N°d'ordre: .....

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



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

Thèse de Doctorat

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

Par

Mme Rabiaa NAIB

Un système de détection d'intrusion dans VANETs
proposition d'une approche inter-couche

Soutenue le 16 - 05 - 2023 devant le jury :

Pr.	FARAOUN Kamel Mohamed	Université de SBA	Président du jury
Dr.	KHOBZAOUI Abdelkader	Université de SBA	Examinateur
Dr.	BENYAHIA Kada	Université de Saida	Examinateur
Dr.	TEGGAR Hamza	Université de Mascara	Examinateur
Dr.	MEKKAOUI Kheireddine	Université de Saida	Directeur de thèse
Pr.	BOUKLI-HACENE Sofiane	Université de SBA	Co-Directeur de thèse

Année Universitaire : 2022 - 2023

Je dédie ce modeste travail à : Mes précieux et chers parents pour leur amour inestimable, leur confiance, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer. Sans eux cette thèse n'aurait pas pu voir le jour car ils étaient là dans mes moments de doute et de panique « MERCI ».

Je n'oublie pas aussi mes soeurs, mes frères, mon époux et mon fils pour leur soutien moral.

Remerciement

En préambule à cette thèse, nous sommes tennus à nous incliner devant 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 sincères remerciements à mes directeurs de thèse : je commence par feu Dr. ALI-CHERIF Moussa que dieu lui ouvre les portes de son paradis. Egalement, messieurs : Pr. BOUKLI-HACENE Sofiane et Dr. MEKKAOUI Khiereddine qui étaient toujours à l'écoute et disponibles tout au long de la réalisation de cette thèse de doctorat, ainsi que pour leur l'inspiration, leur aide et le temps qu'ils ont bien voulu me consacrer. Une pensée aussi pour les respectueux membres des jurys qui vont honorer par leur présence cet aéroopage.

Enfin, nous adressons nos remerciements les plus sincères aux personnes qui nous ont apporté de près ou de loin leur aide et qui ont contribué à l'élaboration de cette thèse de doctorat.

Table des matières

Table des matières **iv**

Liste des figures **vi**

Liste des tableaux **vii**

Préface **1**

1 Les réseaux Véhiculaires (VANETs) **5**
1.1 Les réseaux Adhoc . . . 6
1.1.1 Définition . . . 6
1.1.2 Les caractéristiques . . . 6
1.1.3 Les défis des réseaux Adhoc . . . 7
1.1.4 Applications . . . 8
1.2 Les réseaux véhiculaires (VANETs) . . . 9
1.2.1 Définition . . . 9
1.3 Le système des réseaux véhiculaires (VANETs) . . . 10
1.3.1 Architecture et composants . . . 10
1.3.2 Les modes de communication dans VANETs . . . 11
1.3.3 Les caractéristiques . . . 12
1.3.4 Les applications . . . 13
1.3.5 Les types de messages . . . 14
1.3.6 Normes et Architecture protocolaire des VANETs . . . 15
1.4 Le routage et les méthodes d'accès dans les VANETs . . . 17
1.4.1 Définition . . . 17
1.4.2 Routage basé sur la position (routage géographique) . . . 18
1.4.3 Protocole de routage basé sur la topologie . . . 18
1.4.4 Le routage basé sur la diffusion (Broadcast routing) . . . 19
1.4.5 Le routage basé sur les grappes (Cluster-Based) . . . 19
1.4.6 Le routage Geocast . . . 19
1.4.7 Les protocoles d'accès de la couche MAC dans les VANETs . . . 20
Conclusion . . . 21

2 Le protocole AOMDV et le mécanisme Cross-Layer **22**
2.1 Le routage multi-chemin . . . 23
2.2 Le protocole AOMDV (Ad-hoc On-demand Multipath Distance Vector) . . . 23
2.2.1 Définition . . . 23
2.3 Types de messages AOMDV . . . 24
2.3.1 Le Paquet HELLO . . . 24
2.3.2 Le Paquet RREQ . . . 25
2.3.3 Le Paquet RREP . . . 25

2.3.4 Le Paquet RERR . . . 25
2.4 Le fonctionnement du AOMDV . . . 26
2.4.1 Le processus de découverte de route . . . 26
2.4.2 Le processus de calcul de chemin inverse . . . 28
2.4.3 Entretient des routes . . . 29
2.5 Le mécanisme Inter-Couche . . . 29
2.6 Les principales attaques contre les réseaux VANETs . . . 30
2.6.1 Les Exigences de sécurité . . . 30
2.6.2 Les attaques contre les protocoles de routage . . . 31
2.7 L'attaque Blackhole dans AOMDV . . . 34
2.8 Conclusion . . . 35

3 Contribution I : Mécanisme de sécurité inter-couche contre l'attaque BlackHole dans les MANETs **36**
3.1 Etat de l'art . . . 37
3.2 Modèle de l'attaque blackhole contre le protocole AOMDV . . . 39
3.3 La solution proposée . . . 40
3.4 Evaluation des performances . . . 46
3.4.1 L'environnement de simulation . . . 46
3.4.2 Présentation du simulateur NS2 (Network Simulator Version-2) . . . 47
3.4.3 Les mesures des performances de la simulation . . . 49
3.4.4 Discussions et comparaisons des résultats de simulation . . . 49
Conclusion . . . 58

4 Contribution II : Une méthode inter-couche pour identifier et isoler les noeuds blackhole dans les réseaux adhoc véhiculaires. **59**
4.1 Etat de l'art . . . 60
4.2 Modèle de l'attaque blackhole contre le protocole AOMDV . . . 63
4.3 Motivation et solution proposée . . . 64
4.3.1 Contributions et motivations . . . 64
4.3.2 La solution proposée . . . 65
4.4 Evaluation de la performance . . . 73
4.4.1 L'environnement de simulation . . . 73
4.4.2 Mesures des performances de la simulation . . . 76
4.4.3 Discussions et comparaisons des résultats de simulation . . . 77
Conclusion . . . 81

5 Conclusion et perspective **82**
5.1 Conclusion . . . 83
5.2 Perspectives . . . 84

Liste des publications **85**

Bibliographie **86**

Notations **93**

Liste des figures

1.1 Un réseau Mobile Adhoc (Singh *et al.* 2016) 6
1.2 Les réseaux véhiculaires VANETs (Hota *et al.* 2021) 10
1.3 Les composants des réseaux véhiculaires VANETs (adoptée de (He *et al.* 2015)) 11
1.4 Architecture de communication dans VANETs (adoptée de (Shah *et al.* 2019)) 12
1.5 Arrangement des canaux DSRC (adoptée de (Naik *et al.* 2017)) 16
1.6 Illustration de IEEE 1609.x et IEEE 802.11p dans la pile de protocoles WAVE (adoptée de (Uzcátegui *et al.* 2009)) 17
1.7 La classification des protocoles de routage dans VANETs (Singh & Agrawal 2014) 18
1.8 Classification des protocoles d'accès de la couche MAC dans le standard IEEE 802.11 (Ma *et al.* 2020)) 20

2.1 Structure de la table de routage. (a) AODV, (b) AOMDV (Marina & Das 2001) 24
2.2 Le format de paquet HELLO 24
2.3 Le format de paquet RREQ 25
2.4 Le format de paquet RREP 25
2.5 Le format de paquet RERR 26
2.6 Le chemin de l'envoie des paquets RREQ et RREP 27
2.7 La Mise à jour de la route dans AOMDV (Marina & Das 2001) 28
2.8 Processus de chemin inverse (He *et al.* 2015) 29
2.9 Le processus de maintenance de route 29
2.10 Illustration d'une décision de routage basée sur les trois couches inférieures OSI (PHY, MAC, NET) (Awang *et al.* 2017)) 30
2.11 L'attaque par déni de service (Upadhyaya 2018) 32
2.12 L'attaque sybil (Sharma *et al.* 2021) 33
2.13 L'attaque Blackhole dans VANETs (Zaidi & Faisal 2018) 34
2.14 L'attaque Blackhole (Hassan *et al.* 2020) 34

3.1 Le pseudo-code de la fonction Pre_ReceiveReply(Packet P) (Mistry *et al.* 2010) 38
3.2 l'attaque Blackhole sur le protocole AOMDV dans les MANETs (Bhardwaj & Singh 2014) 40
3.3 Organigramme de la méthode proposée (Naib *et al.* 2019a) 43
3.4 Flot de simulation 48
3.5 PDF des 10 nœuds communicants en fonction du temps de pause (S) . 50
3.6 PDF des 20 nœuds communicants en fonction du temps de pause (S) . 51
3.7 PDF des 30 nœuds communicants en fonction du temps de pause (S) . 51
3.8 PDF des 40 nœuds communicants en fonction du temps de pause (S) . 52
3.9 AE2ED des 10 nœuds communicants en fonction du temps de pause (S) 53

3.10 AE2ED des 20 nœuds communicants en fonction du temps de pause (S) 54
3.11 AE2ED des 30 nœuds communicants en fonction du temps de pause (S) 54
3.12 AE2ED des 40 nœuds communicants en fonction du temps de pause (S) 55
3.13 NRL des 10 nœuds communicants en fonction du temps de pause (S) . 56
3.14 NRL des 20 nœuds communicants en fonction du temps de pause (S) . 56
3.15 NRL des 30 nœuds communicants en fonction du temps de pause (S) . 57
3.16 NRL des 40 nœuds communicants en fonction du temps de pause (S) . 57

4.1 L'attaque Blackhole (Hassan *et al.* 2020) 64
4.2 Diagramme pour le noeud source 68
4.3 Le Diagramme inter-couche 69
4.4 Sélection de trois différentes zones de Malaga de la topologie du réseau (Toutouh & Alba 2011) 74
4.5 Scénario VANET urbain réel de Malaga (Toutouh *et al.* 2012) 74
4.6 Packet Delivery Fraction 78
4.7 Average End-To-End Delay 79
4.8 Normaized Routing Load 80
4.9 Paquets supprimées par les noeuds Black-Hole 81

Liste des tableaux

2.1 Définition des paramètres des paquets de contrôle du protocole AOMDV 26

3.1 Comparaison entre notre solution et les méthodes proposées dans l'état de l'art. 44
3.2 Paramètres de simulation 46

4.1 Comparaison entre notre solution et les méthodes proposées dans l'état de l'art. 70
4.2 Détails des scénarios VANETs. 75
4.3 Paramètres de simulation 75

Liste des Algorithmes

1 Algorithme du noeud source 41
2 Algorithme noeud de destination ou intermédiaire possédant une route fraîche 41
3 Algorithme du noeud blackhole 42
4 Algorithme du noeud blackhole 42

5 Algorithme du noeud source 66
6 Algorithme du noeud de destination ou intermédiaire possédant une route fraîche 67
7 Algorithme du noeud malveillant 67

Introduction Générale

De nos jours les scientifiques et les ingenieurs sont beaucoup plus motivés dans leurs recherches pour l'amélioration de la sécurité routière et le confort des systèmes de transport et cela grace à l'évolution rapide des voitures qui a rendu les VANETs plus attrayants. Les réseaux véhiculaires VANETs sont une classe de réseaux mobiles Adhoc, dans laquelle, les véhicules communiquent et échangent des informations entre eux ou avec une infrastructure fixée sur les bords des routes. Les principales différences entre les réeseaux VANETs et les réseaux MANETs sont : Le changement de la topologie du réseau qui est fréquent et très rapide, la mobilité élevée des noeuds et le motif régulier de déplacement des noeuds.

Les entités de communication dans les VANETs sont divisées comme suit :

— Les unités embarquées (OBU) qui peuvent communiquer librement entre elles sans passerelles fixes préexistantes.

— Les unités de bord de route (RSU) qui disséminent les informations routières.

En outre, la communication dans ce type de réseau peut prendre deux modes :

— La communication de véhicule à véhicule (V2V) où les véhicules de la même zone de couverture communiquent entre eux sans l'utilisation d'une infrastrastructure

— La communication véhicule-infrastructure (V2I) qui est déclanchée lorsqu'un véhicule veut communiquer avec un autre véhicule situé dans une zone de couverture du RSU.

Dans ce dérnier mode on a recours à un médium sans fil comme le DSRC, le Wi-Fi ou le Bluetooth. Un réseau adhoc véhiculaire fournit un système de transport intelligent qui a pour but d'améliorer d'une part, la sécurité du systéme de transport en utilisant des applications de sécurité routière et d'autre part, le confort du système de transport en utilisant des applications de divertissement. Quant aux applications de sécurité, les véhicules partagent des informations d'urgence et de congestion nécéssaires pour éviter et réduire les accidents. Par contre, les applications de divertissement permettent de rendre le voyage plus confortable, tant pour les passagers que pour les conducteurs, comme la connexion Internet, l'écoute de musique, la lecture en continu et les vidéos.

Les communications dans les VANET sont basées sur des protocoles de routage pour, primo, trouver et maintenir le meilleur chemin entre une source et sa destination prévue et secondo, afin d'acheminer les informations dans l'ensemble du réseau. Cinq types de protocoles de routage sont définis dans les VANETs on peut en citer les protocoles de routage basés sur la topologie qui sont adaptés particulièrement aux réseaux adhoc et qui peuvent entre autre etre fragmentés en trois familles : Les protocoles proactifs (OLSR, DSDV), les protocoles réactifs (AODV,AOMDV) et les protocoles hybrides (ZRP). Néanmoins, l'abscence d'infrastructure dans les VANETs rend les réseaux véhiculaire vulnérable aux différentes type d'attaques comme déni de service, le sniffing et autres quant chaque véhicule est en mesure de participer aux décisions de routage.

Dans notre thèse nous nous sommes focalisés sur la sécurité des VANETs contre l'attaque blackhole en commencant par l'analyse du comportement du noeud malicieux pour ensuite proposer une solution inter-couche éfficace contre ce type d'attaque et adéquate pour les VANETs.

Motivations et Contributions

Selon l'organisation mondiale de la santé (OMS) les accidents de la route entrainnent environ 1.3 million de decès par ans. Notre motivation majeure a été de trouver une solution adéquate pour minimiser les dommages matériels et surtout corporels très inquiétants (1.3 million de decès par ans).

Là nous avons fait en sorte que les informations sensibles échangées entre les véhicules soient sécurisées contre tout type de comportement blackhole qui en permanance essaie de falsifier les messages inter véhiculaires.

Les principales contributions dans cette thèse peuvent être divisées en trois parties importantes. Dans la première, nous implémentons et simulons l'attaque blackhole dans un réseau comme MANET et VANET afin de démontrer le niveau de dégradation des performances du réseau et les problèmes de sécurité majeurs qui rendent la communication indisponible à cause de cette attaque.

Dans la deuxième partie, nous visons à sécuriser les MANETs et VANETs contre les attaques par trou noir en identifiant et en ignorant les noeuds malveillants qui pourraient supprimer ou détourner des informations sensibles. Bien qu'à tout moment, les noeuds/ véhicules échangent de nombreux messages comprenant des informations sensibles, telles que des informations d'urgence et de congestion. La principale raison d'isoler les véhicules malveillants est de surmonter le problème de disponibilité dans les réseaux VANETs, car les paquets de données sont abandonnés par ces noeuds et par conséquent, d'éviter les accidents, d'améliorer la sécurité routière et de réduire le taux de mortalité. Plusieurs études ont proposé des solutions pour traiter ce type d'attaque. Contrairement à notre méthode, les solutions proposées sécurisent les VANETs contre les attaques blackhole sans se concentrer sur la contrainte de temps limite importante pour la prise de décision dans les VANETs. Par conséquent, ces solutions ne peuvent pas être adaptées à des scénarios VANET réels.

Dans la troisième partie, notre objectif était de sécuriser les MANETs et VANETs contre l'attaque blackhole dans une période opportune, en faisant cela nous respectons la contrainte de temps limite pour la prise de décision et rendons notre méthode efficace et appropriée dans un scénario MANET et surtout un réseau VANET réel.

Organisation de la thèse

Cette thèse est scindée en cinq chapitres. Nous abordons dans le premier chapitre les réseau mobile adhoc en général, et les réseaux véhiculaires VANETs en particulier (architecture, mode de composants, types de communication caractéristiques, domaines d'application,normes et architecture protocolaire, protocoles de routage). Dans le deuxième chapitre, nous exposerons en détail le protocole de routage multichemins AOMDV allant des différents type de message de contrôle jusq'aux multiples processus de ce protocole de routage. Enfin nous présenterons le mécanisme inter-couche et commenterons la sécuritaire du protocole AOMDV et sa vulnérabilité aux différentes type attaques.

La phase contribution de notre recherche figurera dans le troisième et le quatrième chapitre, dans laquelle on trouvera un état de l'art détaillé des multiples solutions proposées dans la littérature pour sécuriser le protocole de routage AOMDV suivie par une explication d'un nouveau mécanisme de sécurité. On cloturera ces deux derniers

chapitres par l'évaluation des performances des simulations tentées en ayant recours au simulateur réseau NS2 et le générateur des scénarios de mobilité réels SUMO.

Pour conclure, le dérnier chapitre sera une récapitulation générale de notre recherche et proposera quelques perspectives que nous estimons importantes et parfaites pour la sécurité des VANETs contre l'attaque en question.

Les réseaux Véhiculaires (VANETs) 1

Sommaire

1.1 Les réseaux Adhoc 6
1.1.1 Définition 6
1.1.2 Les caractéristiques 6
1.1.3 Les défis des réseaux Adhoc 7
1.1.4 Applications 8
1.2 Les réseaux véhiculaires (VANETs) 9
1.2.1 Définition 9
1.3 Le système des réseaux véhiculaires (VANETs) 10
1.3.1 Architecture et composants 10
1.3.2 Les modes de communication dans VANETs 11
1.3.3 Les caractéristiques 12
1.3.4 Les applications 13
1.3.5 Les types de messages 14
1.3.6 Normes et Architecture protocolaire des VANETs 15
1.4 Le routage et les méthodes d'accès dans les VANETs 17
1.4.1 Définition 17
1.4.2 Routage basé sur la position (routage géographique) 18
1.4.3 Protocole de routage basé sur la topologie 18
1.4.4 Le routage basé sur la diffusion (Broadcast routing) 19
1.4.5 Le routage basé sur les grappes (Cluster-Based) 19
1.4.6 Le routage Geocast 19
1.4.7 Les protocoles d'accès de la couche MAC dans les VANETs 20
Conclusion 21

Les réseaux véhiculaires sont une classe spéciale des réseaux mobiles adhoc MANETs dans laquelle, les noeuds du réseau sont des véhicules qui s'auto-organisent et communiquent sans aucune infrastructure préexistante.L'objecjtif principal des VANETs c'est d'assurer le confort et la sécurité routière. Dans ce premier chapitre nous allons présenter une vue globale sur les réseaux mobiles Adhoc avec leurs principaux caractéristiques, défis et applications. Par la suite, nous allons définir les réseaux véhiculaires VANETs, présenter l'architecture et les composants des VANETs, classifier les modes de communication, exposer les caractéristiques, les applications et le type de messages. On terminera ce chapitre en détaillant les normes et les architectures protocolaires des VANETs.

1.1 Les réseaux Adhoc

1.1.1 Définition

Comme le montre la figure 1.1, un réseau mobile Adhoc (MANET) est un ensemble de noeuds mobiles autonomes, chacun jouant le rôle d'un hôte et d'un routeur (Obidike *et al.* 2018). Ces routeurs s'auto- organisent librement ce qui nous donne des toplogies de réseaux arbitraires et temporaires. Par conséquent, cela permet aux termminaux mobiles des utilisateurs de communiquer entre eux sans aucune infrastructure de communication préexistante (Ilyas 2017). Dans ce type de réseau on trouve deux scenarios de communication : "Communication à saut unique" et "Communication à sauts multiples". Dans le premier scénario, les noeuds source et ceux de destination communiquent directement vu qu'ils se trouvent à portée radio les uns des autres. Par contre dans le deuxième scenario et étant donné que la paire source/destination se trouve hors de portée, les noeuds intermédiaires interviennent pour relayer les messages d'une source vers une destination prévue (Gupta *et al.* 2018) .

