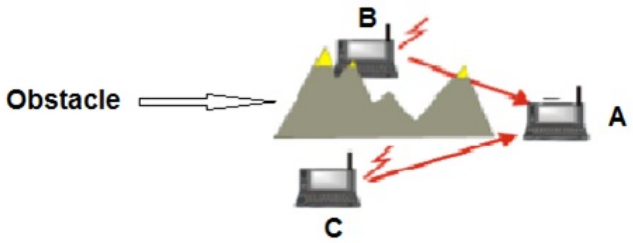

FIGURE 1.4 – *Le problème des noeuds cachés*

1.3.3 Domaines d'utilisation des réseaux ad hoc

Les réseaux ad hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent leur confèrent un accès à une large palette d'applications dont :

Les applications militaires : Les réseaux ad hoc ont été utilisés la première fois par l'armée. En effet, ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes et unités d'une armée.

Les opérations de secours : Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau ad hoc est indispensable pour permettre aux unités de secours de communiquer.

L'utilisation à des fins éducatives : Le déploiement d'un réseau ad hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et étudiants de partager des ressources (fichiers, accès à internet, etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure.

Applications industrielles : Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs (Sensor Networks) peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans , etc.

Mise en oeuvre des réseaux véhiculaires : sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux ad hoc sont alors la solution idéale.

1.3.4 Routage dans les réseaux ad hoc

Tous les types de systèmes de communication exécutent le processus de communication en utilisant un mécanisme appelé routage (Ubéda 2006). Le routage est un ensemble de règles ou d'algorithmes permettant de traiter et de déplacer des données d'un nœud à un autre dans

le réseau (Abd El-nabi 2005). Cette règle détermine le « meilleur » chemin sur lequel les données sont transmises. Les réseaux MANETs ne peuvent pas être utiles sans l'utilisation d'un protocole de routage filable pour le maintien approprié, ainsi établissement du processus de la communication. Un protocole de routage dans MANET utilise un algorithme pour déterminer le transfert de données réseau optimal et les chemins de communication entre les nœeuds du réseau. En même temps, un protocole de routage est responsable de la maintenance et, si nécessaire, de la réparation de tous les chemins. La mobilité des nœuds dans les réseaux ad hoc rend le routage plus complexe.

Le groupe de travail MANET créé par l'organisme IETF (Internet Engeneering Task Force) a défini trois types de protocoles de routage selon la procédure utilisée pour établir et maintenir les routes (Azza *et al.* 2015) : la famille de protocoles réactifs (à la demande), la famille des protocoles proactifs (vu global du réseau), et la famille des protocoles hybride.

Protocole de routage proactif

- Un protocole proactif est un protocole principalement axé sur la maintenance et le rafraîchissement des informations à travers une table de routage vers toutes les destinations possibles (Mbarushimana & Shahrabi 2007). Cette dernière gère le trafic et l'exactitude dans la direction du chemin.

Chaque nœud conserve les informations de routage réseau en échangeant périodiquement des messages de contrôle. Les informations de routage sont généralement conservées dans des tables différentes dépendantes du protocole particulier. La principal différence entre les protocoles proactifs réside dans le schéma de mise à jour de ces tables. Ce mécanisme peut inonder le réseau avec des informations de requête actives pour la maintenance et les mis a jour des informations de routage dans les diffirentes tables.

Le routage proactif introduit et utilise deux approches pour le routage : basé sur l'état de liens ou sur les vecteurs de distance. Les protocoles proactifs permettent une optimisation de recherche de route en terme de côut et de délai de transmission. Toutes les routes sont disponibles immédiatement. Les principaux protocoles de routage appartenant à la famille proactive sont DSDV (Destination Sequence Distance Vector) (Perkins & Bhagwat 1994), TBRPF (Ogier *et al.* 2003) (Topology Dessimination based on Reverse path Forwarding) et le protocole OLSR (Clausen & Jaquet 2003) (Optimized Link State Routing).

Protocole de routage réactif

Les protocoles réactifs est une famille de protocoles n'établissent la route vers une destination qu'à la demande. Dans cette catégorie la découvre de route se fait par inondation du réseau avec des paquets de demande de route. Lorsqu'une route est nécessaire, le nœud source initie un processus de découverte de chemin vers la destination via un paquet de recherche de route transmis de proche en proche dans l'ensemble ou seulement une parti du réseau (Mbarushimana & Shahrabi 2007). Une

fois établie, la route doit être maintenue jusqu'à ce qu'elle ne soit plus nécessaire ou que le nœud de destination devient inaccessible. Les protocoles réactifs échangent le délai de mise à jour du routage pour réduire la surcharge du réseau et optimiser la consommation d'énergie, ce qui est essentiel à la durée de vie de la batterie dans l'environnement MANET.

Les protocoles réactifs sont divisés en deux catégories principales suivant le même principe de routage "à la demande" avec des différences mineures dans principe de la découverte de la route. Ceux qui appartiennent aux catégories de "routage source" permettant aux paquets de données transféré de transporter le chemin complet vers la destination dans l'entête et chaque nœud intermédiaire acheminent en fonction de ces routes. Cela regle le problème du stockage local sur chaque nœud intermédiaire et réduit le surcoût dans le mécanisme du processus de mise à jour. De plus, il permet également à ces nœuds de conserver la mise à jour actuelle pour l'acheminement dans leurs caches et leurs tables d'informations sur les voisins.

Dans la deuxième catégorie de protocoles réactifs "saut par saut" ou "point à point" généralement nommée " Routage à vecteur de distance", un paquet de données inclut uniquement la destination et l'adresse de saut suivante. Selon ce principe, chaque nœud intermédiaire est forcé à mettre à jour les informations sur son voisinage et les informations de routage liées à la destination désirée. Un nœud intermédiaire transmet ces paquets en fonction des informations qu'il contient dans sa table de routage. Ce principe établit une architecture robuste pour faire face à la topologie imprévisible dans les MANET et améliore l'adaptabilité dans le routage. Certains des protocoles de routage sous ce concept sont DSR (Johnson *et al.* 2003) (Dynamic Source Routing), TORA (Kannhavong *et al.* 2007) (Temporally ordered routing algorithm) et AODV (Perkins *et al.* 2003) (Ad-hoc On Demande Distance Vector).

Protocole de routage hybride

Les protocoles de routage hybride est une famille de protocoles capables de combiner deux approches proactives et réactives, peu importe le protocole de base. Par exemple, un nœud communique avec ses voisins jusqu'à une certaine distance (par exemple trois ou quatre sauts) en utilisant un protocole de routage proactif, et utilise un protocole réactif pour communiquer avec les nœuds les plus éloignés. En d'autres termes, le nœud choisira la meilleure façon de communiquer avec les autres. Les protocoles hybrides sont conçus pour améliorer l'évolutivité, permettent aux nœuds proches de communiquer les uns avec les autres et de maintenir des itinéraires proactifs proches (du nœud le plus proche) vers la destination et en parallèle aux nœuds éloignés avec l'utilisation d'une stratégie de découverte de route réactif. Cependant, ce type de protocole peut combiner les inconvénients des deux approches : échange de paquet de contrôle et inondation de l'ensemble de réseaux pour chercher une route vers un nœud éloigné.

Comparaison entre les protocoles réactifs et proactifs

L'avantage majeur des protocoles de routage proactif est d'avoir les routes immédiatement disponibles quand les applications en ont besoin, mais cela nécessite un échange régulier de messages. L'avantage de l'approche réactive par rapport au routage proactif est qu'elle génère des coûts de calcul plus faibles et une charge de paquets plus faible puisque la route est découverte seulement s'il y as le besoin et les nœuds ne sont pas obligés d'échanger périodiquement des informations de routage pour maintenir les tables de routage. Cependant, le principal problème avec le routage à la demande réside dans la grande latence à l'étape de découverte du chemin optimal. Lorsqu'un nœud désire envoyer un paquet à une destination inconnue, il doit attendre jusqu'à ce qu'une route vers la destination soit découverte à la demande. Par contre dans le cas des protocoles proactifs l'envoi est immédiat.

Le tableau ci-dessous montre le compromis entre le routage proactif et réactif

	Proactif	Reactif
Découvert de route	les route vers toutes les destination sont disponible	les routes sont découverte a la demande
Délai	Faible	Élevé
Surcharge	Élevé : diffusion fréquente des informations de topologie	faible : moins de paquets de contrôle générer

TABLE 1.2 – *comparaison entre les protocoles réactifs et poactifs*

Classification de routage basé sur l'architecture

Les algorithme de routage sont également classés en deux catégories selon la topologie, I.e. le routage en cluster et le routage plat.

Routage en clusters

Dans un algorithme de routage en cluster, toutes les décisions de routage sont prises par un contrôleur central. La plupart des protocoles de routages en cluster ont une forme de structure hiérarchique où les nœuds sont rassemblé en groupes et ils élisent un chef qui sera le contrôleur central. Ce contrôleur maintient la connectivité du groupe et diffuse fréquemment des informations de routage vers ses nœuds membres. La figure 1.5 illustre la topologie de routage en cluster.

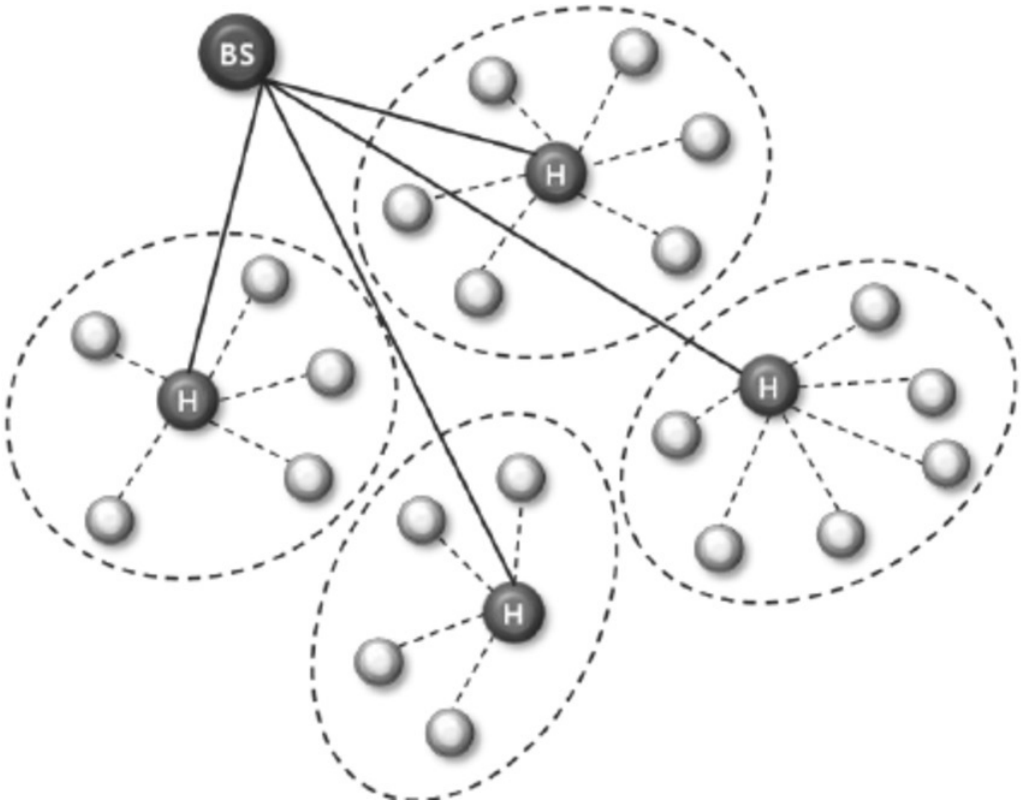

FIGURE 1.5 – *routage en cluster*

Ces techniques de routage peuvent présenter de nombreux inconvénients. Une quantité considérable d'information doit être communiquée aux nœuds leaders, ce qui nécessite l'envoi de données de tous les nœuds du groupe au chef du groupe. Les retards nécessaires pour collecter des informations sur l'état du réseau et pour diffuser les décisions de routage leur sont irréalisables. En matière de mobilité, le mouvement rapide des nœuds peut entraîner une complexité supplémentaire de l'algorithme du réseau. Un membre peut fréquemment rejoindre ou quitter le groupe résultant en un surcoût élève pour maintenir cette structure centralisée. Le problème de la synchronisation peut entraîner une instabilité du réseau lors de mis à jour c'est a dire en cas de changement dans la topologie du réseau. De plus, avoir un point de contrôle unique implique également un point de défaillance unique, une caractéristique très peu souhaitable dans n'importe quel système. Les exemples de routage en cluster sont ZRP (Zygmunt 1997) (Zone Routing Protocole) CBRP (Jiang *et al.* 1999) (Cluster Based Routing Protocol).

Routage plat

Dans le routage plat, tous les nœuds sont équivalents et portent la même responsabilité et il n'y a pas de distinction entre eux .Dans les algorithmes de routage plat le calcul de l'itinéraire est partagé entre les nœuds du réseau. Les nœuds ne sont pas regroupés en grappes ni en une structure hiérarchique. C'est une structure distribuée où tous les nœuds ont les mêmes fonctionnalités et comportements. Les nœuds peuvent prendre

leur propre décision sur la base d'informations locales sans avoir besoin d'être dirigés par un contrôleur central. Cela réduit les frais généraux, et donc, augmente les performances du réseau. De plus, avec ce mécanisme de contrôle décentralisé il n'y a pas de point de défaillance central. Un nœud en panne ou une rupture de lien n'affectera pas le réseau global. Les exemples d'algorithme de routage plat sont DSR (Johnson *et al.* 2003) (Dynamic Source Routing) ,DSDV (Perkins & Bhagwat 1994) (Destination Sequence Distance Vector) et AODV (Perkins *et al.* 2003) (Ad-hoc On Demande Distance Vector).

1.3.5 La sécurité dans les réseaux ad hoc

Les caractéristiques des réseaux ad hoc impact d'une manière visible la sécurité du réseau. Certaines de ces caractéristiques sont le manque d'infrastructure, dynamicité dans la topologie à cause de la mobilité des nœuds et l'accessibilté du réseau aux nœuds légitimes ainsi qu'aux malveillants qui s'introduirent discrètement dans le réseau et nuisent à sécurité du système. Ces caractéristiques uniques mènent à de nombreux problèmes qui affectent le domaine de la sécurité. Le comportement imprévisible des nœuds malveillants et leur rôle dans un environnement distribué posent plusieurs défis non triviaux dans le domaine de la conception de la sécurité. La conception de sécurité dans les MANETs n'est pas seulement axée sur la prévention d'une attaque, elle est également liée à d'autres fonctionnalités comme la performance du réseau et les performances de puissance du nœud.

Le processus de communication des MANETs fonctionne est formé de couches ou il pourrait y avoir de nombreuses attaques dans chacune de ces couches qui entraînent une perte de performance. L'attaque potentielle dans chaque couche décrite dans le tableau 1.3. Les chercheurs à travers le monde ont des approches différentes pour résoudre le problème de sécurité dans chaque couche de communication. Angelos Marnerides (Marnerides 2007) a expliqué qu'en termes de sécurité réseau, le plus important est de savoir comment éviter les attaques directes à partir de la couche inférieure. Sur la base de cette approche, le point essentiel dans les MANETs est de prévoir une infrastructure de sécurité légère qui prend sérieusement en compte les failles qui peuvent se produire sur les couches supérieures. Cette approche modifie généralement le protocole de communication.

En revanche, Saltze et. Al. (Saltzer *et al.* 1984) suggèrent qu'il est préférable d'être plus concerné par la sécurité de bout en bout plutôt que d'appliquer un niveau de sécurité plus faible dans le réseau. Le modèle de sécurité de bout en bout augmente le niveau de la sécurité avant et après l'envoi des données sans interférer avec le protocole de routage réel. Sous cet argument, la couche supérieure est considérée comme plus fiable et plus sûre et chaque mécanisme de sécurité est appliqué de manière à assurer sur les couches inférieures d'interaction quelle que soit la nature non sécurisée du protocole de routage. Notre solution concerne la sécurité dans la couche de protocole de routage.

1.3.6 Les attaques dans Les réseaux ad hoc

Une attaque en informatique est l'exploitation d'une faille (vulnérabilité) d'un système informatique. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

La topologie dynamique, le fonctionnement distribué et les contraintes de ressources sont des caractéristiques uniques des réseaux ad hoc qui augmentent inévitablement la vulnérabilité de ce type de réseau (Prashar & Kapur 2016). De nombreuses caractéristiques pourraient être utilisées pour classer les attaques dans les réseaux ad hoc. Des catégories d'attaque selon l'origine (passive, active), et d'autre selon la nature de l'attaque (externe, interne).

Attaque externes

Les attaques externes sont déclenchées par un nœud malicieux qui n'appartient pas au réseau ou qui n'a pas la permission d'accès. Ces types d'attaques tentent de provoquer une congestion dans le réseau, déni de services (DoS), et injecte de fausse informations de routage pour ensuite rendre le système inutilisable. Les attaques externes empêchent la communication normale du réseau et génèrent un trafic supplémentaires au réseau. Les attaques externes peuvent être classer en deux catégories (Potukuchi & Kant 2017).

Attaques passives

Les MANET sont trés sensibles aux attaques passives. Une attaque passive ne modifie pas les données transmises dans le réseau, elle permet "l'écoute" non autorisée du trafic réseau ou la collecte des données à partir de celui-ci. Un attaquant passif ne perturbe pas le fonctionnement d'un protocole de routage, il tente de découvrir les informations importantes incluse dans le flux de donnée acheminé (Potukuchi & Kant 2017). En général, une attaque passive est lancé par un nœud malveillant qui obtient illigitimement un accès aux ressources réseau sans perturbation du bon fonctionnement du le réseau.

Attaques actives

Les attaques actives sont ont des répercussions plus sévères sur le réseau ce qui perturbe le transfet de flux de données entre les nœuds. Ces attaques actives peuvent être internes ou externes.

Dans ce type d'attaque, un nœud malicieux accède au réseau d'une façon non autorisé en exploitant des vulnérabilités du système afin de mener des infractions telles que la modification des paquets, DoS (déni de service) et la congestion du réseau. Les attaques actives sont généralement lancées par un ou plusieurs nœuds malveillants. Ces nœuds échange les informations de routage par l'injection de fausse information dans le réseau comme ayant le chemin le plus court vers un noeud destinataire (Potukuchi & Kant 2017).

Attaques internes

Les attaques internes sont des attaques déclenchées par des nœuds internes ayant un comportement malveillant. Les attaques internes mènent directement aux attaques sur les nœuds présents dans le réseau et sur les liens entre eux (Potukuchi & Kant 2017; Ranjan *et al.* 2015).

Classification des attaques par couche

Attaques de la couche physique

Un attaquant peut facilement intercepter et lire le contenu d'une trame à partir des signaux radio ouverts en ciblant la couche physique d'un réseau sans fil (Xuan 2007) . Un attaquant peut bloquer ou interférer avec la communication en générant de puissantes transmissions pour inonder les cibles. Le signal de brouillage ne suit pas la définition du protocole et il peut s'agir d'un bruit aléatoire (Wenyuan *et al.* 2005; Dhillon *et al.* 2004).

Attaque de la couche de liaison

Dans cette couche, un attaquant peut générer une trame aléatoire sans importance pour acquérir le canal et provoquer une collision.

Dans cette situation, si le nœud victime continue d'essayer de renvoyer le paquet, il va épuiser son énergie. L'attaquant peut également écouter passivement les trames de la couche de liaison de données. Le protocole de sécurité de la couche liaison "WEP" est vulnérable. Un attaquant lance une attaque passive par écoute et collecte des vecteurs d'initialisation (IV) et ensuite il déduit par cryptanalyse la clé de chiffrement utilisé par le protocole (Hamrioui 2014) .

Attaque de la couche réseau

Dans la couche réseau, l'attaquant agit sur le processus de communication. Plusieurs attaques perturbant le bon fonctionnement de la couche réseau sont connus tels que l'attaque Blackhole, Wormhole, attaque Selfish, attaque Rushing et attaque byzantine.

Attaque de la couche de transport

Dans la couche de transport, un attaquant peut rompre une connexion existant entre services dans deux nœuds en envoyant des faux messages dépassant le numéro de séquence à l'un ou l'autre des nœuds de la connexion. Cela fait que le nœud continue d'envoyer une demande de retransmission pour le message manqué. Un attaquant "session Hijacking" prend la place du nœud victime et prend en charge la session TCP entre la victime et le serveur (Hamrioui 2014) .

Attaque de la couche application

Les attaques pouvant être effectuées dans la couche application, telle que virus, vers, chevaux de Troie, spywares, porte dérobée (i.e. backdoor). Parmi les applications ciblée on trouve FTP, HTTP et SMTP, ou des fichiers

d'application et de données sur la victime (Hamrioui 2014).

Couche	Problème de sécurité
Application	répudiation, Corruption de données, virus, porte de derrière (Backdoor).
Transport	détournement de session, Inondation (SYN)
Réseau	Blackhole, Wormhole, usurpation, byzantine, consommation des ressources
Liaison de donnée	Analyse du trafic, Surveillance, perturbation,
Physique	brouillage du signal, Interception, Écoute
Multi-couche	Déni de service, l'homme au milieu (MITM)

TABLE 1.3 – *les attaque par couche*

Les principales attaques contre les réseaux ad hoc

Il y a plusieurs types d'attaques dans les MANETs (Xuan 2007; Kannhavong *et al.* 2007). Dans cette partie, nous expliquons les principales attaques qui auront le plus de dégâts et de dysfonctionnement dans les réseaux MANET telles que l'attaque de partition, l'attaque de détour, le débordement de table de routage, la réplication de paquet, l'attaque par usurpation d'identité de session (session hijacking), attaque rushing, wormhole, trou noir (Blackhole), et attaque par déni de service (DoS).

Attaque de partition (partition attack)

Un attaquant peut tenter de partitionner le réseau en injectant des fauts paquets de routage pour empêcher qu'un ensemble de nœuds d'atteidre un autre ensemble et ainsi deviser l'ensemble du réseau.

Attaque par détournement

Un attaquant peut tenter d'amener un nœud à utiliser des déviations à travers des routes non optimales. Ainsi un des nœuds coopèrent pour créer une boucle de routage.

Dépassement de la table de routage (Routing table overflow)

L'objectif principal de cette attaque est de créer un débordement de la table de routage et d'empêcher la création de nouvelles routes légitimes, par exemple un attaquant tente de créer des routes vers des nœuds inexistants.

La réplication de paquets (packet replication)

Dans cette attaque un nœud malveillant réplique l'état du paquet pour provoquer une confusion inutile dans le processus de routage. Cela provoque la dépense de beaucoup de ressources des nœuds légitimes, comme consommation excessive de bande passante et d'enrgie disponible pour épuiser les batteries.

Piratage de session (Session hijacking)

Un point faible est que la plupart des processus d'authentification ne sont effectués qu'une seule fois au début d'une session. Un adversaire pourrait essayer d'apparaître comme un nœud authentique et détourne une session déja établie.

Attaque d'usurpation d'identité (identity theft attack)

Les attaquants essaient de copier le comportement ou l'action d'un nœud autorisé pour obtenir les mêmes fonctionnalités que le nœud d'origine, soit pour utiliser les ressources réseau qui pourraient lui être inaccessibles dans des circonstances normales, soit pour tenter de perturber la fonctionnalité réseau en injectant de fausse information de routage (Bayyati 2009). L'attaque de l'homme au milieu (MITM man in the middle)

est dans cette catégorie d'attaque. Un adversaire peut lire ou falsifier des messages entre des utilisateurs légitimes sans que l'un d'eux sache qu'il a été attaqué.

Attaque précipitée (Rushing attack)

Dans ce type d'attaque un nœud malveillant tente de modifier les paquets ROUTE REQUEST, de modifier la liste des nœuds et d'envoyer ce paquet au prochain nœud. Dans AODV, un nœud source demande de trouver un chemin vers la destination en déclenchant un processus de découverte de chemin en inondant les messages RREQ. Dans cette inondation, le nœud intermédiaire traite et transmet uniquement le premier RREQ reçu et rejette le reste. C'est le point où une attaque précipitée (Rushing) aura lieu. Un attaquant peut facilement envoyer un faux RREQ avant qu'un nœud intermédiaire légitime ne transmet l'un des bons RREQ initiés par la source. De cette manière, l'attaquant parvient à créer son propre processus de découverte de fausse route et à gérer cette source comme initiateur si les RREQ n'obtiennent pas de routes utilisables vers la destination. Par conséquent, cela fournit à l'attaquant le contrôle du réseau et perturbe le processus d'établissement de route entre la satation source et la destination.

Wormhole

Un nœud malveillant reçoit le trafic du réseau à partir d'une certaine position et rejoue le trafic sur une position différente. Après l'écoute, le nœud malveillant fait en sorte que les tunnels falsifient les informations de routage vers des nœuds légitimes de manière à réaliser un lien virtuel sous son contrôle (Khabbazian *et al.* 2009). Les nœuds légitimes ne peuvent pas détecter l'expéditeur parceque le nœud malveillant a altéré les en-têtes des paquets de routage. En outre, il a réussi à se rendre invisible pour le reste des nœuds participants. L'attaque pourrait empêcher la découverte de toute route autre que par le trou de ver (wormhole).

Attaque de trou noir (blackhole)

Une attaque de trou noir est structurée par deux phases. La première phase aura lieu lorsque le nœud malveillant exploite le schéma de routage et sous certaines altérations de message (c'est-à-dire, modification d'informations dans le paquet) et se présente comme un nœud ayant un meilleur chemin valide vers une destination. Cette annonce de route est fausse parceque le nœud à l'intention d'intercepter des paquets. La deuxième phase aura lieu après avoir obtenu la route valide, le nœud malveillant crée un trou noir dans le réseau en interceptant les paquets sans effectuer la retransmission. Un attaquant avancé peut supprimer une sélection de paquets et créer un transfert de données de routage sur tout le réseau afin d'amener a une défaillance critique dans le routage. De plus, il pourrait y avoir des modifications mineures sur certains paquets entrants et permettre au nœud malveillant d'être invisible et indétectable par le reste des nœuds.

1.3.7 Le déni de service

DOS est une attaque active qui tente de rendre la ressource indisponible à ses utilisateurs prévus. L'attaquant tente d'empêcher les utilisateurs légitimes d'accéder au service offert par le réseau (Abusalah *et al.* 2008). DOS peut être réalisé de manière classique en inondant les nœuds pour bloquer le système ou d'interrompre son fonctionnement. Sur la couche réseau, un adversaire pourrait lancer une DOS sur les protocoles de routage, cela conduit à une dégradation de la qualité de service (QoS) par la non-retransmission et la suppression de certains paquets du protocole de routage.

Selon l'IETF (Internet Engineering Task Force), RFC 4949 (Shirey 2007) définit l'attaque comme "un acte par lequel une entité tente d'éviter les services de sécurité et de violer la politique de sécurité d'un système". De plus la combinaison de plusieurs attaques peut conduire à une détection difficile. Dans le contexte des MANET, l'attaque DOS ne conduit pas seulement a l'épuisement des ressources, telles que la bande passante, l'énergie de la batterie ou les cycles du processeur (CPU), mais aussi elle isole les noeuds légitimes du réseau (Xing & Wang 2006).

la plupart des travaux de recherche utilisent le terme DoS pour définir certaines classes de menaces de sécurité contre certains services réseau, ou encore avec des attaques d'inondation dans d'autres domaines de sécurité tels que le cloud computing (Chou 2013).