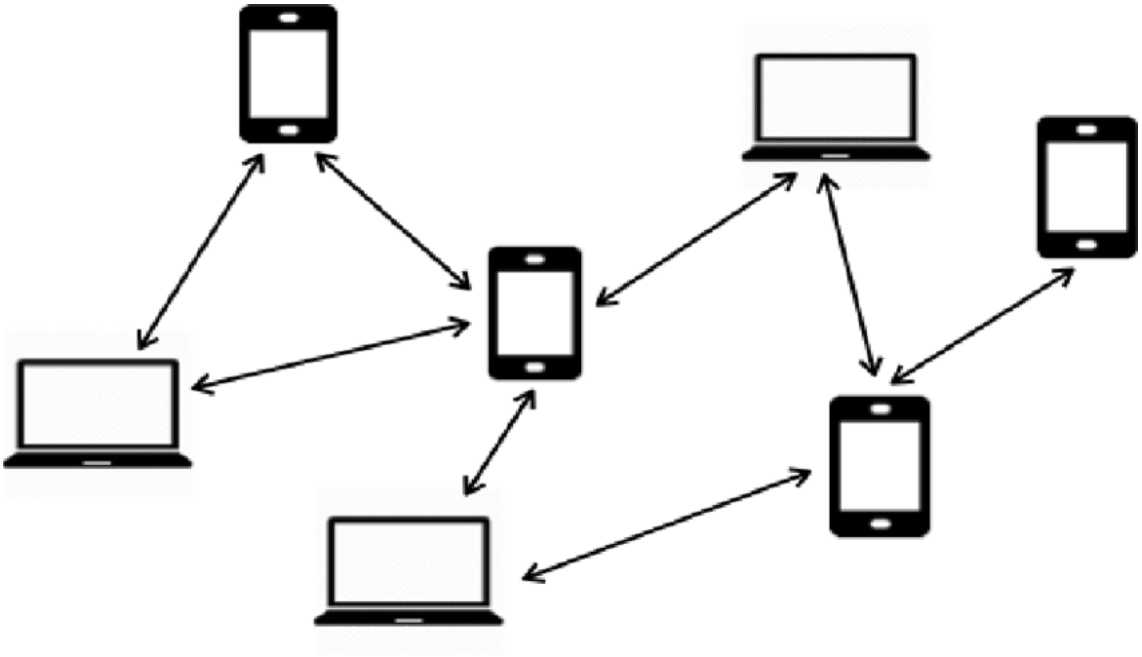


Figure 1.1 – *Un réseau Mobile Adhoc (Singh et al. 2016)*

1.1.2 Les caractéristiques

Les MANETs ont plusieurs caractéristiques particulières (Ali & Kulkarni 2015) :

✓Fonctionnement distribué

Il se caractérise par l'abscence d'infrastructure ou d'un contrôle central des opérations du réseau qui est distribué entre les noeuds. Les noeuds qui participent à un MANET doivent coopérer les uns avec les autres et communiquer entre eux. Chaque noeud fait office de relais selon les besoins, pour remplir des fonctions spécifiques telles que le routage et la sécurité.

✓Routage à sauts multiples

Un réseau adhoc est qualifiés par « multi saut » car plusieurs noeuds mobiles peuvent participer au routage et servir comme routeurs intermédiaires. Si un noeud veut envoyer des informations à un autre noeud qui se trouve en dehors de son domaine de communication, le paquet doit être renvoyé par un ou plusieurs noeuds intermédiaires.

✓Terminal autonome

Dans un MANET, chaque noeud mobile est un noeud autonome. Il peut effectuer deux tâches :hôte et routeur.

✓Topologie dynamique

Dans un MANET, la topologie du réseau peut changer de façon aléatoire et à des moments imprévisibles. Les noeuds sont libres de se déplacer arbitrairement dans le domaine du réseau à des vitesses différentes. Par conséquent, les noeuds du MANET établissent dynamiquement un routage entre eux lorsqu'ils se déplacent, formant ainsi leur propre réseau.

✓Terminaux légers

Dans la plupart des cas, les noeuds de MANET sont mobiles, avec une capacité d'unité centrale réduite, un stockage de faible puissance et une petite taille de mémoire, de manière à ce que les gens puissent facilement les emporter partout.

✓Support physique partagé

Le support de communication sans fil se caractérise par le fait qu'il est accessible à toute entité ayant un équipement approprié et des ressources adéquates. Par conséquent, l'accès au canal est sans limite.

1.1.3 Les défis des réseaux Adhoc

La mobilité, la nature « multi-saut », et l'absence d'infrastructure des réseaux adhoc créent un certain nombre de défis qui doivent être relevés. Parmi eux, on peut énumérer (Obidike *et al.* 2018; Rana & Gupta 2015) :

✓La topologie dynamique du réseau

C'est les déplacements fréquents des noeuds, Entraînant des ruptures fréquentes de chemins ce qui complique la conception d'un tel réseau.

✓La bande passante limitée

Le recours à un médium de communication partagé est l'une des caractéristiques essentielles des réseux moblies adhoc. Dans ce type de communication la bande passante réservée à un hôte est réstreinte.

✓Les contraintes d'énergie

Les noeuds de réseau sont alimentés par des sources d'énergie consommables, telles que les batteries, dont la durée de vie est limitée. Cette énergie limitée est consommée par chaque noeud du réseau pour exercer un rôle de routeur et traiter les données.Par conséquent, le paramètre de l'énergie limitée est un problème critique dans la conception d'un réseau ad hoc.

✓La perte de paquets due à une erreur de transmission

En cas d'une erreur de transmission les paquets de données peuvent être perdus. Cette perte sera causée par des collisions de trafic, des interférences ou de ruptures fréquentes de chemins.

✓Les menaces limitées sur la sécurité physique

Les réseaux sans fil mobiles sont généralement plus vulnérables aux menaces de sécurité physique Que les réseaux filaires fixes. La sécurité de ce type de réseau repose sur la sécurité de chaque noeud du réseau vu que c'est des noeuds autonomes. Par consequent tous les noeuds du réseau sont sujets aux attaques internes et externes.

✓La surcharge de routage

La mobilité des noeuds dans le réseau adhoc permet de créer les routes périmées dans la table de routage, ce qui provoque une surcharge de routage.

1.1.4 Applications

Au départ, le déploiment des réseaux mobiles adhoc et les toutes premières applications ont été surtout axés sur le secteur militaire. Mais avec le temps elles ont été rejointes également par les applications non militaires qui elles aussi ont augmenté de manière significative. Les MANETs, dans l'industrie commerciale ainsi que, dans la communauté des normes ont été l'objet d'une grande attention (Ahmed & Khalifa 2017; Obidike *et al.* 2018).

✓Les réseaux véhiculaires VANETs

Ils permettent à un ensemble de véhicules intélligents de communiquer entre eux sans aucune infrastructure. Cette communication vise à améliorer la sécurité et le confort du système de transport.

✓Les réseaux tactiques

Ils viennent en aide aux besoins de communication et de coordination entre les soldats, les véhicules militaires et le siège de l'information.

✓Les services d'urgence

Très utile en cas de catastrophes imprévisibles comme, les inondations, les tremblements de terre ou les incendies.

✓Les réseaux de capteurs

Ils ont pour but d'interconnecter une multitude de dispositifs de détection d'un coût faible et d'une faible puissance. Existants également dans la surveillance et la mesure de variables entre autre les changements de pression,la température, PIPELINE etc.,

✓L'environnement commercial et civil

Très utile dans le commerce électronique comme le paiement électronique qui permet à l'utilisateur d'effectuer un échange électronique d'argent ou de service.

✓Les applications éducatives

Utilisées dans les communications adhoc dans le cadre de conférences, de réunions ou de cours.

✓Les techniques de divertissement

Parmi les différentes techniques de divertissement fournies par les MANET, on trouve : Les jeux multi-utilisateurs et les aimants domestiques robotisés avec accès extérieur à l'internet.

1.2 Les réseaux véhiculaires (VANETs)

1.2.1 Définition

Les VANETs sont un cas particulier de réseaux mobiles adhoc (MANETs) (Sakiz & Sen 2017) Où les entités communicantes sont des véhicules. Dans un réseau véhiculaire le mouvement des véhicules est limité aux routes existantes et la topologie change rapidement en raison de la grande mobilité des véhicules contrairement aux MANETs(Quyoom *et al.* 2020). Les réseaux adhoc véhiculaires (VANETs) contiennent deux catégories de noeuds. La première, est constituée d'unités embarquées (OBU) qui peuvent communiquer entre elles librement sans passerelles stationnaires préexistantes (Al-Kahtani 2012), pour établir une communication de véhicule à véhicule (V2V) (Mokhtar & Azab 2015). La deuxième est composée des Road Side Units (RSU) qui utilisent des radios DSRC (Dedicated Short Range Communication) (Engoulou *et al.* 2014). Ces noeuds constituent l'infrastructure du réseau et assurent la communication entre le véhicule et l'infrastructure (V2I). (Al-Kahtani 2012).En outre, le réseau ad hoc véhiculaire fournit un système de transport intelligent (ITS) où les véhicules échangent de nombreux messages comprenant des informations sensibles sur de possibles urgences ou d'encombrements pour améliorer la sécurité du système de transport. VANETs utilisent aussi un autre type d'applications qui assure le confort des passagers (connexion à internet, ecoute de la musique etc..).

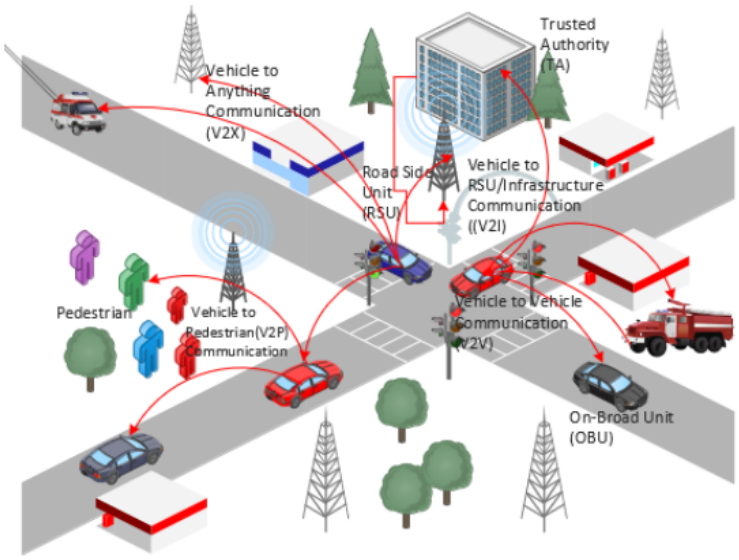


FIGURE 1.2 – *Les réseaux véhiculaires VANETs (Hota et al. 2021)*

1.3 Le système des réseaux véhiculaires (VANETs)

1.3.1 Architecture et composants

Une communication dans un réseau véhiculaire peut étre établie par les deux principaux composants suivant (voir la figure 1.2) :

✓OBUs

Les «OBUs» (On-Board Units) sont des unités de communications intégrées dans chaque véhicules permettant l'échange des informations entre les véhicules ou entre un véhicule et des points d'accès stationnaires situés sur la route, appelés RSUs (Road Side Units) (Hamdi *et al.* 2020). Cette dernière communication est assurée en utilisant les signaux DSRC (Dedicated Short Range Communication).

✓RSUs

Les «RSUs» (Road Side Units) sont des unités de communications aux véhicules installées aux bords des routes. Ces unités de communication jouent le rôle d'un routeur qui oriente les informations nécéssaires entre les véhicules, comme l'état de la route et les informations météorologiques (Chihi 2017).

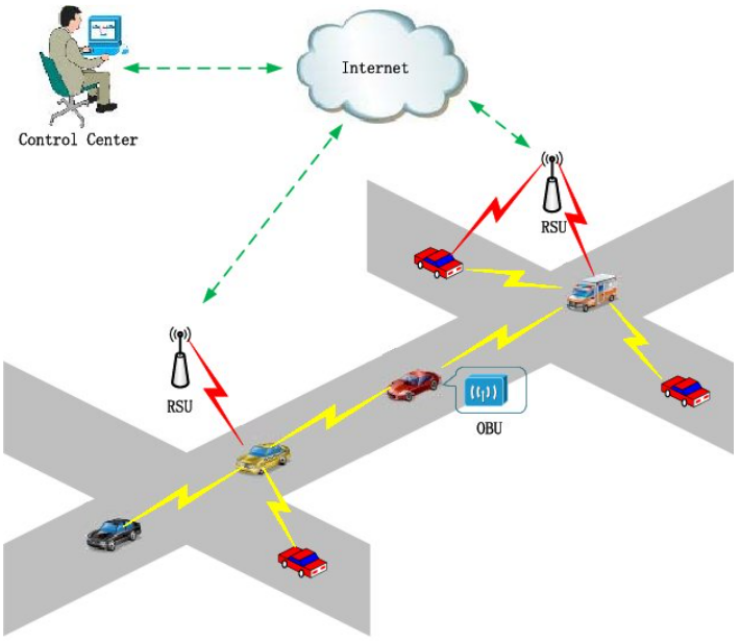


FIGURE 1.3 – *Les composants des réseaux véhiculaires VANETs (adoptée de (He et al. 2015))*

1.3.2 Les modes de communication dans VANETs

Comme mentionné précédemment, les réseaux véhiculaires sont composés de deux unités de communication. L'une mobile, l'autre fixe (RSU). Ces deux dernière s, communiquent entre elles pour améliorer la sécurité routière et le confort des passagers. Les modes de communication peuvent etre de véhicule à véhicule (V2V) ou de véhicule à infrastructure.

✓La communication véhicule-à-véhicule (V2V)

Dans ce mode communication, les véhicules rentrent en contact entre eux librement comme le montre la figure 1.4 sans aucune infrastructure préexistante, en utilisant les OBUs. Ce type de communication utilise des supports de communications particularisés par une courte latence et un taux de transmission élevé. La communication V2V prévoie plusieurs scénarios de diffusion d'alertes : le freinage d'urgence, la collision, la décélération, etc.(Hasrouny *et al.* 2015).

✓La communication véhicules à infrastructure

Comme le montre la figure 1.4 et contrairement au mode de communication V2V, dans le mode V2I les véhicules communiquent avec les infrastructures routières (RSUs) afin d'accéder aux multiples services comme l'accès à Internet, l'échange de données de voiture à domicile,l'information météorologique etc... Ce mode offre un taux de transmission de données élevé entre les véhicules et les unités en bordure de route (RSU)(Arif *et al.* 2020).

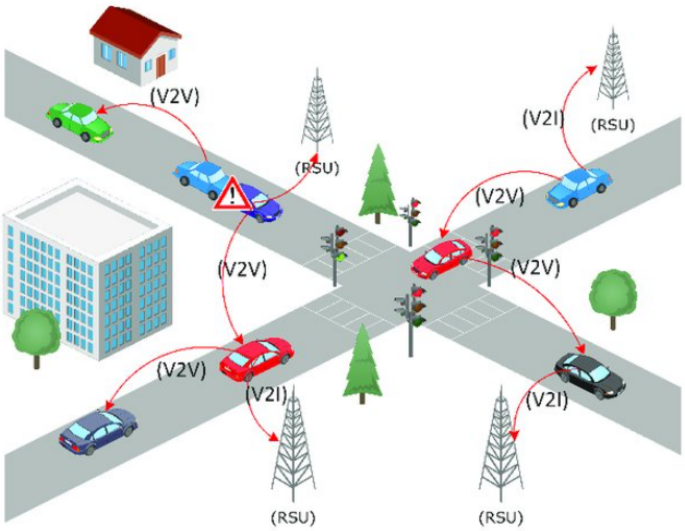


FIGURE 1.4 – *Architecture de communication dans VANETs (adoptée de (Shah et al. 2019))*

1.3.3 Les caractéristiques

Comme les réseaux véhiculaires sont une sous classe de MANETs, ils ont en commun quelques simulitudes. A l'inverse, les VANETs possèdent leurs propres caractéristiques qui les différencient des autres types de réseaux adhoc. Ces caractéristiques (Hamdi *et al.* 2020; Laouiti *et al.* 2017) sont :

✓Une topologie hautement dynamique

La topologie des VANET change toujours car les véhicules sont en mouvement permanent et une communication V2I ou V2V peut se produire à n'importe quel moments et dans un laps de temps très court.

✓La mobilité prédictible

Contrairement au réseau adhoc, la mobilité dans un réseau véhiculaire est pédictible car les mouvement des véhicules sont contrôles par la structure et la conception de la route. En outre, les véhicules du réseau sont tenus à respecter les panneaux de signalisation et les feux de circulation.

✓Une densité de réseau variable

Dans un réseau véhiculaire le nombre de véhicules est relatif à l'environnement (rural, ville, périphérique, autoroute) et au temps comme les heures de pointe. La densité du réseau peut être très élevée pendant un embouteillage ou dans les zones encombrées, et très faible dans les zones rurales. Elle dépend des zones et varie en fonction de la densité du trafic. En effet, le trafic routier peut être très dense comme dans le cas des embouteillages durant les heures de pointe dans les grandes villes. Dans les zones rurales ou de bonne heure dans les grandes agglomérations, le trafic routier est faible.

✓L'absence de la contrainte d'énergie

Contrairement aux réseaux sans fil adhoc où les noeuds du réseau sont alimentés par des source d'energie limitées. Dans un réseau véhiculaire les véhicules n'ont aucune contrainte en matière de consommation d'énergie car chaque véhicule est doté d'une grande capacité d'énergie à partir des batteries rechargeables qui fournissent une énergie continue.

✓La capacité de calcul élevé

Dans un réseau véhiculaire chaque véhicule peux avoir multiples moyens de calcul : capteurs ,processeurs, GPS, capacité importante de stockage installés dans les OBUs. Ces derniers permettent de donner et partager des informations nécessaires comme la position ,la direction et la vitesse actuelle d'un véhicule. Ainsi,la capacité de calucul de chaque véhicule augmente.

✓Des canaux variables en temps et en fréquence

Dans un réseau véhiculaire, les véhicules se déplacent à grande vitesse dans un environnement où il peut y avoir des obstacles physiques au signal sans fil tels que des bâtiments, des arbres, etc... ce sont des facteurs évidents qui provoquent un affaiblissement de la communication dans le temps ou en fréquence avec une intensité supérieure à celle des autres réseaux mobiles.

1.3.4 Les applications

L'évolution rapide des voitures rend les VANETs attrayants pour la recherche, motivant les ingénieurs en développement et les scientifiques à améliorer la sécurité routière et le confort des systèmes de transport (Naib *et al.* 2021). Pour atteindre cet objectif, plusieurs applications spécifiques ont été dévelopées aux réseax véhiculaires. Le développement de telles applications a connu une forte croissance (Toh 2007). Les application peuvent être classées en trois catégories : primo, les applications de divertissement et de confort, qui offrent une certaine aisance et commodité aux occupants du véhicule. Secondo, les applications d'optimisation et amélioration du trafic qui facilitent la conduite en diminuant la complexité de sa pratique. Tertio,les applications de prévention et de sécurité du trafic routier qui diminuent le nombre de décès liés à la conduite et aux accidents(Lee & Atkison 2021).

✓les applications de divertissement et de confort

Aujourd'hui, la présence d'un ou de plusieurs types d'applications de divertissement est indispensable dans toutes les activités humaines. C'est pour cette raison que VANETs attirent l'attention et l'intérêt des utilisateurs par les differents types d'applications offertes qui garantissent le confort aux occupants de véhicule.

Le but de cette catégorie d'applications c'est pas la participation dans la sécurité routiére, mais plutôt d'offrir de la joie, du plaisir et du contentement aux conducteurs et passagers, et rendre le voyage agréable, quelle que soit la longeur du trajet. Parmi ce genre d'applications on peut se connecter à internet, jouer, écouter de la musique, procéder à des payements électroniques et tchater avec autrui.

✓Les applications d'optimisation et amélioration du trafic

Ces applications de gestion de trafic sont axées sur l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Cette spécificité améliore la sécurité routière en diminuant le nombre de décès. Elles consistent à fournir aux conducteurs des informations leur permettant d'adapter leur parcours à la situation du trafic routier. Cette catégorie d'applications vise à équilibrer la circulation des véhicules sur les routes pour une utilisation efficace de la capacité des routes et des carrefours et à réduire par conséquent les pertes humaines, la durée des voyages et la consommation d'énergie. . ..etc. Parmi ce type d'applications figurent (Hamdi *et al.* 2020) :

— Le contrôle intelligent du trafic.

— Les péages sans trafic.

— Le contrôle de la vitesse.

— Le guidage routier et navigation améliorée.

— Le contrôle de l'état des routes.

✓Les applications de prévention et de sécurité du trafic routier

Elles visent à améliorer la sécurité routière et protoger la vie des occupants des véhicules en diminuant et en évitant les accidents qui causent des pertes humaines et matérielles. Cette amélioration consiste à partager des informations critiques sensibles et nécéssaires concernant les incidents routiers, les informations sur le voisinage et la gestion des incidents entre les véhicules ou entreles véhicules et le RSU sous forme d'alertes.

Grâce aux alertes, le conducteur sera averti et informé de toutes les situations dangereuses (accidents, informations météorologiques, travaux routiers..) qui peuvent entrainer de nombreuses pertes en vie humaine et matérielle.

1.3.5 Les types de messages

Les applications d'un sytème de transport intelligent (ITS) exigent une stratégie de communication qui appartient à l'un ou aux deux des deux types de message suivants :(Santa *et al.* 2014)

✓L'échange périodique d'informations sur le statut

Ce type de message est envoyé périodiquement par un terminal sous forme d'un paquet de données contenant toutes les informations nécéssaires aux conducteurs

pour étre informés sur l'état du véhicule ou des terminaux routiers. Les informations contenants dans le pacquet de donnés sont : la localisation, la vitesse ou l'identifiant du terminal.

Parmi les applications qui peuvent utilisées ce type de message on trouve : Les application d'optimisation et amélioration du trafic comme la surveillance à distance des véhicules, où les informations sur l'état des véhicules sont collectées périodiquement. ou les applications de sécurité comme celles de la prévention coopérative des collisions, où le message contien des informations cinématiques nécéssaires sur les véhicules voisins pour détecter les impacts potentiels.

✓Les notifications asynchrones

Ces messages contiennent toutes les informations importantes sur un évenement précis. Ils sont diffusés fiablement à un terminal unique ou à un groupe de terminaux grace aux informations importatntes contenues dans ces messages et leurs effets éventuels sur la sécurité routière. Ce type de message est purement utilisé dans les applications de prévention et de la sécurité du trafic routier.

Selon l'architecture de communication ITS de référence ISO/ETSI (European Telecommunications Standards Institute), l'ETSI (19) a défini deux services de messagerie de base suivants : le message de sensibilisation coopérative (the Cooperative Awareness Message (CAM)) et le message décentralisé de notification environnementale (the Decentralized Environmental Notification Message (DENM)).

Les Messages périodiques dits « Cooperative Awareness Basic Service (CAMs) »

Comme l'indique son nom CAM (Cooperative Awareness Basic Service) permet d'assurer un service de sensibilisation de base dans les réseaux ITS coopératifs. Pour ce faire, un support d'application est installé pour assurer la diffusion periodique des messages contenant des informations de présence et de localisation, ainsi que l'état de base. Ces messages sont envoyés à toutes les unités voisines ITS à un saut, permettant aux receveurs de ces messages d'avoir une vision sur toutes les stations situées dans sa zone de voisinage et de se comporter en conséquence en se basant sur toutes les informations importantes comme, les positions, les mouvements et les caractéristiques pertinentes.

Les messages d'alerte dits «Decentralized Environmental Notifications Messages (DENMs) »

Les messages DENMs sont transmis lors d'une constatation d'un événement important qui affecte (lié à) la conduite ou la circulation pour le signaler et le notifier. Chaque évenement est identifié par : *"un type"* associé au type d'événement détecté (une panne de véhicule, un embouteillage etc) ; *"une position"* représentant une zone géographique ; *"l'heure de détection de l'événement"*, qui correspond à l'heure d'expiration de l'évenement ; *"une zone de destination"* décrivant la zone de transmission des message DENM parmi les stations ITS ; et *"une fréquence de transmission"*. Contrairement aux messages CAMs la diffusion des messages DENMs se fait en multi sauts.

1.3.6 Normes et Architecture protocolaire des VANETs

Les communications véhicule-à-véhicule et véhicule-à-infrastructure dans les VANETs reposent sur une technologie de communication sans fil, appelée Dedicated Short Range Communication (DSRC). Cette technologie a été deployée afin de permettre aux

applications de prévenir d'éventuelles collisions.(Kenney 2011) DSRC est un membre de la famille des protocoles IEEE 802.11 (Wi-Fi). Ses couches PHY et MAC sont définies dans la norme IEEE 802.11p.(Rayamajhi *et al.* 2018)

✓DSRC

En 1999, la Commission fédérale des communications (FCC) des États-Unis a alloué 75MHz du spectre de Communications à courte portée (DSRC = Dedicated Short Range Communication) dans la bande des 5.9 GHz Pour être utilisé exclusivement dans les communications véhicule-à-véhicule et véhicule-à-infrastructure. La bande de spectre 5.850 - 5.925 GHz a été allouée aux applications DSRC.(Naik *et al.* 2017) la signification du terme " Short Range" dans DSRC est que la communication s'effectue dans des distances plus courtes que les services cellulaires et WiMax.(Kenney 2011), l'objectif principal de DSRC est de supporter les applications de sécurité routière afin de réduire le nombre d'accidents.

Comme illustré dans la Figure 1.5, Le spectre de DSRC est divisé en 7 canaux larges de 10 MHz. Le canal 178 (Ch. 178) est le canal de contrôle (CCH), qui est généralement limité seulement aux communications de sécurité. Les six autres canaux de service (SCHs), Ch. 172,174, 176, 180, 182, et 184, sont disponibles pour un usage de sécurité ou de non sécurité et enfin, une bande de garde large de 5 MHz.

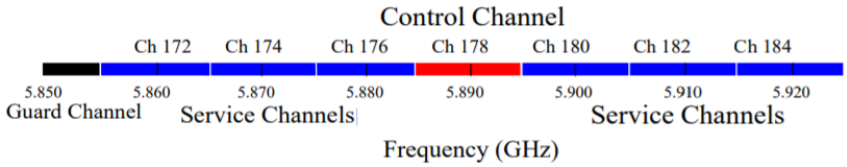


FIGURE 1.5 – *Arrangement des canaux DSRC (adoptée de (Naik et al. 2017))*

✓802.11p

En modifiant la spécification de 802.11a, l'ASTM (société américaine pour les essais des matériaux) définit une nouvelle norme appelée IEEE 802.11p pour répondre aux problèmes de bruit de l'alimentation électrique et à l'environnement de communication à bord des véhicules.(Association *et al.* 2010) Cette version modifiée de la norme IEEE 802.11a/g définit la couche MAC et la couche PHY en tenant compte de l'environnement de communication des véhicules dans la norme IEEE 802.11, qui est un standard LAN sans fil classique(Kim *et al.* 2018).

La norme 802.11p réduit la largeur de la bande du canal en utilisant une de 10 MHz comme canal de base, afin de diminuer l'influence de l'évanouissement sélectif en fréquence qui se produit dans un environnement routier à grande vitesse (Kim *et al.* 2018). Cette utilisation reduit aussi la probabilité de collisions pour un nombre donné de transmissions de trames par seconde.(Kenney 2011) De plus, elle utilise la fréquence de 5,850-5,925 GHz plutôt que la bande industrielle, scientifique, et médicale (ISM). Dans une communication où cette norme est appliquée, une procedure d'authentification n'est pas nécessaire pour établir une communication d'un véhicule avec RSU. Cette spécificité peut causer des problémes de sécurité.(Kim *et al.* 2018)

La norme 802.11p spécifie non seulement la partie transmission de données des protocoles mais aussi les fonctions de gestion associées à la couche corespondante PMLE et MLME (bloc entité de gestion de la couche physique et bloc entité de gestion de la couche MAC respectivement) (voir la figure 1.6)

Comme le montre la figure 1.6 la norme IEEE 1609.4 est incluse dans la deuxième couche OSI de la pile des protocoles WAVE. Cette norme est consacrée au contrôle de fonctionement multicanaux et également les taches de gestion.

Quant à la norme IEEE 1609.3 qui est située dans la troisième et la quatrième couche de l'OSI, elle est consacrée au WSMP (WAVE Short messages protocol) qui est responsable aux échanges des courts méssages. Elle décrit également comment incorporer les protocoles traditionnels IPV6, UPD et TCP dans le système.

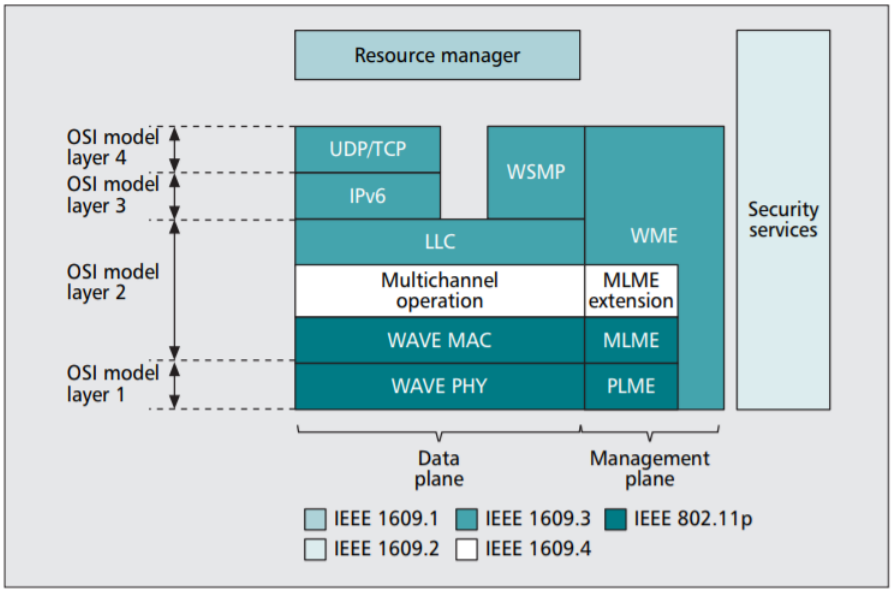


FIGURE 1.6 – *Illustration de IEEE 1609.x et IEEE 802.11p dans la pile de protocoles WAVE (adoptée de (Uzcátegui et al. 2009))*

1.4 Le routage et les méthodes d'accès dans les VANETs

1.4.1 Définition

Afin de faciliter la communication au sein du réseau, Un protocole de routage est utilisé pour découvrir les routes entre les noeuds. L'objectif principal d'un tel protocole de routage est l'établissement correct et efficace des routes entre une paire de noeud afin que les messages puissent être livrés en temps opportun. L'idée principale de ces protocoles est de maximiser les performances en minimisant d'une part, le temps de livraison des paquets, d'autre part, l'utilisation de la bande passante et enfin, la consommation d'énergie. Le routage dans les VANET a été largement analysé au cours des dernières décennies.

Comme illustré dans la figure 1.7 les protocoles de routage dans VANETs sont principalement classés en deux catégories différentes en fonction de leurs accusations de position et la formule de mise à jour des routes (Singh & Agrawal 2014). Il s'agit de :

— Protocole de routage basé sur la position
— Protocole de routage basé sur la topologie
— Protocole de routage basé sur la diffusion
— Protocole de routage basé sur les grappes
— Protocole de routage basé sur le géocast

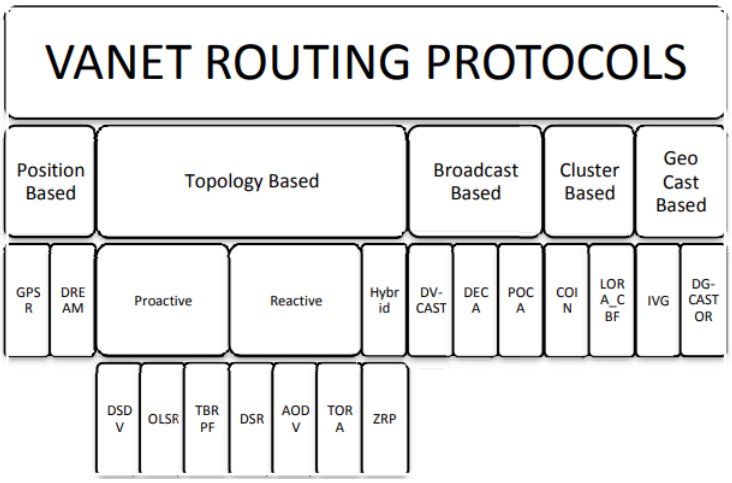


FIGURE 1.7 – *La classification des protocoles de routage dans VANETs (Singh & Agrawal 2014)*

1.4.2 Routage basé sur la position (routage géographique)

Dans ce type de protocole de routage, le noeud source communique avec la destination en utilisant sa position géographique en plus de son adresse réseau. les decisions de transmission dans un tel protocole de routage sont basées sur la position de la destination. Par exemple, le GPSR (Greedy Perimeter Stateless Routing) (Karp & Kung 2000) est l'un des protocoles les plus connus dans la littérature, dans lequel le routage greedy transmet toujours le paquet au noeud le plus proche géographiquement de la destination.(Singh & Agrawal 2014)

GPSR (Greedy Perimeter Stateless Routing) Le GPSR est un protocole de routage basé sur le positionnement géographique, qui est utilisé pour faire des décisions de transfert de paquets de donnée et de contrôles. Ce protocole se compose de deux parties : le « greedy forwarding » qui correspond à une méthode de choix du prochain noeud transmetteur de paquets, en se basant sur les informations de la position des noeuds voisins et de la destination des paquets. Ce processus de greedy forwarding se répète, jusqu'à ce que le paquet atteint la destination prévue. Quant à la deuxième partie de GPSR elle est en fait une méthode pour contourner les obstacles et les zones géographiques vides, qui ne présentent aucun candidat transmetteur dans le voisinage.(Karp & Kung 2000)

1.4.3 Protocole de routage basé sur la topologie

Ces protocoles ont été conçus spécialement pour les réseaux adhoc, où l a transmission des paquets de données et de contrôle est basé sur les informations de liaison disponibles qui existent dans le réseau. Cette famille de protocoles peut être divisée en trois catégories (Singh & Agrawal 2014) :

— Proactifs.

— Réactifs.

— Hybrides.

Les protocoles proactifs Dans les protocoles de routage proactifs, les chemins vers les destinations prévues sont déterminés au démarrage et maintenus en utilisant un processus périodique de mise à jour de route. Les protocoles de routage proactifs ont

pour mission de maintenir les informations de routage cohérentes et à jour de chaque noeud par rapport à tous les autres noeuds du réseau. La différence entre ces protocoles se situe dans la façon dont les informations de routage sont mises à jour. Nous citons par exemple, le DSDV qui est un protocole à vecteur de distances et le GSR, et l'OLSR (Clausen & Jacquet 2003) qui sont des protocoles à état de liens.

Les protocoles réactifs À l'opposé des protocoles proactifs, les protocoles réactifs adoptent une approche différente. En effet, la détemination du chemein de routage est déclenchée à la demande. Ils n'ont pas besoin de transmission périodique d'informations topologiques du réseau. Parmi les protocoles de routage réactifs les plus connus on peut citer : AODV et AOMDV.

Les protocoles hybrides Ces dérniers combine les mécanismes des deux protocoles su-cités : proactifs et réactifs. Dans cette approche, les protocoles hybrides utilisent les méthodes proactives (messages périodiques de contrôle) pour découvrir les routes dans un voisinage prédéfini. Les techniques d'inondation des protocoles réactifs sont spécialisées pour obtenir les routes vers les noeuds lointains. Le protocole ZRP (Beijar 2002) est le protocole hybride le plus renommé dans la littérature.

1.4.4 Le routage basé sur la diffusion (Broadcast routing)

La méthode de diffusion est fréquemment utilisée dans VANETs à chaque fois que le noeud de destination se trouve hors de portée de la transmission du noeud source. Cette méthode consiste à diffuser le paquet à travers tout le réseau entre tous les noeuds disponibles à l'intérieur du domaine de diffusion(Singh & Agrawal 2014).
Ce type de protocole de routage est principalement utilisé pour les applications de sécurité, tels que : le partage du climat, celui du trafic, de l'état des routes entre les véhicules, des alertes d'urgence et des annonces diverses. Parmi les protocoles de broadcast qui ont été proposés, nous avons : le protocole de diffusion distribuée pour les véhicules (DV-CAST), le protocole de diffusion fiable en fonction de la position (POCA) et le protocole de diffusion fiable en fonction de la densité (DECA).(Singh & Agrawal 2014).

1.4.5 Le routage basé sur les grappes (Cluster-Based)

Ce type de routage présente un regroupement de plusieurs véhicules possédant des caractéristiques communes telles que : la vitesse, la direction, etc. Afin de former une grappe (cluster), un cluster Head est nécéssaire pour gérer la communication entre les différents noeuds à l'intérieur d'un cluster ou avec d'autres cluster tout en créant une infrastructure réseau virtuelle qui permet l'évolutivité. Le regroupement pour un réseau ouvert de communication inter-véhicules (COIN) et LORA_CBF sont les principaux algorithmes de ces techniques de routage.(Singh & Agrawal 2014)

1.4.6 Le routage Geocast

Le routage Geocast est essentiellement un routage multidiffusion basé sur la localisation. Son objectif est de délivrer le paquet d'un noeud source à tous les autres noeuds dans une région géographique spécifique (Zone of Relevance, ZOR). De nombreuses applications VANET bénéficieront du routage geocast. Par exemple la signalisation instantanée de l'accident par un véhicule aux véhicules voisins. Ce type de routage est caractérisé par : une livraison fiable des paquets dans une topologie

hautement dynamique une déminution de la surcharge du réseau et enfin, une congestion. L'IVG et le DG-CASTOR figurent parmi les exemple de routage geocast.

1.4.7 Les protocoles d'accès de la couche MAC dans les VANETs

Dans un réseau VANET les transmissions des messages de sécurité et non-sécurité doivent être fiables et opportunes. Ces messages nécéssitent une qualité de service (QoS) crédible (Ma *et al.* 2020). Pour surmonter tout problème, les protocoles d'accès dans la couche "MAC" pérfectionnent la sécurité et l'efficacité des véhicules sur la route dans les VANETs en diffusant des messages de sécurité de manière crédible et rapide (Nguyen *et al.* 2018).

Comme le montre la figure 1.8, les protocoles MAC actuels pour les VANET sont répartis dans les quatre catégories qui suivent :

— les protocoles MAC distribués à canal unique (c'est-à-dire IEEE 802.11p, les protocoles TDMA distribués et basés sur l'emplacement (DTMAC) et les protocoles de mobilité et d'évitement des collisions, TDMA MAC distribué et basé sur l'emplacement (DTMAC) et MAC sensible à la mobilité et évitant les collisions (MoMAC)).

— Les protocoles MAC centralisés à canal unique (c'est-à-dire le MAC adaptatif à accès multiple par répartition dans le temps (VAT-MAC), MAC équitable et sensible à la vitesse (SAFE-MAC), TDMA à base de grappes (CBT) et MAC directionnel basé sur les priorités (PDMAC)).

— Les protocoles MAC multicanaux distribués (c'est-à-dire IEEE 1609.4, predictive TDMA MAC (PTMAC), space-division-TDMA (SD-TDMA), MAC multicanal asynchrone à accès au canal basé sur la priorité (PCS-AMMAC), multi-canal distribué multi-priorité adaptatif (APDM) et black-burst-based MAC (BB-MAC)).

— Les protocoles MAC multicanaux centralisés (c'est-à-dire VeMAC, MAC multi-canal coordonné amélioré (IC-MAC), MAC multicanal basé sur la contention et l'élimination à plusieurs tours (VEC-MAC), MAC en grappe TDMA amélioré (ETCM), et l'accès directionnel au support avec évitement des collisions (CADMA)).

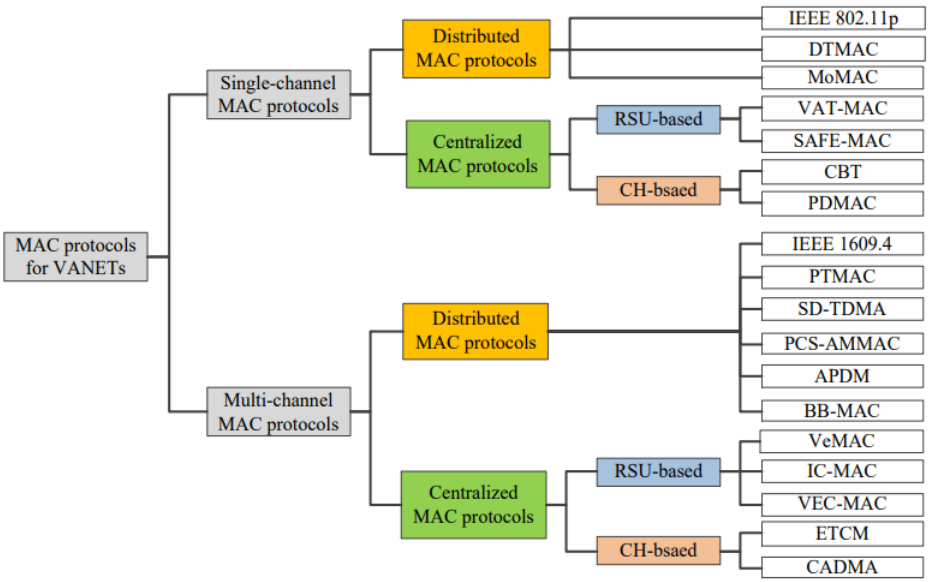


FIGURE 1.8 – *Classification des protocoles d'accès de la couche MAC dans le standard IEEE 802.11 (Ma et al. 2020))*

Conclusion

L'évolution rapide des voitures rend les réseaux véhiculaires attrayants pour la recherche, ce qui motive les ingénieurs et les scientifiques du développement à améliorer la sécurité routière et le confort des systèmes de transport. Les communications dans un tel réseau sont basées sur des protocoles de routage pour trouver le meilleur chemin entre la source et la destination prévue puis acheminer les informations dans tout le réseau. Dans le chapitre suivant l'un des procotoles de routage multichemin les plus connu dans VANETs AOMDV (Ad-hoc On-demand multipath distance vector routing protocol) sera présenté tout en exposant ses paquets de contrôle et ses principaux processus de routage. Comme tout autre protocole de routage, AOMDV il est également lui aussi vulnérable à différents types d'attaques. Nous allons par la suite aborder les différents problèmes de sécurité qui dégradent l'éfficacité de l'AOMDV comme : le déni de service et l'attaque blackhôle.