Selon (Vigna *et al.* 2004), les attaques de Dos sont connues comme des attaques de disponibilité, des attaques de sécurité qui menacent la disponibilité des services de routage. Dans le contexte du routage ad hoc, nous définissons DoS comme « une série de comportements malveillants élémentaires pouvant réduire ou rendre les services du routage indisponible complètement ». en d'autres termes, comme illustré dans la figure 1.6 l'attaque DoS n'est pas une attaque, mais un résultat final d'une ou plusieurs séquences d'attaques.

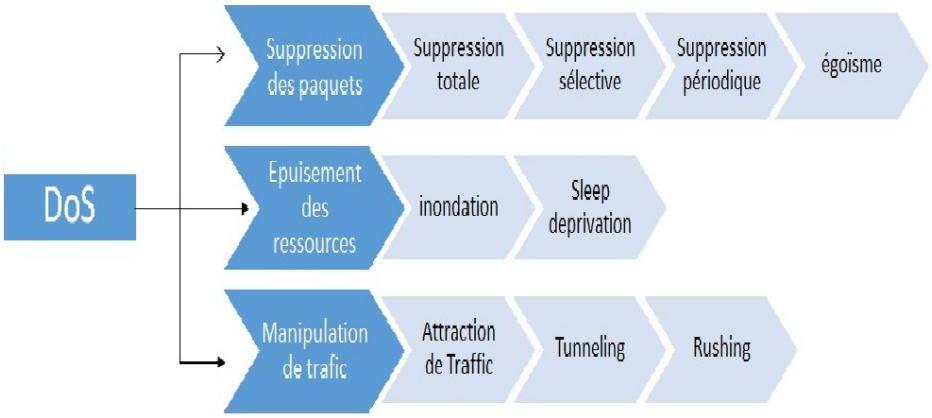

FIGURE 1.6 – *Déni de service*

CONCLUSION DU CHAPITRE

Les réseaux sans fil en général et les MANETs en particulier sont des types de réseaux intéressants et très utilisés dans divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation physique comme le câble, La disponibilité . Les nœuds dans ce type de réseaux communiquent entre eux en multisaut ce qui nècessite un protocole de routage. Ces réseaux utilisent des protocoles de routage permettant d'établir des chemins optimaux toute en utilisant les ressources d'une façon rationnel. Le chapitre suivant introduit un des procotoles de routage les plus connu qui est le protocle OLSR toute en décrivant ces messages de contrôle et son principe de routage. Ce protocole est vulnérable comme tout autre protocole de routage à différents types d'attaques. Dans la suite , nous évoquerions les problèmes de sécurité qui dégrade ces performances comme le déni de service et l'attaque blackhôle.

Le protocole OLSR 2

Sommaire

2.1 OLSR (Optimized Link State Routing Protocol) 25
2.2 Les paquets de contrôle du protocole OLSR 27
2.2.1 HELLO 27
2.2.2 TC (Topology Control) 29
2.2.3 Multiple Interface Declaration (MID) 30
2.2.4 Host and Network Association (HNA) 30
2.3 La selection des MPRs 31
2.4 Construction de la table de routage 33
2.5 la sécurité dans OLSR 34
2.5.1 Les attaques contre le protocole OLSR 36
2.6 Conclusion 40

Optimized Link State Routing Protocol (OLSR) fait partie des protocoles de routages les plus utilisés dans les réseaux ad hoc. OLSR est un protocole proactif pour les réseaux ad hoc permet d'optimiser routage d'état de lien classique par une inondation sélective de paquets en utilisant des nœuds spécifiques appelés relais multipoint (Multi point Relay MPR). Malgré tous les avantages qui présente, ce protocole souffre de problèmes en termes de sécurité et de protection contre les attaques. Il est vulnérable comme tout autre protocole de routage à différents types d'attaques telles que l'usurpation d'identité, l'usurpation des liens, corruption des données, le déni de service et l'attaque blackhole.

2.1 OLSR (Optimized Link State Routing Protocol)

OLSR est un protocole de routage proactif pour les réseaux mobiles ad hoc (Clausen & Jaquet 2003). Le protocole hérite de la stabilité d'un algorithme d'état de lien classique avec l'avantage d'avoir des itinéraires immédiatement disponibles en cas de besoin en raison de son caractère proactif. OLSR est une version optimisée du routage à état de lien classique adapté aux réseaux mobiles ad hoc.

OLSR minimise l'inondation classique du trafic de contrôle par une inondation sélective en utilisant seulement des nœuds spécifiques appelés MPR pour effectuer la retransmission des messages de contrôle voir figure 2.1. Cette technique réduit considérablement le nombre de retransmissions requis pour inonder un message à tous les nœuds du réseau(Abdalla *et al.* 2011).

Les nœuds MPR réduisent le nombre des paquets dupliqués diffusés sur le réseau et seulement eux sont autorisés à diffuser les messages de contrôle, les autres nœuds utilisent ces messages pour construire leurs vue globale du réseau. Chaque nœud choisit son MPR parmi ces voisins symétrique. Ils comptent sur ces nœuds MPR pour atteindre les voisins symétriques à deux sauts. Chaque nœud MPR maintient la liste des nœuds qui l'ont sélectionnée comme MPR. Cette liste est appelée liste de sélection MPR.

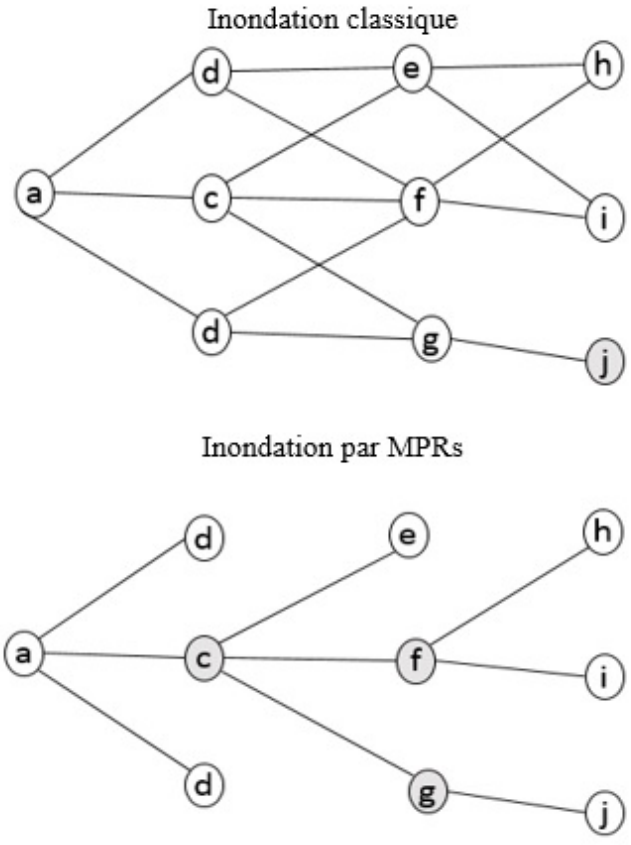

Figure 2.1 – *Optimisation de l'inondation en utilisant les MPRs*

OLSR peut également optimiser la réactivité aux changements topologiques en réduisant l'intervalle de temps pour la transmission d'un message de contrôle périodique(Saddiki *et al.* 2017).

En outre, comme OLSR maintient continuellement des itinéraires à toutes destinations dans le réseau, le protocole est bénéfique pour le trafic modèle où un grand nombre de nœuds communiquent avec un autre un grand sous-ensemble de nœuds.

Le protocole est particulièrement adapté pour les réseaux denses a faible mobilité, car l'optimisation effectuée à l'aide de MPR fonctionne bien dans ce contexte. Plus le réseau est grand et dense, plus l'optimisation peut être réalisée par rapport à l'algorithme d'état de liaison classique (Abdalla *et al.* 2011; Raffo *et al.* 2005; Saddiki *et al.* 2017). La figure 2.2 ci-dessous illustre l'optimisation apportée par le protocole OLSR et la technique des MPRs dans un contexte plus surchargé.

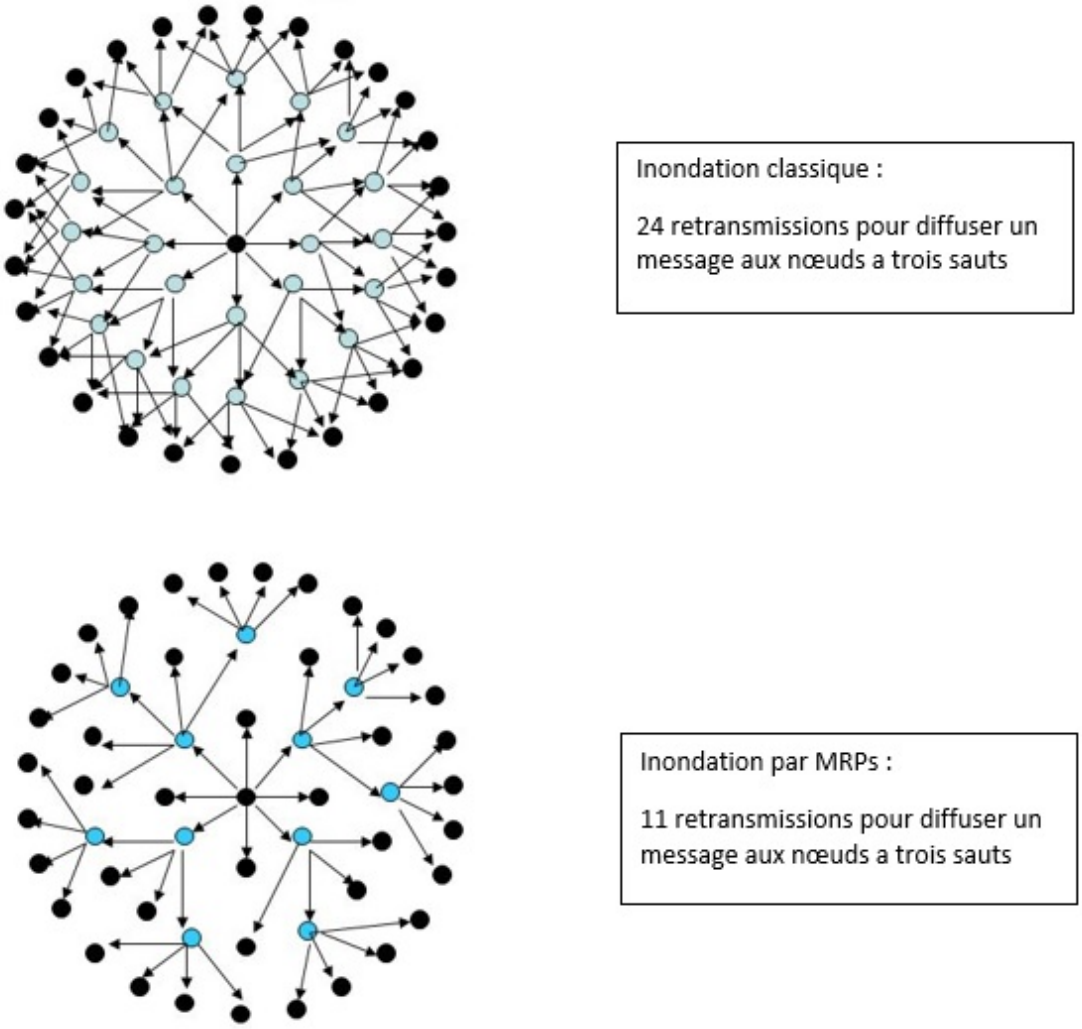

FIGURE 2.2 – *Optimisation de l'inondation en utilisant les MPRs*

OLSR est conçu pour fonctionner de manière complètement distribuée et ne dépend d'aucune entité centrale (Clausen & Jaquet 2003). Le protocole ne demande pas de transmission fiable des messages de contrôle. Chaque nœud envoie les messages de contrôles périodiquement, et peut donc supporter une perte raisonnable de certains de ces messages. De telles pertes se produisent fréquemment dans les réseaux de radiocommunication en raison des collisions, ainsi que d'autres problèmes de transmission.

En outre, OLSR prend en charge les extensions de protocoles tels que le fonctionnement en mode veille et le routage multicast. Ces extensions peuvent être introduites comme des ajouts au protocole sans violé la compatibilité avec les versions antérieures. OLSR utilise le protocole UDP port 698 attribué par IANA (Internet assigned Numbers Authority) pour une utilisation exclusive du protocole. OLSR ne nécessite aucune modification du format des paquets IP. Ainsi toute la pile IP existante peut être utilisée tel quel le protocole interagit uniquement avec gestion de table de routage.

2.2 Les paquets de contrôle du protocole OLSR

OLSR suit la logique du routage à état de liens, qui peut être divisé en deux branches principales. La première étape est la découverte du voisinage par l'échange d'informations sur l'état de liens de chaque nœud. La deuxième étape est la diffusion de la topologie et la construction de la table de routage complète pour chaque nœud du réseau. Afin d'assurer les deux principales fonctionnalités, OLSR diffuse périodiquement et principalement deux messages de contrôle pour indiquer l'état de la topologie : Le message HELLO qui est diffusé par tous les nœuds pour détecter les voisins à un et à deux sauts, détecter la direction du lieu (symétrique ou asymétrique) ainsi que la selection des MPRs. Le message de contrôle de topologie (TC) est diffusé uniquement par les nœuds MPR, et il indique la liste des voisins qui ont choisi ce nœud comme MPR. Ce message de contrôle est utilisé pour calculer les tables de routage(Clausen & Jaquet 2003; Raffo *et al.* 2005).

2.2.1 HELLO

Un message HELLO est le message diffusé périodiquement par l'ensemble des nœuds dans le réseau qui est utilisé pour la détection des voisins et la sélection MPR. Dans OLSR, chaque nœud génère un message HELLO périodiquement. Le message HELLO d'un nœud contient sa propre adresse et la liste de ses voisins à un saut. En échangeant des messages HELLO, chaque nœud peut apprendre une topologie complète jusqu'à deux sauts. Les messages HELLO sont échangés localement par les nœuds voisins et ils ne sont pas transmisent plus loin qu'un voisin direct. La figure ci-dessus représente la structure globale du message HELLO.

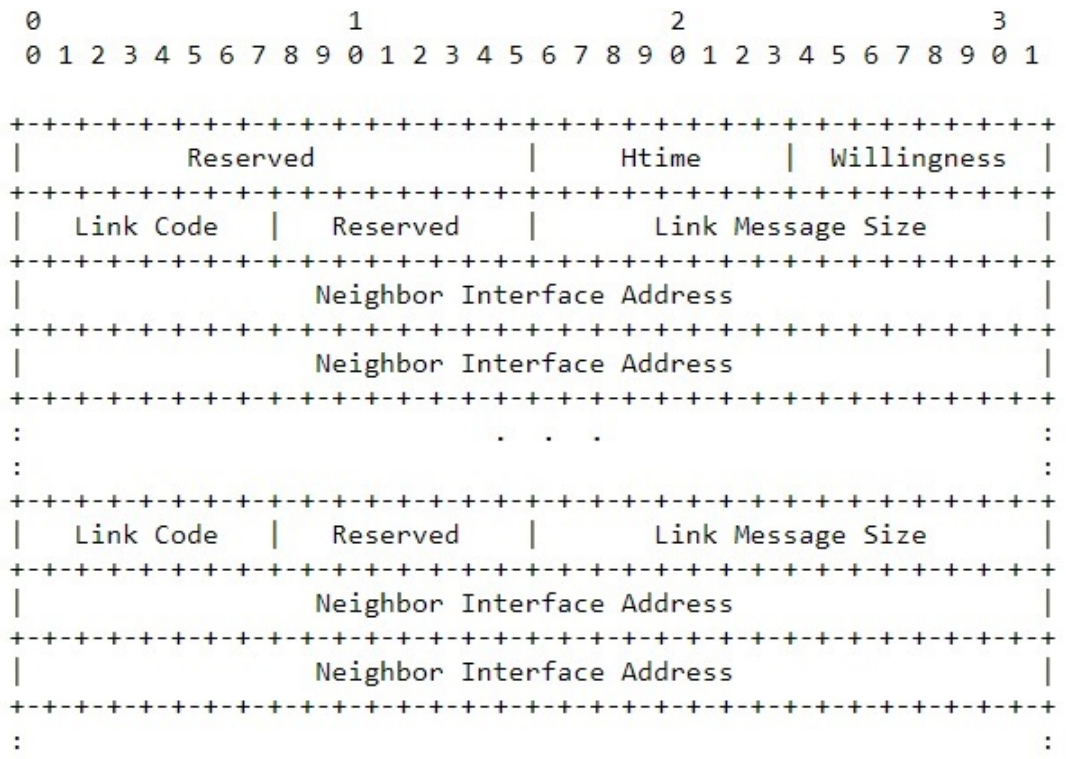

FIGURE 2.3 – *Structure du paquet HELLO*

Réserved : Ce champ doit être défini sur "oooooooooooo" pour être conforme à cette spécification.

HTime : Ce champ représente l'intervalle d'émission du HELLO utilisé par le nœud sur cette interface particulière, c'est-à-dire, le temps avant la transmission du prochain HELLO. L'émission de l'intervale du message HELLO est représenté par sa mantisse (quatre bits les plus élevés de Champ Htime 'a') et par son exposant (les quatre bits les plus bas de Htime champ 'b'). En d'autres termes :

$HTime = C * (1 + a/16) * 2^b$ [en secondes]

Willingness : Ce champ spécifie la volonté d'un nœud de porter et acheminer le trafic pour les autres nœuds. Un nœud avec willingness WILL NEVER ne doit jamais être sélectionné comme MPR. Un nœud avec willingness WILL ALWAYS doit toujours être sélectionné comme MPR. Par défaut, un nœud devra annoncer un Willingess de WILL DEFAULT.

Link Code : ce champ spécifie des informations sur le lien entre l'interface de l'expéditeur et la liste des voisins. Il spécifie également des informations sur l'état du voisin. Les codes non connus par un nœud sont ignorés en mode silencieux.

Link Message Size : La taille du message de lien, compté en octets et mesuré depuis le début du champ "Link Code" et jusqu'au prochain "Link Code" .

Neighbor Interface Address : représente l'adresse d'une interface d'un nœud voisin.

2.2.2 TC (Topology Control)

Un message TC est utilisé pour construire la table de routage. En OLSR, chaque nœud MPR génère et diffuse périodiquement des messages TC. Ces messages contiennent la liste des sélecteur MPR (MPR Selector Set). En OLSR, seuls les nœuds MPR sont responsables de la transmission et la retransmission des messages TC. Ainsi, à la réception des messages TC de tous les nœuds MPR, chaque nœud peut avoir une vue globale sur la topologie du réseau et peut construire une route vers chaque nœud dans le réseau. La figure 2.4 représente la structure globale du message TC.

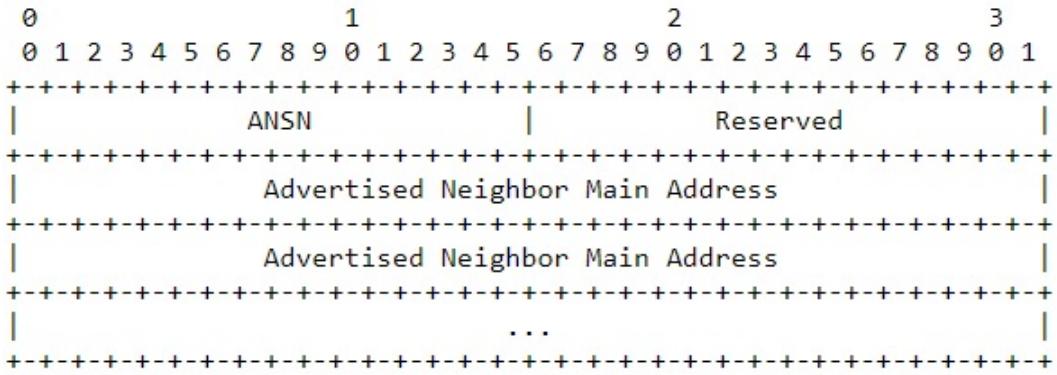

FIGURE 2.4 – *Structure du paquet TC*

Advertised Neighbor Sequence Number (ANSN) : un numéro de séquence est associé au voisin annoncé. Chaque fois qu'un nœud détecte un changement, il incrémente ce numéro de séquence. Ce numéro est envoyé dans ce champ ANSN du message TC pour garder une trace des informations les plus récentes. Lorsqu'un nœud reçoit un message TC, il peut décider sur la base de ce champ si les informations reçues concernant les voisins annoncés par le nœud d'origine sont plus récents que ceux qu'il à déjà.

Reserved : Le champ est réservé et doit être défini sur "0000000000000000" pour la conformité avec ce document.

Advertised Neighbor Main Address : Ce champ contient l'adresse principale du nœud voisin qui a permis la sélection de ce nœud comme MPRs (MPR selector).

2.2.3 Multiple Interface Declaration (MID)

Il existe également un autre type de message appelé Multiple Interface Declaration (MID). Ce message est utilisé pour informer les autres nœuds que le nœud actuel a plus d'une interface. Chaque nœud avec plusieurs interfaces doit annoncer périodiquement les informations décrivant sa configuration d'interfaces aux autres noeuds dans le réseau. Ceci est accompli en inondant le message MID à tous les nœuds du réseau via le mécanisme d'inondation par MPR. La figure 2.5 ci-dessus représente la structure globale du message MID.

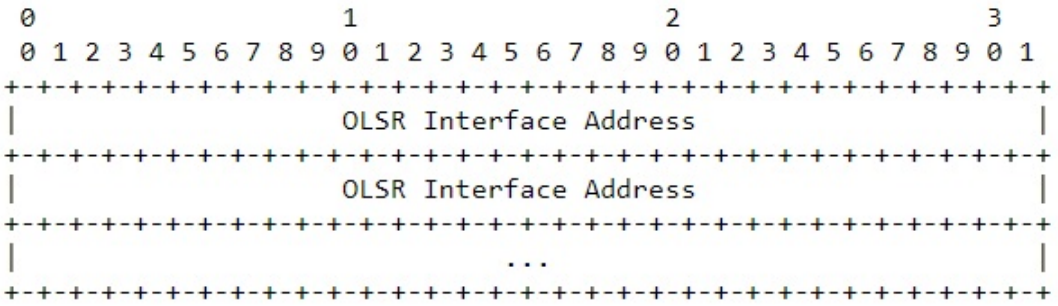

FIGURE 2.5 – *Structure du paquet MID*

OLSR Interface Address Ce champ contient l'adresse des interfaces OLSR supplémentaires du nœud, en excluant l'adresse principale des nœuds qui indique dans l'adresse de l'expéditeur.

2.2.4 Host and Network Association (HNA)

le protocole OLSR a ajouté également un autre type de message appelé HNA (Host and Network Association) dans le but de déclarer les sous-réseaux et les hôtes qui ne fassent pas partie du réseau ad hoc joignable par un noeud qui peut jouer le rôle de passerelle. Ce message est émis périodiquement par le noeud externe du réseau Manet contenant suffisamment d'informations pour que les destinataires construisent des table de routage appropriée. Le message HNA permet d'ajouter la possibilité d'injecter une information du routage externe dans un réseau MANET. Ce message contient deux champs :

Network Address L'adresse réseau du réseau associé.

Netmask Le masque de réseau, correspondant à l'adresse réseau correspondant.

2.3 La selection des MPRs

Le concept des MPRs est utilisé pour réduire la surcharge des messages d'inondation dans le réseau en minimisant la diffusion en double dans la même région. L'ensemble MPR est un sous-ensemble des voisins symétriques avec une cardinalité minimale pour atteindre l'ensemble de tous les nœuds à deux sauts avec des liens symétriques. Chaque nœud du réseau sélectionne un ensemble de nœuds dans son voisinage symétrique à un saut pouvant retransmettre ses messages. Cet ensemble de nœuds voisins sélectionnés est appelé l'ensemble des relais multipoint (MPR set) de ce noeud. Les voisins directs du noeud qui n'appartienne pas à l'ensemble des MPRs peuvent recevoir et traiter les messages diffusés et ils ne sont pas autorisés à retransmettre les messages reçus.

Après le processus d'échange des messages Hello, chaque nœud découvre l'ensemble des voisins directs, ainsi qu'au voisin à deux sauts, et à travers ces informations, tous les nœuds calculent l'ensemble MPR selon le protocole d'origine d'écrit dans RFC3626 comme suit (Clausen & Jaquet 2003) :

- Définir N comme le sous-ensemble des voisins symétriques, et N2 comme le sous-ensemble du voisinage symétrique à deux sauts, à l'exclusion des nœuds accessibles uniquement par voisins symétriques ayant le champ Willingess égale à WILL NEVER et les noeuds membres de N.
- Calculer le degré de chaque nœud dans le sous-ensemble N (degré (y) est le nombre de voisins du noeud y excluant le noeud effectuant le calcul et le noeud membres du sous-ensemble N).
- Ajouter à l'ensemble des MPRs les nœuds dans N, qui sont les seuls nœuds à fournir une accessibilité à un nœud dans N2 et supprimer tous les nœuds couverts à partir de N2.
- tant que l'ensemble N2 n'est pas vide
  1. Calculer l'accessibilité des membres de N (le nombre de noeud atteignable à partir de N2).
  2. Ajouter à l'ensemble des MPRs le noeud avec une haute atteignabilité. Dans le cas de plusieurs choix, sélectionnez le nœud avec le plus haut degré.
  3. enlever tous les nœuds couverts de l'ensmbe N2.

La figure 2.6 illuste les étapes de l'algorithme de la sélection des nœuds MPRs.