Le protocole AOMDV et le mécanisme Cross-Layer

2

Sommaire

2.1 Le routage multi-chemin 23
2.2 Le protocole AOMDV (Ad-hoc On-demand Multipath Distance Vector) 23
2.2.1 Définition 23
2.3 Types de messages AOMDV 24
2.3.1 Le Paquet HELLO 24
2.3.2 Le Paquet RREQ 25
2.3.3 Le Paquet RREP 25
2.3.4 Le Paquet RERR 25
2.4 Le fonctionnement du AOMDV 26
2.4.1 Le processus de découverte de route 26
2.4.2 Le processus de calcul de chemin inverse 28
2.4.3 Entretient des routes 29
2.5 Le mécanisme Inter-Couche 29
2.6 Les principales attaques contre les réseaux VANETs 30
2.6.1 Les Exigences de sécurité 30
2.6.2 Les attaques contre les protocoles de routage 31
2.7 L'attaque Blackhole dans AOMDV 34
2.8 Conclusion 35

Les communications dans les réseaux VANET sont basées sur des protocoles de routage afin de trouver le meilleur chemin d'une source vers la destination prévue et d'acheminer les informations dans l'ensemble du réseau. Le vecteur de distance multivoie à la demande (AOMDV) est l'un des protocoles de routage multivoies les plus utilisés dans les réseaux VANET. Dans le processus de routage chaque véhicule se comporte comme un routeur dans le réseau pour participer à l'opération de routage ; par conséquent, cette caractéristique rend le protocole AOMDV vulnérable à plusieurs attaques, telles que les attaques de type Sybil et blackhole. Les méthodes de sécurité des réseaux VANETs basées sur le mécanisme inter-couche sont parmi les solutions les plus efficaces. Dans ce chapitre le protocole AOMDV et le mécanisme inter-couche seront détaillés, ainsi que les types de menaces dans VANETs.

2.1 Le routage multi-chemin

Le routage "à chemin unique" **"single-Path"** consiste à trouver et à maintenir un seul chemin entre une source et une destination durant le processus de découverte de route. Ce mécanisme ne garantit pas une transmission efficace des données dans un réseau VANET où, la fréquence des reptures des liens est élevée, à cause de la topologie hautement dynamique et à la vitesse très elevée des véhicules.

Afin d'excéder les limites du routage "à chemin unique" **"single-Path"**, le concept de routage par trajets multiples est apparu dans les années 1990. Le but principal était d'améliorer la tolérance aux erreurs et à l'équilibrage de la charge des réseaux mobiles adhoc (Fu *et al.* 2020). Le routage "multi-chemin" **"Multipath"** permet de calculer multiples chemins sans boucle entre les noeuds sources et la destination durant un seul processus de découverte de route. Par conséquent, le nombre de processus de découverte de route sera diminué et en cas de défaillance du lien, le processus de récupération de la route est plus rapide et plus efficace. Contrairement au protocole de routage à chemin unique , un nouveau processus de découverte d'itinéraire n'est déclenché que lorsque tous les chemins multiples entre la source et la destination échouent (Naib *et al.* 2021).

2.2 Le protocole AOMDV (Ad-hoc On-demand Multipath Distance Vector)

2.2.1 Définition

AOMDV (Ad-hoc On-demand multipath distance vector) est un protocole de routage développé par (Marina & Das 2001). Ce protocole de routage améliore le protocole de routage bien connu AODV (Zaidi & Faisal 2018) en termes de diminution de la latence de découverte de route et de l'overhead de routage. L'avantage d'AOMDV est que le processus de découverte de route calcule de multiples chemins sans boucle et sans lien (Meddeb Makhlouf & Guizani 2019) entre les noeuds sources et destinations. C'est-à-dire les chemins qui mènent d'une source vers une destination bien précise n'ont pas de liens en commun. Par conséquent, lorsque la liaison est défaillante, le processus de récupération de la route est plus rapide et efficace. Contrairement au protocole de routage à chemin unique AODV, une nouvelle découverte de route n'est nécessaire, que si toutes les routes deviennent non valides.Ceci réduit considérablement les latences et la surcharge de la procédure de découverte de route.La route est maintenue en renvoyant un paquet d'erreur de route (RERR) au noeud source pour supprimer la liaison défaillante et déclencher un nouveau processus de découverte si cette route est toujours nécessaire pour relayer le paquet de données.

Certains champs ont été ajoutés dans la table de routage AOMDV et d'autres ont été modifiés par rapport à ceux du protocole de routage AODV (figure 2.1). Cette table de routage contient les champs suivants :

destination : L'adresse du noeud de distination.

sequence number : Le numéro de séquence.

advertised_hopcount : « Advertised hopcount » (nombre de sauts à annoncer) est utilisé pour maintenir plusieurs routes sans boucles de routage.

nexthop : L'adresse du noeud le plus proche à travers lequel un paquet peut passer.

expiration_timeout : Le temps d'expiration.

La figure 2.1 illustre la structure des éléments de la table de routage pour AODV et AOMDV. Dans AOMDV, "advertised_hopcount" est utilisé au lieu du "hopcount" dans AODV .La "route_list" sert à remplacer le "nexthop" ; ce nouveau changement définit plusieurs nexthops avec des hopcounts respectifs. Cependant, tous les nexthops se partagent toujours le même numéro de séquence de destination. Chaque fois que le numéro de séquence est mis à jour, le nombre de sauts annoncé est initialisé.

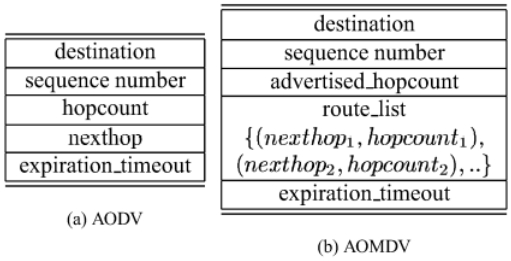


FIGURE 2.1 – *Structure de la table de routage. (a) AODV, (b) AOMDV (Marina & Das 2001)*

2.3 TYPES DE MESSAGES AOMDV

Comme tout les protocoles de routage, dans AOMDV la recherche et la maintenance d'un chemin optimale entre une source et une destinantion sont basées sur un ensemble de paquets de conroles cités ci-dessous.

2.3.1 Le Paquet HELLO

C'est le paquet de contrôle qui est responsable de la maintenance des liens. La diffusion de ce paquet est périodique. Lorsque ce type de message n'est pas réceptioné cela implique, que le noeud voisin n'est pas accessible de ce fait le lien est automatiquement interrompu.

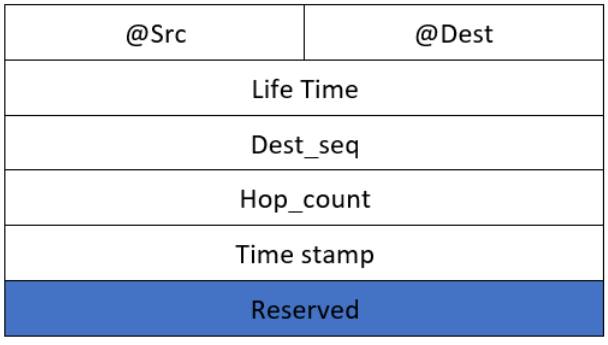


FIGURE 2.2 – *Le format de paquet HELLO*

2.3.2 Le Paquet RREQ

" Route Request Packet " est un paquet de contrôle diffusé en brodcast vers tout le voisinage du noeud source. La diffusion de RREQ est déclanchée lors du lancement du processus de decouverte de route.

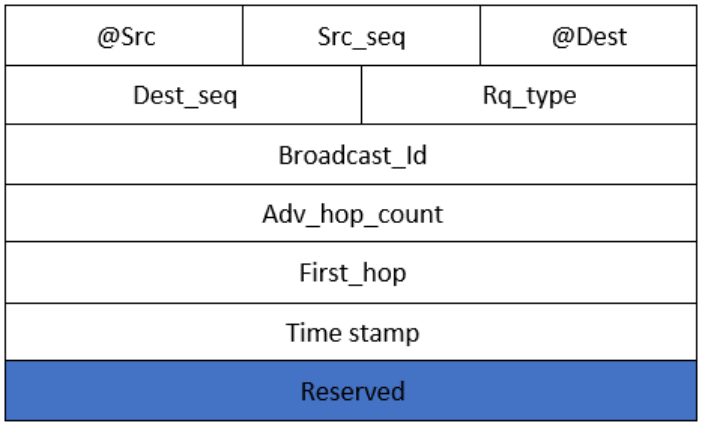


FIGURE 2.3 – *Le format de paquet RREQ*

2.3.3 Le Paquet RREP

" Route Reply Packet " est un paquet de contrôle envoyé par la destination après avoir reçu un RREQ paquet. En d'autre terme c'est une répense au message RREQ.

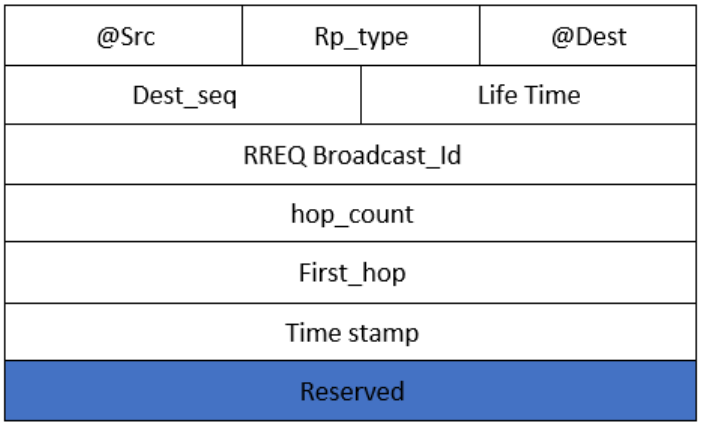


FIGURE 2.4 – *Le format de paquet RREP*

2.3.4 Le Paquet RERR

"Route Error Packet", est un message d'erreur diffusé par un noeud lorsque aucune route n'est détectée. En recevant ce type de message, tous les noeuds seront informés par le chemin invalide et désactivent cette route par la suite.

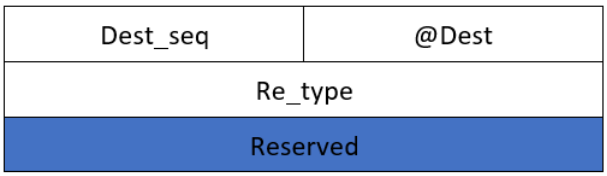


FIGURE 2.5 – *Le format de paquet RERR*

Le tableau 2.1 présente la sginification de tous les champs inclus dans les paquets de contrôle cité ci-dessus.

Paramètres	Signification
@Src, @Dest	Adresse des noeud source et destination
Src_seq, Dest_seq	Numéro de séquence des noeud source et destination
Broadcast_id	Identificateur de broadcast des messages envoyés
Adv_Hop_Cnt	Maximum du nombre de sauts parmi les chemins multiples disponibles vers la destination
Life Time	Durée de vie du message
First_Hop	Premier noeud à traverser dans le chemin de la source vers la destination
Hop count	Nombre de sauts séparant le noeud source du noeud destinataire
Timestamp	Utilisé pour connaitre la latence des messages
Rq_type, Rp_type, Rq_type	Type de paquet pour les paquets RREQ, RREP et RERR
Reserved	Champs réservé dans le paquet

TABLE 2.1 – *Définition des paramètres des paquets de contrôle du protocole AOMDV*

2.4 Le fonctionnement du AOMDV

2.4.1 Le processus de découverte de route

Dans AODV, chaque requête reçue par un noeud pendant le processus de découverte de route définit potentiellement une route alternative vers la source. Par exemple, chaque copie du paquet de requête RREQ arrivant à un nœud définit une route alternative vers la source. Cependant, accepter naïvement toutes ces copies va engendrer une formation de boucles dans les routes. Afin d'éliminer la possibilité de formation de boucles, AOMDV utilise la même condition que pour AODV, et qui consiste à n'accepter une nouvelle requête que si son nombre de sauts est inférieur au nombre de sauts courant et que son numéro de séquence est supérieur au numéro de séquence courant.

AOMDV ajoute une nouvelle notion « advertised hopcount ». L'advertised hopcount du nœud i pour une destination d représente le maximum hopcount des chemins disponibles d'un nœud i vers la destination d et il est considéré comme le nombre de sauts qui ne change jamais pour le même numéro de séquence. En plus, chaque nœud maintient une liste, firsthop list, pour chaque RREQ afin de garder une trace de la liste

des voisins de la source à partir desquels une copie de RREQ a été reçue.

Les noeuds intermédiaires, doivent garder les copies dupliquées de RREQ contrairement à AODV. Chaque copie est vérifiée pour voir si elle procure un nouveau chemin disjoints vers la source. Dans cette étape le noeud intermédiaire contrôle sa liste **"firsthop_list"** avec le champ **"firsthop"** (le voisin de la source) de la copie du paquet RREQ. Si on s'assure que RREQ apporte un nouveau chemin, la règle de mise à jour de route de la Figure 2.7 sera automatiquement sollicitée. Le noeud intermédiaire envoie un RREP vers la source dans le but de vérifier si d'une part, le chemin inverse peut être mis en place et d'autre part, si celui vers la destination est valide.

La destination doit vérifier que les chemins inverses peuvent être mis en place. Elle doit garantir que les liens soient disjoints, uniquement avec ses voisins. Au-delà du premier saut, le RREP suit les chemins inverses qui ont été mis en place et qui sont déjà formés. Chaque RREP arrivant à un nœud intermédiaire peut suivre plus d'un chemin inverse. La destination répond à k copies de RREQ. Le paramètre k est utilisé pour contrôler le nombre de RREP émis par la destination.

L'inondation des deux paquets de contrôle RREQ et RREP est illustrée dans la figure 2.6.

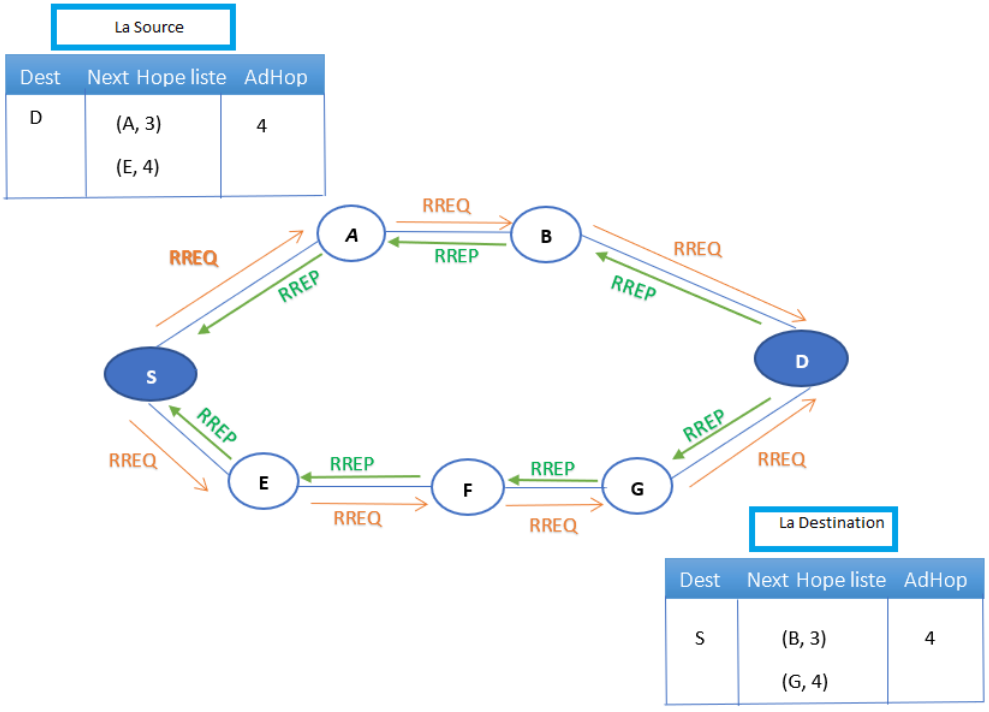


FIGURE 2.6 – *Le chemin de l'envoie des paquets RREQ et RREP*

if$(seqnum_i^d < seqnum_j^d)$ **then**

$seqnum_i^d := seqnum_j^d$;
if$(i \neq d)$ **then**
$advertised_hopcount_i^d := \infty$;
$route_list_i^d = \text{NULL}$;
insert $(j, advertisd_hopcount_j^d + 1)$ **into** $route_list_i^d$;

else
$advertised_hopcount_i^d := 0$;
endif
elseif $(seqnum_i^d = seqnum_j^d)$ **and**
$((advertised_hopcount_i^d, i) > (advertised_hopcount_j^d, j))$ **then**

insert $(j, advertisd_hopcount_j^d + 1)$ **into** $route_list_i^d$;

endif

FIGURE 2.7 – *La Mise à jour de la route dans AOMDV (Marina & Das 2001)*

La mise à jour de la route dans AOMDV est utilisée chaque fois qu'un noeud **"i"** reçoit une annonce d'itinéraire vers une destination **"d"** d'un voisin **"j"**. Les variables $seqnum_i^d$" , "advertised_hopcountx_i^d" et "route_listx_i^d" représentent le numéro de séquence, le nombre de sauts annoncés et la liste des routes pour la destination **"d"** au noeud **"i"** respectivement.

2.4.2 Le processus de calcul de chemin inverse

La figure 2.8 illustre le calcul du chemin inverse **"reverse path"** dans le processus de découverte de route. Dans cette figure, lorsqu'un noeud source "S" souhaite envoyer des données à la destination "D", un nouveau processus de découverte d'itinéraire est déclenché en diffusant un paquet RREQ de la source "S" à ses voisins "A" et "B".

À la réception du paquet RREQ, les noeuds voisins enregistrent leur propre identité dans les RREQ en tant que "dernier saut" et respectivement une entrée de chemin inverse est ajoutée dans leur table de routage comme (A-S et B-S). Les paquets RREQ sont transmis par "A" et "B" en tant que RREQ (A) et RREQ (B) respectivement au nœud "C", qui formera deux chemins inverses disjoints (C-A-S) et (C-B-S), puis il transmettra le RREQ (A) à ses voisins (en supposant que le RREQ (A) atteigne C rapidement). Les noeuds "E" et "F" forment à leur tour des chemins inverses vers la source (E-C-A-S et F-C-A-S), respectivement.

Après cela, ils reçoivent RREQ (A) et le diffusent à la destination "D". Dans la dernière étape, la destination "D" forme un chemin inverse vers la source "S" (D-E-C-A-S) (supposons que "D" reçoit la première RREQ (A) de E). Comme la deuxième copie de RREQ (A) est reçue de "F" avec le même "dernier saut", le chemin inverse est considéré comme un chemin inverse non disjoint. Il ne sera donc pas établi. Ainsi, "D" répondra au RREQ avec le paquet RREP, qui sera transmis en utilisant le chemin inverse calculé.

Comme AOMDV ne fournit pas de mécanisme de sécurité et que la fraîcheur des routes est basée uniquement sur le numéro de séquence de la destination, ce protocole

est vulnérable à diverses attaques comme l'attaque blackhole, qui exploite le numéro de séquence comme une vulnérabilité.

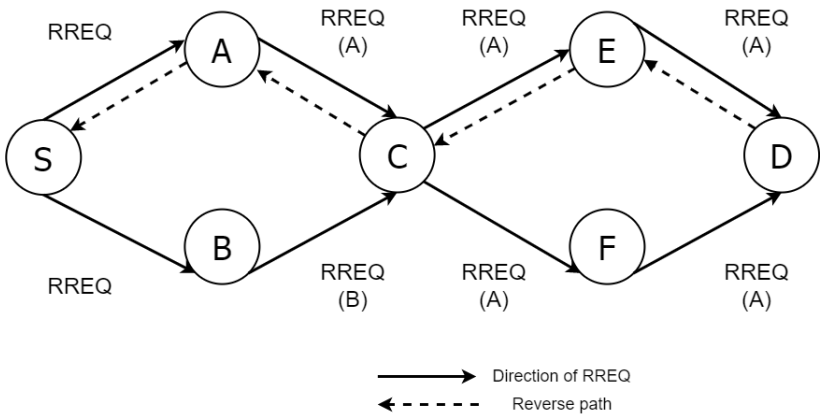


FIGURE 2.8 – *Processus de chemin inverse (He et al. 2015)*

2.4.3 Entretient des routes

Le processus de maintenance de route dans AOMDV est basé sur le paquet de contrôle **"RERR"** (voir figure 2.9). Ce paquet est généré par un noeud une fois qu'une rupture de lien est détectée en énumérant les destinations perdues. Le RERR est envoyé en amont par un noeud vers le noeud source. La transmission du RERR prend deux concepts : **En Broadcast**,En cas d'existence de multiples sauts précédents, qui utilisaient ce lien,et **En Unicast** S'il n'y a aucun saut multiple précédent.(Taha *et al.* 2017) Après la réception du paquet RERR si l'émetteur est le saut suivant du noeud destinataire,le récepteur invalidera cette route dans sa table de routage, puis il propagera le RERR à la source. La transmission sera arrêtée lorsque le paquet atteindra le noeud source. Un processus de découverte de route est relancé si la source a toujours besoin de cette route et que toutes les routes alternatives soient en panne.

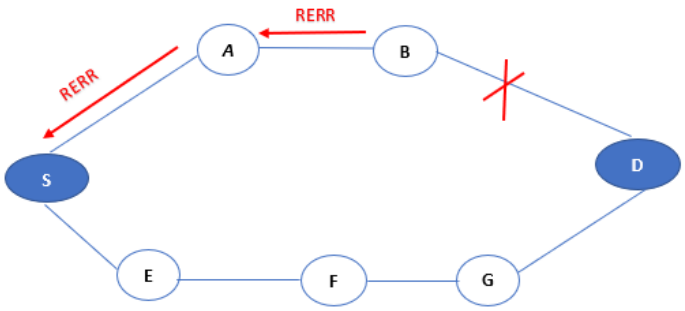


FIGURE 2.9 – *Le processus de maintenance de route*

2.5 Le mécanisme Inter-Couche

On appelle un mécanisme de routage à couche unique **"Single-Layer"** lorsque les décisions dans un processus de routage sont prises sans aucune utilisation de paramètres importants situés dans les trois plus basses couches (Physique, MAC et réseau) du modéle OSI. ce routage à couche unique n'offre pas assez de fléxibilité

pour répondre aux besoins d'une commuication sans fil dans un envirenement comme VANET où,la topologie est fortement dynamique et la vitesse des véhicules est élevée. Ce qui rend toujours la possibilité d'offrir de bonnes performances en terme de delais un problème majeur (Liang *et al.* 2015) .

Afin d'excéder les limites du mécanisme à couche unique, une nouvelle approche de la conception inter-couche **"Cross-Layer"** a été introduite. Cette approche exploite la dépendance entre les couches de protocole OSI où les informations sont échangées entre les couches pour améliorer les performances du réseau(Awang *et al.* 2017).

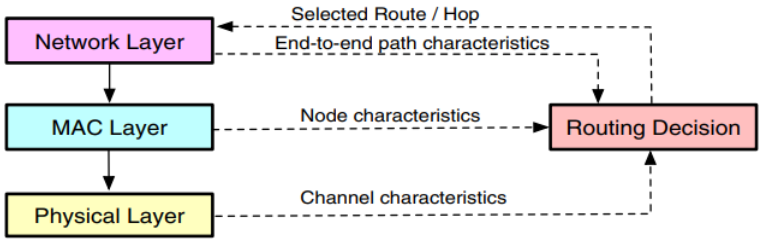


FIGURE 2.10 – *Illustration d'une décision de routage basée sur les trois couches inférieures OSI (PHY, MAC, NET) (Awang et al. 2017))*

La figure 2.10 représente une décision générale d'acheminement inter-couches faisant intervenir les trois couches inférieures PHY, MAC et NET de l'OSI.

Cet échange d'information entre les trois couches permettra au protocole de routage d'être plus robuste face à des problèmes telles que la congestion et l'interférence.

2.6 Les principales attaques contre les réseaux VANETs

2.6.1 Les Exigences de sécurité

Comme les applications des VANET sont diverses, leurs communications et leurs exigences de sécurité au niveau système pourraient aussi être diverses (Razzaque *et al.* 2013). Il est important de respecter les exigences de sécurité de base pour pouvoir faire face aux menaces et aux attaques de sécurité. Les exigences de sécurité importantes pour les réseaux véhiculaires sont citées ci-dessous(Talpur & Gurusamy 2021).

✓Authentification

Comme une première étape de sécurité dans les VANETs le véhicule doit s'authentifier avant de demander un service au système.**Cette étape peut prendre deux types** : Le premier type permet à un réseau de distinguer les noeuds de confiance des noeuds malicieux. Dans ce cas, une authentification de noeud est nécéssaire où, le nouveau noeud doit authentifier son identité plus son adresse et les informations connexes, ce faisant, il devient une partie d'un nouveau réseau. Dans le deuxième type, c'est les messages transmis entre deux véhicules qui doivent s'authentifier pour prouver leurs intégrités(Talpur & Gurusamy 2021).

✓Confidentialité

Pendant la communication entre entités (vehicule ou infrastructure), les étrangers ne sont pas en mesure de comprendre les informations confidentielles qui appartiennent à chaque entité (Engoulou *et al.* 2014). La confidentialité utilise des méthodes de cryptage

basées sur des clès et certificats de confiance pour garantir l'accès uniquement à l'utilisateur légitime des données (Talpur & Gurusamy 2021).

✓Intégrité

L'intégrité garantit qu'un message n'a pas été modifié entre le moment de son envoie et de sa réception. Elle protège contre la création, la destruction ou la modification non autorisée des données (Engoulou *et al.* 2014). L'intégrité peut être obtenue par l'utilisation du hachage et de la cryptographie (Moghraoui 2015)

✓La non-répudiation

Cet objectif de sécurité permet de prouver l'origine des données. Cela signifie qu'un véhicule authentifié ne devrait pas être en mesure de nier l'envoi d'un message après qu'il ait été divulgué par une autorité de confiance (TA) (Ogundoyin 2020).

✓La disponibilité

La disponibilité est considérée comme une des exigences de sécurié les plus importantes pour garantir que toutes les ressources et les services prévus sur le réseau sont disponibles en tout moment. Assurer cette exigence offre un bon fonctionement du réseau en cas de panne. Cette exigence peut étre menacée par différentes attaques de type dénis de services (DOS) (Talpur & Gurusamy 2021).

2.6.2 Les attaques contre les protocoles de routage

Les VANETs sont basés sur des protocoles de routage et le véhicule se comporte comme un routeur dans le réseau pour participer au processus de routage ; cette caractéristique rend donc tous les protocoles de routage comme l'AOMDV vulnérables à plusieurs attaques, parmi eux on trouve :

✓Le Déni de service

Les attaques par déni de service(DoS) sont des attaques sérieuses contre la disponibilité,ce type d'attaque vise à empécher l'accès aux services par l'utilisateur légitime. Dans tel attaque le véhicule malveillants génèrent de faux messages de routage afin de perturber le fonctionement, de capter l'attention ou de contrôler le réseau (Zaidi & Faisal 2018).

La figure 2.11 illustre une attaque DOS dans laquelle la voiture C est l'attaquant qui bloque l'accès aux services de la RSU aux autres utilisateurs (voitures B, D, E, F, G et H).

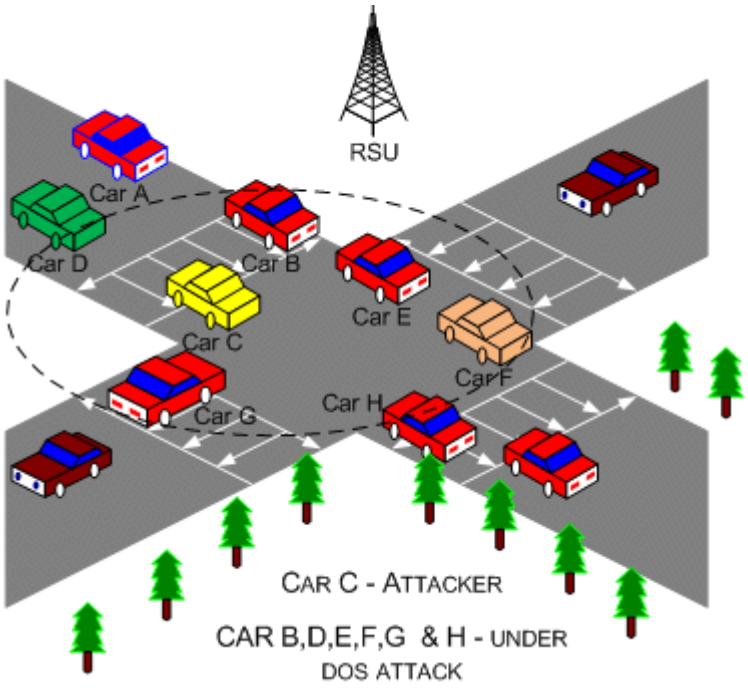


FIGURE 2.11 – *L'attaque par déni de service (Upadhyaya 2018)*

✓L'attaque par déni de service distribué (DDOS)

Ce type d'attque est plus efficace et très difficile de le prévenir ou de le tracer car, plusieurs véhicules malveillants lancent une attaque contre un véhicule légitime depuis différents endroits en utilisant différents créneaux horaires pour envoyer ces messages(Zaidi & Faisal 2018).

✓L'attaque sybil

L'attaque sybil est une attaque néfaste où le véhicule malicieux envoie plusieurs messages aux autre véhicules du réseaux avec une identité falsifiée de l'expéditeur et, ce faisant, il crée l'illusion de l'existence de plusieurs faux véhicules, nuit à l'utilisateur légitime et détruit les performances du réseau(Zaidi & Faisal 2018). Comme le montre la figure 2.12 le nœud dont l'identité est falsifiée est appelé nœud Sybil.

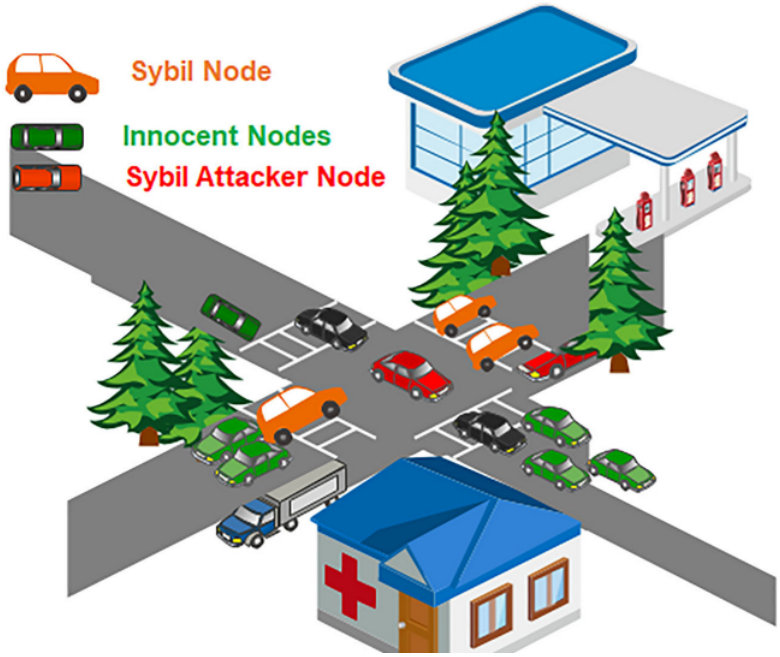


FIGURE 2.12 – *L'attaque sybil (Sharma et al. 2021)*

✓L'attaque Worm Hole

C'est une variante de l'attaque du trou noir,où les véhicules malicieux créent un tunnel entre l'émetteur et le récepteur avec un minimum hope count. Cette spécificité va convaincre l'émetteur d'envoyer ses paquets de données par cette route avec un minimum hope count créé par des véhicules malveillants. Comme la communication entre la source et la destination est initiée à travers ce tunnel malveillant, les véhicules malveillants peuvent supprimer, modifier les paquets de données transmis ou les utiliser à leur avantage (Zaidi & Faisal 2018).

✓L'attaque Blackhole (trou noir)

Dans une telle attaque, le véhicule malveillant vise à rendre la communication indisponible. Pour atteindre cet objectif, le véhicule malveillant persuade la source d'envoyer ses paquets de données par son intermédiaire parce qu'il possède la route la plus récente vers la destination. Cela se fait en falsifiant les informations de routage. Après avoir reçu les paquets de données, le véhicule malveillant les supprime au lieu de les transmettre à leur destination (Naib *et al.* 2021).

Comme le montre la figure 2.13 les voitures honnêtes D et C transmettent des paquets à des voitures malicieuses (véhicules blackhole). Ces voitures créent un trou noir dans le réseau et ne communiquent pas les paquets reçus aux autres véhicules légitimes, c'est-à-dire E et F.

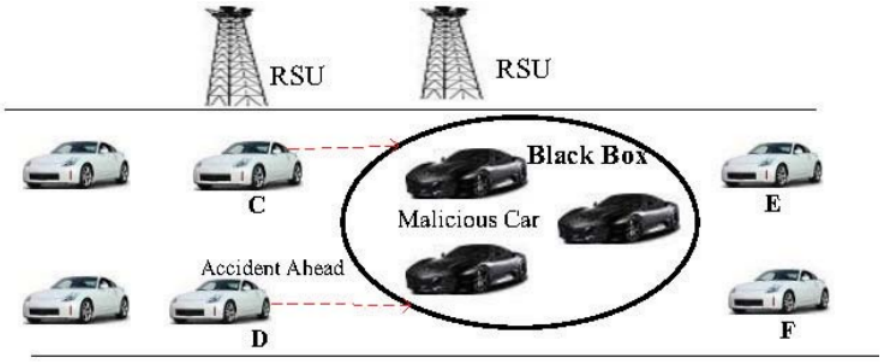


FIGURE 2.13 – *L'attaque Blackhole dans VANETs (Zaidi & Faisal 2018)*

✓L'attaque Man in middle

Dans l'attaque de l'homme au milieu, les véhicules malintentionnés visent à avoir accès aux informations que les véhicules source et destination essayaient de s'envoyer en s'insèrant dans la communication entre ces deux véhicules. Et là, le véhicule malicieux injecte de fausses informations entre les véhicules.(Zaidi & Faisal 2018)

2.7 L'ATTAQUE BLACKHOLE DANS AOMDV

Une attaque par trou noir est un type d'attaque par déni de service, où le noeud malveillant exploite le concept d'avoir la route la plus récente vers une destination spécifique en termes de numéro de séquence plus élevé. Il répond immédiatement au RREQ avec un RREP corrompu contenant un numéro de séquence plus élevé dans le processus de découverte de route. Le nœud source supposera que ce nœud blackhole possède effectivement la route la plus récente vers la destination, et trouve qu'il n'est pas nécessaire d'accepter les RREP des autres. Ainsi, la source enverra tous les paquets de données à ce nœud malveillant, qui les supprimera au lieu de les relayer (Naib *et al.* 2021).

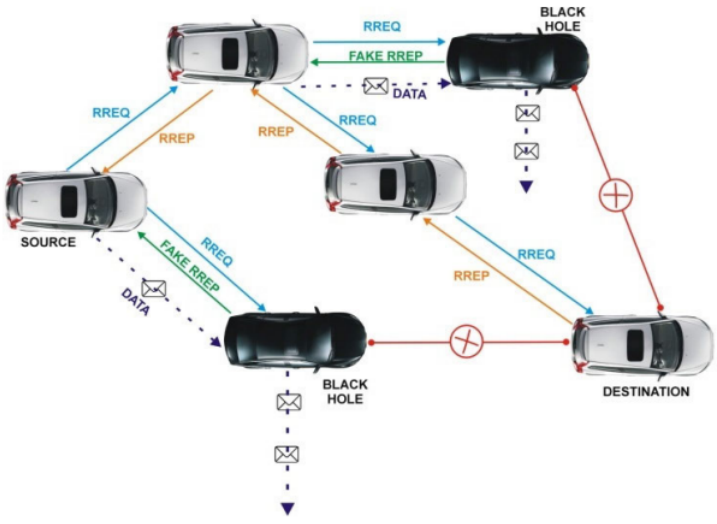


FIGURE 2.14 – *L'attaque Blackhole (Hassan et al. 2020)*

Dans la figure 2.14, le noeud source "SOURCE" veut envoyer des paquets de données au noeud "DESTINATION". Pour ce faire, "SOURCE" diffuse RREQ aux noeuds voisins. Le noeud blackhole "Blackhole" répond directement avec un paquet FAKE RREP avec un numéro de séquence plus élevé. Par ce fait, "Blackhole" oblige la source "SOURCE" à le sélectionner comme prochain saut vers la destination pour la transmission des paquets de données. Le noeud malveillant "Blackhole" supprime à son tour tous les paquets de données reçus.

2.8 Conclusion

Dans ce chapitre nous avons presenté la technique de routage multi-chemin et exposé le protocole de routage multi-chemin AOMDV avec tous ses types de messages de contrôles et leurs roles. Par la suite, et tout au long du fonctionement de l'AOMDV, nous avons définis les étapes suivantes : Le processus de découverte de route, Le processus de calcul de chemin inverse, l'envoi de la répense RREP et le processus d'entretien des routes. Puis nous avons jugé utile d'expliquer le mecanisme Inter-Couche dans les protocoles de routage. Pour clore ce chapitre, on a examiné l'aspect sécuritaire du protocole AOMDV et sa vulnérabilité aux differentes attaques dans un environnement distribué comme VANETs . Dans la prochaine étape, nous discuterons des solutions proposées pour sécuriser le protocole AOMDV contre l'attaque blackhole.

Contribution I : Mécanisme de sécurité inter-couche contre l'attaque BlackHole dans les MANETs

3

Sommaire

3.1 Etat de l'art 37
3.2 Modèle de l'attaque blackhole contre le protocole AOMDV 39
3.3 La solution proposée 40
3.4 Evaluation des performances 46
3.4.1 L'environnement de simulation 46
3.4.2 Présentation du simulateur NS2 (Network Simulator Version-2) 47
3.4.3 Les mesures des performances de la simulation 49
3.4.4 Discussions et comparaisons des résultats de simulation 49
Conclusion 58

Les réseaux mobiles adhoc (MANET) sont un ensemble de noeuds mobiles qui communiquent entre eux tout en partageant le même support de transmission sans fil, sans la présence d'une infrastructure prédéfinie ou d'une autorité de contrôle centrale. AOMDV est l'un des protocoles de routage multivoies bien connus, conçu pour ce type de réseaux. Comme tous les protocoles de routages réactifs, AOMDV réduit la génération d'un grand trafic dans le réseau pour éviter que le réseau soit saturé, en éliminant au maximum les inondations. Malgré cette caractéristique AOMDV est vulnérable aux différentes attaques comme blackhole. Vu que les noeuds du réseau ont la particuarité d'être un routeur, le noeud malicieux blackhole capture le trafic des données des noeuds voisins, puis supprime tous les paquets reçus ce qui détériore les performances du réseau. Dans ce chapitre, nous introduisons l'attaque du trou noir (blackhole attack). Ensuite, nous présenterons quelques travaux connexes. Après, nous présenterons une nouvelle méthodologie inter-couches pour détecter et isoler le noeud de blackhole. Enfin, nous exposerons la simulation et l'évaluation des performances de notre solution par rapport à l'AOMDV sujet à une attaque de trou noir.

3.1 Etat de l'art

Les solutions proposées pour sécuriser AOMDV contre l'attaque blackhole dépendent des mécanismes de détection qui peuvent être divisés en deux catégories. Dans la première catégorie, les chercheurs utilisent des méthodes cryptographiques et la valeur de confiance, dans la deuxième catégorie, la solution consiste à améliorer le protocole de routage en modifiant les paquets de contrôle ou le processus de découverte de route.

Dans (Deng *et al.* 2002) les auteurs ont proposé une solution pour contourner l'attaque du trou noir dans le protocole AODV. Cette solution consiste à utiliser une route supplémentaire vers le nœud intermédiaire qui rediffuse le message RREQ pour vérifier s'il existe une route entre ce nœud intermédiaire et le destinataire. Dans le processus de vérification, les auteurs ajoutent un champ next hop dans le paquet RREP et utilisent deux paquets supplémentaires (Further Request, FurtherReplay). Lorsque le nœud intermédiaire répond au RREQ, il renvoie les informations sur le prochain saut. Le nœud source, après avoir reçu un RREP, extrait l'information du nexthop et envoie une FurtherRequest au prochain saut de ce nœud intermédiaire pour vérifier s'il a une route vers le nœud intermédiaire qui a envoyé un RREP et dispose d'une route vers le nœud de destination. Le prochain saut répondra avec un paquet FurtherReplay et ensuite, quand le noeud source recevra ce paquet, il sortira le résultat de la vérification. Le résultat peut prendre trois cas de figure.