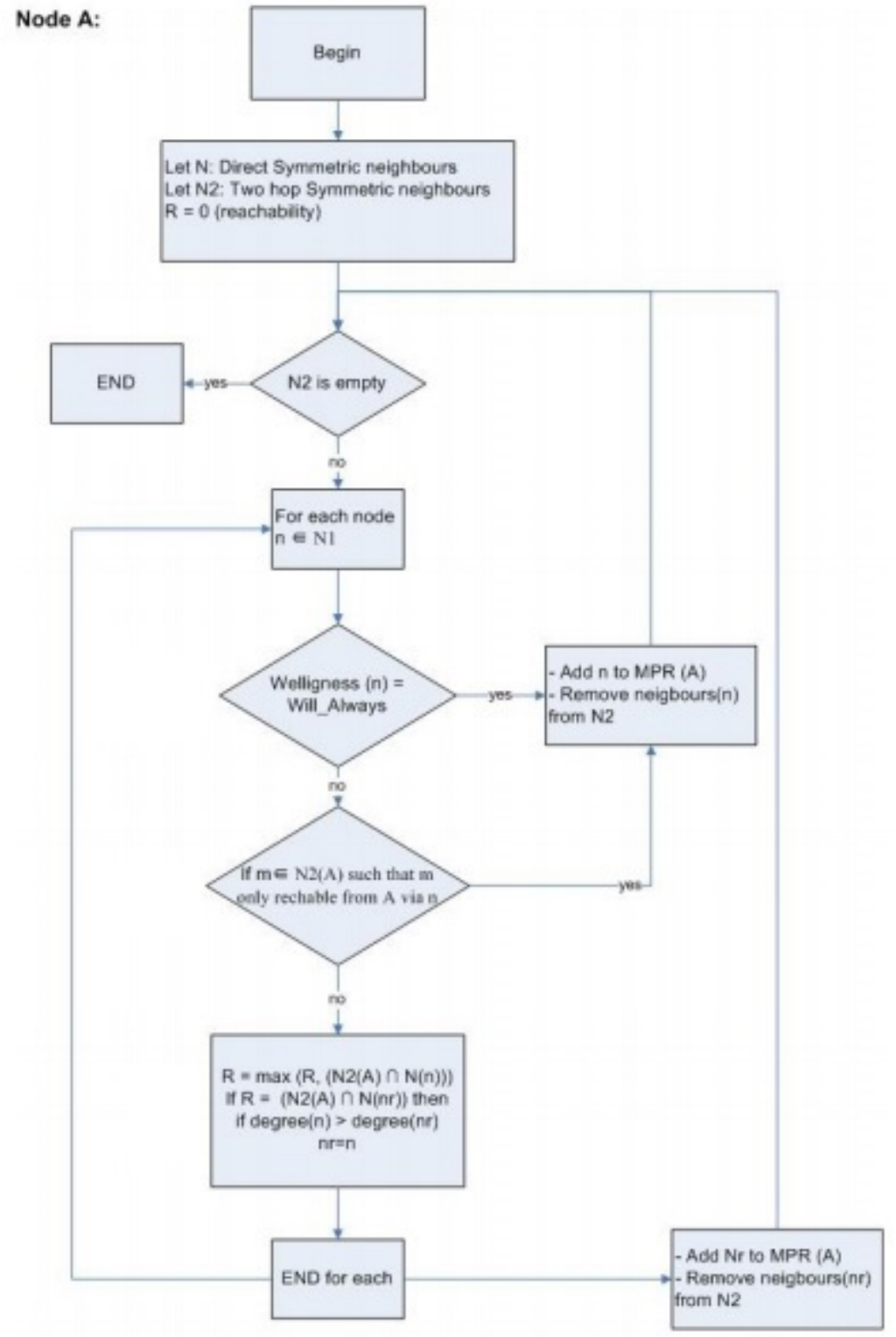

FIGURE 2.6 – *La sélection des MPRs*

2.4 Construction de la table de routage

OLSR est un protocole de routage proactive ce qui fait que les routes doivent être établi avant la demande et la table de routage doit être complète (Clausen & Jaquet 2003; Singh *et al.* 2018). Chaque noeud doit avoir une table de routage complète avec une route vers chaque autre noeud dans le réseau. Pour calculer la table de routage, le protocole OLSR a besoin d'échanger les messages HELLO entre les noeuds voisins directs pour détecter l'ensemble de voisinages à un et à deux sauts, et d'inonder le réseau d'une manière optimisée avec les paquets TC qui sont générés, transmit et retransmit seulement par les noeuds sélectionnés en tant que MPRs. La table de routage contient les champs suivants :

R.dest.addr : L'adresse du noeud de distination

R.next.addr : L'adresse du prochain saut

R.dist : La metric en nombre de sauts

R.iface.addr : L'adresse du noeud local.

Afin de remplir les tuples de tous les noeuds, c'est-à-dire calculer et recalculer la table de routage complètent de chaque noeud, l'algorithme de routage suit les étapes suivantes :

— Toutes les entrées de la table de routage sont supprimées.
— Ajouter les nouvelles entrées de routage en commençant par les voisin direct avec un liens symétrique en tant que nœuds de destination. Pour chaque tuple les informations sont rempli comme suite :

  R.dest.addr = l'adresse du voisin direct ;

  R.next.addr = l'adresse du voisin direct ;

  R.dist = 1 ;

  R.iface.addr = l'adresse du noeud local ;

— L'étape suivante consiste à remplir les tuples des noeuds voisins à deux sauts. Les informations de routage sont remplies comme suite :

  R.dest.addr = l'adresse du voisin à 2 sauts ;

  R.next.addr = R.next.addr de l'entrée dans la table de routage tel que : R.dest.addr = N.neighbor.main.addr du tuple à deux sauts ;

R.dist = 2 ;

R.iface.addr = l'adresse R.iface.addr de l'entrée dans la table de routage tel que : R.dest.addr == N.neighbor.main.addr du tuple à deux sauts ;

— L'étape suivante consiste à remplir les tuple de 3 sauts et plus d'ou l'information provient des paquets TC reçus via les noeuds MPRs. Pour chaque entrée dans la table de topologie, si T.dest.addr ne correspond pas à R.dest.addr de toute entrée d'itinéraire dans la table de routage et son T.last.addr correspond à R.dest.addr d'une entrée de route, si elle n'existe pas dans la table de routage, une nouvelle entrée de route doit être enregistrée dans la table de routage où :

R.dest.addr = l'adresse de destination dans la tuple à ajouter.

R.next.addr = l'adresse du prochain saut via l'entrée de topologie.

R.dist = h + 1 (en commençant par h=2 pour les voisin à 3 saut et incrementé à chaque fois par 1

R.iface.addr = l'adresse de l'interface local.

2.5 LA SÉCURITÉ DANS OLSR

OLSR devient un protocole de routage populaire dans les MANET(Abdalla *et al.* 2011; Raffo *et al.* 2005). Le protocole OLSR a de nombreux avantages principalement, réduire le nombre de paquets diffusés en double sur le réseau en utilisant des nœuds MPR, ainsi que la disponibilité des routes instantanément lors d'une demande et avoir une vue global sur la topologie du réseau ce qui est considéré comme l'un des principaux avantages des protocoles de routage proatifs. Cependant, le manque d'infrastructure (il n'est pas nécessaire de passer par un point d'accès pour se connecter au réseau) et l'utilisation d'une topologie dynamique posent de nombreux problèmes affectant le domaine de la sécurité. D'autre part, la technique d'inondation utilisant les nœuds MPR rend le protocole moins sécurisé car seuls ces nœuds sont responsables de l'information. En d'autre termes seulement une seule connectivité utile a été exploitée.

Les caractéristiques des réseaux Manets en général et les caractéristiques du protocole OLSR en particulier, ainsi que la possibilité d'existence des noeuds malveillants dans les réseaux rend le protocole de plus en plus vulnérable aux différentes menaces et aux nombreux types d'attaque qui affecte le bon fonctionnement du réseau (Junhai *et al.* 2009; Raffo *et al.* 2005; Saddiki *et al.* 2017). Les attaques contre le protocole OLSR peuvent être classées en deux grandes familles :

— Les attaques contre les protocoles proactifs telles que :

  — Le sniffing : C'est l'attaque la plus classique. Par définition, un réseau sans fil est ouvert, c'est à dire non sécurisé (Kannhavong *et al.* 2007). Cette attaque consiste à écouter les transmissions des différents utilisateurs du réseau sans fil, et de récupérer n'importe qu'elle données transitant sur le réseau si celles-ci ne sont pas cryptées. Il s'agit d'une attaque sur la confidentialité. Pour un cas particulier la menace est faible car les données sont rarement confidentielles(Clausen & Jaquet 2003) . En revanche, dans le cas d'un réseau d'entreprise, l'enjeu stratégique peut être très important.
  — le brouillage : le protocole OLSR est vulnérable au brouillage, non seulement le protocole OLSR mais tous les autres protocoles de routage utilisés sur réseaux ad hoc. Le brouillage est une attaque informatique qui consiste à générer une grande quantité d'interférences radio. Le bruit généré par l'attaquant rend l'échange des informations utiles entre les nœuds très difficile voire impossible, notamment leurs routes respectives, et empêche ainsi la construction d'un réseau.
  — Le débordement de la table de routage (Routing table overflow) : le protocole OLSR est vulnérable à cette attaque dont le principe est de créer un débordement de la table de routage en créant des routes vers des nœuds inexistants dans les réseaux. Le but de cette attaque est d'empêcher la création de nouvelles routes légitimes.
  — le déni de service : le déni de service consiste à rendre inopérant un système afin d'en empêcher l'accès à des utilisateurs réguliers. Cela consiste, par exemple, à saturer le réseau en multipliant artificiellement le nombre de demandes et cela peut provoquer un affaiblissement rapide des batteries. Ce type d'attaque est particulièrement difficile à déceler. Les impacts ne sont pas francs et la localisation géographique de la source nécessite des équipements d'analyse radio sophistiqués.
  — Jamming : Le jamming est une attaque très connue qui s'en prend à la communication sans fil. Lors d'une attaque de jamming, un noeud malicieux envoie des signaux sur la même fréquence utilisée par le réseau sans fil pour brouiller les ondes radio (Sahu *et al.* 2016; Baiad *et al.* 2016; Vanamala & Rao 2017; Alagha *et al.* 2001; Murthy & Manoj 2004). Les nœuds légitimes du réseau ne peuvent plus communiquer du fait de ce brouillage radio. Or, un réseau sans accès au médium (le jamming) est une attaque de type déni de service du fait qu'elle rend le réseau hors-service . Cette attaque est en général exécutée à l'aide d'un dispositif plus performant que de simples nœuds à cause des exigences énergétiques nécessaires et pour arriver à perturber le réseau de façon continue.
  — le spooffing : le spooffing consiste à usurper soit l'adresse IP, soit l'adresse MAC d'une autre machine. En modifiant l'adresse IP source dans l'entête du paquet, le récepteur croira avoir reçu

un paquet de cette machine. Si le serveur considérait cette machine comme noeud de confiance, beaucoup de données sensibles pourront être consultées, modifiées, voire même supprimées.

— insertion de boucles infinies : ce type d'attaque est exécuté par deux ou plusieurs nœuds malveillants dans le réseau. Cette attaque consiste à envoyer un nombre infini de messages sur le réseau afin de saturer le réseau. les attaquants envoient sans cesse des messages dans le réseau comme un jeu de ping-pong, les nœuds légitimes vont consommer leur énergie et le réseau va être saturé (Alagha *et al.* 2001; Murthy & Manoj 2004).

2.5.1 Les attaques contre le protocole OLSR

Génération incorrecte du trafic par usurpation d'identité : le but du noeud malveillant est de s'insérer dans le protocole de routage et de perturber la topologie du réseau , dans cette attaque le noeud malveillant prétend en être un autre en usurpant l'identité (Spoofing de l'adresse du noeud), en envyant un faut message HELLO à son voisin. La figure 2.7 montre que le noeud 'c' usurpe l'identité du noeud 'b', les noeuds 'd', 'e' sont persuadés d'être connectés au noeud 'b', mais en fait il échange avec le noeud c, qui prétend être le noeud ' b '.

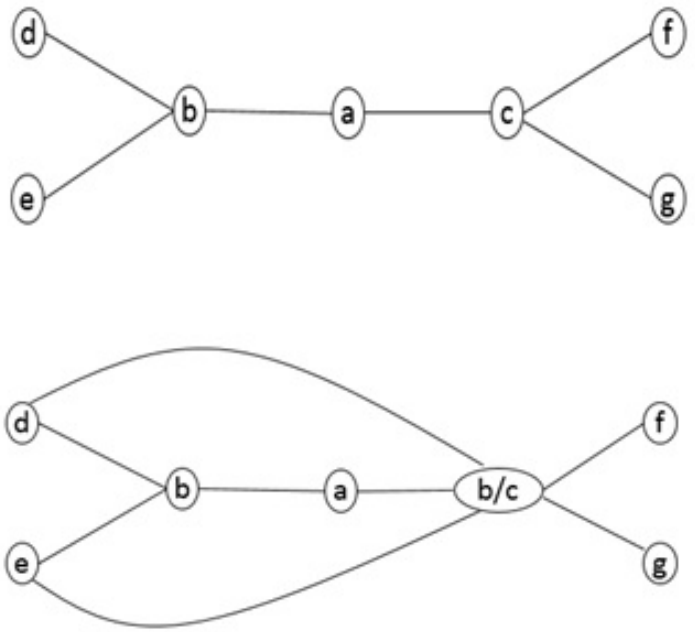

FIGURE 2.7 – *usurpation d'identité*

Génération incorrecte du trafic par usurpation de liens : dans ce type d'attaque un nœud malveillant peut forcer sa sélection en tant que MPR en ajoutant dans son propre message Hello un faux lien vers un nœud non existant dans le réseau. Par conséquent, le nœud cible tombe dans

une situation où le seul moyen d'atteindre la destination est de passer par le nœud attaquant. En se référant au processus de sélection, il doit ajouter ce noeud à l'ensemble MPR. Par conséquent, l'attaquant peut intercepter tous les messages et qui peut également modifier ou supprimer les paquets reçus. la figure 2.8 illustre le sénario le l'attaque.

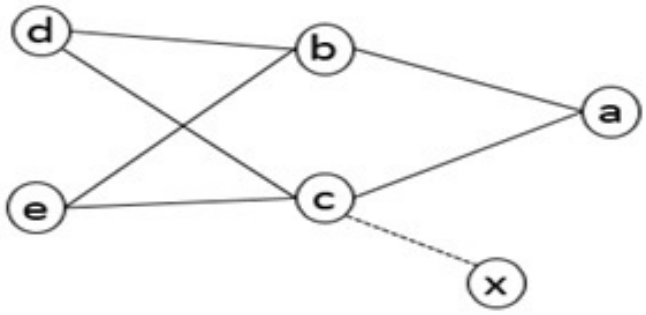

FIGURE 2.8 – *usurpation de liens 1*

On peut lancer une autre attaque fondée sur le même principe que la dernière décrit ci-avant, celle-ci est également basée sur l'usurpation de lien dans le but d'être sélectionné en tant que nœud MPR. Dans cette attaque, après avoir obtenue l'information des voisins à deux sauts, le nœud malveillant annonce dans son propre message HELLO un ensemble de voisinages symétriques avec les voisins à un et deux sauts. Cette fausse information donne plus de poids au nœud malicieux durant le processus de sélection des MPR. En conséquence, les oeuds cibles choisissent cet attaquant pour transmettre des paquets. En revanche, l'attaquant peut mal utiliser ou rejeter les paquets reçus. La figure ci-dessus illustre le sénario de l'attaque.

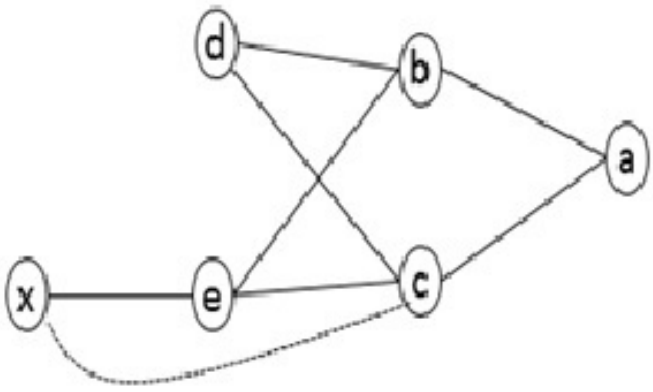

FIGURE 2.9 – *usurpation de liens 2*

On peut lancer une autre attaque dans la même famille par la création des faux liens. dans le protocole OLSR chaque nœud sélectionne ses MPR pour atteindre tous les voisins symétriques à deux sauts. Donc, si un noeud malicieux veut s'assurer sa sélection comme MPR, il peut déclarer des faux liens avec l'ensemble des voisins à deux sauts de la cible, c'est-à-dire avec ses trois sauts voisins . Dans cette attaque, la première étape consiste à détecter l'ensemble de voisinages à trois sauts à partir du paquet TC reçu, puis à générer un message HELLO contenant cet ensemble de nœuds.

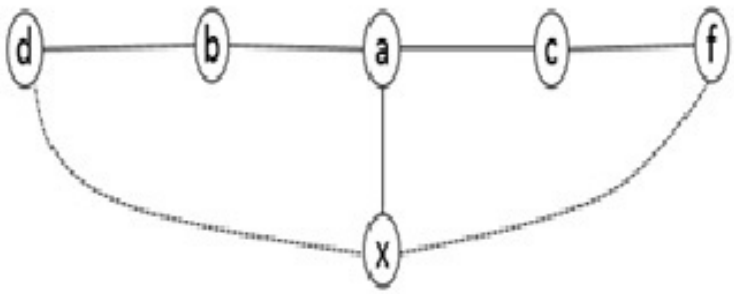

FIGURE 2.10 – *usurpation de liens 3*

Wormhole une attaque wormhole ou de trou de ver (Adnane *et al.* 2013) est l'une des attaques les plus sophistiquées et sévères dans les MANET. Dans cette attaque, une paire d'attaquants enregistre les paquets à un endroit et répond à un autre emplacement utilisant un réseau privé à haute vitesse. La gravité de cette attaque est qu'elle peut être lancée contre toutes les communications incluant ceux qui fourni l'authenticité et la confidentialité. l'attaque de trou de vers (Abusalah *et al.* 2008) utilise une connexion hors bande entre deux noeuds malveillants physiquement éloignés, on appelle cette connexion un tunnel wormhole . Ce tunnel peut être installé via une connexion filaire reliant les deux attaquants aux bouts du tunnel ou grâce à une radio sophistiquée qui possède une meilleure portée que celles des autres noeuds . Dans la pratique, cette attaque devient intéressante quand les noeuds sont physiquement éloignés (une dizaine de sauts). Cette attaque permet de créer beaucoup de faux liens et de fausses routes en faisant croire à des noeuds qu'ils sont peu éloignés afin de dérouter une partie du trafic vers ce canal malicieux. Le but de l'attaquant est donc créer une fausse topologie logique voire de détourner une grande partie du trafic permettant ensuite de lancer d'autres types d'attaques comme des attaques par sélective forwarding ou des dénis de service. la figure ci-dessus montre un exemple de l'attaque wormhole. Dans la figure, nous supposons que les nœuds X1 et X2 sont deux attaquants et que le noeud S est la cible.

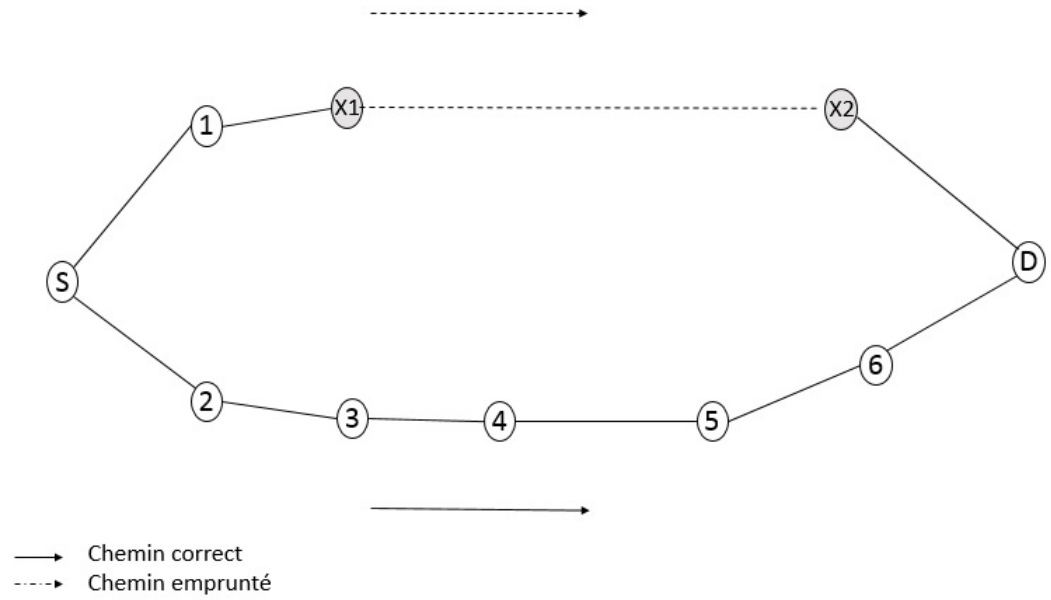

FIGURE 2.11 – *l'attaque Wormhole*

Blackhole l'attaque Blackhole ou l'attaque de trou noir est une attaque classée comme un attaque active dangereuse comme le déni de service. Cette attaque a un grand effet sur les protocoles proactifs (Murthy & Manjo 2004) , notamment sur OLSR. cette attaque est structurée en deux phases, La première phase aura lieu lorsque le nœud malveillant exploite le schéma de routage et sous certaines altérations de message (c'est-à-dire, modification d'informations dans le paquet) pour forcer sa sélection en tant que MPR (en générant un faux message HELLO avec modification de champ Welligness, usurpation d'identité, usurpation de liens). La deuxième phase aura lieu après avoir été sélectionné comme MPR, le noeud malicieux crée un trou noir dans le réseau en interceptant les paquets sans effectuer la retransmission. Dans une attaque plus sévère, le noeud malicieux supprime une partie de paquets et crée un transfert de données de routage sur tout le réseau afin d'amener à une défaillance critique dans le routage.

2.6 Conclusion

Dans ce chapitre nous avons presenter le protocole OLSR en détaille. Nous avons commencé par les caractéristiques du protocole, par la suite presenté les differents message de contrôle pour avoir la topologie du réseau ainsi que l'algorithme de sélection des MPRs, enfin on a discuté l'aspect sécuritaire du protocole OLSR et les vulnérabilités aux attaques.

Dans le chapitre suivant nous discuterons les solutions proposées pour sécuriser le protocole OLSR contre les différentes attaques qui peuvent ruiner au comportement du protocole et nous présenterons un type d'attaque blackhole catégorisée comme attaque déni de service.

Contribution I : Mécanisme de sécurité contre l'attaque BlackHole

3

Sommaire

3.1 Etat de l'art 42
3.2 Modèle de l'attaque blackhole contre le protocole OLSR 48
3.3 Intérêt de la simulation : 50
3.3.1 Network Simulator 2 (NS2) 50
3.3.2 La mesure de performance 52
3.4 Simulation de l'attaque 53
3.5 Mécanisme de sécurité 55
3.5.1 Phase I 55
3.5.2 Phase II 57
3.6 Simulation et analyse 61
Conclusion 64

MANET est un réseau sans fil formé par la coopération d'un nombre arbitraire de nœuds qui se déplaçant de manière aléatoire dans des directions arbitraires. La communication entre les nœuds est établie en utilisant des protocoles de routage. Dans le scénario d'un réseau dense à faible mobilité, nous utilisons des protocoles de routage proactifs. Le protocole OLSR est l'un des protocoles de routage proactifs utilisés. Bien que le protocole OLSR présente de nombreux avantages, il reste vulnérable aux attaques telles que le trou noir. Dans ce chapitre, nous commençons par un état de l'art sur les travaux présentés, ensuite nous présentons une attaque du type blackhole dans laquelle le nœud malveillant annonce des faux liens avec ces voisins à trois sauts , ce qui peut conduire à la sélection de ce nœud comme MPR. une fois sélectionné, il peut détourner tout le trafic. Nous démontrons la gravité de cette attaque grâce à une simulation détaillée en utilisant le simulateur NS2. Après cela, nous présentons un mécanisme de sécurité pour détecter et isoler les nœuds malveillants.

3.1 Etat de l'art

Avec l'utilisation croissante des réseaux sans fil dans les comunications, la sécurité est devenue une question importante. Récemment, il ya eu beaucoup de recherches sur protocoles de sécurité, cependant, ces réseaux reste toujours vulnérables aux attaques telles que le déni de service.

Beaucoup de travaux antérieurs sur les attaques ont principalement porté sur les méthodes cryptographique. Dans Dhillon et al. (Dhillon *et al.* 2004), pour sécuriser le protocole OLSR, les auteurs ont mis en oeuvre une autorité de certification (CA certificate Authority) entièrement distribuée et ils ont intégré avec le protocole OLSR. Dans ce schéma chaque nœud demande à une autorité de certification d'authentifier ces clés. la figure 3.1 ci-dessous représente le schéma proposé.

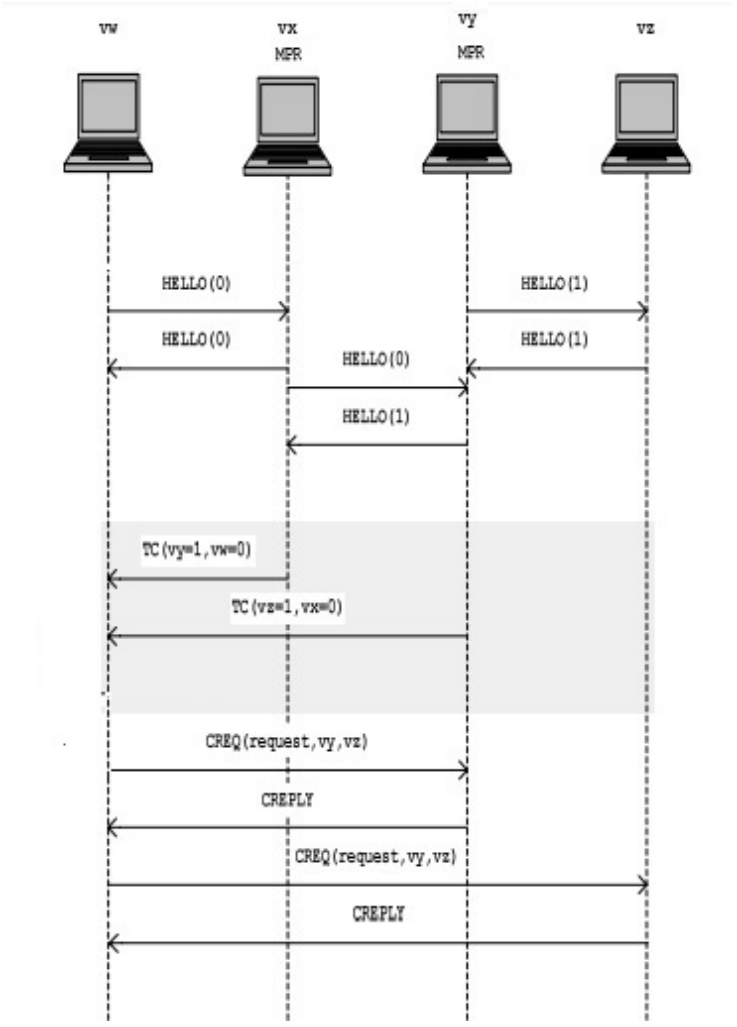

Figure 3.1 – *Schéma d'authentification*

Les auteurs supposent que le réseau est initialisé avec au moins k actionnaires. Un actionnaire peut être un nœud de confiance dans OLSR incluant les MPR. Un nœud entrant doit découvrir au moins k actionnaires a qui demander un certificat. Comme illustré à la figure 3.1, ils ont mis en œuvre deux dispositions en utilisant Les paquets de contrôle OLSR sans augmenter leur longueur. Le premier est à travers les messages HELLO. En définissant un bit réservé dans leurs messages HELLO, les nœuds peuvent indiquer s'ils ont des parts partielles et sont disposés à fournir un service. Ces messages HELLO identifie seulement les actionnaires à un saut. En raison de possibilité de ne pas y avoir d'actionnaire au sein de la distance d'un nœud, ils utilisent également des messages TC pour notifier l'identité des actionnaires. Chaque MPR utilise son message TC pour annoncer quels nœud dans l'ensemble de sélecteur MPR prétendre être actionnaires. Ces messages TC sont diffusés à l'ensemble du réseau et fournissent un moyen efficace d'informer chaque nœud de tous les actionnaires actuels. ils ont également modifié les messages TC dans la section réservée pour spécifier un compte C de nœud dans le jeu de sélecteurs MPR, qui prétendent être actionnaires. Ils trieront par la suite la liste des annonces par l'annonce d'un nœud voisin pour que les premiers C soient actionnaires. Lorsqu'un nœud reçoit des messages TC, il l'utilise pour construire sa table de routage et en même temps pour construire une table des nœuds actionnaires (maintient leur adresse IP supposé unique et vérifiable, ainsi que leur distance en matière de nombre de sauts).