- Dans le premier cas, si la réponse est oui, alors le noeud intermédiaire n'est pas un nœud de trou noir et là, le nœud source commence à envoyer les paquets de données.
- Dans le second cas, si le nexthop n'a pas de route vers le nœud intermédiaire mais a une route vers le nœud de destination, le RREP provenant du nœud intermédiaire requis est supprimé et une nouvelle route vers le nœud de destination est utilisée.
- Dans le troisième cas, si le prochain saut n'a pas de route ni vers le noeud intermédiaire ni vers le noeud de destination. Le noeud source se voit contraint de déclencher un autre processus de découverte de route.

Un message d'ALARME est envoyé à l'ensemble du réseau pour isoler le nœud malveillant. Le coté négatif de cette solution c'est l'augmentation de la surcharge du réseau et du délai moyen de bout en bout à cause des échanges des paquets Further Request, FurtherReplay et ALARM

Afin d'assurer une protéction contre les attaques de type Blackhole, une amélioration de la sécurité du protocole de routage AODV est proposée dans (Mistry *et al.* 2010). Dans cette approche, le noeud source appelle une fonction supplémentaire "Pre_ReceiveReply(Packet P)" qui est illustrée dans la figure 3.1. Dans cette dernière le noeud source après avoir reçu le premier RREP, attendra le "MOST WAIT TIME" (c'est-à-dire la moitié de la valeur du temps pendant lequel le noeud source attend les messages de contrôle RREP avant de régénérer RREQ). Pendant ce temps, le nœud source s'attelera à quatre opérations bien détérminées :

- Il enregistrera tous les messages de contrôle RREP qui arrivent dans la table "Cmg_RREP_Tab".
- Il extraira le RREP avec un numéro de séquence plus élevé et également l'identité du nœud malicieux, ce qui permet de rejeter tout RREP provenant de ce dit nœud.
- Il sélectionnera le RREP ayant le numéro de séquence de destination le plus élevé dans la table Cmg RREP Tab et continue le processus normal d'AODV.

— Il videra la table "Cmg_RREP_Tab".

Cette solution est considérée comme simple et efficace à mettre en œuvre. La logique dans cette aproche peut détecter les noeuds malveillants avec une très bonne augmentation de PDR par rapport au AODV après une attaque. Or, le problème dans cette approche est qu'elle provoque une augmentation du délai moyen de bout de bout et la surcharge du réseau.

```
The Proposed Algorithm : at Source Node:

  Pre_ReceiveReply (Packet P){

     t0 = get(current time value)
     t1=t0 + MOS_WAIT_TIME
     while(CURRENT_TIME <= t1){
       Store P.Dest_Seq_No and P.NODE_ID In
       Cmg_RREP_Tab table
     }
     while (Cmg_RREP_Tab is not empty) {
       Select Dest_Seq_No from table
       if (Dest_Seq_No >>>=Src_Seq_No){
            Mali_Node=Node_Id
            discard entry from table
       }
     }
     select Packet q for Node_Id having
     highest value of Dest_Seq_No
     ReceiveReply(Packet q)
    }
```

FIGURE 3.1 – *Le pseudo-code de la fonction Pre_ReceiveReply(Packet P) (Mistry et al. 2010)*

Un routage AOMDV multivoies basé sur la confiance combiné à un chiffrement doux **"soft-encryption"** pour sécuriser AOMDV contre les attaques par trou noir dans les réseaux adhoc (T-AOMDV) est proposé dans (Huang *et al.* 2011). Dans cette approche, le message du noeud source est segmenté en trois parties qui sont chiffrées à l'aide d'un cryptage doux. Après cela, ces parties sont acheminées séparément par différents chemins multiples basés sur la confiance, puis décryptées par le noeud de destination pour récupérer le message original. Cependant, cette approche souffre d'une consommation d'énergie excessive et d'une latence en raison de l'utilisation des opérations cryptographiques.

Dans (Rani & Kumar 2013), Rani et son groupe de travail ont proposé une amélioration du protocole AOMDV pour la détection de l'attaque du blackhole. Cette amélioration consistait à modifier deux paquets : Le paquet RREQ en ajoutant un nouveau champ nommé First hop et le paquet RREP en ajoutant le champ originator, qui sert à mémoriser l'identité du noeud de destination ou du noeud intermédiaire avec une nouvelle route vers la destination. De plus, chaque noeud maintient une table de légitimité qui contient deux champs : Le premier nommé "sélection" qui indique

combien de fois un noeud a été sélectionné pendant la découverte du chemin et le second intitulé "succès" qui montre combien de fois la destination a reçu le paquet de données avec succès à travers le chemin qui contient le noeud. Le rapport de légitimité (succès/sélection) est calculé pour identifier le noeud malveillant. Des lors, plus le rapport de légitimité est faible, plus il y a de fortes chances que le noeud soit malveillant. Néanmoins, cette amélioration du protocol AOMDV augmente le délai moyen de bout en bout et la surcharge de routage en raison de la transmission du paquet de changement de route supplémentaire.

Pandikumar et son groupe de travail ont appliqué une technique mesurable pour atténuer les noeud de trous noirs dans les MANET avec le protocole AOMDV (Pandikumar *et al.* 2017). La technique proposée consistait à utiliser un système de détection d'intrusion (IDS), qui modifiait le protocole AOMDV. L'expéditeur doit d'abord vérifier l'état du numéro de séquence quel que soit le moment où il reçoit un RREP. Ainsi, si le numéro de séquence du nouveau RREP n'est pas inférieur au numéro de séquence maximal, cela veut dire que le paquet est envoyé par l'attaquant avec le numéro de séquence 2^{32}. De ce fait, le noeud source rejette le nouveau RREP. Dans le cas contraire,le noeud source met à jour sa table de routage en utilisant le numéro de séquence et les règles de comptage de sauts. L'inconvénient de cette solution c'est que dans le réseau il n'y a que les noeuds source qui sont en mesure de détecter les noeuds blackhole. Les autres noeuds du réseau ne sont pas notifiés sur l'identité des noeuds malveillants.

Une cryptographie à courbes elliptiques (ECC), qui est une technique de cryptographie à clé publique, permet de sécuriser les paquets contre les attaques par trou noir dans(Sultana & Ahmed 2018). Dans cette approche,la sélection des chemins multiples d'une source à la destination sera faite en utilisant le protocole AOMDV. Les données seront cryptées et décryptées en utilisant des clés publiques et privées. Là, la source crypte le paquet avec une clé secrète. La destination déchiffre à son tour le message crypté pour obtenir les données originales. Ainsi, le noeud malveillant ne peut pas décrypter le message reçu car la possibilité de récupérer la clé privée est nulle. Toutefois, cette méthode nécessite beaucoup de calculs comme le cryptage, le décryptage et la génération des cléfs. Ces calculs entament l'énergie du réseau. L'annonce des cléfs publiques provoque également une augmentation de la surcharge du réseau.

3.2 Modèle de l'attaque blackhole contre le protocole AOMDV

L'attaque Blackhole est parmi l'une des attaque dans la couche réseau et est aussi une sorte d'attaque par déni de service. Dans cette attaque, le noeud malveillant après avoir reçu un paquet RREQ, envoie immédiatement un faux paquet REPP avec un numéro de séquence plus élevé (Naib *et al.* 2019b) afin d'être sélectionné comme faisant partie du chemin le plus court et le plus récent vers le noeud attaqué.

Par conséquent, le noeud source suppose que le noeud malveillant possède la route la plus récente vers la destination, donc il ignore tout paquet RREP reçu des autres noeuds. Il commence alors à envoyer les paquets de données au noeud blackhole. Ce qui entraine l'abondon des paquets de données capturés par le noeud malveillant.

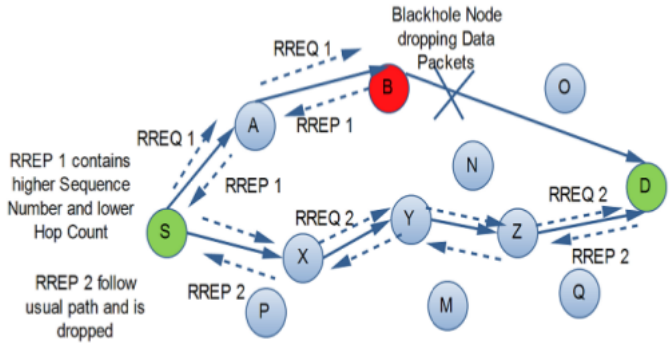


FIGURE 3.2 – *l'attaque Blackhole sur le protocole AOMDV dans les MANETs (Bhardwaj & Singh 2014)*

Dans la figure 3.2, nous supposons que le noeud S veut envoyer des paquets de données au noeud D. B est un noeud malveillant. Le noeud B répond directement à la requête RREQ envoyée à D par un faux paquet RREP avec le numéro de séquence le plus élevé. Après cela, S choisit le RREP de ce noeud malveillant. Dans ce cas, le noeud B réalise une attaque de type trou noir dans le réseau en supprimant tous les paquets de données reçus.

Afin d'évaluer le protocole AOMDV et tester l'effet de cette attaque dont il est sujet, nous avons procédé à une étude de simulation détaillée.

3.3 La solution proposée

Dans notre solution proposée, nous visons à sécuriser le protocole de routage AOMDV contre les attaques de trous noirs dans les MANET à l'aide du mécanisme inter-couche. Notre méthode introduit une phase supplémentaire "validation du chemin" par l'interaction entre la couche réseau et la couche d'accès au support pour vérifier si le noeud intermédiaire est un noeud de confiance ou pas. Dans cette phase de validation, nous avons utilisé la variable XMIT REASON avec deux valeurs : XMIT REASON REPLAY DST et XMIT REASON REPLY IN pour indiquer l'initiateur du RREP. Si le noeud intermédiaire possède une nouvelle route vers le noeud de destination, il donne automatiquement la valeur de la variable XMIT_REASON à la valeur XMIT_REASON_RREPLY_IN au niveau de la couche MAC avant d'envoyer le paquet PREP. Le même processus est utilisé pour la destination mais avec la valeur de XMIT_REASON_REPLY_DST. Si la valeur de XMIT REASON est différente des deux valeurs supplémentaires su-citées, le noeud source aura pour tâche de :

- Identifier le noeud malveillant.
- Ajouter le noeud malicieux "BHN" à la liste des trous noirs.
- Supprimer les chemins qui transitent par le BHN.
- Choisir un autre itinéraire parmi les multiples chemins calculés.
- Supprimer le paquet RREP falsifié.

Dans le cas contraire, le noeud intermédiaire deviendra un noeud de confiance.

Les algorithmes suivants détaillent le comportement des trois noeuds suivants : Malveillant, source, destination ou intermédiaire possédant une route fraîche .

Algorithme 1 : Algorithme du noeud source

```
XMIT_REASON_RREP_DST Destination cross-layer information;
XMIT_REASON_RREP_IN Intermediate node cross-layer information;
VI_BH List of blackhole nodes;
RP_SRC The sender of RREP;
DST_ADDR The RREP destination address;
SRC The source node;
.....
SEND RREQ;
Receive RREP ;
if DST_ADDR==SRC then
    /* i'm the intended receipient of RREP */
    if FIND(VI_BH,RP_SRC)==TRUE then
        /* The sender of RREP belongs to BH list */
        Remove paths that transit through BHN;
        Delete RREP;
    else
        /* Cross layer check and validation of the path */
        if (XMIT_REASON_ == XMIT_REASON_RREP_DST) or
         (XMIT_REASON_ == XMIT_REASON_RREP_IN) then
            /* The originator of RREP is DST or IN or FW */
            Go to FINISH;
        else
            /* The originator of RREP is Blackhole node */
            Delete RREP;
            ADD RP_SRC to VI_BH;
            Remove paths that transit through BHN;
            Choose a diffrent path from the routing table;
            Delete RREP;
        end
    end
end
FINISH
```

Algorithme 2 : Algorithme noeud de destination ou intermédiaire possédant une route fraîche

```
Receive RREQ ;
/*i'm the destination or the intermediate node that have fresh route to the
  destination */
Prepare RREP ;
XMIT_REASON_ == XMIT_REASON_RREP_DST ;
/*At the medium access layer : In the case of IN*/
XMIT_REASON_ == XMIT_REASON_RREP_DST ;
SEND RREP ;
FINISH
```

Algorithme 3 : Algorithme du noeud blackhole

```
Receive RREQ ;
/* At meduim acces layer : Do nothing */
XMIT_REASON_ ==0 ;
SEND RREP immediately with higher sequence number ;
FINISH
```

Algorithme 4 : Algorithme du noeud blackhole

```
Receive RREQ ;
/* At meduim acces layer : Do nothing */
XMIT_REASON_ ==0 ;
SEND RREP immediately with higher sequence number ;
FINISH
```

La figure 3.3 présente l'organigramme qui résume toutes les étapes de notre processus.

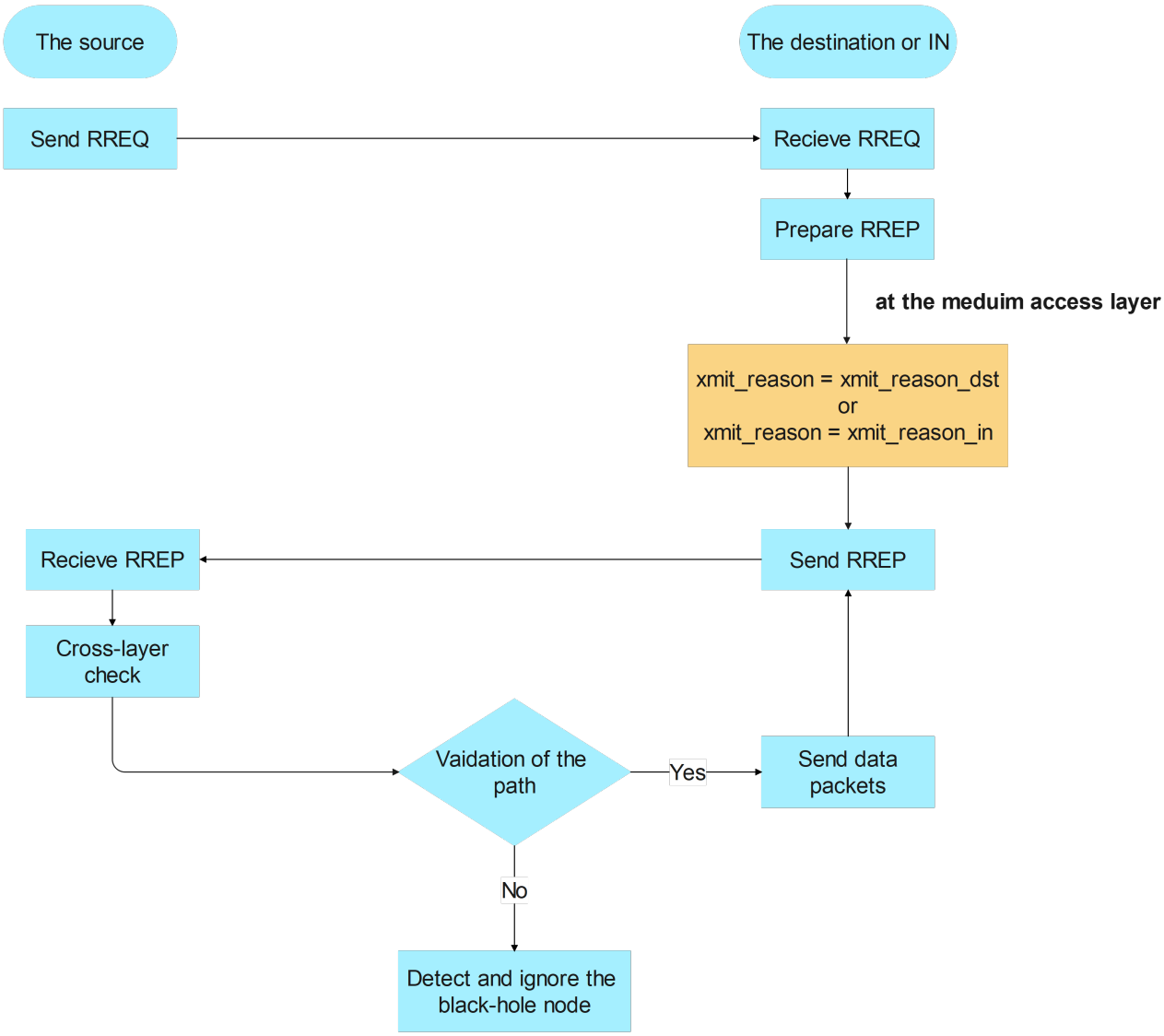


FIGURE 3.3 – *Organigramme de la méthode proposée (Naib et al. 2019a)*

TABLE 3.1 – *Comparaison entre notre solution et les méthodes proposées dans l'état de l'art.*

No.	Références	Protocole	Base de données	Simulateur	Avantages	Incovénients
1	(Deng *et al.* 2002)	AODV	Simulation	NS2	Détection du comportement des neuds malveillants	Augmentation de la surcharge de réseau et du délai moyen de bout en bout
2	(Mistry *et al.* 2010)	AODV	Simulation	NS2	Détection des noeuds blackhole	Augmenter le délai moyen de bout en bout et de la surcharge de routage
3	(Huang *et al.* 2011)	AOMDV	Simulation	NS2	Assurer une sécurité efficace contre les attaques par blackhole	Augmentation excessive de la consommation d'énergie et soufre d'une latence énorme. Peut échouer dans une attaque interne.
4	(Rani & Kumar 2013)	AOMDV	Simulation	NS2	Amélioration du protocole AOMDV contre l'attaque blackhole	Augmentation du délai moyen de bout en bout et de la surcharge de routage
5	(Pandikumar *et al.* 2017)	AOMDV	Simulation	NS2	Détection du comportement malveillant dans le réseau	Les noeuds qui sont différents du noeuds source n'ont pas une information sur l'identité du noeud blackhole

Continued

Table 3.1 – *Comparaison entre notre solution et les méthodes proposées dans l'état de l'art.*

No.	Références	Protocole	Base de données	Simulateur	Avantages	Incovénients
6	(Sultana & Ahmed 2018)	AOMDV	Simulation	NS2	Détection éfficace du noeud malveillant externe.	Augmentation de la surcharge de routage et du coût de la consomation d'énergie
6	(Naib *et al.* 2019a)	AOMDV	Simulation	NS2	Détection efficace des attaques blackhole externes et internes. Amélioration du taux de livraison des paquets. N'augmente pas les coûts de calcul et de communication	

Comme illustré dans le tableau 3.1 l'objectif principal des métodes présentées dans l'état de l'art est de protéger le protocol de routage contre le comportement malveillant du noeud blackhole. Sécuriser un protocol de routage se fait soit en améliorant son processus de découvert de route (Deng *et al.* 2002; Mistry *et al.* 2010; Pandikumar *et al.* 2017; Rani & Kumar 2013) en ajoutant des paquets de contrôle ou des tables. Soit en utilisant des méthodes cryptographiques (Huang *et al.* 2011; Sultana & Ahmed 2018) pour sécuriser les données partagées.

Cependant les méthodes basées sur l'amélioration du processus de découverte de route agrandissent la valeur du délai moyen de bout en bout et la charge de routage normalisée à cause de l'échange des paquets de routages additionels et du temps de collect des paquets RREP. En plus, les techniques basées sur des méthodes cryptographiques nécessitent une puissance de calcul importante. Cette caractéristique consomme l'énergie des noeuds, ce qui réduit la durée de vie du réseau.

3.4 Evaluation des performances

3.4.1 L'environnement de simulation

Nos résultats ont été obtenus après de multiples simulations en faisant varier le nombre et la mobilité des noeuds communicants (10, 20, 30 et 40). Pour les simulations, certains paramètres ont été utilisés. Comme le montre le tableau suivant, nous avons comparé notre solution CRAOMDV avec l'AOMDV normal et l'AOMDV avec une attaque du trou noir. Dans nos scénarios de simulation, le réseau est composé de 50 noeuds mobiles dont 3 malveillants. Le NS2 (Raja Kumar *et al.* 2021) a été utilisé comme simulateur. Les paramètres de simulations figurent dans le tableau 3.2

Paramètres	Valeur
Zone de simulation (m * m)	1500 * 300
Nombre de noeuds	50
Temps de simulation (s)	900
Modèle de mobilité	Random way point
Vitesse maximale (m/s)	20
Pause time (s)	0, 30, 60, 120, 300, 600, 900
Nombre de noeuds communicants	10, 20, 30, 40
La couche application	Constant Bit Rate (CBR)
Taille des paquets	512 bytes
Débit de paquets	4 packet/second
La couche MAC	802.11
La couche réseau	AOMDV - BHAOMDV - CRAOMDV
Nombre des noeuds blackhole	3

Table 3.2 – *Paramètres de simulation*

3.4.2 Présentation du simulateur NS2 (Network Simulator Version-2)

En général les simulateurs réseaux autorisent les développeurs à créer et à simuler de nouveaux modèles sur un réseau arbitraire en spécifiant à la fois le comportement des noeuds du réseau et les canaux de communication (Toor & Jain 2017).