Dans (Adjih *et al.* 2005), les auteurs ont proposé une architecture d'authentification pour sécuriser le protocole OLSR, où seulement les nœuds authentifiés peuvent participer au routage. L'architecture proposée par les auteurs utilise en effet l'authentification, fournie par des méthodes cryptologiques. Ensuite, le réseau peut ensuite être divisé en deux parties : nœuds authentifiés et nœuds non authentifiés.

— Pour les nœuds authentifiés : Par défaut, le comportement des nœuds authentifiés est supposé correct.Cependant, il est supposé qu'un participant peut commencer à agir comme adversaire, donc la politique effectue des contrôles continus.
— Pour les nœuds non authentifiés : protection, le but est de les empêcher de perturber le réseau.

L'architecture proposée par Adjih et al. repose sur des techniques cryptographiques asymétriques. Elle cible deux types de cryptographie asymétrique : techniques basées sur l'identité, où la clé publique d'un nœud est dérivée de l'identifiant de certains les oeud, d'autres techniques asymétriques traditionnels, où une clé publique existe mais doit être distribuée (éventuellement avec certificat).

Plus récemment, dans (Baadache & Belmehdi 2014), les auteurs ont proposé une approche pour détecter le modèle de l'attaque balckhole du type simple et coopératif dans un réseau ad hoc à plusieurs sauts et comme un objectif secondaire, les auteurs ont proposé la détectection des attaques par modification et de relecture des messages. Ils considèrent que les attaques de modification et de relecture des messages sont totalement ignorées dans les approches existantes, alors qu'ils représente une étape essentielle pour acheminer les paquets aux nœuds distinataire. Les auteurs ont supposé que les liens sans fil sont bidirectionnels, parce que la solution nécessite un échange bidirectionnel de paquets. ils ont supposé aussi que le nœud source no partage une clé commune avec des nœuds intermédiaires nj, 1 j m, où m est le nombre de nœuds dans le chemin de bout en bout. En outre, ils supposent également que le nœud source no approuve le nœud de destination nm1, c'est-à-dire le nœud de destination ne divulgue en aucun cas sa clé partagée. Les auteurs notent que ces hypothèses sont toutes raisonnables et pratiquement réalisables. Ils démontrent l'efficacité de la solution proposée dans le protocole de routage réactif (AODV) et le protocole de routage proactif (OLSR). Le but de cette approche est la vérification du bon acheminement des paquets par des nœuds intermédiaires en utilisant un accusé de réception authentifié de bout en bout (E2E).

Une solution contre les attaques par usurpation de liens dans le réseau en utilisant la localisation géographique des autres nœuds avec une infrastructure de signature a été proposée par Raffo et al. dans (Raffo *et al.* 2005). Il part du principe ou si chaque nœud est capable de connaître la bonne position de tout autre nœuds dans le réseau, l'attaque par usurpation de liens ne peut pas réussir. Chaque nœud compare ces données géographiques au routage des données reçu (c'est-à-dire le voisin et l'ensemble de liens). Si une information contradictoire est trouvée, un faux message de routage est détecté. Une mesure de sécurité supplémentaire est obtenue en utilisant une antenne directionnelle. Ceci permet à un nœud de connaître la direction à partir de laquelle un message reçu a été transmis, et le rend donc beaucoup plus difficile pour les nœuds malveillants d'usurper leurs propre emplacement. En outre, la disponibilité de l'information géographique à propos de nœuds dans le réseau ouvrent des spéculations à propos de nouvelles fonctionnalités possibles dans le standard OLSR, telles que l'amélioration de la sélection MPR et des prévisions de rupture de liaison. Dans cette approche, tous les nœuds doivent avoir un equipement GPS et chaque nœud déclare sa position géographique à travers les messages de contrôle. Ensuite, chaque nœud peut détecter toute falsification d'information en comparant la portée de transmission maximale avec la distance entre deux nœuds. Cependant, cette approche n'est pas pratique dans les scénarios réels en raison du fait que de nombreux nœuds dans le réseau ne sont pas équipés d'un GPS.

Adnane et al. (Adnane *et al.* 2013) présentent un mécanisme de sécurité basée sur la confiance dans le protocole OLSR en utilisant le langage de spécification de confiance. Ils présentent comment le raisonnement basé sur la confiance peut permettre à chaque nœud d'évaluer le comportement des autres nœuds, ainsi détecter et isoler le nœud malveillant. Ils utilisent des solutions de prévention et de contre-mesures pour résoudre les situations de incohérence et contrer les nœuds malveillants avec peu de modifications en restant compatibles avec le protocole OLSR.

La solution adoptée par les auteurs est basée sur la confiance pour sécuriser le protocole OLSR en trois étapes. La première étape est l'analyse des relations de confiance implicite dans OLSR. Cette analyse met en évidence les mesures possibles pour rendre OLSR plus fiable en exploitant les opérations et les informations déjà présentes dans le protocole. Pour détecter les nœuds malveillants, ils ont développé dans la seconde étape, un raisonnement basé sur la confiance en corrélant les informations fournies dans les messages OLSR reçus. L'intégration de ce raisonnement permet à chaque nœud de vérifier la cohérence du comportement des autres nœuds et de valider implicitepment les relations de confiance établies. Enfin, la troisième étape complète la seconde en proposant deux solutions complémentaires : la prévention pour résoudre certaines vulnérabilités du protocole OLSR, et les contre-mesures pour arrêter et isoler les nœuds malveillants.

Ces propositions correspondent au raisonnement de confiance qui a été fait par chaque nœud. En résumé, ils ont démontré que la solution permet de vérifier si le comportement des autres nœuds du réseau est conforme aux spécifications de OLSR. L'approche proposée apporte peu de modifications sur les paquets OLSR, et elle est toujours compatible avec OLSR et SOLSR. Enfin, l'approche proposée par les auteurs peut être appliquée plus généralement à d'autres protocoles dans un environnement spontané et auto-organisé. La spécification explicite des relations de confiance conduit à identifier si les sous-jacentes hypothèses pour le fonctionnement d'un protocole sont réalistes ou non. De plus, des relations de confiance explicite peuvent être utilisées dans l'analyse formelle de la correction des vulnérabilités de protocole.

Schweitzer et al. (Schweitzer *et al.* 2016) présentent un mécanisme de confiance basé sur la réputation pour améliorer la coopération entre les nœuds dans le processus de routage appelé déni de contradictions avec nœud fictif (DCFM Denial Contradictions with Fictitious Node Mechanism). Le mécanisme à pour but d'empêcher une attaque d'isolement de nœud dans laquelle l'attaquant manipule la victime dans la nomination de l'attaquant comme un seul MPR, donnant à l'attaquant le contrôle sur la communication canal. Ce mécanisme s'appuie sur les connaissances internes acquises par chaque nœud pendant le routage avec l'augmentation des nœuds virtuels (fictifs). De plus, DCFM utilise les mêmes techniques utilisées par l'attaque pour l'empêcher. La surcharge des nœuds virtuels supplémentaires diminue tant que la taille du réseau augmente, ce qui est conforme à l'affirmation générale "OLSR fonctionne mieux sur les grands réseaux". La première exigence de la méthode proposée est que chaque nœud n'utilisera que les informations dont il dispose, sans se fier à toute

autorité de confiance centralisée ou locale. La technique proposée ne vérifie pas activement le message HELLO, mais vérifie plutôt son intégrité en cherchant des contradictions entre les messages HELLO et la topologie connue,ce qui permet que lors de la nominations des MPRs, aucune contradiction ne soit trouvée. Même face à des contradictions, un MPR peut être nommé pour tous les voisins à deux sauts pour lesquels c'est le seul nœud qui fourni l'accessibilité. Il ne peut cependant pas être désigné comme MPR unique pour deux sauts voisins qui peuvent être atteints par d'autres chemins.

Raghu et Krishna dans (Potukuchi & Kant 2017) ont proposé une nouvelle solution pour sécuriser le protocole OLSR via un modèle de confiance basé sur la réputation pour le routage proactif. La méthode proposée a été intégrée au protocole OLSR. L'idée de cet approche est de calculer la valeur de confiance consolidée (CTV) des nœuds en combinant la confiance directe (DT) et les valeurs de confiance secondaire (ST). Le CTV est utilisé pour identifier nœuds fiables pour établir un chemin de confiance pour la transmission de données coopérative entre la source et la destination. Le modèle de confiance proposé comporte trois étapes : calcul de confiance directe (DT), le rapports de confiance secondaire (ST) et calcul de la valeur de confiance consolidée (CTV). Afin d'assurer le mecanisme, Chaque nœud doit observer les activités des nœuds voisins dans la réalisation des exigences d'opération de routage telles que le comportement des transmissions de paquets. Cette étude considère la liste des activités de réseau à observer comme des indicateurs de confiance. De plus l'observation de chaque mesure de confiance aide à identifier les attaques de routage. Lorsqu'un nœud transmet le paquet, il commute la radio dans le mode promiscous et observe passivement le comportement d'acheminement de paquets d'un nœud voisin. Pour ce faire, chaque nœud maintient deux compteurs pour enregistrer le nombre de succès et d'échec de chaque indicateur de confiance. Avec ces valeurs, chaque nœud initie le calcul de confiance pour chaque intervalle de mise à jour (TUI). La construction de la table de routage est la majeure partie du processus OLSR. Chaque nœud crée ou met à jour la table de routage lorsqu'il reçoit le message TC des nœuds MPR. Chaque MPR est responsable de la préparation des informations d'état et de l'envoie périodique de messages TC. Quand de nouvelles valeurs de confiance sont disponibles, chaque nœud à la possibilité de mettre à jour sa table de routage. l'objectif était de proposer un modèle de confiance basé sur la réputation lors de l'exécution du protocole OLSR à fin d'isoler les nœuds malveillants du processus de routage sans génerer des frais supplémentaires.

Pour faire face à l'attaque blackhole ou le nœud malicieux fixe le champ Welligness à WILL ALWAYS pour assurer sa sélection autant qu'un nœud MPR pour ensuite perturber le bon fonctionnement du réseau, Zougagh et al. (Zougagh *et al.* 2014) ont présenté un nouvel algorithme heuristique pour la sélection des MPR. Dans cette version modifiée aucune priorité n'est donnée au nœud avec la valeur willigness plus haute, par contre elle est considéré comme une nouvelle approche pour sélectionner les nœuds MPR par couverture additionnelle. Cet algorithme donne la priorité à un nœud avec un willigness plus petit et couvre le maximum des nœuds dans deux sauts voisins et qui ne montre pas de fortes caractéristiques pour influencer la sélection MPR. L'approche proposée élimine la possibilité de la sélection du nœud malveillant en tant que MPR par falsification du champ welligness.

Abdalla et al. (Abdalla *et al.* 2011) présentent un schéma de collaboration pour détecter et isoler un nœud malveillant dans le protocole OLSR. Dans cette approche, les auteurs ont développé un système de détection d'intrusion basé sur la communication E2E entre la source et la destination. Le système de détection d'intrusion proposé appartient à la détection basée sur des spécifications avec des nœuds coopératifs distribués qui conviennent au MANETs et il est subdivisé en deux parties. La première partie est la validation du chemin de communication en envoyant périodiquement des messages. La deuxième partie concerne la recherche de nœuds malveillants dans le chemin invalide. Le processus commence par l'envoi de messages de validation (PVM) périodiquement à la destination à un intervalle spécifié, et le nœud destinataire doit confirmer au nœud source avec une réponse PVM pour vérifier la validité du chemin par lequel les paquets de données sont transmis. Le processus de détection de nœud malveillant proposé valide le chemin de communication puis détecte et isole nœuds malveillants dans les chemins invalides. Il est basé sur la collaboration d'un groupe de nœuds pour prendre des décisions précises. Le nœud attaquant détecté avec succès est ajouté à une liste noire qui est diffusée à tous les voisins directs et ainsi de suite à tous nœuds de réseau. Ensuite, tous les nœuds voisins reçoivent cette liste et cela donne une autre confirmation en envoyant un message PVM aux attaquants pour être certain que ce nœud est en fait un attaquant. Après confirmation, il renvoie la liste noire à ses voisins avec une meilleure évaluation. Lorsque le voisin reçoit cette liste noire, il exclut l'attaquant de la table de routage pour ignorer les tentatives d'attaque.

Les chercheurs dans (Baiad *et al.* 2016) proposent une nouvelle technique pour détecter l'attaque blackhole basée sur une coopération entre les couches (cross layer). Les auteurs présentent deux schémas de détection qui permettent l'échange d'informations entre deux et trois couches respectivement. Le premier schéma utilise les informations entre la couche physique et la couche réseau, tandis que le second repose sur les couches physiques, MAC et réseau pour permettre une détection efficace et fiable. Dans la technique de détection de couche physique, chaque utilisateur légitime se voit attribuer une clé de signature qui est multipliée par le message, et chaque nœud de surveillance utilise l'approche du maximum

de vraisemblance pour déterminer si le message est légitime ou non. D'autre part, la technique de détection MAC surveille le nombre de requêtes RTS / CTS (Request To Send Clear To Send) entre tous les voisins tandis que la technique de surveillance coopérative est mise en œuvre sur la couche réseau pour entendre les paquets échangés entre les voisins.

3.2 Modèle de l'attaque blackhole contre le protocole OLSR

Dans cette section, nous présentons un type d'attaque blackhole basée sur l'usurpation de lien. Le principe de cette attaque consiste à annoncer des faux liens avec les voisins à deux et à trois sauts. En d'autres mots, le nœud malveillant comprend une liste des deux et trois sauts voisins dans son prochain message HELLO. Cette attaque est divisée en deux parties, d'abord le nœud malveillant commence par une écoute passive dans le réseau sans générer de messages HELLO pour obtenir une vue globale de la topologie du réseau. La figure 3.2 présente la topologie de l'attaque avec un seul nœud Malicieux 'M' qui cible le nœud 'A' afin de diviser le réseau et perturber son fonctionnement. Dans cette topologie on a le nœud 'A' sélectionner autant qu'un nœud MPR par le nœud 'B' et 'C' et à son tour il a sélectionné le nœud 'B' et 'C' pour atteindre le nœud 'D' et 'F' respectivement.

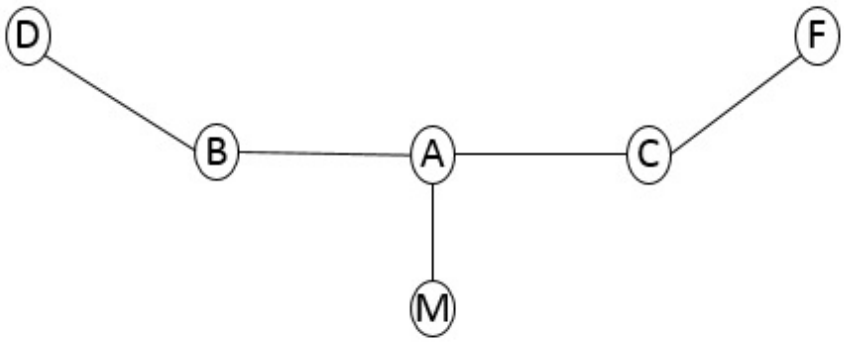

Figure 3.2 – *Topologie de l'attaque*

La première phase de l'attaque consiste à s'insérer dans le réseau et obtenir les informations nécessaires pour lancer l'attaque. Le nœud malicieux 'M' obtient des informations sur son voisinage symétrique un et deux sauts à partir des messages Hello reçus par le nœud 'A' contenant les nœuds 'B' et 'C', a noté que les messages Hello sont envoyés en broadcast à tous les nœuds dans sa zone de couverture et le nœud malicieux 'M' fait partie de son voisinage physique.

Concernant les nœuds voisins à trois sauts , ils sont détectés via les messages TC généré et retrmansmit par le nœud 'A' (seuls les nœuds

MPRs diffusent les messages TC et le nœud 'A' est déjà sélectionné comme MPR).

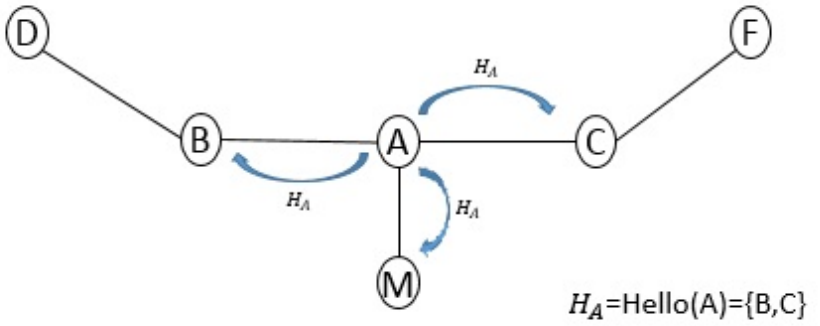

FIGURE 3.3 – *Informations via les messages HELLO*

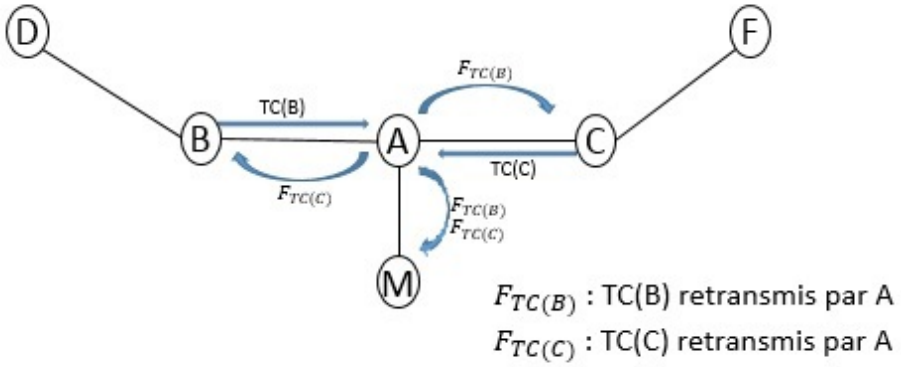

FIGURE 3.4 – *Informations via les messages TC*

Après l'obtention de toutes les informations nécessaires pour lancer l'attaque, le nœud malicieux passe à la deuxième phase de l'attaque. Au cours de la deuxième phase, l'attaquant se présente dans le réseau et génère un message Hello incluant l'ensemble des faux liens avec tous les nœuds découverts dans la première partie. Le résultat de ces falsifications est la sélection constante du nœud malveillant en tant que MPR par le nœud 'A' ce qui lui permet de recevoir le trafic pour ensuite supprimer les paquets reçus "blackhole" et perturber le fonctionnement du réseau "déni de service". Les figures 3.3 , 3.4 et 3.5 illustrent la sélection forcée du nœud malveillant 'M' en tant que MPR.

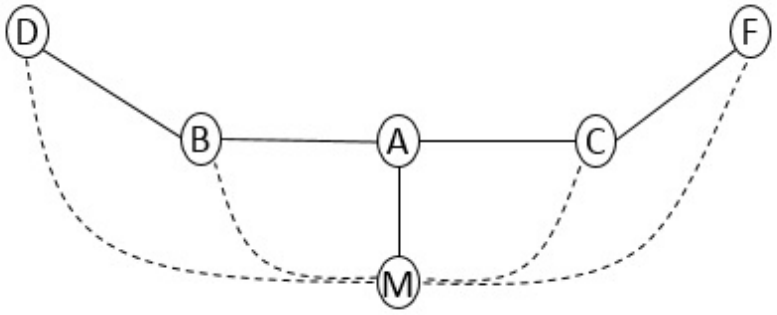

FIGURE 3.5 – *Modèle de l'attaque blackhole*

Afin d'évaluer le protocole OLSR et tester l'effet de cette attaque contre le protocole, nous avons procédé à une étude de simulation détaillée.

3.3 INTÉRÊT DE LA SIMULATION :

Une expérimentation directe effectuée sur le terrain peut se révéler coûteuse, irrationnelle ou même impossible. Il serait même inconcevable dans notre étude de mettre en ouvre un réseau ad hoc, de déplacer les nœuds et changer les paramètres pour comparer un algorithme de routage sous différents modèles de mobilité. C'est à cause des difficultés liées à l'expérimentation directe et dans le but aussi de pouvoir examiner facilement et rapidement les variantes du système étudié que l'on cherche à réaliser un modèle de ce système dont on peut analyser numériquement le comportement et sur la base de cette analyse, inférer le comportement du système réel lui-même. La simulation permet ainsi de tester à moindre coût les nouveaux protocoles et d'anticiper les problèmes qui pourront se poser dans le futur

3.3.1 Network Simulator 2 (NS2)

Présentation de NS2 : Network Simulator (NS) est l'un des logiciels de simulation de réseaux informatiques le plus utilisé dans le domaine de la recherche scinetifique. Il est essentiellement élaboré à base de la conception par objets, de la réutilisation du code et de modularité (Issariyakul & Hossain 2012). Il est aujourd'hui un standard de référence en ce domaine, plusieurs laboratoires de recherche recommandent son utilisation pour tester les nouveaux protocoles.

Le simulateur NS actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulation de grande taille (le test du passage à l'échelle) (Issariyakul & Hossain 2012). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme FTP. À titre d'exemple la liste des principaux composants actuellement disponibles dans NS2.35 par catégorie est :

— Application : Web, ftp, http, telnet, générateur de trafic (CBR,VBR...)

— Transport : TCP, UDP, RTP, SRM
— Routage unicast : Statique, dynamique (vecteur de distance) AODV, DSR, AOMDV,...
— Routage multicast : DVMRP, PIM ;
— Gestion de file d'attente : RED, DropTail, Token bucket.
— Système d'accés au support : CSMA/CD, CSMA/CA, aloha , liens point à point ...

NS est un outil de simulation de réseaux de données. Il est développé en C++ avec une interface textuelle utilisant le langage OTcl (Object Tool Command Language) qui est une extension objet du langage de commande TCL (Tool Command Language). Du point de vue de l'utilisateur, la mise en œuvre de ce simulateur se fait via une étape de programmation qui décrit la topologie du réseau et le comportement de ses composants, puis vient à l'étape de simulation proprement dite et enfin les résultats obtenus (Fichier trace et fichier NAM) peuvent être visualisé avec l'outil NAM (Network Animator) et analyser en utilisant des programmes Java , scripts AWK ou Perl pour permettre de tracer des graphes par des outils comme Xgraph, Microsoft Excel ou GNUplot (un traceur de graphes). La figure suivante représente un flot de simulation avec NS2 .

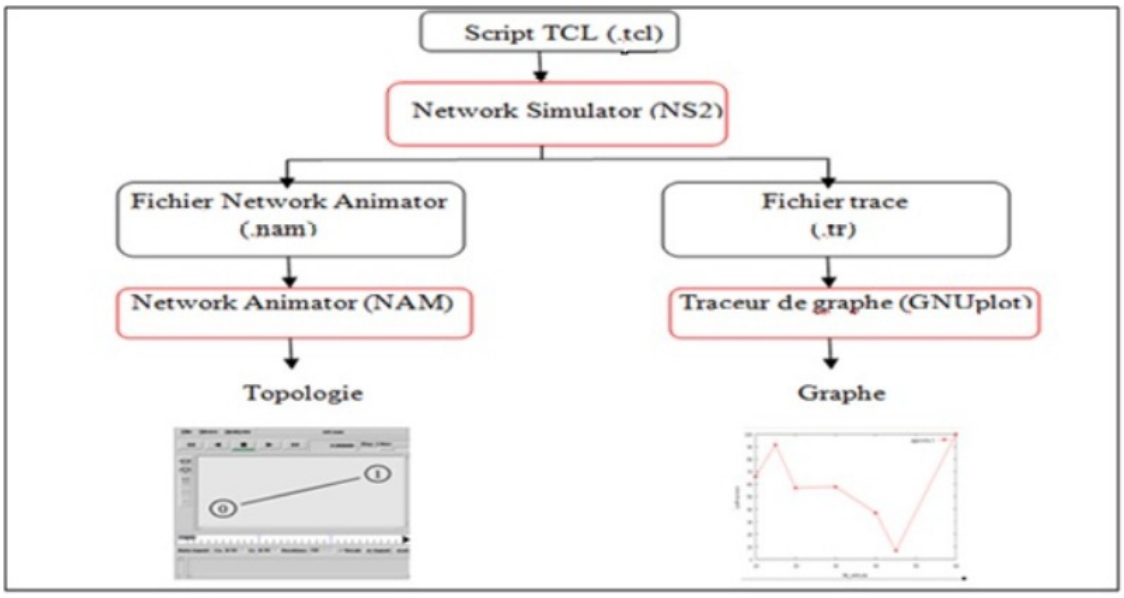

Figure 3.6 – *Flot de simulation*

TCL/TK/OTCL :

TCL (Tools Command Langage) : Tcl est un langage script interprété, traité par un interpréteur TCL(NS par exemple). Il s'inspire principalement des langages C, Lisp, sh et awk. Ce langage à typage dynamique est multi-plateformes, extensible, facile à apprendre. Les programmes écrits en TCL sont en fait des fichiers textes constitués des commandes.

TK (Tool kit) : TK est une extension pour Tcl qui est une bibliothèque pour créer des interfaces graphiques portables.

OTCL : OTcl est une extension orientée objet de Tcl. Les commandes Tcl sont appelées par un objet.

NAM (Network Animator) : NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Par exemple, il est capable de représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine. Ce logiciel est souvent appelé directement depuis les scripts TCL pour NS-2, pour visualiser directement le résultat de la simulation.

GNUplot : GNUplot est un autre utilitaire utilisé sous linux et qui permet lui aussi de fournir un compte-rendu graphique, mais cette fois-ci sous forme de courbes statistiques. Les formats de données acceptés en entrée sont de type deux dimensions (x et y). Les valeurs dans chaque ligne sont séparées par des espaces ou des colonnes, et les données peuvent être à deux ou à plusieurs colonnes.

AWK : Programmation script à partir pour calculer les déférents paramètres qui ont était générer par le fichier trace.

3.3.2 La mesure de performance

Les métriques de mesure de performance constituent un outil non redoutable pour tester un protocole et mesurer ces performances. Ils sont généralement utilisés dans les études de comparaison de performances. Dans notre étude, nous avons pris en compte les métriques les plus utilisés dans les travaux connexes qui sont :

Pdr (packet delivery ratio) : Représente le pourcentage de paquets bien livrés à leurs destinations par rapport au paquet transmis dans le réseau. Il est calculé comme suit :

$$PDR = 100 * \frac{PaquetsRecu}{PaquetsEnvoyer}$$

paquets perdu : ce paramètre représente le nombre de paquets abandonnés lors de la transmission des paquets de la source à la destination.

overhead : représente le nombre de paquets de contrôle de routage divisés par le nombre de paquets de données reçues.