Parmi les simulateurs les plus connus on trouve NS2 (Network Simulator Version-2), qui est un simulateur d'événements discret et open source. Il est conçu spécialement pour la recherche sur les réseaux. L'open source signifie que tous les utilisateurs peuvent étudier librement le code source, le modifier ou le distribuer (Toor & Jain 2017). NS2 supporte la simulation filaire et sans fil de fonctions et de protocoles tels que TCP, UDP, etc. Sa flexibilité et son comportement modulaire rendent ce type de simulateur de réseau bien connu (Kabir *et al.* 2014).

Ce simulateur est écrit dans deux languages : Le premier etant le C++ qui définit le mécanisme interne des objets de simulation tandis que Tool Command Language orienté objet (OTcl) est utilisé plutôt dans le contrôle des scénarios de simulation et dans la planification des evénements.

Ces deux languages sont couplés à l'aide de TclCL. NS2 exécute des simulations pour explorer différentes questions comme l'interaction des protocoles, le contrôle de la congestion, l'effet de la dynamique du réseau, l'évolutivité, etc.

La sortie de la simulation est sous forme de texte ou d'animation. Pour interpréter ces résultats de manière graphique et interactive, des outils tels que NAM (Network AniMator), XGraph (Talukdar *et al.* 2021) et Gnuplot (Li & Wang 2021) sont utilisés.

La sortie de la simulation de type texte peut étre transformer en une présentation plus flexible.

Parmi les caractéristiques du NS2 :

- Il fournit la simulation d'une diversité de protocoles HTTP, TCP, UDP,SRM, RTP et certains algorithmes de routage.
- Il englobe pratiquement toutes les variantes de TCP, les différentes formes de multidiffusion, les réseaux câblés, les protocoles de routage adhoc (AODV, AOMDV, OLSR etc..), la diffusion de données, les satellites et autres.
- Il couvre tous les modèles de propagation qui sont diférents des téléphones cellulaires.
- Le NS2 utilise différents générateurs de scénarios : Générateur de topologie, générateur d'agents et générateur de routage.
- Dans NS2, le planificateur d'événements conserve la traçabilité du temps de simulation et relâche tous les événements dans la file d'attente en faisant appel aux composants réseau appropriés.
- Il assure l'animation et la représentation des résultats de simulation par le NAM et le X-Graph.

La figure 3.4 illustre les principales étapes de simulation avec NS2 en commençant par le script de simulation jusqu'à l'animation des résultats de cette simulation.

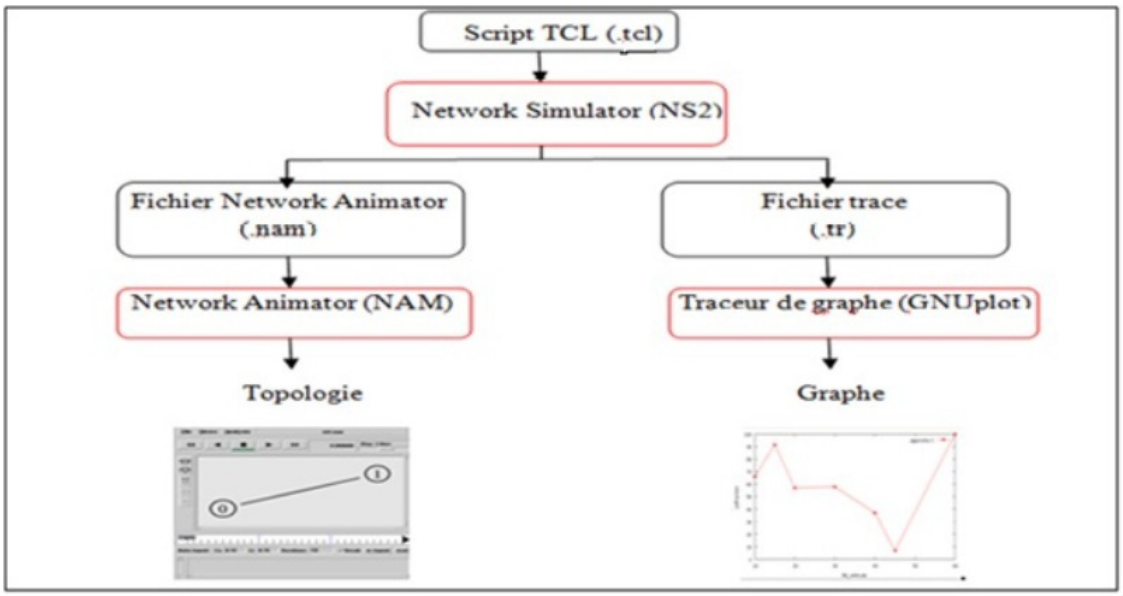


FIGURE 3.4 – *Flot de simulation*

TCL/TK/OTCL

✓**TCL (Tools Command Langage) :** Le langage de script TCL a été créé par John Ousterhout alors qu'il travaillait à l'Université de Californie, Berkeley (Nampally & Raghavender Sharma 2017). TCL est un langage de programmation de scripts : Interprété, dynamique et similaire à PERL ou Python. Ce langage de commande est à base de chaînes de caractères avec une syntaxe très simple. TCL permet d'assembler les blocs de construction du logiciel de façon interactive. Il est extensible grâce aux langages C, C++ et Java.

✓**TK (Tool kit) :** Est un ensemble d'outils widgets multiplateformes permettant de créer des interfaces utilisateurs graphiques (GUI).

✓**OTCL :** OTCL représente la hiérarchie interprétée. Cette dernière est une interface utilisateur qui est utilisée pour créer et configurer le réseau.

✓**NAM (Network Animator) :** Nam est un outil d'animation basé sur Tcl/TK pour visualiser les traces de simulation de réseaux et les traces de paquets du monde réel (isi.edu 2022). Il gère la disposition de la topologie, l'animation au niveau des paquets et divers outils de contrôle des données.

✓**GNUplot :** GNUPlot est un logiciel qui joue un role de grapheur qui trace des graphiques d'une donnée ou d'une fonction mathématique. La raison principale de ce grapheur c'est de permettre aux scientifiques et aux étudiants de visualiser des fonctions et des données mathématiques de manière interactive. Il supporte plusieurs platformes tels que Linux, OS/2, MS Windows, OSX, VMS.

✓**AWK :** AWK est un langage de script qui consiste à traiter ,extraire et formater les données d'un fichier texte en entrée avec des résultats dans un format demandé.

3.4.3 Les mesures des performances de la simulation

Dans cette section, les mesures quantitatives les plus connues sont utilisées pour l'évaluation de AOMDV normal, AOMDV sous l'attaque de trou noir et notre solution CRAOMDV.

Ces mesures sont : La fraction de livraison de paquets (PDF), le délayage de bout en bout (AE2ED) et la charge de routage normalisée (NRL). Ces métriques sont étudiées avec différents nombres de connexions.

✓PDF (Packet Delivery Fraction) :

Cette métrique représente le rapport entre tous les paquets de données livrés à leurs destinations et les paquets de données envoyés par la source dans le réseau. Un protocole de routage est performant lorsque la valeur du Packet Delivery Fraction (PDF) est plus élevée, ce qui signifie que les paquets de données ont atteint avec succès la couche d'application du noeud de destination.

$$PDF = \frac{\sum Paquets\ reçus}{\sum paquets\ envoyés} \times 100 \tag{3.1}$$

✓AE2ED (Average end-to-end delay) :

Cette métrique est définie comme le temps moyen nécessaire pour transmettre avec succès le paquet de données d'une source à sa destination.

$$AE2ED = \frac{E2ED}{\sum paquets\ reçus} \tag{3.2}$$

Avec :

E2ED= $\sum TR_{(i)} - TS_{(i)}$

$TR_{(i)}$: Moment où le paquet de données est reçu par la destination.
$TS_{(i)}$: Moment où le paquet de données est émis par la source.

✓Normalized routing load :

Il est calculé comme le rapport entre la somme des paquets de routage transmis et la somme des paquets de données reçus.

$$NRL = \frac{\sum Paquets\ de\ routage}{\sum paquets\ reçus} \tag{3.3}$$

3.4.4 Discussions et comparaisons des résultats de simulation

Les graphes du PDF

Les figures (3.5,3.6, 3.7, 3.8) décrivent comment le nombre de noeuds de communication et le temps de pause influencent le taux de livraison des paquets. Les figures montrent clairement la corrélation inverse entre le nombre de noeuds communicants et le PDF, ceci est dû à la surcharge du réseau et à la saturation des files d'attente dans AOMDV normal, BH_AOMDV et CRAOMDV, ce qui entraîne une perte de données. Dans la plupart des cas AOMDV, BH_AOMDV et CRAOMDV le PDF diminue dès que la mobilité baisse et que le nombre de noeuds communicants augmente (pt300 et pt900).

Lorsque les noeuds communiquent avec une faible mobilité, le chemin entre eux devient plus long, ce qui entraîne une plus grande probabilité de perte de données. Comme on peut le voir dans 3.5,3.6, 3.7, 3.8 le PDF dans BH_AOMDV est plus faible que la PDF dans AOMDV normal et notre approche CRAOMDV parce que dans BHAOMDV, les paquets de données ont été supprimés par les noeuds de trou noir. "CRAOMDV" D'après les résultats des simulations, la valeur du PDF dans notre mécanisme "CRAOMDV" est presque comme le AOMDV sans attaque et meilleure que l'AOMDV avec une attaque par trou noir.

PDF 10 nœuds communicants :



FIGURE 3.5 – *PDF des 10 nœuds communicants en fonction du temps de pause (S)*

PDF 20 nœuds communicants :

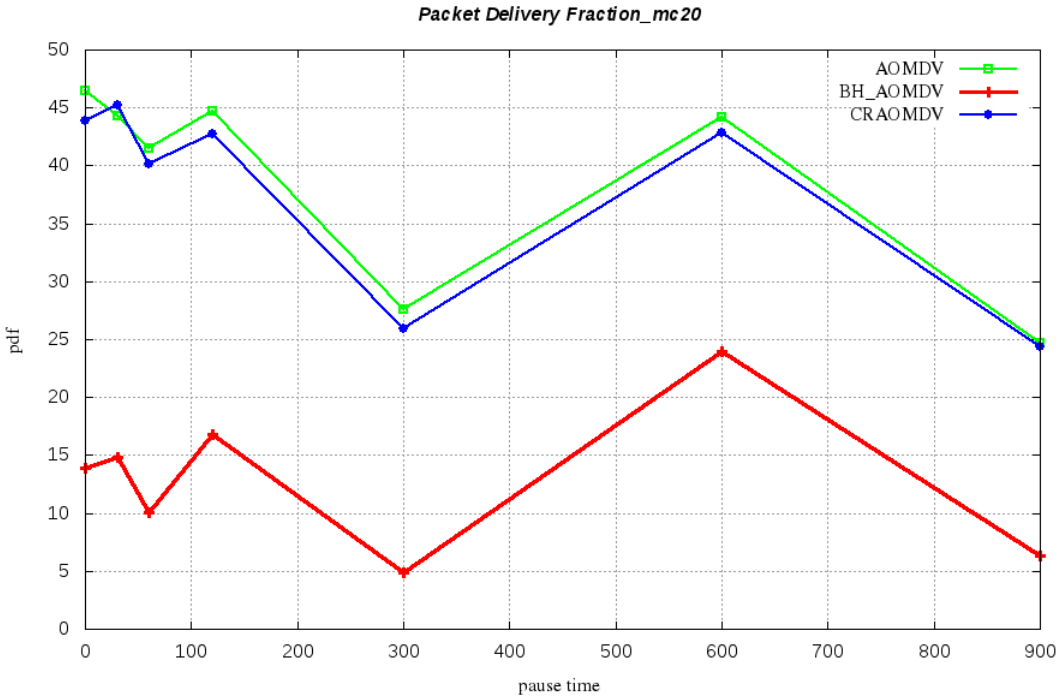


FIGURE 3.6 – *PDF des 20 nœuds communicants en fonction du temps de pause (S)*

PDF 30 nœuds communicants :

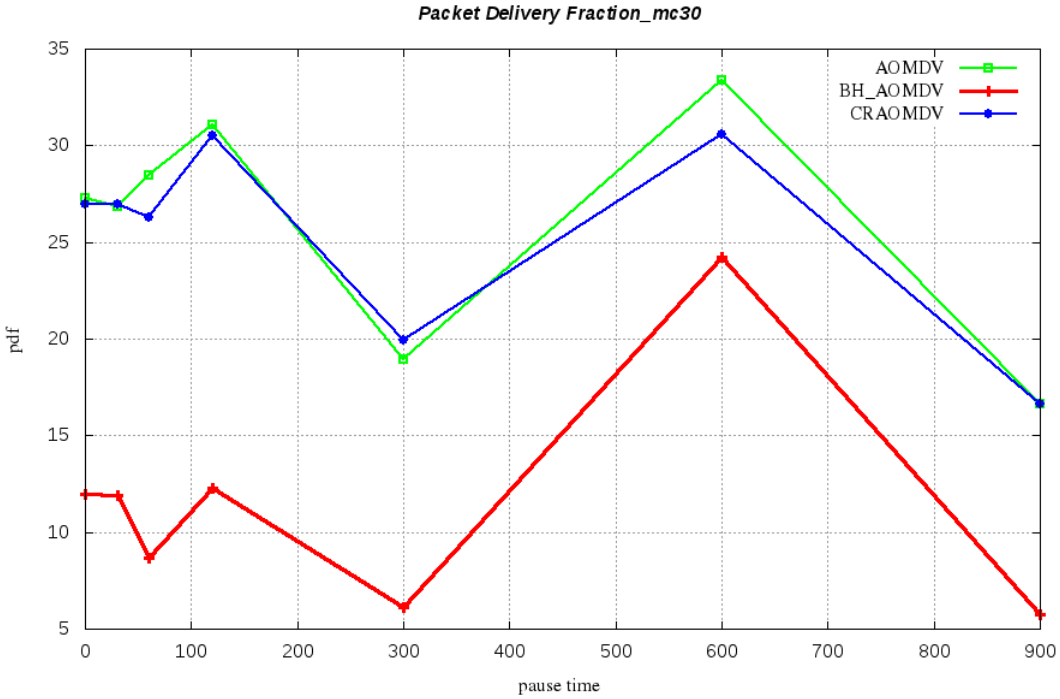


FIGURE 3.7 – *PDF des 30 nœuds communicants en fonction du temps de pause (S)*

PDF 40 nœuds communicants :



FIGURE 3.8 – *PDF des 40 nœuds communicants en fonction du temps de pause (S)*

Les graphes de AE2ED

D'après les figures ci-dessus (3.9,3.10, 3.11, 3.12) nous pouvons observer que, tant que le nombre de noeuds communicants augmente, l'AE2ED augmente en raison d'un niveau élevé de congestion du réseau. Dans la majorité des graphes (3.9,3.10, 3.11, 3.12) la valeur du l'AE2ED augmente une fois que la mobilité reduite (pause time : 600 - 900). Cela est du à la diminution de la somme des paquets reçus (voir les figures du PDF).

BH_AOMDV présente un délai nettement inférieur à celui d'AOMDV et de CRAOMDV, car les paquets de données ont été abandonnés immédiatement par les noeuds de trou noir sans être dans les tampons ou retardés. Dans la figure 3.9 la valeur du l'AE2ED enregistre un affaiblisement important dans le cas de BH_AOMDV d'où une mobilité trés faible (pause time : 600 - 900) presque égale à zéro. Cela peut étre éxpliqué par le positionement des noeuds blackhol hors de portés des noeuds communicants et avec l'affaiblissement continu de la mobilité, aucun paquet de donnée ne va étre supprimé par les noeuds malveillants. Par conséquent, la valeur de E2ED sera inférieure à la somme des paquets reçus. Cette meilleure performance de BH_AOMDV en terme de AE2ED est justifiée par :

— Premièrement la grande valeur du PDF de BH_AOMDV dans le cas des 10 noeuds communicants avec pause time 600 - 900 par rapport aux autres cas.

— Deuxièmement, la petite valeur du NRL de BH_AOMDV dans le même intervalle de temps (pause time : 600 - 900) avec les 10 noeuds communicants par rapport aux autres cas.

Notre solution CRAOMDV a une valeur de l'AE2ED élevée par rapport au protocole AOMDV normal avec MC10 et MC20 (10 et 20 sources), Cela peut être expliqué par le temps supplémentaire nécessaire au noeud source pour la vérification et la validation du chemin vers la destination. Cependant, CRAOMDV a un meilleur délai que AOMDV

lorsque le nombre de nœuds est élevé (30 et 40 sources) et que la mobilité est plus grande. Ce qui prouve l'efficacité de notre solution, le temps moyen nécéssaire pour la transmission des paquets de données avec succès est faible malgré la présence des noeuds blackhole et une énorme mobilité.

AE2ED 10 nœuds communicants :

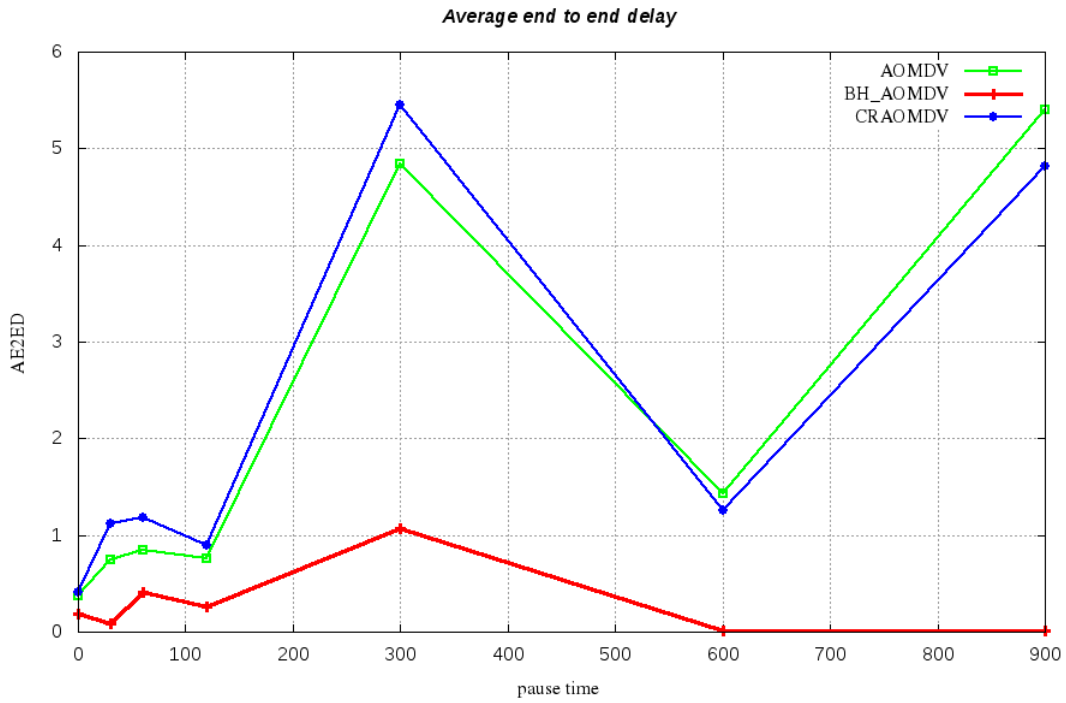


FIGURE 3.9 – *AE2ED des 10 nœuds communicants en fonction du temps de pause (S)*

AE2ED 20 nœuds communicants :