3.4 Simulation de l'attaque

Afin de tester l'efficacité du processus de l'attaque blackhole, nous effectuons une étude de simulation détaillée en utilisant le simulateur de réseaux connu NS-2.35. Le scénario est composé de 25 nœuds, Où dix nœuds communiquent et le nombre de nœuds malveillants varient entre 0 et 3. La plage de transmission des nœuds est définie sur 250 mètres, dans une zone de taille 1000 * 1000 mètres pendant 100 secondes. Nous avons mis les paramètres de simulation comme indiqué dans le tableau suivant :

Simulateur	NS2.35
Temps de simulation	100 secondes
Plage de transmission	250 mètres
Type de trafic	CBR
charge utile de données	512 bytes
taux de paquet	4 paquets/s
nombre totale de nœud	25
nombre de nœud communicant	10
nombre de nœud malveillant	1, 2, 3

Table 3.1 – *Paramètre de simulation*

Résultat de simulation

Nous notons dans les résultats présentés que OLSR pour représenter les performances du protocole original sans aucune modification, et BH_OLSR pour représenter le protocole OLSR sous une attaque blackhole présenté précédement.

La figure 3.7 illustre une comparaison basée sur le PDR (taux de paquets envoyer avec succès) entre le protocole OLSR original et le protocole sous l'attaque blackhole présenté précédement OLSR sans attaque présente de bonnes performances, cependant, sa performance sous attaque blackhole montre une dégradation considérable tant que le nombre des nœuds malveillant augmente, ce qui confirme que le nombre de nœuds malveillants affecte la performance du protocole. La dégradation de PDR est due aux paquets ignorer par les nœuds malveillants dans le réseau.

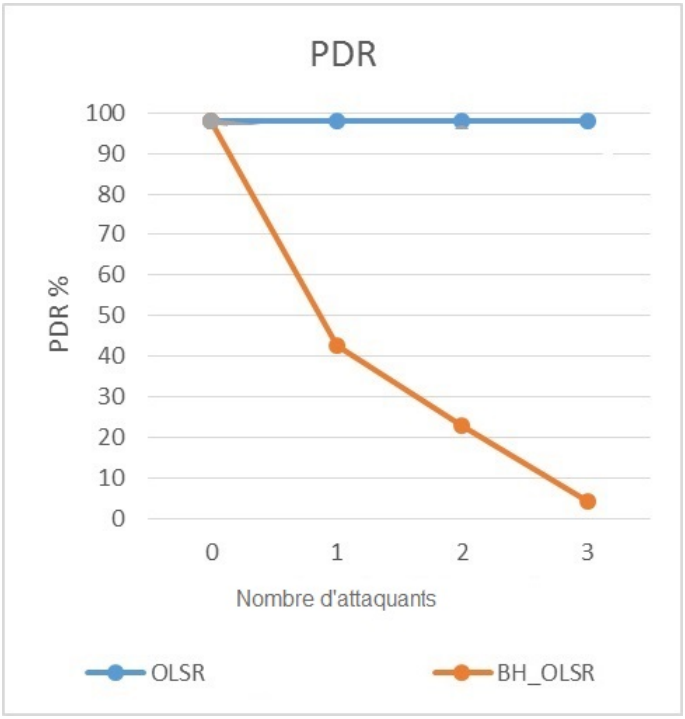

FIGURE 3.7 – *Taux de délivrance*

Dans la figure 3.8, nous observons que l'attaque affecte directement les performances du protocole. On constate que le nombre de paquets perdus augmente à mesure que le nombre de nœuds malveillant augmente. Cela peut être justifié du fait que plus qu'on a de nœuds malveillants, il y aura une grande partie du réseau qui peut être touchée par l'attaque.

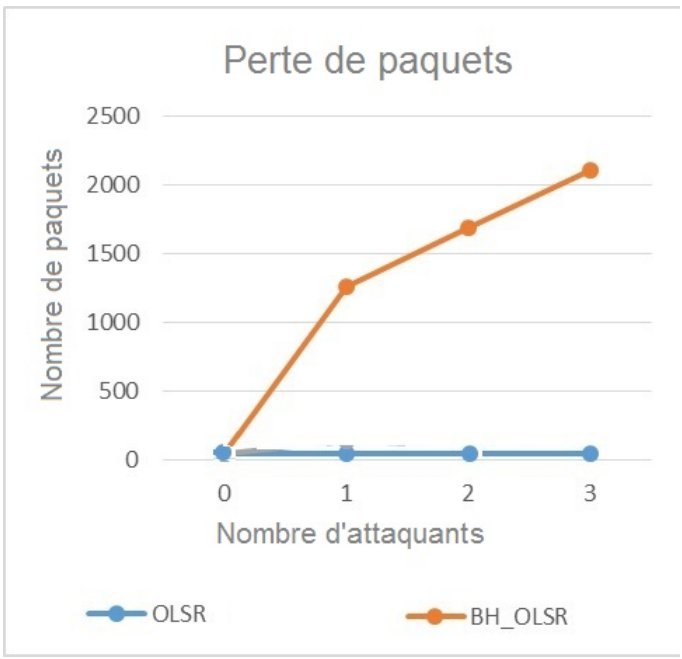

FIGURE 3.8 – *paquets perdus*

La figure 3.9 illustre la surcharge dans un réseau de 25 nœuds avec 10 nœuds communicants, et montre une comparaison entre le protocole OLSR standard et le protocole BH_OLSR pour tester la gravité de l'attaque blackhole. On observe que la surcharge du réseau est plus importante dans la situation où il y aura 3 nœuds attaquants. La surcharge du réseau est représentée par le nombre de paquets de contrôle par rapport aux paquets données dans l'ensemble du réseau, le fait que l'ensemble des nœuds du réseau génère des paquets de contrôle périodiquement et que les nœuds malicieux suppriment tous les paquets de donnée affecte considérablement la surcharge du réseau (plus de paquets de contrôle et beaucoup moins de paquets donnés).

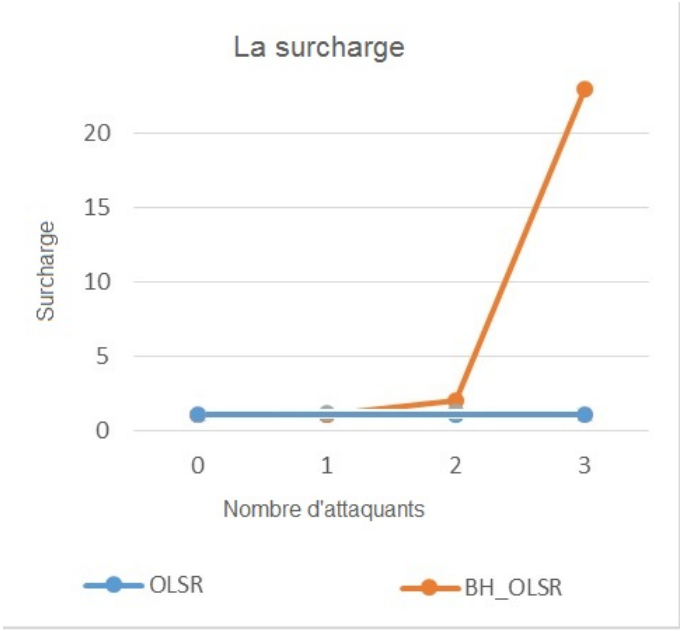

Figure 3.9 – *la surcharge*

3.5 Mécanisme de sécurité

Dans cette section, nous présentons une technique de détection de l'attaque blackhole dans le protocole OLSR. Dans ce type d'attaque, le nœud malveillant crée des faux liens avec les voisins à deux et trois sauts, et injecte cette fausse information dans le réseau, cela peut conduire à la sélection de ce nœud comme MPR et il peut facilement perturber le trafic par la suppression des paquets passant par lui. Afin de détecter ces nœuds malveillants, un processus de vérification des liens est déclenché chaque fois qu'un nœud présente un comportement suspect. Notre approche comporte deux phases importantes.

3.5.1 Phase I

Le but de la première phase est la détection un comportement suspect du nœud qui inonde le réseau par de fausses informations. Si c'est le cas,

le nœud doit être mis dans la liste des nœuds suspects. Pour cela, nous suivons ces étapes. Chaque nœud :

— calcule la moyenne des liens symétriques entre les voisins direct en utilisant cette équation :

$$Avg(node) = \sum_{nbset=0}^{nbset.length} \frac{Neighbors.link}{Neighbors.length}$$

— Partage les informations calculées avec l'ensemble du voisinage à un saut en utilisant le champ "reserved" dans le paquet Hello contenant la moyenne calculé.

— après avoir reçu un paquet Hello, il vérifie la valeur de l'AVG déclaré (la valeur doit être positive, sinon le nœud est considéré comme suspect), après cela, chaque nœud calcule la grande moyenne. Cette valeur représente la moyenne des liens symétriques dans une grande surface dans le réseau.

$$Large.Avg(node) = \sum_{nbset=0}^{nbset.length} \frac{AVG}{Neighbors.length}$$

— Le seuil est fixé comme suite :

$$THRESHOLD = Cel(Large.Avg) + 1$$

(eq)

Enfin, si un nœud annonce avoir plus de liens par rapport au seuil, nous ajoutons l'adresse du nœud à la liste des nœuds suspects.

Pour résumer le comportement des nœuds pour l'étape de la suspections dans notre proposition, nous présentons l'algorithme utilisé lors de la première phase.

Algorithme 1 : Calcule du seuil

```
Begin;
for (it = NbSet.BEGIN, it = NbSet.END it++) do
    Nbr.Link += Nbr.Link(it);
Avg (CURRENT.Node) = Nbr.Link/NbSet.lengh;
for (it = NbSet.BEGIN, it = NbSet.END it++) do
    if AVG > o then
        Avg+=Avg(it);
    else
        Suspect.list.add(node);
Larg.Avg (node) =Avg/NbSet.lengh;
THRESHOLD = Cel(Larg.Avg) + 1;
```

le nombre de liens de chaque nœud doit être vérifié comme suite :

Algorithme 2 : Vérification du nombre de liens

```
if Number.link(Node) > THRESHOLD then
    Suspect.List.add(Node);
else
    nœud légitime;
```

3.5.2 Phase II

La deuxième phase du processus de détection comprend la vérification de la fiabilité des liens d'un nœud suspect. À ce stade, nous introduisons deux paquets INF REQ et INF REP.

INF REQ : diffusé par un nœud qui détecte un voisin suspect afin de confirmer les liens déclarés par le nœud suspect. Le message INF REQ est envoyé dans un rayon maximal de voisinage de deux sauts en fixant la valeur du temps de vie (Time To Live) du paquet IP à deux (TTL = 2). Cela signifie que seuls les nœuds voisins à un et deux sauts reçoivent ce message. Le paquet de vérification comprend trois champs principaux.

- Solicited Information (SI) : l'adresse du nœud qui déclenche le processus de vérification (utilisée également pour envoyer la réponse au nœud source du message)
- Sender : l'adresse du nœud source du paquet
- Suspect (SU) : adresse du nœud suspect.

INF REP : est le message de réponse des paquets INF REQ. Ce message contiens trois champs principaux.

- Acknowledgment Node (AN) : le nœud qui répond à INF REQ
- Source Node (SN) : l'adresse du nœud source du paquet
- Destination Node (DN) : l'adresse du nœud destinataire du paquet, cette adresse est extraite des paquets INF REQ (SI).

Le but de l'échange de ces paquets est de vérifier les liens déclarés par les nœuds suspects. Les nœuds SI vont envoyer le paquet INF REQ lorsqu'ils détectent un comportement suspect dans un ensemble de voisinage. Chaque nœud qui reçoit le paquet INF REQ vérifie s'il a un lien valide avec le nœud suspect. Sinon, il renvoi une reponse négative (en utilisant un paquet INF REP) au nœud SI (le choix de la réponse négative est adopté pour empêcher l'envoi du nœud malveillant de fausses informations contenant une validation de lien avec usurpation d'identité également pour réduire le nombre des paquets de contrôle dans le réseau).

Algorithme 3 : Traitement du Paquet INF REQ

```
Receive.Inf.Req(SI, Sender, SU)
while True do
    Verify();
    Prepare.Inf.Rep();
    Sent.Inf.Rep(Inf.Rep);
```

Lorsque le nœud SI reçoit le paquet INF REP, il vérifie si l'adresse source de ce paquet est déclarée comme voisin par le nœud suspect, si c'est le cas, le SI incrémente la liste des liens invalides déclarés par le nœud suspect. Après cela, le nœud SI calculera le taux des liens invalide déclaré par le nœud suspect.

Algorithme 4 : Traitement du Paquet INF REP et test de nœuds suspects

```
Receive.Reply(An, Sc, DN);
if An in Nbset.Suspect then
    Untrusted.Link.Increment();
else
    Rien;
```

$$Rate(invalid.link) = (\frac{Valid.link}{Declared.link}) * 100$$

Enfin, pour faire la distinction entre les ruptures des liens dû à la mobilité et ceux dû aux attaques, nous avons fixé un deuxième seuil dans le but d'ajouter une nouvelle vérification avant d'isoler un suspect pour éviter les cas des faux positives. Le SI ajoutera le nœud suspecté dans la liste noire si le taux des liens invalides dépasse ce seuil.

Algorithme 5 : Validation des nœuds suspects et remplissage de la liste noir

```
if Rate(invalid.link) > THRESHOLD2 then
    BlackList.add(SU);
else
    Rien;
```

Lorsque nous ajoutons un nœud à la liste noire, il ne doit jamais être sélectionné comme MPR. Pour assurer cette régle, chaque nœud voisin du nœud défini le champ WELIGNESS du nœud considéré comme malveillant à WILL_NEVER.

Après avoir appliqué le schéma proposé, nous avons veillé à ce que les nœuds malveillants qui diffusent des fausses informations dans les réseaux seront bloquées, et il ne sera jamais sélectionné comme MPR à base de son identité dans le réseau (l'adresse logique ou physique). Cependant, dans le cas d'une deuxieme attaque combinée avec l'attaque blackhole, le nœud malveillant peut reconstituer le même comportement avec une identité usurpée. Par conséquent, si nous appliquons notre algorithme, il peut ajouter un nœud légitime à la liste noire à cause du comportement d'un nœud attaquant. Pour s'assurer que ce cas ne se produira jamais, nous devons nous assurer que le nœud malicieux serai bloqué et pas un autre nœud légitime. Pour répondre à cette exigence, nous faisons appel aux méthodes cryptographiques pour vérifier l'identité des nœuds, chaque nœud envoi son message avec une signature numérique avant de diffuser des paquets aux voisins. À présent, quand un nœud est ajouté à la liste noire, nous sommes sûrs que nous avons ajouté seulement les attaquants.

Efficacité du seuil dans un graphe biparti La valeur du seuil est choisie de manière à détecter le lien suspect déclaré par les voisins symétriques dans le réseau. Nous montrons l'efficacité de ce seuil dans un graphe biparti de deux sous-ensembles (U, V), avec les cardinalités n et m respectivement.

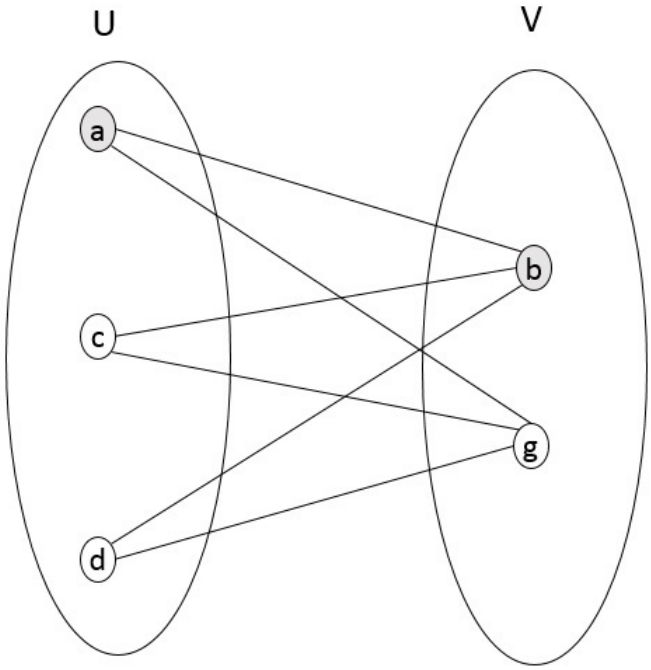

FIGURE 3.10 – *graphe biparti*

Théorème Soit (U, V) un graphe biparti complet avec Card (U) = n et Card (V) = m.

Soit 'a' un nœud dans U, et 'b' un nœud dans V. Supposons que le nœud 'b' attaque le nœud 'a'. Soit T le seuil définit par l'équation (eq).

- supposons que n = m : Si 'b' ajouter un faux lien, alors degré (b)> T, 'a' suspect 'b'.
- supposons que n> m : Alors il existe p $\in$ N* tel que n = m + p, si 'b' ajoute deux fausses liaisons, alors degré (b)> T, 'a' suspect 'b'.
- supposons que n <m : Alors il existe p $\in$ N* tel que n = m - p, si 'b' ajoute p + 1 faux liens, alors : degré (b)> T, 'a' suspect 'b'.

Démonstration

— Si n = m
Le nombre de liens à chaque nœud égal à m, l'AVG égal à m, et le grand AVG également égal à m.

Maintenant, si un nœud malveillant ajoute un faux lien, la nouvelle moyenne sera m + (nombre de liens ajoutés / m), et le nombre de liens d'un nœud malveillant sera m + nombre de liens ajoutés.
Si un nombre de liens ajoutés, égale ou dépasse deux liens. Le nœud sera suspecté (nombre des liens> SEUIL).

— Si n > m

$$Large.Avg(node) = \sum_{nbset=0}^{nbset.length} \frac{AVG}{Neighbors.length}$$

$$nbr.link(a) = m$$
$$nbr.link(b) = n$$

$$Avg(a) = \frac{m}{m+1}(n+1)$$

$$Avg(b) = \frac{n}{n+1}(m+1)$$

$$Large.Avg(a) = \frac{m}{m+1}(\frac{(n+1)^2 + n(m+1)^2}{(m+1)(n+1)})$$

nous considérons

$$n = m + p$$

Ensuite nous vérifions si l'événement se déclenche avec un faux lien

$$Thsd(a) < n + 1(Faut\,lien)$$

$$Cel(Large.Avg(a)) + 1 < m + p + 1$$

nous démontrons que :

$$Cel(Large.Avg(a)) + 1 - (m + p + 1) < 0$$

Après remplacement et simplification on trouve :

$$-pm^3 - (p^2 - 3p - 2)m^2 + (p^2 - 3p - 2)m - p^2 - p$$

Avec p=1 et m>1

$$-m^3 + 4m^2 - 4m - 2 < 0$$

L'événement est donc déclenché avec un faux lien dans ce cas. Il est automatiquement déclenché dans le cas de p> 1 car il y a plus de liens par rapport à un cas précédent.

— Si n <m

Le nœud malveillant doit ajouter de plus en plus de liens pour forcer sa sélection en tant que MPR, si un nœud malveillant ajoute |p| liens, on se retrouve avec la même valeur de lien avec l'autre sous-ensemble U, un autre lien déclaré et l'événement serait déclenché.

3.6 Simulation et analyse

Afin de tester l'efficacité du mécanisme proposé contre l'attaque blackhole basée sur l'usurpation de liens, nous avons effectué une étude de simulation détaillée utilisant le simulateur de réseaux connu NS-2.35. Le scénario est composé de 25 nœuds. Où dix nœuds communiquant et le nombre des nœuds malveillants varient entre 1 et 3. La portée de transmission des nœuds est définie sur 250 mètres en avec une propagation en FREESCAPCE, dans une zone de simulation de taille de 1000 * 1000 mètres pendant 100 secondes. Les paramètres de simulation sont indiqué dans le tableau suivant :

Simulateur	NS2.35
Temps de simulation	100 secondes
Plage de transmission	250 mètres
Type de trafic	CBR
charge utile de données	512 bytes
taux de paquet	4 paquets/s
nombre totale de nœud	25
nombre de nœud communicant	10
nombre de nœud malveillant	1, 2, 3

Table 3.2 – *Paramètre de simulation*

Résultat de simulation

Nous notons dans les résultats présentés que l'OLSR représente les performances du protocole original sans aucune modification, et que BHOLSR représente OLSR sous une attaque blackhole, et le New OLSR représente le protocole OLSR renforcé par le mécanisme de détection proposé pour faire face aux attaques.

La figure 3.11 illustres le nombre de paquets transmit avec succès en fonction du nombre de nœuds malveillants dans un scénario de 25 nœuds. Notons que le nombre des paquets transmis connaît une dégradation avec l'augmentation des nœuds attaquants dans le réseau, Cela est dû au comportement du nœud malicieux qui va dominer l'accés au support pendant le temps d'attaque. On observe qu'après notre solution le PDR connaît une amélioration considérable par rapport à la première expérience (sous l'attaque), qui se rapproche du cas d'un réseau composé seulement des nœuds légitimés dû à la détection et l'isolation rapide des nœuds malicieux qui perturbe le bon fonctionnement du réseau.

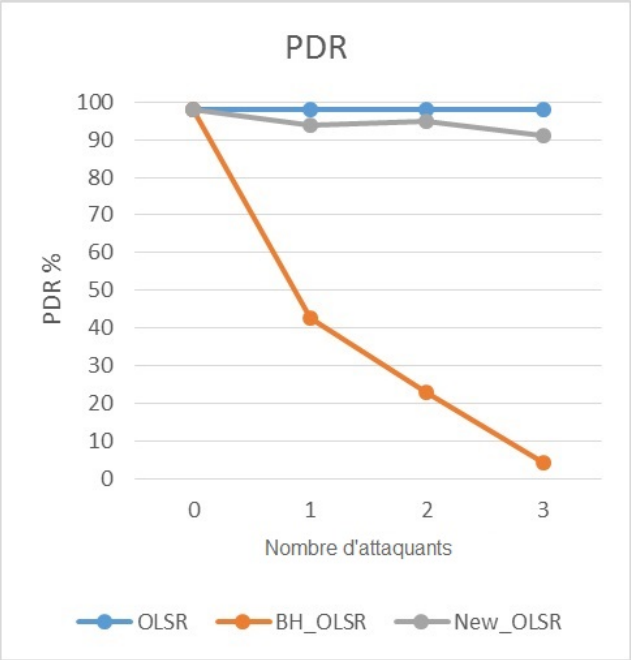

FIGURE 3.11 – *Taux de delivrance*

Dans la figure 3.12, nous observons que l'attaque affecte la performance du protocole en augmentant le nombre de paquets perdus avec l'augementation des nœuds de malveillant dans le réseau. On remarque clairement que le protocole OLSR renforcé par le mécanisme proposé présent des bonnes performances et on constate une diminution des nombres de paquets perdus en raison de détection et isolation des nœuds malveillants.

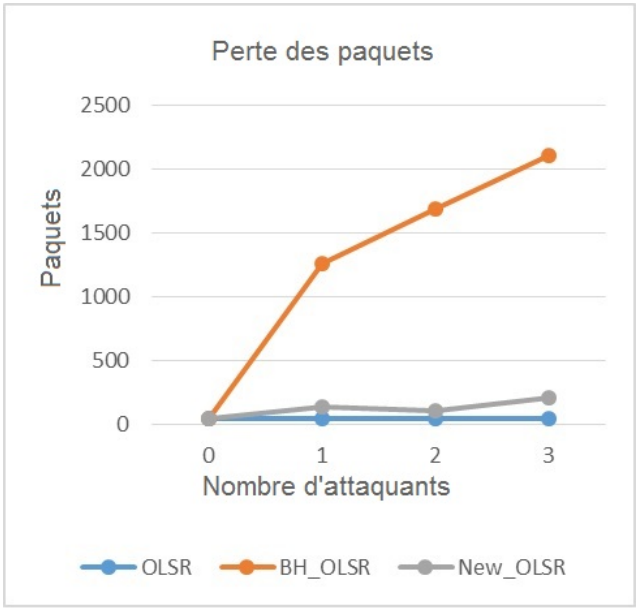

FIGURE 3.12 – *Paquets perdus*

La figure 3.13 montre une surcharge élevée sur le réseau sous l'attaque. Cela est dû à la réduction des nombres de paquets de données reçues. Dans la solution proposée "New OLSR", le surcharge dans le réseau diminue par rapport à "BH OLSR". En outre, on constate une légère augmentation par rapport à l'OLSR sans attaque. Le réseau n'a pas été surchargé car le processus de vérification est lancé seulement en cas de suspection, ainsi que le paquet de vérification est diffusé dans un rayon maximal de deux sauts.

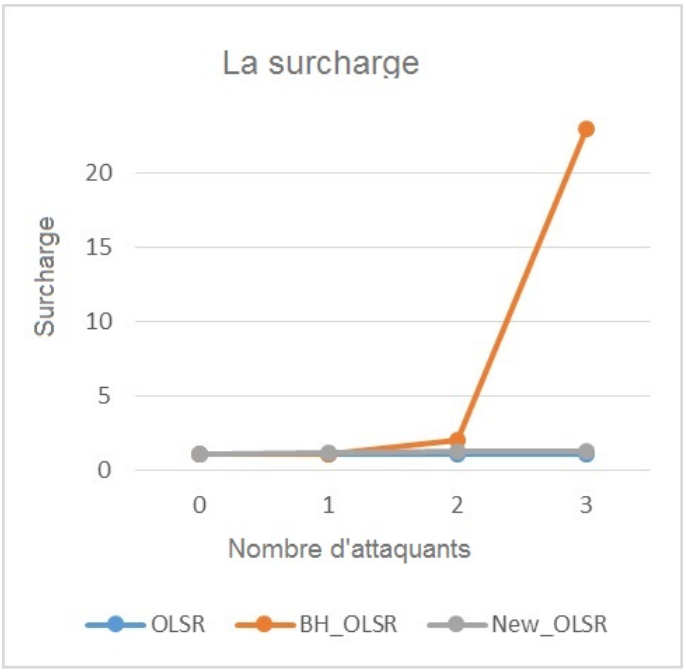

FIGURE 3.13 – *Surcharge*

Conclusion du chapitre

Dans ce chapitre, nous avons discuté les solutions proposées à travers le monde pour sécuriser le protocole OLSR contre les différentes attaques qui peuvent nuir au bon comportement du protocole. Nous avons présenté un type d'attaque blackhole catégorisée comme un déni de service. L'idée principale de cette attaque est l'ajoute des voisins trois sauts dans l'ensemble du voisin symétrique afin de forcer la sélection en tant que nœud MPR pour ensuite dévier tout le trafic. Après cela, nous avons présenté une technique pour contrer cette attaque. Notre solution proposée est basée sur une vérification optimisée des liens si un nœud présente un comportement suspect. Nous avons démontré l'efficacité de notre schéma basé sur les métriques de performance à travers une étude de simulation détaillé NS-2.

Dans le chapitre suivant, nous présenterons l'attaque black hole coopératifs et son effet sur le protocole OLSR. Elle est lancé par un ensemble de nœuds malicieux et elle se base sur la diffusion de fausses informations pour perturber le bon fonctionnement du protocole. pour conter cette attaque nous proposerons un mécanisme collaboratif à base de valeur de confiance ce constituera notre deuxième contibution.

Contribution II : Mécanisme de sécurité contre l'attaque Blackhole coopérative

4

Sommaire

4.1 Etat de l'art 66
4.2 Modèle de l'attaque Blackhole coopérative 69
4.3 Simulation de l'attaque Coopérative 73
4.4 Mécanisme proposé 76
4.5 Simulation et discussions des résultats 83
Conclusion 86

L'objectif principal du protocole de routage est de découvrir la route depuis n'importe quelle source vers n'importe quelle destination dans le réseau. Pour cela, le groupe de travail MANET a défini trois catégories de protocoles de routage : protocoles réactifs tels que AODV, où la route est découverte à la demande, des protocoles proactifs tels que OLSR, ceux qui découvre et mainteint toutes les routes vers n'importe quel nœud dans le réseau, et les protocoles hybrides comme ZRP qui combine les deux catégories précédentes. Le protocole OLSR est l'un quatres protocoles les plus utilisé dans les réseaux Manets. Le concept clé de ce protocole par rapport au protocole d'état de liens classique est l'utilisation de nœuds appelé Multipoints Rely (MPR). Le MPR réduit le nombre de paquets dupliqués diffusés sur le réseau. Cette caractéristique peut être exploitée par un nœud de mauvaise conduite et force sa sélection comme MPR en usurpant des liens avec d'autres nœuds dans le réseau. Dans ce chapitre, nous présentons la vulnérabilité d'OLSR protocole face à l'attaque Blackhole coopératifs lancé par deux ou plusieurs nœuds malicieux. Cette attaque est basée sur l'annonce des fausses informations dans le réseau sans laisser de trace visible. Après cela, nous proposons un nouveau schéma optimisé appelé Neighbours-Trust-Based. L'idée principale est la collaboration entre voisins pour calculer une valeur de confiance de chaque nouveau MPR afin de détecté les nœuds malveillant dans le réseau.

4.1 Etat de l'art

Le protocole OLSR (Optimized Link State Routing) est l'un des protocoles de routage célèbres dans le réseau sans fil dans lequel les routes sont immédiatement disponibles en cas de besoin. Il a de nombreux avantages comme la réduction des paquets dupliqués diffusés sur le réseau en utilisant des nœuds MPR. Cependant, le manque d'infrastructures et l'utilisation d'une topologie dynamique crée de nombreux problèmes qui affectent le domaine de la sécurité, en outre, la technique d'inondation utilisant les nœuds MPR rend le protocole moins sécurisé, car seuls ces nœuds sont responsables de l'information de telle sorte qu'une seule connectivité est exploitée, ce qui rend le protocole OLSR vulnérable à de nombreux types d'attaques (Kannhavong *et al.* 2007; Abdalla *et al.* 2011).

Le but du nœud de malveillant est de s'insérer dans le processus du routage et perturber la topologie du réseau. Les attaques contre le protocole sont généralement basées sur la génération du trafic incorrecte, par exemple l'usurpation d'identité dans les messages HELLO et TC et le routage incorrect du trafic. Les attaques bien connues dans cette catégorie sont Wormhole et Blackhole. Dans cette partie, nous nous intéressant à l'attaque coopérative par deux ou plusieurs nœud malveillant dans le réseau.

L'attaque du trou noir est catégorisée comme une attaque déni de service trés dangereuse qui cause des sérieux dommages et perturbations dans la topologie de réseau. La plupart des travaux antérieurs se sont concentrés sur la sécurité basée sur les méthodes cryptographiques.

Dans (Baadache & Belmehdi 2014), les auteurs ont proposé une approche basée sur l'authentification des connexions entre les nœuds avec accusé de réception afin de vérifier l'expédition correcte de paquets par les nœuds intermédiaires. Le schéma de solution peut détecter les attaques de trou noir simple et coopératif dans les réseaux ad hoc avec multi-sauts. Ils démontrent l'efficacité de la solution proposée dans le protocole de routage réactif (AODV) ainsi que le protocole de routage proactif (OLSR). Le but de cette approche est de vérifier l'exactitude des paquets transmis par des nœuds intermédiaires en utilisant une authenticité end-to-end (E2E) avec acquittement . Cependant, la limitation majeure de la solution basée sur la cryptographie est que ces méthodes empêchent les l'attaques externes, mais reste vulnérable à une attaque interne.

Semchedine et Mehamel dans (Semchedine *et al.* 2016) ont proposé une extension du protocole OLSR pour le sécuriser contre l'attaque du trou noir, l'extension est appelé Crypto routage d'état de liaison optimisé(CRY OLSR). Ce mécanisme proposé est basé sur la cryptographique asymétrique qui permet l'identification, puis l'isolation des nœuds malveillants dans le réseau. Cependant, la cryptographie moderne basée sur les algorithmes de cryptage asymétriques est généralement lourd et peut facilement influcer sur l'énergie des nœuds et conduire à l'épuisement des batteries.

Les solutions proposées pour sécuriser le protocole utilisant les méthodes cryptographiques ont des inconvénients. D'abord, il y aura une

surcharge importante dans le réseau en raison de l'échange des informations supplémentaires, deuxièmement, l'utilisation des infrastructures de sécurité demande une tierse partie ou une clé publique avec un calcul coûteux, ce qui va à l'encontre de la nature des MANETs.

Un système de détection d'intrusion pour les nœuds mobiles les utilisant la construction stratégique d'un routage sécurisé dans le protocole OLSR aété proposé dans (Kaur *et al.* 2013). Dans ce mécanisme, l'idée est de vérifier si le nœud élu comme MPR est un nœud normal ou non. La technique permet à chaque nœud mobile communicant de surveiller la réputation, le facteur de suspicion, et l'occurence de la menace par le calcule du degré de la vulnérabilité. Le modèle est capable d'explorer les adversaires dans le réseau sous la forme de nœuds normaux. La solution proposée est basé sur l'identification de fausses informations envoyées par des nœuds à travers des messages HELLO lors de la sélection MPR. Cette identification est faite par le système d'identification et d'infiltration.

Abdalla et Afsari. (Abdalla *et al.* 2011) ont présenté un schéma de collaboration entre un groupe de nœuds voisin pour détecter et isoler un nœud malveillant dans le protocole OLSR. Dans cette approche, les auteurs ont développé système de détection d'intrusion basé sur E2E (End-To-End) entre la source et la destination, puis la prise de décisions se fait en collaboration dans un groupe de voisins. En outre, une fois qu'un nœud malveillant est détecté il sera ajouté à une liste noire et lance un processus d'échange entre tous les nœuds du réseau pour les informer de la liste des attaquants. Chaque nœud confirme la réception des informations en envoyant un message appelé PVM.

Baiad et al. (Baiad *et al.* 2016) ont proposé un nouveau schéma cross-layer coopérative pour détecter l'attaque de trou noir qui cible généralement la qualité du service de routage d'état de liaison optimisé sécurisé protocole (QoS-OLSR) dans les réseaux ad hoc véhiculaire (VANETs). La technique de détection d'une attaque de trou noir est basée sur la coopération entre couches afin d'améliorer la détection. Les auteurs ont présenté deux schémas de détection, pour permettre l'échange d'informations entre les couches du modèle OSI, la premiere est à travers la couche physique et la couches réseau, tandis que la seconde repose sur les couches physique, MAC et réseau.

Une nouvelle solution pour protéger le protocole OLSR contre l'attaque d'isolement en employant la même tactique utilisée par l'attaque elle-même est présentée dans (Schweitzer *et al.* 2016). La solution présentée par les auteurs est appelé le mécanisme de déni decontradiction les nœud fictisf (DCFM, Denial Contradictions with Fictitious node Mechanism) qui détectent les contradictions entre les messages HELLO et la topologie du réseau. Les auteurs démontrés par la simulation que leur technique protège plus de 95 pour cent des attaques avec une diminution de 5 pour cent sur les frais généraux nécessaires tant que la taille du réseau augmente.

Vanamala et Rao présentent dans (Vanamala & Rao 2017) une approche pour optimiser les performances du protocole OLSR en intégrant des stratégies de construction de la décision de routage contre la mauvaise modélisation et la mauvaise conduite des nœuds dans le réseau ad hoc. La

solution proposée représente une modélisation des nœuds pour compléter le système de détection d'intrusion pour les nœuds mobiles en utilisant la construction stratégique de la décision de routage sécurisé dans le protocole. La technique permet de profiler les nœuds normaux et le nœud malveillant basé sur un certain nombre du paquet de données échangé par les nœuds pour calculer le degré de sa vulnérabilité.

Les auteurs dans(Jenomactaline & Joywinniewise 2016) ont proposé un mécanisme dotant OLSR avec le système Homomorphic Linear Authenticator (HLA) afin de détecter l'attaque du trou noir. Le principe est de calculer la véracité de l'information de perte de paquets renseigné par les nœuds. Cet algorithme a pour but de préserver les informations privées et de trouver le chemin optimal pendant la transmission. Le protocole proposé est adapté de tel sorte qu'il puisse assuré la confidentialité, l'évitement des collision avec une faible génération de frais supplémentaires.

Pour atténuer l'effet des attaques blackhole dans OLSR, Prateek et son équipe présentent dans (Prateek *et al.* 2017) une technique basés sur la réputation appelée RRM (Reputation Routing Model). Ce modèle est axé sur la confiance calculée à partir des informations du routage afin de l'utiliser ensuite pour concevoir le modèle d'acheminement à abse de réputation. Les auteurs prouvent que le mécanisme proposé peut isoler les nœuds malveillants et sélectionne le chemin de confiance sans modifier le protocole d'origine avec une petite augmentation de la surcharge dans le réseau.

Dans (Prateek & Koushik 2018), les auteurs ont réutilisé le modèle proposé précédemment (Routage de réputation-Modèle). Dans ce modèle les auteurs ont introduit le concept de confiance à l'aide du modèle de routage avec réputation dans le protocole en tant que contre-mesure contre les attaques de manipulation sur OLSR basées sur la modification. Ces attaques incluent la modification des messages HELLO et TC avec de fausses informations sous trois formes TC-Blackhole, HELLO-Blackhole et TCHELLO-Blackhole.

4.2 Modèle de l'attaque Blackhole coopérative

Comme nous l'avons mentionné précédemment, l'attaque Blackhole est catégorisée comme une attaque active et dangereuse qui crée de sérieux problèmes de sécurité. Dans cette section, nous présentons un nouveau type d'attaque Blackhole coopératif contre le protocole OLSR lancé par deux ou plusieurs nœuds malveillants. Le but de ces nœuds est de perturber le fonctionnement habituel de la topologie du réseau. Cependant, pour atteindre l'objectif d'attaque, l'un où les deux nœuds malveillants doivent être sélectionnés comme MPR, car seuls ces nœuds peuvent transmettre le trafic dans le réseau selon la spécification de OLSR. Une fois que le nœud malicieux assume le rôle de nœud MPR, il peut facilement détourner le trafic qui passent par lui.Dans ce genre d'attaque, les nœuds malveillants entrent dans le réseau silencieusement sans générer des messages HELLO, et obtiennent une vue globale de la topologie du réseau. Les nœuds malveillants reçoivent les informations sur les voisins symétriques à deux sauts via les messages HELLO, et les trois sauts voisins ou plus sont détectés grâce au message TC diffusé par le nœuds MPR. Les informations sur les voisins de trois sauts sont plus que suffisantes pour commencer et terminer la perturbation. L'attaque est divisée en deux parties avec effectivement deux nœuds Malveillants X1 et X2 (mode X1 : passive $\longmapsto$ désirable, Mode X2 : passive $\longmapsto$ auto) comme indiqué sur la figure 4.1.

Passive : le mode passive indique le comportement du nœud malveillant dans la première partie. L'état de X1 et X2 indique l'écoute passive pour obtenir des informations sur les voisins de deux sauts de la cible (ses trois sauts voisins) via paquet de TC. Dans la figure 4.1 à la fin de la première partie, chaque nœud (X1, X2) obtient des informations sur (f, g, h, i).

Désirable : c'est l'un des deux modes d'attaque possibles dans la deuxième partie pour assurer une synchronisation efficace entre un nœud coopératif. Le mode désirable est le mode choisi par le nœud qui contrôle une attaque, c'est celle qui commence à ajouter les faux liens avec la moitié des liens détectés dans la première partie (l'écoute passive) puis diffuse le premier faux message HELLO (intelligemment pour remplacer au minimum deux MPR).

Auto : Le mode auto est l'autre mode possible dans la deuxième partie. Le nœud ayant ce mode n'est pas autorisé à générer le message HELLO, ni ajouter les faux liens tant qu'il n'a pas reçu l'ordre de du nœud ayant le mode désirable. Assez simple, seulement après avoir reçu un message HELLO du partenaire, il ajoute le reste des liens dans son propre HELLO message.

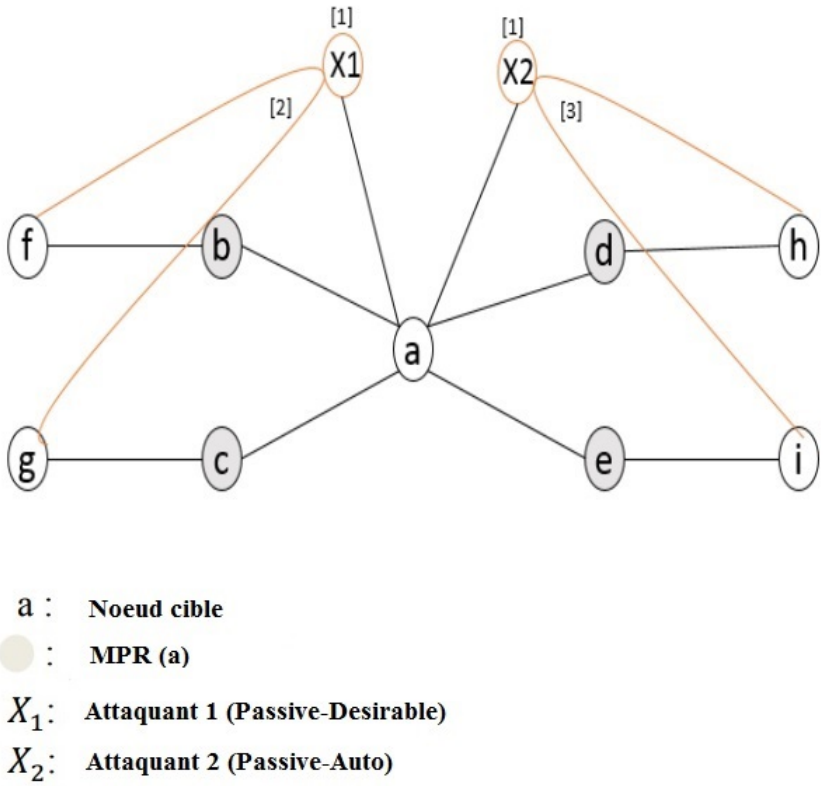

FIGURE 4.1 – *l'attaque Blackhole coopérative 1*

La figure 4.1 illustre les étapes de l'attaque coopérative lancée par les nœuds malveillant X1 et X2. Dans cet exemple, le nœud 'a' sélectionne l'ensemble des nœuds MPR (b, c, d, e) pour atteindre (f, g, h, i) respectivement. Dans la première étape, les nœuds malicieux X1 et X2 entrent silencieusement dans le réseau sans générer des messages HELLO et obtient des informations sur les voisins à deux sauts de la cible 'a' via les paquets TC et qui sont (f, g, h, i). À noter que vers la fin de la première étape X1 et X2 obtiennent les mêmes informations. Dans la deuxième partie, l'attaquant ayant le mode désirable X1 crée des liens usurpés vers les nœuds 'f', 'g' et transmet le message HEELO contenant ces informations à la cible 'a' et au partenaire X2 Ainsi son travail est terminé. Une fois X2 reçoit l'information, il génère un message HELLO contenant 'h' et 'i' comme voisins. finalement cible devra changer son ensemble MPR en ajoutant X1 et X2 au lieu de (b, c, d, e).

Avant l'attaque : MPR (a) = b, c, d, e / b $\longrightarrow$ f ; c $\longrightarrow$ g ; d $\longrightarrow$ h ; b $\longrightarrow$ f ; [$\longrightarrow$: Couverture].

[1] : écoute passive pour obtenir les voisins a deux sauts de la cible a (f, g, h, i).

[2] : X1 (Désirable) génération d'un message HELLO avec 'f' et 'g' comme voisins.

[3] : X2 (auto) génèration d'un message HELLO avec 'h' et "i" en tant que voisins.

Après l'attaque : MPR (a) = X1 , X2 / X1 $\longrightarrow \{f, g\}$; X2 $\longrightarrow \{h, i\}$; [$\longrightarrow$: Couverture].

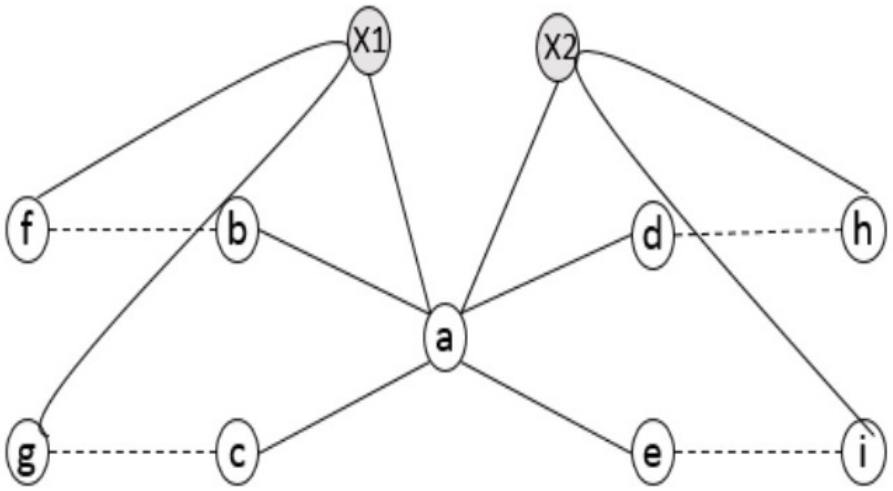

FIGURE 4.2 – *l'attaque Blackhole coopérative 2*

Le résultat de la falsification du message HELLO est la sélection constante de nœuds malveillants comme MPR à la place des nœuds légitimes. Comme nous le savons le nœud MPR joue un rôle très important dans le réseau, donc si le nœud MPR n'est pas un nœud de confiance, il peut partitionner le réseau en injectant des informations pour empêcher un ensemble de nœuds d'atteindre un autre. Dans notre cas, les nœuds malveillants ont réussi une partition de la topologie du réseau, chaque transmission vers une destination dans le réseau qui est le nœud «a» doit passer par X1 ou X2 parce que ceux-ci sont les seuls MPR de 'a'. Enfin, les nœuds malicieux peuvent contrôler le réseau et ils sont en mesure d'ignorer tout ou un ensemble de paquets passant à travers eux.

Ci-dessous dans la figure 4.3, nous présentons un résumé de l'attaque collaborative entre X1 / X2 pour perturber le fonctionnement habituel de la topologie de réseau.

a : Le nœud cilble
X1 : Attaquant1 (passive desirable)
X2 : Attaquant2 (passive auto)
N2hop[target] : les nœuds voisins à deux sauts de la cible.

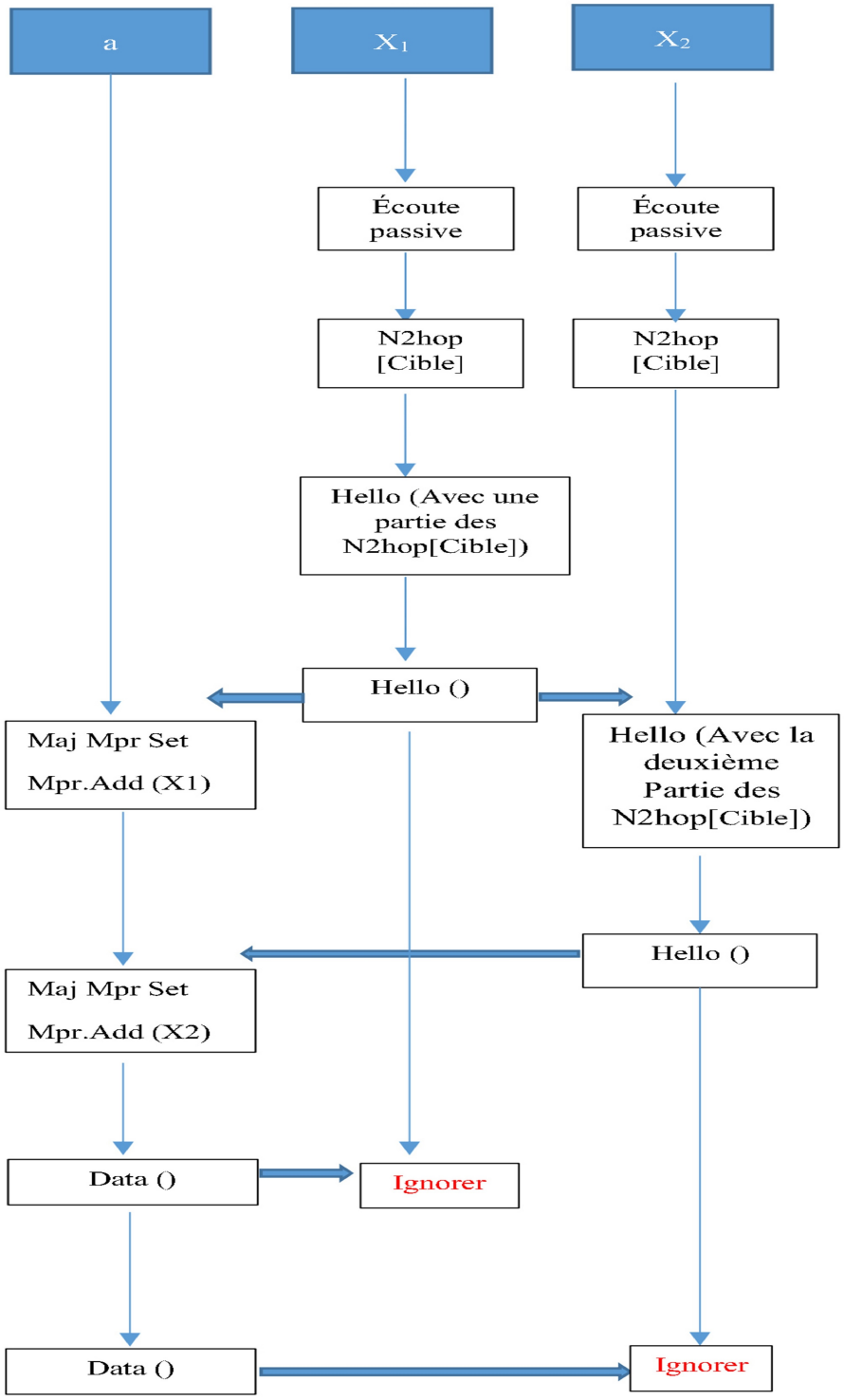

FIGURE 4.3 – *l'attaque coopérative contre OLSR*

4.3 Simulation de l'attaque Coopérative

Afin de prouver l'efficacité de l'attaque coopérative proposée, nous avons effectué des simulations détaillées en utilisant le simulateur de réseaux NS-2.35. Les scénarios de simulation sont composés de 50 nœuds. Où 5, 10, 15 nœuds communiquent et le type de trafic est le débit binaire constant (CBR) avec un débit de paquets de 4 paquets / s. Le nombre de nœuds malveillants est fixé à 2, la portée de transmission des nœuds est fixée à 200 mètres, dans une zone de taille 1000 * 1000 mètres. La durée totale de la simulation est fixée à 150 secondes. Dans notre environnement de simulation, nous supposons que tous les nœuds ont les mêmes caractéristiques et chaque nœud possède seulement une seule interface. Les paramètres de simulation utilisés dans ce document sont présentés dans tableau suivant :

Simulateur	NS2.35
Temps de simulation	150 secondes
Portée de transmission	200 mètres
Type de trafic	CBR
charge utile de données	512 bytes
taux de paquet	4 paquets/s
nombre totale de nœud	50
nombre de nœud communicant	5, 10, 15
nombre de nœud malveillant	2

Table 4.1 – *Paramètre de simulation*

Dans cette simulation, nous mesurons certains paramètres comme indicateur de performance tel que le taux de livraison de paquets (PDR), nombre de paquets perdus, et frais généraux (coût addictif).

taux de livraison de paquets (PDR) : représente le pourcentage de paquets livrés à leurs destinations avec succés par rapport aux paquets transmis dans le réseau.

Paquet perdu : Ce paramètre représente le nombre de paquets abandonnés lors de la livraison de paquets de la source à la destination.

la surcharge (coûts additifs) : représente le rapport entre le nombre de tous les paquets de contrôle et le nombre de paquets de données bien reçus.

Résultats de la simulation

Nous notons dans les résultats présentés les performances du protocole original sans aucune modification comme que "OLSR", et " BH-OLSR" pour représenter le protocole sous une attaque Blackhole présenté au-dessus.

La figure 4.4 illustre une comparaison basée sur le PDR (taux de paquets envoyer avec succès) entre le protocole OLSR original et le protocole sous l'attaque Blackhole discuté au-dessus. OLSR sans attaque présente de bonnes performances, cependant, sa performance sous attaque Blackhole montre une dégradation considérable due aux paquets supprimés par les nœuds malveillants dans le réseau.

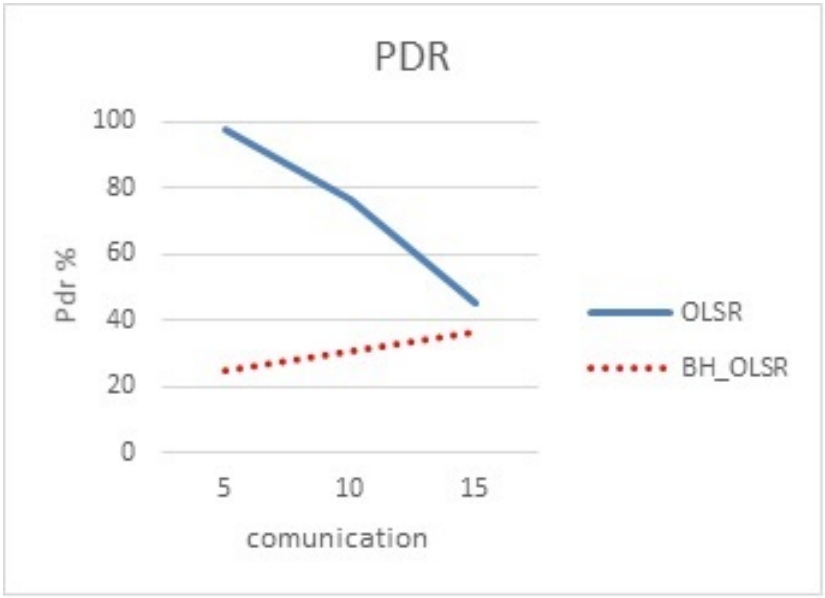

FIGURE 4.4 – *taux des paquets transmis (PDR)*

Dans la figure 4.5, nous observons que l'attaque affecte la directement sur les performances du protocole. On constate que le nombre de paquets perdus connaît une augmentation considérable sous l'attaque. Cela peut être justifié du fait que plus que le nombre des nœuds malveillants augmente, plus qu'il aurait de perte de paquets causés par les nœuds malicieux dans le réseau.

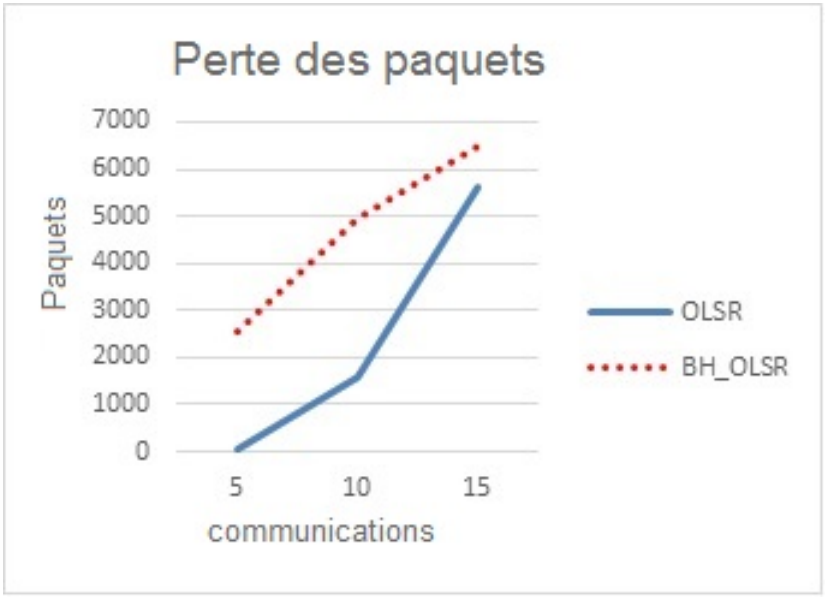

FIGURE 4.5 – *Nombre des paquets perdu*

La figure 4.6 illustre la surcharge dans un réseau de 50 nœuds avec 5, 10, 15 nœuds communicants, et montre une comparaison entre le protocole OLSR standard et le protocole OLSR sous l'attaque pour tester la gravité de l'attaque Blackhole. On observe que la surcharge du réseau est plus importante dans le cas de peu de communication due au nombre limité des paquets de données. La surcharge du réseau est représentée par le nombre de paquets de contrôle par rapport aux paquets donnés dans l'ensemble du réseau, le fait que l'ensemble des nœuds du réseau génère des paquets de contrôle périodiquement et que les nœuds malicieux suppriment tous les paquets de données affectent considérablement la surcharge du réseau.

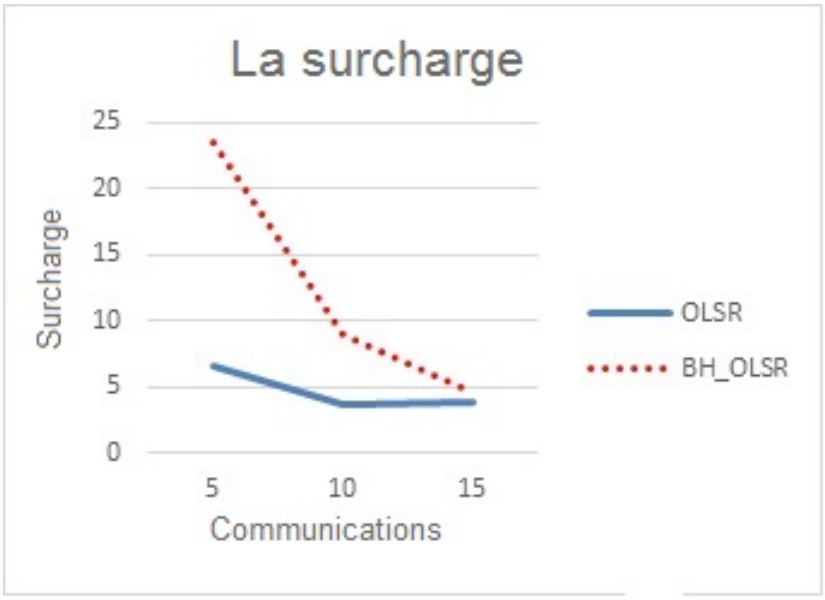

FIGURE 4.6 – *La surcharge du réseau*

4.4 Mécanisme proposé

La plupart des travaux cryptographiques ont été proposés pour permettre aux protocoles d'authentifier les nœuds du réseau et de protéger l'intégrité des informations de routage. La plupart de ces solutions ont été proposées en tant que stratégies préventives contre la modification malveillante des informations de routage, qui se produit généralement avant le lancement d'une attaque par suppression des paquets. Cependant, l'inconvénient majeur de ces solutions est une surcharge importante dans le réseau dû à l'échange d'informations supplémentaires, elles sont également coûteuses en matière d'énergie consommée par les nœuds.

Dans cette section, nous présentons notre mécanisme optimisé pour faire face à l'attaque coopérative de trou noir dans le protocole OLSR. Comme les services de routage de MANET reposent sur la coopération de nœuds de réseau, la meilleure solution pour faire face à une attaque de trou noir coopérative est une solution collaborative entre les nœuds voisins. Dans ce sens, nous présentons notre approche appelée "Neighbours-Trust-Based".

Nous savons qu'OLSR est un protocole de routage proactif ou chaque nœud possède une vue globale de la topologie du réseau. Chaque nœud a des informations sur l'ensemble de ses voisins. Nous supposons qu'un attaquant x force sa sélection autant qu'MPR par le nœud 'a' en incluant 'd','e' dans la liste ses liens symétriques, tel que 'd','e" sont des nœuds voisins à deux voisins de 'a'.

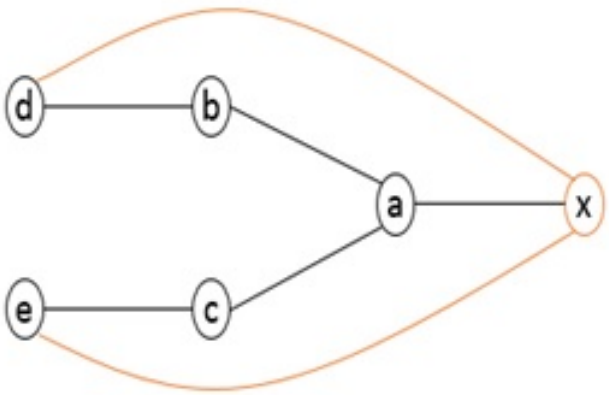

Figure 4.7 – *Usurpation des liens*

Nous savons que 'd' était déjà couvert par 'b'. Le nœud 'b' peut donc facilement identifier la crédibilité du lien déclaré par un attaquant (le lien est symétrique) si cela est demandé par le nœud cible. C'est le point clé de ce que nous allons présenter ci-dessous :

$$Soit : a \rightarrow b; a \rightarrow c; b \rightarrow d; c \rightarrow e$$

ou [$\rightarrow$: un liens Symétrique].

$$a \rightarrow b \rightarrow d; a \rightarrow c \rightarrow e$$

ou [$\rightarrow$ x $\rightarrow$ couvert par x]

Alors : MPR (a) = $\{b, c\}$

On suppose qu'un attaquant x rejoint le réseau

$$a \rightarrow b; a \rightarrow c; b \rightarrow d; c \rightarrow e; x \rightarrow a; x \dashrightarrow d; x \dashrightarrow e;$$

ou [$\rightarrow$: un lien symétrique et $\dashrightarrow$: un faux lien].

Sans vérification : a $\rightarrow$ x$\rightarrow$ d, e

$$MPR(a) = x;$$

Solution : 'b' connais l'ensemble de voisin de d via le message HELLO de 'd' ;
'b' vérifie : d $\rightarrow$ x dans N1(d). [N1 : voisinage a un saut]
'c' connais l'ensemble de voisin de 'e' via le message HELLO de 'e' ;
'c' vérifie : e $\rightarrow$ x dans N1(e). [N1 : voisinage a un saut]
Si la valeur de confiance de 'x' est inférieur au seuil
MPR (a) = $\{b, c\}$

Pour assurer notre mécanisme, il est plus qu'importants de synchroniser la communication entre chaque nœud et ses voisins. Dans notre solution, il n'y a pas de nouveau paquet de contrôle ajouté, nous utilisons seulement les champs réservé contenu dans un paquet HELLO avec une structure optimisée de paquet et un algorithme léger. Pour bien comprendre ce mécanisme nous suivons ces étapes :

— Nous rappelons la structure du paquet HELLO

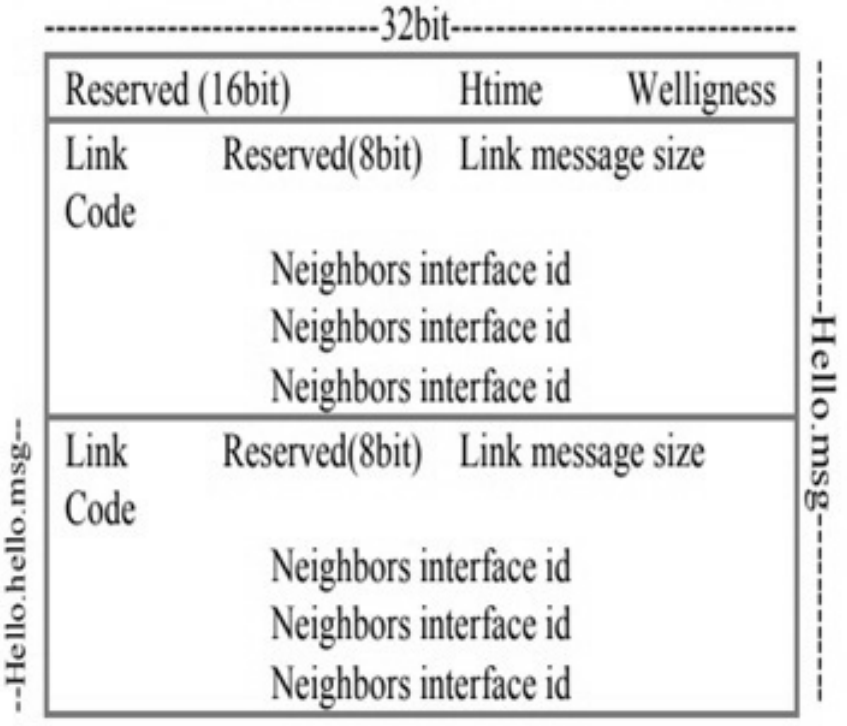

FIGURE 4.8 – *structure du paquet HELLO*

— Le champ 'Reserved' est toujours défini sur 'o'. 'Htime' est l'intervalle d'émission des messages HELLO. Le champ "Weligness'" décrit la volonté du nœud actuel de transporter et de transmettre des paquets à d'autres nœuds. Le champ "Link code" indique des informations sur l'état du lieu entre l'interface de l'expéditeur et l'ensemble d'interfaces voisin suivant. 'Neighbor interface Address' spécifie l'adresse du nœud voisin.
Le champ réservé (16 bits) dans HELLO msg est restructuré logiquement en trois champs : TV (Trusted value), Tag et NodeVerif comme suit :

TV	Tag	NodeVerif
8 bits	2 bits	6 bits

TABLE 4.2 – *le champ 'reserved'*

TV : La valeur de confiance, représenté sur huit bits de champ réservé, indique le taux de liens de confiance (en pourcentage). Cette valeur est calculée par les voisins du nœud demandant l'information. Elle représente le taux des liens symétriques valides entre le nœud suspecté et les voisins communs. La valeur de confiance est calculée comme suit (Nombre de liens de confiance / nombre de voisins communs) :

$$TV(neighbors) = \frac{\sum Valid.link}{\sum Link(neighbors) \cap Link(Suspected))}$$

La valeur de confiance est calculée comme suite :

Let

$$x : Le\ noeud\ suspect$$
$$a : Le\ noeud\ cible$$
$$u : Les\ voisin\ du\ noeud\ cible$$
$$Valid.link = \emptyset$$

For

$$u \in Link(x)$$
$$\exists b \in Link(a)$$
$$If\ \forall u \cap Link(u) \neq \emptyset\ and$$
$$x \cap Link(u) \neq \emptyset$$

$$Then\ Valid.link = Valid.link \cup u$$

End For

$$TV = \frac{|Valid.link|}{|Link(u) \cap Link(x)|}$$

Par exemple dans la figure 4.7 le nœud demandant l'information est 'a', les nœuds 'b', 'c' calcule la valeur de confiance de 'x', par exemple en cas de 'b' la valeur est calculée comme suit :

$$Link(x) = d, e$$
$$Link(b) = d$$
$$Link(x) * Link(b) = d$$
$$x \not\exists Link(d)$$
$$x \rightarrow d \neq Valid.link$$

$$TV = \frac{|Valid.link|}{|Link(b) \cap Link(x)|}$$

$$Link(x) = d, e$$
$$Link(c) = e$$
$$Link(x) * Link(c) = e$$

$$x \not\exists Link(e)$$
$$x \to e \neq Valid.link$$

$$TV = \frac{|Valid.link|}{|Link(c) \cap Link(x)|}$$

La valeur de confiance est calculée et annoncée au nœud demandant l'information uniquement par les voisins ayant un lien commun avec le nœud suspect et qui satisfaisait la condition suivante :

$$Link(node) \cap Link(Suspect) \neq \emptyset$$

Tag : représente deux bits du champ réservé qui indiquent le type d'information dans le paquet HELLO comme suite :

0 : Paquet normal : un message HELLO sans autres informations.
1 : paquet de demande : un message HELLO qui indique la présence d'un nœud soupçonné à vérifier.
2 : paquet de réponse : un message HELLO qui contient une réponse du voisin.

— le processus de vérification de confiance est lancé par un nœud qui détecte une modification dans un ensemble MPR (supposons que x est un nouveau MPR pour couvrir d, e), il génère un paquet HELLO comme suit :

Tag = 1 ;
NodeVerif = x ;
HELLO.HELLO.msg = d, e, avec un code (LinkCode='0')

— Pour chaque voisin recevant un message HELLO avec Tag égal à "1" (paquet de sollicitation) :

  — Récupéré l'identifiant du nœud demandé à vérifier (NodeVerif = x).

  — Récupéré la liste desliens déclarés par x (HELLO.HELLO.msg = d, e).

S'il existe un voisin en commun, la valeur de confiance est calculé pour répondre au nœud demandant l'information. Dans le cas ou le nœud 'd' est un voisin en commun, il vérifie le lien entre 'x' et 'd' et répond dans le prochain message HELLO comme Suite :
Tag=2
TV= TV Calculé
Node. Verif= x

— Lorsque le nœud demandant l'information reçoit une réponse de ses voisins avec la valeur TV calculé par chaque nœud, il calcule la moyenne comme suite (AVGTV) :

$$AVGTV = \frac{\sum TV(Responder_Neighbors)}{Responder_Neighbors}$$

— Enfin, si AVGTV est inférieur au seuil, le nœud x est considéré comme un nœud malveillant, il sera ensuite ajouté à une liste noire avec un champ de Weligness égal à WillNever pour assurer la non sélection autant qu'un nœud MPR.

Ci-dessous dans la figure 4.9, nous présentons un résumé du mécanisme proposé pour faire face à l'attaque de trou noir collaboratifs dans le protocole OLSR.

a : Le nœud cilble
X1 :Attaquant1(passive$\longmapsto$ desirable)
X2 :Attaquant2(passive$\longmapsto$ auto)
N2hop[target] : les nœuds voisins a deux sait de la cible.
TV : la valeur de confiance.
AVG : la moyenne des AV reçu
TRS : Le seuil.
Blacklist : La liste noire des nœuds détectés

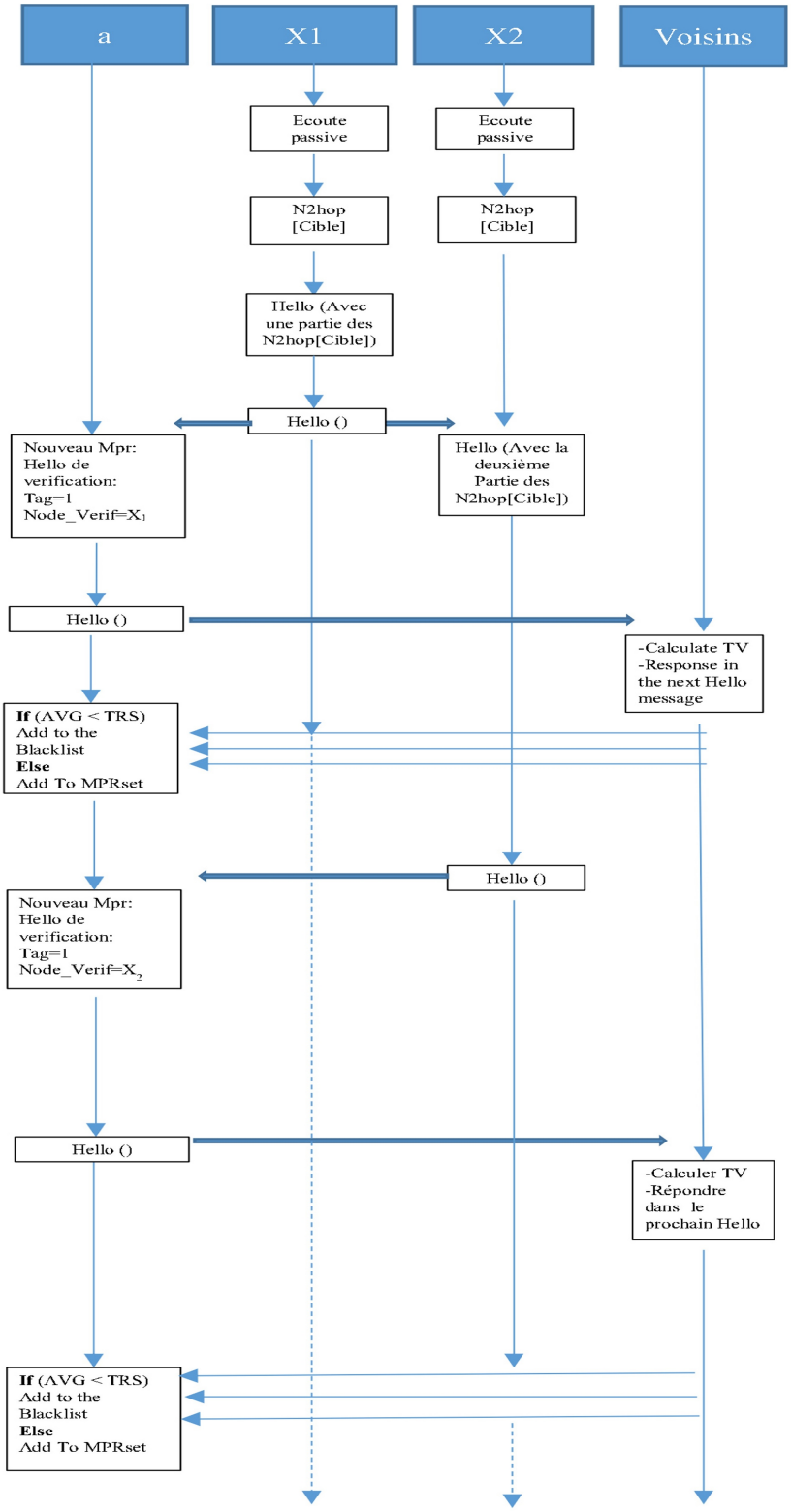

FIGURE 4.9 – *le mécanisme de sécurité*

4.5 Simulation et discussions des résultats

Afin d'évaluer l'efficacité du mécanisme proposé, nous avons effectué des simulations détaillées en utilisant le simulateur de réseaux NS-2.35. . Le scénario de simulation est composés de 50 nœuds. Où 5, 10, 15 nœuds communiquent et le type de trafic est le débit binaire constant (CBR) avec un débit de paquets de 4 paquets / s. Le nombre de nœuds malveillants est fixé à 2, la portée de transmission des nœuds est fixée à 200 mètres, dans une zone de taille 1000 * 1000 mètres. La durée totale de la simulation est définie sur 150 secondes. Dans notre environnement de simulation, nous supposons que tous les nœuds ont les mêmes caractéristiques et chaque nœud est doté d'une interface sans fil. Les paramètres de simulation utilisés dans ce document sont résumés dans tableau ci-dessous :

Simulateur	NS2.35
Temps de simulation	150 secondes
Portée de transmission	200 mètres
Type de trafic	CBR
charge utile de données	512 bytes
taux de paquet	4 paquets/s
nombre totale de nœud	50
nombre de nœud communicant	5, 10, 15
nombre de nœud malveillant	2

Table 4.3 – *Paramètre de simulation*

Dans cette simulation, nous mesurons les paramètres indicateurs de performance suivante : le taux de livraison de paquets (PDR), nombre de paquets perdus, et frais généraux (coût addictif).

Résultat de simulation

Les résultats de simulation fournis dans les figures (4.10, 4.11 et 4.12) présentent les performances des protocoles sous les mêmes scénarios sous OLSR d'origine, OLSR sous l'attaque Blackhole, avec la solution proposée dans (Saddiki *et al.* 2017) et avec le nouveau schéma proposé.
Nous notons dans le résultat présenté que l'OLSR représente la version standard du protocole, BH-OLSR représente OLSR sous une attaque coopérative trou noir, DIBH-OLSR représente une solution proposée dans

(Saddiki *et al.* 2017), et NTB-OLSR représente notre technique proposée (Neighbours-Trusted-Based).
La figure 4.10 représente le taux de distribution de paquets en fonction du nombre de communications. Nous présentons dans ce graphe une comparaison entre un comportement normal d'OLSR (sans et sous attaques) et NTB-OLSR renforcé par un mécanisme de défense. Il a été observé que OLSR sans l'attaque présente de bonnes performances, cependant, sa performance sous attaque de trous noirs montre une dégradation considérable, également en DIBH-OLSR car la performance est présentée contre une attaque coopérative et non pas un seul attaquant. La dégradation de PDR est due aux paquets supprimer par des nœuds malveillants dans le réseau. Le NTB-OLSR montre une amélioration au niveau du PDR due à la détection de tous les nœuds malveillants.

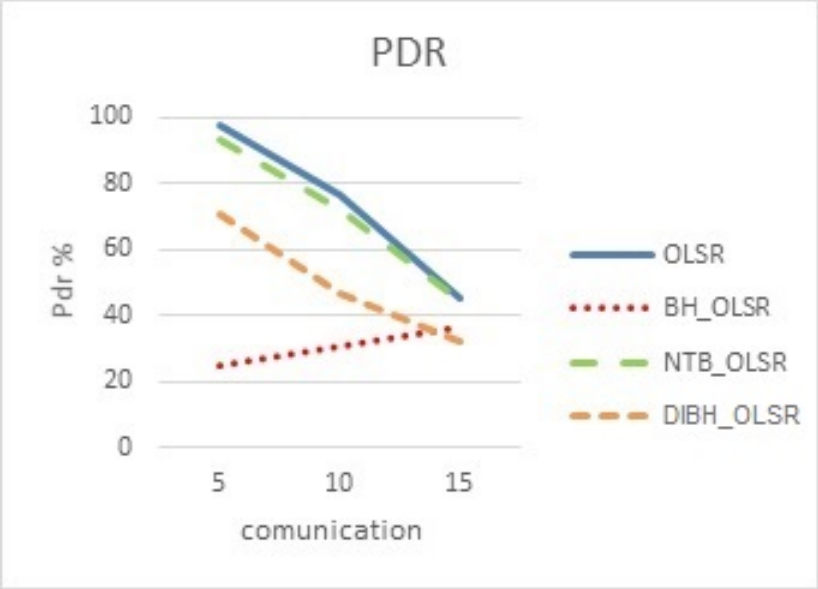

FIGURE 4.10 – *Taux des paquets transmis avec succès (PDR)*

La figure 4.11 illustre que l'attaque affecte clairement les performances du protocole OLSR normal en augmentant le nombre de paquets supprimés par les nœuds malveillants. Encore une fois, le graphe montre que l'attaque n'a aucun effet sur notre proposition, mais ce type d'attaque peut passer sous le seuil fixé dans DIBH-OLSR et le nombre de paquets supprimés augmente au fur et à mesure que le nombre de communications augmente. Dans le mécanisme proposé NTB-OLSR, la solution diminue le nombre de paquets perdus après la détection de tous les nœuds malveillants dans le réseau.

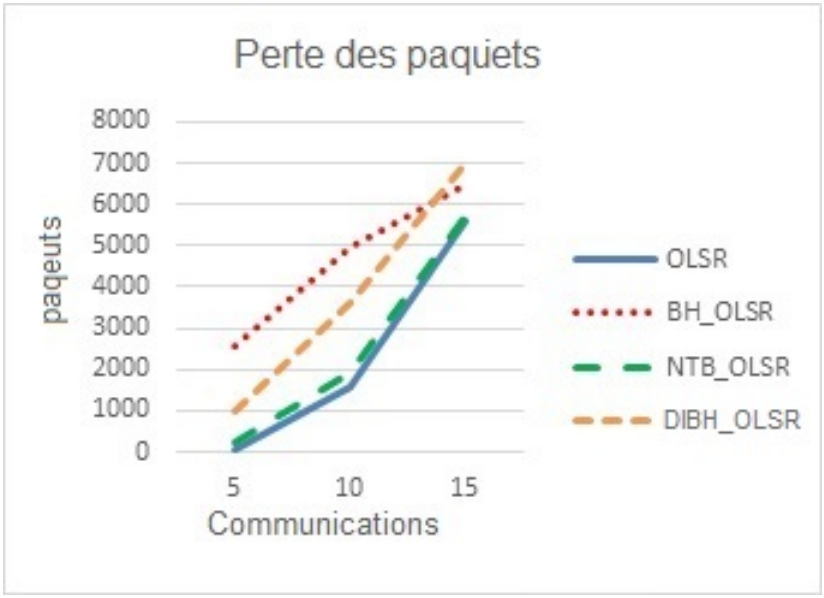

FIGURE 4.11 – *Nombre des paquets perdu*

Comme le montre la figure 4.12, on observe une augmentation de la surcharge dans le réseau sous attaque. Selon la technique d'attaque le nombre de paquets de données reçues est petit par rapport au paquet de contrôle généré. Cependant, dans notre schéma proposé, les nœuds malveillants sont détectés et isolés dans la seconde phase lorsque la valeur de confiance était inférieure au seuil. Ainsi, le nombre de paquets de données transmises avec succès augmente. Cela rend le réseau beaucoup moins surchargé.

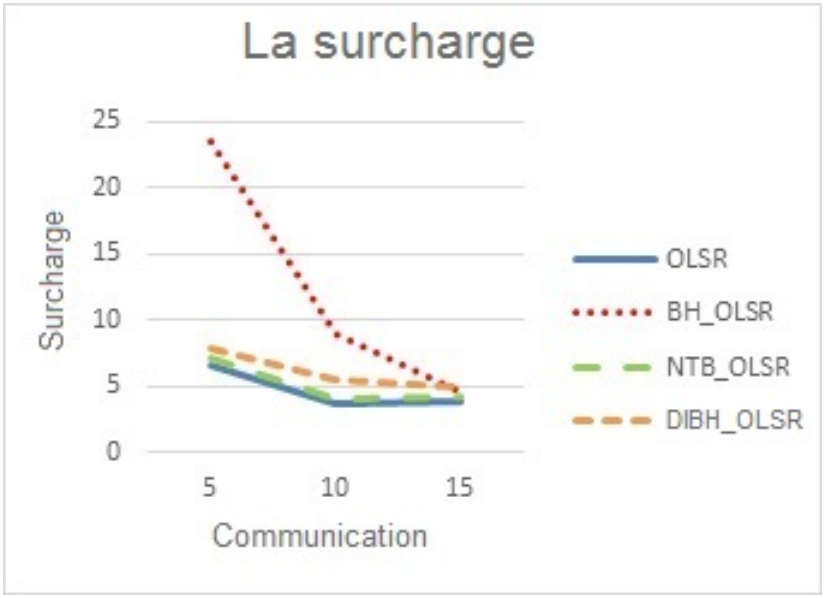

FIGURE 4.12 – *La surcharge dans le réseau*

Conclusion du chapitre

Dans ce chapitre, nous avons discuté les problèmes de sécurité dans les MANET, en particulier dans le protocole OLSR et de sa vulnérabilité contre les attaques de trous noirs coopératifs. Nous avons présenté un nouveau type d'attaque coopératif. L'idée principale de cette attaque est d'ajouter intelligemment des liens usurpés par deux nœuds malveillants, de cette façon il force la sélection des deux nœuds malveillants en tant que MPR et détourne le trafic. Après cela, nous avons présenté un nouveau schéma optimisé appelé «Neighbours-Trust-Based», le noyau de notre travail est de collaborer avec les voisins pour calculer une valeur de confiance de chaque nouveau MPR. La synchronisation entre les nœuds est plus que nécessaire pour garantir le schéma proposé. La solution est implémentée sans ajouter de nouveau paquet de contrôle. Nous avons démontré l'efficacité de notre système en se basant sur les métriques de performance à travers une simulation détaillé sous NS-2.

Conclusion et perspective 5

Sommaire

5.1 Conclusion 88
5.2 Perspective 89

5.1 Conclusion

Dans cette thèse, nous nous sommes intéressé par l'aspect sécuritaire des réseaux mobiles ad hoc. Le travail a été focalisé sur le protocole proactif OLSR et la vulnérabilité contre l'attaque blackhole, blackhole coopératifs et déni de service. En effet, le protocole OLSR présente beaucoup d'avantage tel que les bonnes performances dans les réseaux denses à faible mobilité, mais malheureusement, en raison des caractéristiques des réseaux ad hoc d'une part, et les techniques utilisées dans le protocole tel que l'inondation par MPR d'autre part, rend OLSR de plus en plus vulnérable aux attaques principalement l'attaque par déni de service. Afin de pallier à ces problèmes nous avons proposé un mécanisme de sécurité basé sur la vérification optimisée des informations propagées dans le réseau. Pour atteindre cet objectif, nous avons dans un premier temps commencé par l'état de l'art qui nous a permis de bien comprendre la problématique et d'avoir une idée bien détailler sur les solutions proposées par différents chercheurs à travers le monde. Cependant, la revue de cet état de l'art nous a permis de conclure qu'il reste encore des problématiques ouvertes.

Nous avons présenté un schéma de détection contre le modèle de l'attaque blackhole basée sur l'usurpation de lien. Le mécanisme présenté est divisé en deux parties, l'objectif de la première phase est de détecter un comportement suspect du nœud qui inonde de fausses informations dans le réseau en échangeant une moyenne calculée par chaque nœud pour aboutir à un seuil à ne pas dépasser par les nœuds dans le réseau, sinon il sera considéré comme un suspect. La seconde partie est basée sur une vérification optimisée des liens du suspect en échangeant des messages dans chaque zone, les événements sont déclenchés lorsqu'un nœud présente une très bonne performance par rapport au reste des nœuds de sa zone. Nous avons également proposé une solution contre la deuxième forme de l'attaque blackhole (blackhole coopératif). Cette solution est basé sur la confirmation de la confiance d'un nœud avant la sélection autant qu'un MPR.

Enfin nous avons évalué notre solution à travers des simulations sous le simulateur NS-2. À travers différents scénarios, et en variant le nombre des nœuds attaquant dans le réseau, nous avons montré l'efficacité du mécanisme proposé pour renforcer le protocole OLSR contre l'attaque blackhole (déni de service). Les résultats ont montré que la solution proposée augmente considérablement le taux des paquets transmis avec succès sans affecter la surcharge dans le réseau.

5.2 Perspective

À l'issue de cette thèse, nous pouvons distinguer des perspectives laissant envisager certains travaux complémentaires. Notre travail ne constitue qu'une partie de ce qui doit se faire dans la sécurité des MANETs. Dans le mécanisme proposé, nous avons focalisé le travail sur l'attaque blackhole et déni de service contre le protocole de routage OLSR. Nous proposons d'abord d'évaluer le mécanisme de sécurité avec d'autres types d'attaque qui peuvent perturber le fonctionnement du protocole, ainsi faire étendre le mécanisme de détection de manière à inclure une large plage d'attaques et de menaces (à partir des attaques inhérentes au protocole OLSR aux attaques communes contre un protocole de routage proactif).

Ensuite dans le mécanisme proposé dans le chapitre IV, nous avons focalisé le travail sur la confiance entre les nœuds basés sur l'état des liens et les fausses déclarations au niveau des liens, dans un autre point, de des futurs travaux nous proposons d'adapter notre proposition avec d'autres métriques telles que l'énergie afin de sécuriser la version du protocole OLSR ou l'énergie est considéré comme un critère trés important lors de la sélection des nœuds MPR.

Enfin, Nous avons utilisé le simulateur réseau NS-2 pour tester les protocoles de routage, anticipé les problèmes, et prouvé la crédibilité des solutions proposées. Il serait intéressant de tester les mécanismes proposés dans un environnement réel pour comparer et valider les résultats obtenus par simulations.

Liste des publications

Journal internationale

K. Saddiki, S. Boukli-Hacene, P. Lorenz, M. Gilg, "Black hole attack detection and ignoring in OLSR protocol", International Journal of Trust Management in Computing and Communications, Inderscience Publishers, Vol. 4, No. 1, 2017, pp. 75-93.

Conference internationale

K. Saddiki, S. Boukli-Hacene, P. Lorenz, M. Gilg, "Trust-Neighbors-Based to mitigate the cooperative black hole attack in OLSR protocol", Sixth International Symposium on Security in Computing and Communications, SSCC'18, September 19-22, 2018, Bangalore, India.

Bibliographie

[Aarti & Tyagi 2013] S.S. Aarti et S.S. Tyagi. *Review on MANETs characteristics, challenges, application and security attacks*. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 5, pp.252-257, 2013.

[Abd El-nabi 2005] T. H. Abd El-nabi. *Modeling And simulation Of a routing protocol for Ad Hoc Networks combining Queuing Network analysis and ant colony algorithms*. PhD thesis, Thesis University Deuisburg-Essen, 2005.

[Abdalla *et al.* 2011] A. M. Abdalla, I. A. Saroit, A. Kotb et A. H. Afsari. *Misbehavior nodes detection and isolation for MANETs OLSR protocol*. Procedia Computer Science, vol. 3, pages 115–121, 2011.

[Abusalah *et al.* 2008] L. Abusalah, A. A. Khokhar et M. Guizani. *A survey of secure mobile ad hoc routing protocols.* IEEE Communications Surveys and Tutorials, vol. 10, no. 1-4, pages 78–93, 2008.

[Adjih *et al.* 2005] C. Adjih, D. Raffo et P. Muhlethaler. *Attacks against OLSR : Distributed key management for security*. In 2nd OLSR Interop/Workshop, Palaiseau, France, volume 14, pages 1–5, 2005.

[Adnane *et al.* 2013] A. Adnane, C. Bidan, De Sousa J. et Rafael T. *Trust-based security for the OLSR routing protocol*. Computer Communications, vol. 36, no. 10-11, pages 1159–1171, 2013.

[Ahmadi 2010] S. Ahmadi. Mobile wimax : A systems approach to understanding ieee 802.16 m radio access technology. Academic Press, 2010.

[Alagha *et al.* 2001] K. Alagha, G. Pujolle et G. Vivier. Réseaux de mobiles et réseaux sans fil. Eyrolles, 2001.

[Azza *et al.* 2015] M. Azza, S. Boukli Hacene et K. M. Faraoun. *A Cross Layer for Detection and Ignoring Black Hole Attack in MANET*. International Journal of Computer Network and Information Security, vol. 7, no. 10, page 42, 2015.

[Baadache & Belmehdi 2014] A. Baadache et A. Belmehdi. *Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks*. Computer Networks, vol. 73, pages 173–184, 2014.

[Baiad *et al.* 2016] R. Baiad, O. Alhussein, H. Otrok et S. Muhaidat. *Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET*. Vehicular Communications, vol. 5, pages 9–17, 2016.

[Bayyati 2009] A. Bayyati. *Security Management for Mobil Ad hoc Network of Networks (MANoN)*. dissertation, Monfort University, Leicester United Kingdom,, 2009.

[Boukhalda 2006] L. Boukhalda. *Prise en compte de la qualité de service dans les réseau mobiles Ad-Hoc*. PhD thesis, University paris XII, 2006.

[Chou 2013] T. S. Chou. *Security threats on cloud computing vulnerabilities*. Internationnal Journal of Computer Science and Information Technology, 5(3) : 79-88, 2013.

[Clausen & Jaquet 2003] T. Clausen et P. Jaquet. *Optimized Link State Routing Protocol OLSR*. IETF Request for Comments : 3626, 2003.

[Dahlman *et al.* 2013] E. Dahlman, S. Parkvall et J. Skold. 4g : Lte/lte-advanced for mobile broadband. Academic press, 2013.

[De Aguiar *et al.* 2009] A. B. De Aguiar, Neto A. M. S. Cunha R. P. P. et R. F. Pinheiro. *A Novel Model for Optimized GSM Network Design*. arXiv preprint arXiv :0909.1045, 2009.

[Dhillon *et al.* 2004] D. Dhillon, T. S. Randhawa, M. Wang et L. Lamont. *Implementing a fully distributed certificate authority in an OLSR MANET*. In Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, volume 2, pages 682–688. IEEE, 2004.

[Farahani 2008] S. Farahani. *ZigBee Wireless Networks and Transeivers*. 1st Edition. Elsevier,, 2008.

[Farooq *et al.* 2010] T. Farooq, D. Llewellyn-Jones et M. Merabti. *Mac layer dos attacks in ieee 802.11 networks*. In The 11th Annual Conference on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2010), Liverpool, UK. Citeseer, 2010.

[Geier 1999] J. Geier. *Wireless LANs Implementating interoperable networks*. Macmillan Network Architecture ef developpement Series USA, 1999.

[Gupta 2016] N. K. Gupta. Inside bluetooth low energy. Artech house, 2016.

[Hamrioui 2014] S. Hamrioui. *Incidences de l'amélioration des interactions entre les protocoles MAC-routage et MAC-transport sur la performance d'un MANET*. PhD thesis, University mouloud maamri, 2014.

[Hauspie 2001] M. Hauspie. *Spécification et implémentation de la couche de communication sans fil pour Objets Mobiles Communicant*. PhD thesis, PhD thesis, Laboratoire d'informatique fondamentale de Lille, 2001.

[Issariyakul & Hossain 2012] T. Issariyakul et E. Hossain. *Introduction to Network Simulator 2 (NS2)*. In Introduction to Network Simulator NS2, pages 21–40. Springer, 2012.

[Jamalipour 2003] A. Jamalipour. *The Wireless Mobile Internet, Architecture, Protocols and Services*. John Wiely & Sons Ltd, 368-384., 2003.

[Jenomactaline & Joywinniewise 2016] P. J. Jenomactaline et D. C. Joywinniewise. *Black Hole Attack Detection Using HlA with Optimized Link State Routing Protocol In Wanet*. International Journal Of Engineering And Computer Science ISSN : 2319-7242 Volume 5 Issue 10,Page No. 18649-18654, 2016.

[Jiang *et al.* 1999] M. Jiang, L. Jinyang et Y.C. Tay. *Cluster Based Routing Protocol(CBRP)*. draft-ietf-manet-cbrp-spec-01.txt,, 1999.

[Johnson *et al.* 2003] D. Johnson, Y. Hu et D. Maltz. *The dynamic source routing protocol for mobile ad hoc networks (DSR)*. draft-ietf-manetdsr-09. txt, 2003.

[Junhai *et al.* 2009] L. Junhai, Y. Danxia, X. Liu et F. Mingyu. *A survey of multicast routing protocols for mobile ad-hoc networks*. IEEE communications surveys & tutorials, vol. 11, no. 1, pages 78–91, 2009.

[Kannhavong *et al.* 2007] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato et A. Jamalipour. *A survey of routing attacks in mobile ad hoc networks*. IEEE Wireless communications, vol. 14, no. 5, 2007.

[Kaur *et al.* 2013] H. Kaur, M. Bala et V. Sahni. *Performance Evaluation of AODV OLSR and ZRP Routing Protocols under the Black hole attack in MANET*. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), vol. 2, no. 6, 2013.

[Khabbazian *et al.* 2009] M. Khabbazian, H. Mercier et V. K. Bhargava. *Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks*. IEEE Transactions on Wireless Communications, vol. 8, no. 2, pages 736–745, 2009.

[Labiod 2002] H. Labiod. *Etude sur le Wifi pour le conseil stratégique des technologies de l'information(CSTI)*. ENST, 2002.

[Lindemann & Thummler 2001] C. Lindemann et A. Thummler. *Performance analusis of the general packet radio service*. In 21st International Conference on Distributed Computing System,, 2001.

[Marnerides 2007] A. Marnerides. *Working with the GridKit Overlay Framework The secure AntHocNet Iverlay*. PhD thesis, Thesis Lancaster University,, 2007.

[Mbarushimana & Shahrabi 2007] C. Mbarushimana et A. Shahrabi. *Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks*. In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, volume 2, pages 679–684. IEEE, 2007.

[Murthy & Manjo 2004] C. Murthy et B. S. Manjo. *Ad Hoc Wireless Networks : Architecture and protocols*. Prentice Hall communication engineering and emerging technologies series Upper Saddle River, 2004.

[Murthy & Manoj 2004] C. S. R. Murthy et B.S. Manoj. *Ad hoc Wireless Networks Architectures and Protocols*. Prentice Hall Communication Engineering and Emerging Technologies Series, 2004.

[Nuaymi 2007] L. Nuaymi. *WiMAX : Technology for Broadband Wireless Networking*. John Wiley & Sons Ltd, 2007.

[Ogier *et al.* 2003] R. Ogier, M. Lewis et Templin F. *Topology dissemination based on reverse-path forwarding (TBRPF)*. IETF Internet Draft, 2003.

[Paolo 2005] S. Paolo. *Topology Control in Wireless Ad Goc and Sensor Networks*. Jhon Wiley & Sons Ltd, 2005.

[Perkins & Bhagwat 1994] C. E. Perkins et P. Bhagwat. *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers*. In ACM SIGCOMM computer communication review, volume 24, pages 234–244. ACM, 1994.

[Perkins *et al.* 2003] C. Perkins, E. Belding-Royer et S. Das. *Ad hoc on-demand distance vector (AODV) routing*. Rapport technique, IETF Internet Draft, 2003.

[Potukuchi & Kant 2017] R. V. Potukuchi et K. Kant. *Trust aware cooperative optimised link state routing protocol*. International Journal of Systems, Control and Communications, vol. 8, no. 1, pages 1–21, 2017.

[Prashar & Kapur 2016] L. Prashar et R. K. Kapur. *Performance analysis of routing protocols under different types of attacks in MANETs*. In Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2016 5th International Conference on, pages 405–408. IEEE, 2016.

[Prateek & Koushik 2018] S. K. Prateek et K. Koushik. *Countering Control Message Manipulation Attacks on OLSR*. In Proceedings of the 19th International Conference on Distributed Computing and Networking, ICDCN '18, pages 22 :1–22 :9, New York, NY, USA, 2018. ACM.

[Prateek *et al.* 2017] S. K. Prateek, K. Koushik et K. Charles. *Reputation Routing in MANETs*. In In 2017 IEEE 85th Vehicular Technology Conference (VTC-Fall). IEEE, 2017.

[Pujolle 2014] G. Pujolle. Les réseaux. edition Eyrolle, 2014.

[Raffo *et al.* 2005] D. Raffo, C. Adjih, T. Clausen et P. Mühlethaler. *Securing OLSR using node locations*. In Wireless Conference 2005-Next Generation Wireless and Mobile Communications and Services (European Wireless), 11th European, pages 1–7. VDE, 2005.

[Ranjan *et al.* 2015] R. Ranjan, N. K. Singh et A. Singh. *Security issues of black hole attacks in MANET*. In Computing, Communication & Automation (ICCCA), 2015 International Conference on, pages 452–457. IEEE, 2015.

[Richardson 2000] K. W. Richardson. *Umts overview*. Electronics & Communication Enfeneering Journal, 2000.

[Saddiki *et al.* 2017] K. Saddiki, S. Boukli-Hacene, P. Lorenz et M. Gilg. *Black hole attack detection and ignoring in OLSR protocol*. International Journal of Trust Management in Computing and Communications, vol. 4, no. 1, pages 75–93, 2017.

[Sahu *et al.* 2016] Y. Sahu, M.A. Rizvi et R.K. Kapoor. *Intruder detection mechanism against DoS attack on OLSR*. In Eco-friendly Computing and Communication Systems (ICECCS), 2016 Fifth International Conference on, pages 99–103. IEEE, 2016.

[Saltzer *et al.* 1984] J. H. Saltzer, D. P. Reed et D. D. Clark. *End-to-end arguments in system design*. ACM Transactions on Computer Systems (TOCS), vol. 2, no. 4, pages 277–288, 1984.

[Schweitzer *et al.* 2016] N. Schweitzer, A. Stulman, A. Shabtai et R. D. Margalit. *Mitigating denial of service attacks in OLSR protocol using fictitious nodes*. IEEE Transactions on Mobile Computing, vol. 15, no. 1, pages 163–172, 2016.

[Semchedine *et al.* 2016] F. Semchedine, A. Moussaoui, K. Zouaoui et S. Mehamel. *CRY OLSR : Crypto Optimized Link State Routing for MANET*. In Multimedia Computing and Systems (ICMCS), 2016 5th International Conference on, pages 290–293. IEEE, 2016.

[Shirey 2007] R. W. Shirey. *Inetrnet Security Glossary*. Version 2. Network Working Group, 2007.

[Siddiqui *et al.* 2015] F. Siddiqui, S. Zeadally et K. Salah. *Gigabit wireless networking with IEEE 802.11 ac : technical overview and challenges*. Journal of Networks, vol. 10, no. 3, page 164, 2015.

[Singh *et al.* 2018] A. Singh, G. Singh et M. Singh. *Comparative Study of OLSR, DSDV, AODV, DSR and ZRP Routing Protocols Under Blackhole Attack in Mobile Ad Hoc Network*. In Choudhury S. Singh R. et A. Gehlot, editeurs, Intelligent Communication, Control and Devices, pages 443–453. Springer Singapore, 2018.

[Soin *et al.* 2009] C. Soin, R. Jain et A. Tamimi. *Scheduling in IEEE 802.16 e mobile WiMAX networks : key issues and a survey*. IEEE Journal on selected areas in communications, vol. 27, no. 2, pages 156–171, 2009.

[Stojmenovic 2002] I. Stojmenovic. *Handbook of wireless Networks and Mobile computing*. John Wiley & Sons,, 2002.

[Tanenbaum 2003] A. Tanenbaum. *Réseaux.* 4eme edition, Pearson Education, 2003.

[Ubéda 2006] S. Ubéda. *Réseau ad hoc : principe et routage, Réseau mobiles ad hoc et réseau de capteurs sans fil*. PhD thesis, ermes Science, Lavoisier., 2006.

[Vanamala & Rao 2017] C.K. Vanamala et G. R. Rao. *Strategic modeling of secure routing decision in OLSR protocol in mobile ad-hoc network*. In Computer Science On-line Conference, pages 201–208. Springer, 2017.

[Vigna *et al.* 2004] G. Vigna, S. Gwalani, K. Srinivasan, E. M. Belding-Royer et R. A. Kemmerer. *An intrusion detection tool for AODV-based ad hoc wireless networks*. In Computer Security Applications Conference, 2004. 20th Annual, 2004.

[Wenyuan *et al.* 2005] X. Wenyuan, T. Wade, W. Timothy et Z. Yanyong. *The Feasibility of Launching and Detecting Jamming attack in wireless networks*. in 6th ACM internationnal Symposium on Mobile Ad Hoc Networking and Computing, 2005.

[Xing & Wang 2006] F. Xing et W. Wang. *Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Network*. . In IEEE Military Communication Conference. MILCOM, pages 1-7, 2006.

[Xuan 2007] Y. Xuan. *Defence system on DDos attack in Ad Hoc network*. PhD thesis, Thesis Auburn University Alabama, ., 2007.

[Zougagh *et al.* 2014] H. Zougagh, A. Toumanari, R. Latif, Y. Elmourabit et N. Idboufker. *Modified olsr protocol for detection and prevention of packet dropping attack in manet*. International Journal of Computer Applications, vol. 100, no. 17, 2014.

[Zygmunt 1997] J. H. Zygmunt. *A new routing protocol for the recon gurable wireless networks*. In . In Proceedings of 6th IEEE International Conference on Universal Personal Communications, IEEE ICUPC'97, San Diego, California, USA, volume 2, pages 562-566. IEEE, IEEE,, 1997.

Notations

IEEE	Institue of Electricol and Electronicol Engenies
WPAN	Wireless Personal Area Networks
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WWAN	Wireless Wide Area Network
BSS	Basic Service Set
ESS	Extended Service Set
BTS	Base Tranceiver System
IBSS	Independent Basic Service Set
Ack	Acknowledgment
RTS	Request To Send
CTS	Clear To Send

PDA : Personal Digital Assistant.

WiMAX	Worldwide Interoperability for Microwave Access
GSM	Groupe Spécial Mobile
GPRS	General Packet Radio Service
EDGE	Enhanced Data GSM Environment
UMTS	Universal Mobile Telecommunication System
HomeRF	Home Radio Frequency

OSI	Open System Interconnexion
QoS	Quality Of Service
TCP	Transfer Control Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
WEP	Wired Equivalent Privacy
IV	Initialisation Vector
ANSN	Advertised Neighbor Sequence Number
Wi-Fi	Wireless Fidelity
AP	Access Point
IP	Internet Protocol
ESS	Extended Service Set
IANA	Internet Assigned Numbers Authority
MANET	Mobil Ad Hoc Network
CA	Certeficate Authoriy
CH	Cluster Head
PKI	Public Key Infrastructure
UDP	User Datagram Protocol
TTL	Time To Live
SN	Sequence Number
VANET	Vihicular Ad hoc NETwork
ID	IdDentity

GPS	Global Position System
OLSR	Optimized Link State Protocol
MPR	MultiPoint Rely
TC	Topology Control
MID	Multiple Interface Declaration
HNA	Host and Network Association
DSDV	Destination Sequence Distance Vector
TBRPF	Topology Dessimination based on Revers Path Forwarding
AODV	(Ad-hoc On Demande Distance Vector
RREQ	Route Requeste
RREP	Route Reply
CBR	Constant Bit Rate
DSR	Dynamic Source Routing
ZRP	Zone Routing Protocol
CBRP	Cluster Based Routing Protocol
IETF	Internet Engeneering Task Force
SYN	Synchronize
MIDM	Man In The Middle
MAC	Medium Access Control
DOS	Denial Of Service
DDOS	Destributed Denial Of Service
NS	Netowrks Simulator
TCL	Tool Command Language

TK	Tool kit
OTCL	Object Tool Command Language
NAM	Network Animator
PDR	packet delivery ratio

الملخص

إن الشبكات الانية هي عبارة عن شبكات يتم تشكيلها ديناميكيًا من خلال التعاون العشوائي بين مجموعة من العقد المستقلة التي تنظم نفسها تلقائيًا بحيث يمكن نشرها بسرعة ، والتي يجب أن تكون قادرة على التكيف مع التحركات المختلفة التي قد تحدث داخل الشبكة الانية . لا تصبح هذه الشبكات مفيدة إلا باستخدام بروتوكولات التمرير التي يمكن الاعتماد عليها لتمرير الحزم من المصدر إلى الوجهة. يرفع هذا النوع من البروتوكولات تحديات جديدة من حيث الأمن والحماية من مختلف التهديدات. لسوء الحظ هم عرضة لأنواع ميخلفة من الهجمات مثل رفض الخدمة (الثقب الأسود). في أطرحتنا، نحن مهتمون بالجانب الأمني على مستوى طبقة الشبكة (اوبصغ)، ودراسة تأثير هجمات رفض الخدمة التي تعطل الأداء السليم لهذه الشبكات. وأخيرا اقتراح آلية أمنية فعالة ضد هذه التهديدات

Résumé

Les réseaux mobiles "Ad hoc" sont des réseaux formé de façon dynamique grâce à la coopération d'un ensemble arbitraire de nœuds indépendant qui s'organisent automatiquement de façon à être rapidement déployables, et qui doivent pouvoir s'adapter aux différents mouvements pouvant intervenir au sein des nœuds mobiles. Ces réseaux ne peuvent pas être utiles sans l'utilisation des protocoles de routage fiable pour acheminer les paquets de la source à la destination. Ces derniers soulèvent de nouveaux défis en termes de sécurité et de protection contre et les menaces. Malheureusement ils sont vulnérables à différents types d'attaques telles que le Déni de service (Black hôle). Dans notre thèse nous somme intéresser par l'aspect sécuritaire des MANET (Mobil Ad Hoc Network) au niveau de la couche réseau (OLSR), Etudier l'effet des attaques de type déni de service qui perturbent le bon fonctionnement de ces réseaux. Pour Enfin proposer un mécanisme de sécurité efficace contre ces menaces.

Abstract

MANETs are wireless networks dynamically formed by the cooperation of an arbitrary set of independent nodes which organize themselves automatically to be rapidly deployable, and which must be able to adapt to the conditions of the network. Ad hoc networks can not be useful without the use of reliable routing protocols to route packets from source to destination. These routing protocols raise new challenges in terms of security and protection against threats. Unfortunately, they are vulnerable to different types of attacks such as Denial of Service (Black Hole). In our thesis, we are interested by the security aspect of the MANET (Mobil Ad Hoc Network) at the network layer (OLSR), Study the effect of denial of service attacks that disrupt the proper functioning of these networks. Finally, we propose an effective security mechanism against these threats.