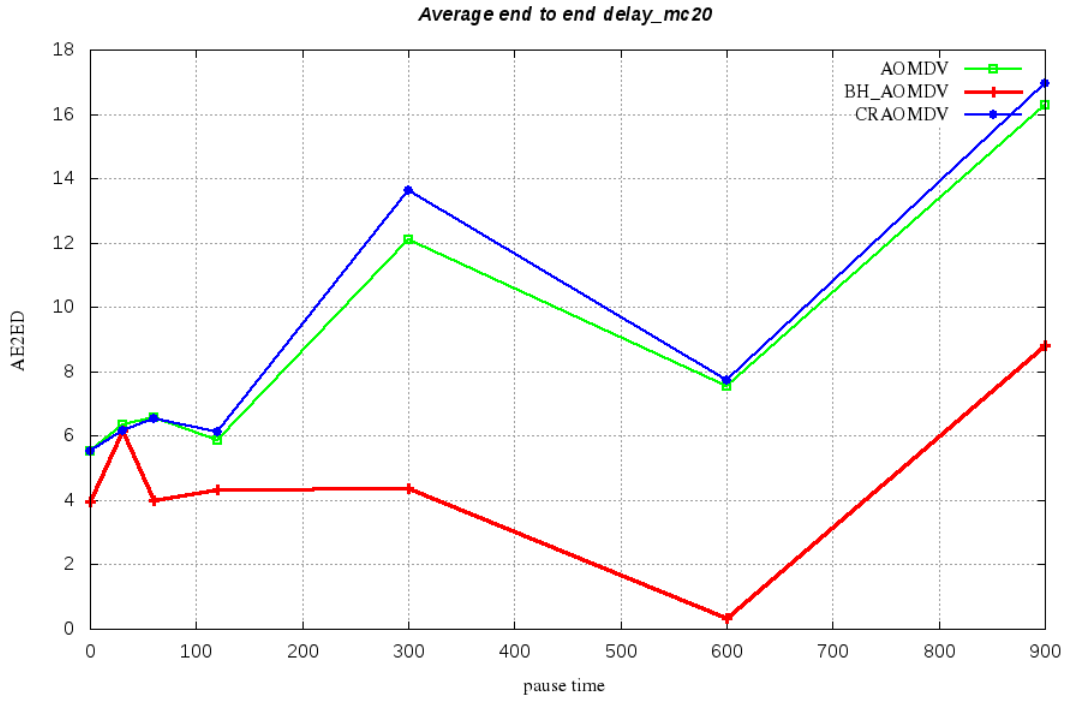


FIGURE 3.10 – *AE2ED des 20 nœuds communicants en fonction du temps de pause (S)*

AE2ED 30 nœuds communicants :

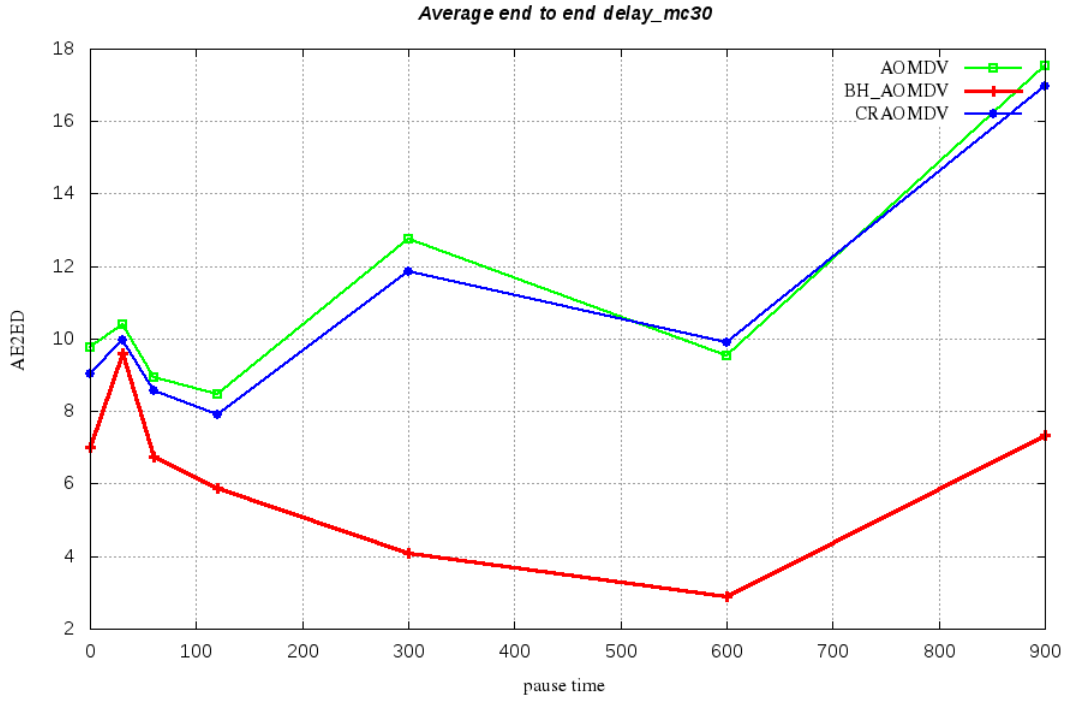


FIGURE 3.11 – *AE2ED des 30 nœuds communicants en fonction du temps de pause (S)*

AE2ED 40 nœuds communicants :

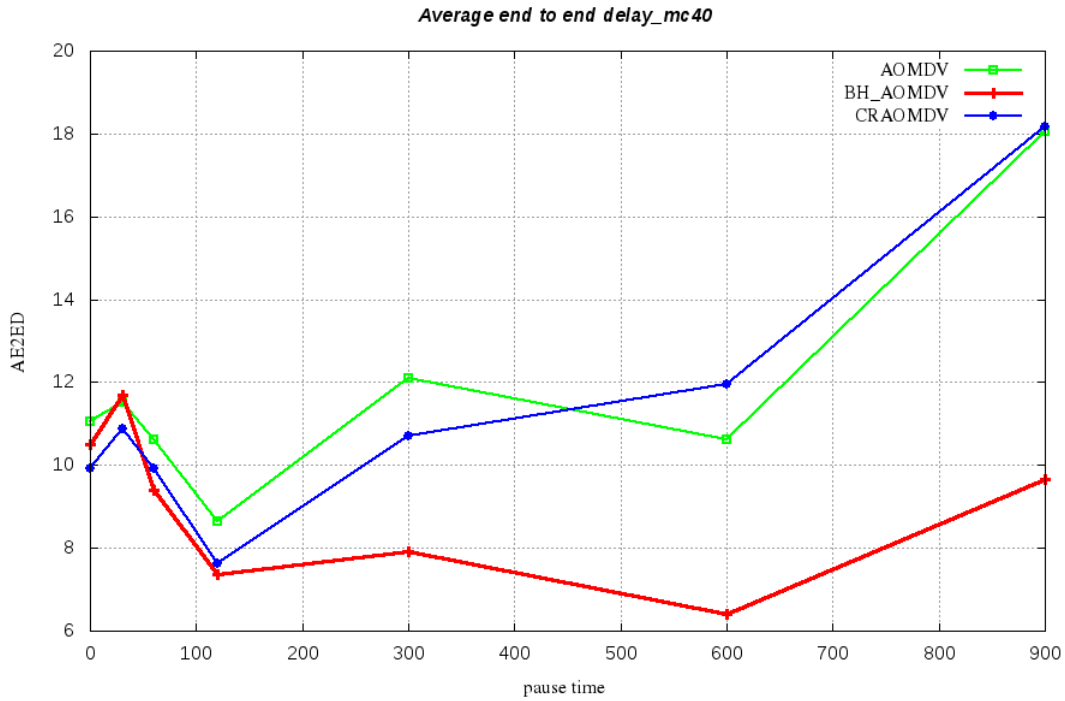


FIGURE 3.12 – *AE2ED des 40 nœuds communicants en fonction du temps de pause (S)*

Le graphe de charge de routage normalisé (NRL)

Pour la métrique NRL, les figures (3.13,3.14, 3.15, 3.16) illustrent que la valeur de NRL est plus élevée lorsque la mobilité des noeuds est plus importante (60s, 300s), en raison du changement imprévisible de la topologie. Ce changement fréquent de topologie amplifie le nombre de paquets de contrôle. Dans AOMDV en cas d'attaque par trou noir (BH_AOMDV), la somme des paquets livrés à la destination est inférieure à la somme des paquets de routage, ce qui amplifie la valeur du NRL par rapport à l'AOMDV normal et CRAOMDV.

D'après ces résultats, il est clair que notre solution CRAOMDV est plus efficace que la solution AOMDV en cas d'attaque par trou noir en raison du nombre plus élevé de paquets de contrôle dans BH_AOMDV.

La valeur de NRL dans CRAOMDV est un peu élevée par rapport à AOMDV normal. Cela peut s'expliquer par les paquets de routage envoyés par le noeud source pour trouver un nouveau chemin vers la destination après avoir supprimé tous les chemins passant par le noeud malveillant.

NRL 10 nœuds communicants :

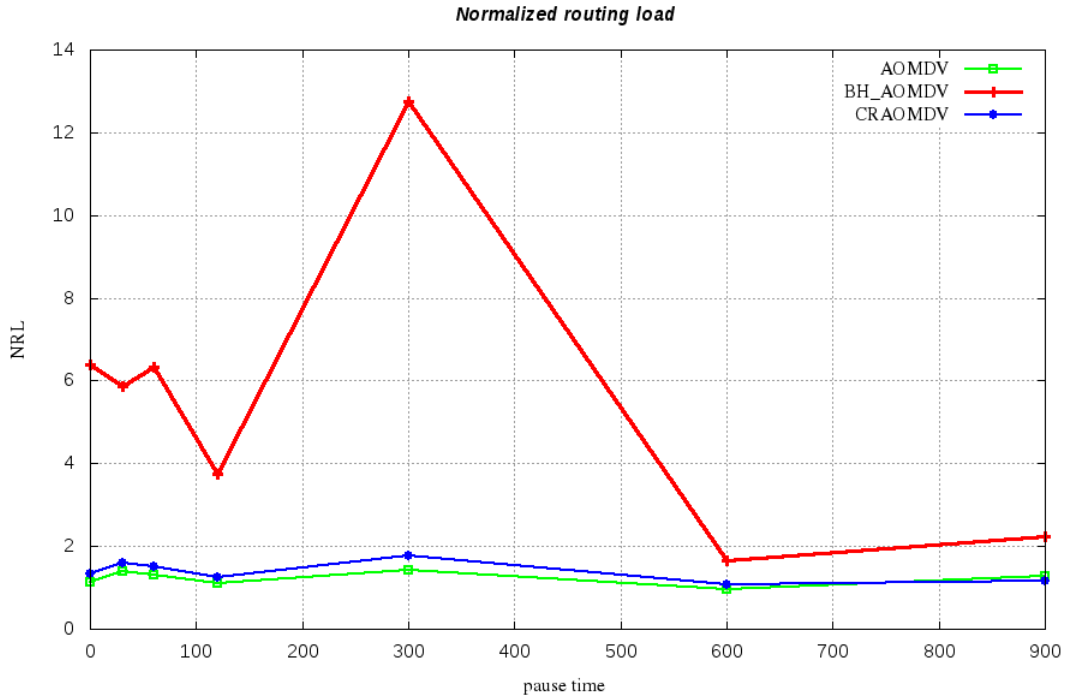


FIGURE 3.13 – *NRL des 10 nœuds communicants en fonction du temps de pause (S)*

NRL 20 nœuds communicants :

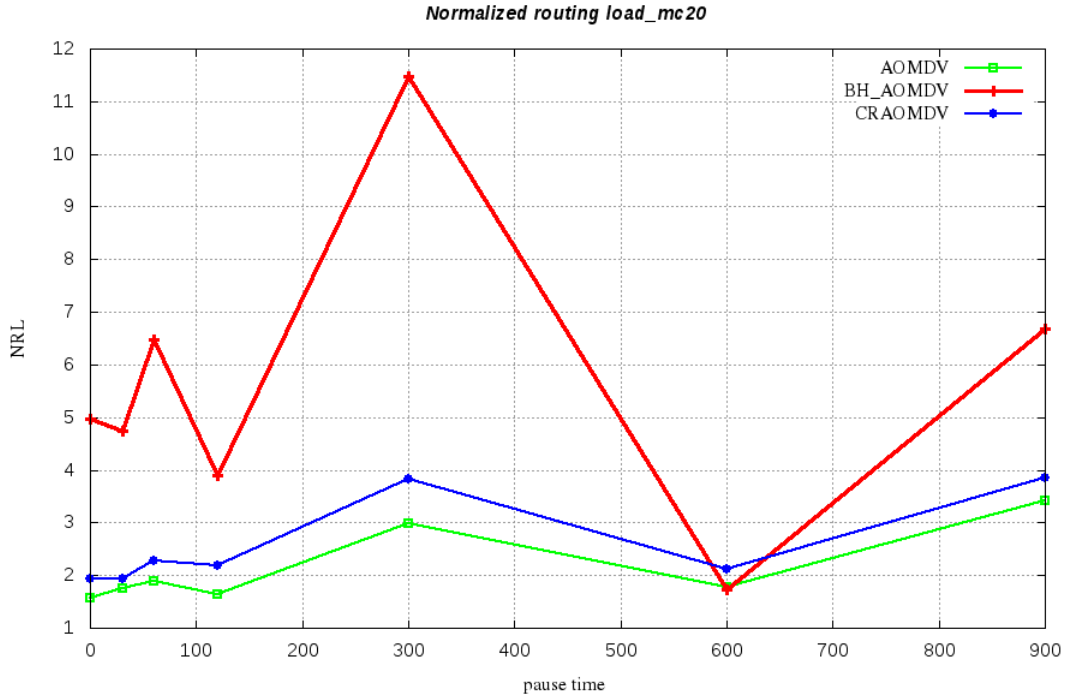


FIGURE 3.14 – *NRL des 20 nœuds communicants en fonction du temps de pause (S)*

NRL 30 nœuds communicants :

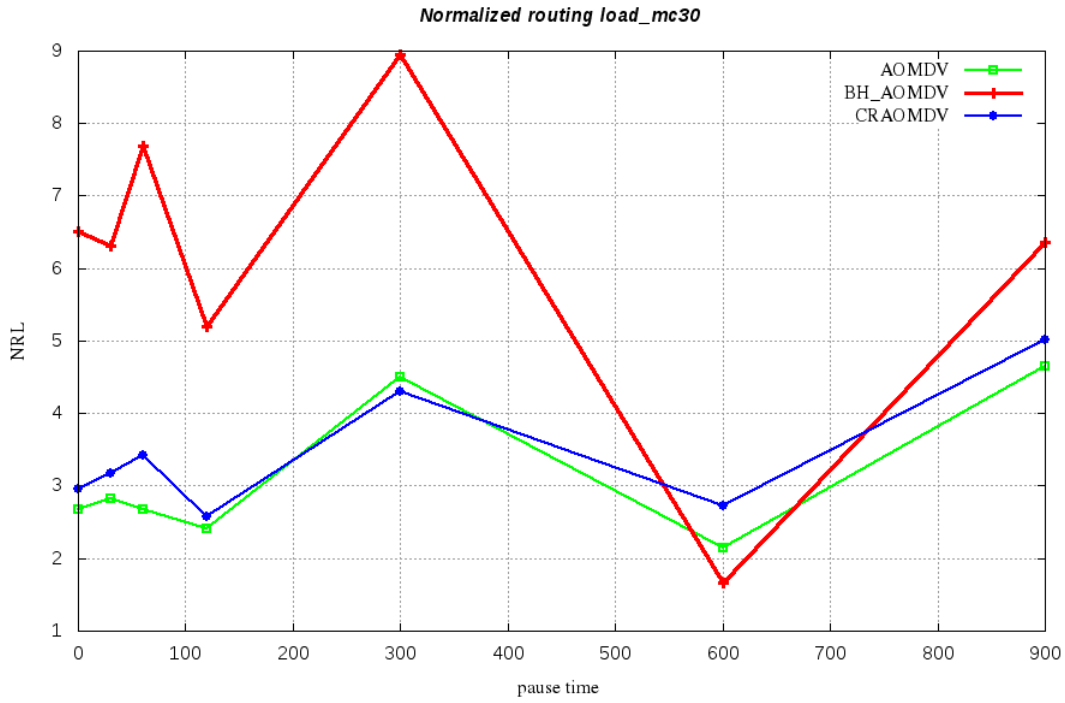


FIGURE 3.15 – *NRL des 30 nœuds communicants en fonction du temps de pause (S)*

NRL 40 nœuds communicants :

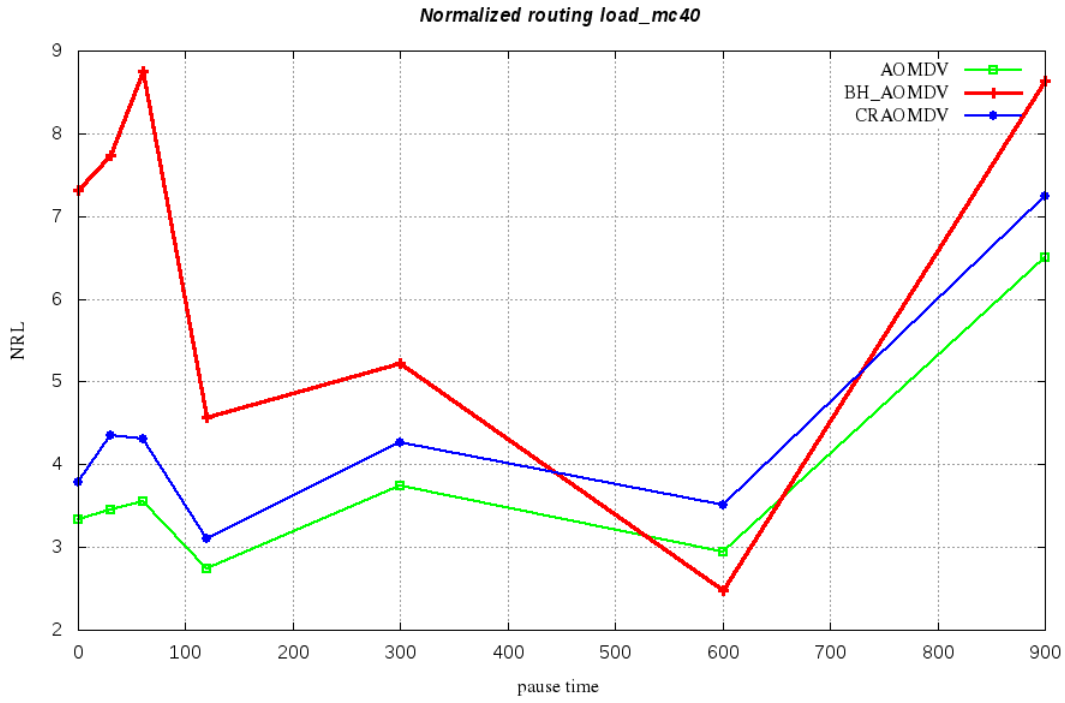


FIGURE 3.16 – *NRL des 40 nœuds communicants en fonction du temps de pause (S)*

Conclusion

Dans ce chapitre, nous avons présenté les problèmes de sécurité dans les MANETs notamment la vulnérabilité des protocoles de routage aux attaques par trou noir. Nous avons également analysé l'impact de cette attaque sur le protocole de routage AOMDV et aussi exposé certaines solutions proposées contre ce type d'attaque. De même, nous avons développé une nouvelle approche inter-couches pour identifier et ignorer les noeuds malveillants et ainsi trouver un chemin de confiance vers la destination.

Notre solution a été simulée à l'aide du NS2 et comparée à l'AOMDV normal et à l'AOMDV dans le cadre d'une attaque par trou noir.

Les performances de la simulation démontrent que notre solution CRAOMDV est presque aussi performante que l'AOMDV normal et beaucoup meilleure qu'AOMDV sous l'attaque BLACK-HOLE ceci en améliorant le PDF et en réduisant à la fois la latence de découverte de route et l'overhead de routage. Par conséquent, cela prouve l'efficacité de notre solution inter-couches.

Dans la continuité de notre travail, nous allons proposer un mécanisme de sécurité inter-couche efficace dans les réseaux véhiculaires pour éliminer l'impact de l'attaque blackhole dans le protocole de routage AOMDV.

Contribution II : Une méthode inter-couche pour identifier et isoler les noeuds blackhole dans les réseaux adhoc véhiculaires.

4

Sommaire

4.1 Etat de l'art 60
4.2 Modèle de l'attaque blackhole contre le protocole AOMDV 63
4.3 Motivation et solution proposée 64
4.3.1 Contributions et motivations 64
4.3.2 La solution proposée 65
4.4 Evaluation de la performance 73
4.4.1 L'environnement de simulation 73
4.4.2 Mesures des performances de la simulation 76
4.4.3 Discussions et comparaisons des résultats de simulation 77
Conclusion 81

Le manque d'infrastructures et les changements imprévisibles de la topologie dus à la vitesse élevée des véhicules intelligents, en particulier sur l'autoroute, soulèvent une diversité de défis et de problèmes dans la sécurité des réseaux ad-hoc véhiculaires. Les communications V2V dans les VANET sont basées sur des protocoles de routage afin d'une part, de trouver le meilleur chemin de la source à la destination prévue et pour acheminer les informations dans l'ensemble du réseau. Le vecteur de distance multivoies à la demande (AOMDV) est l'un des protocoles de routage multivoies le plus utilisé dans les réseaux VANET. Comme nous l'avons mentionné précédemment, les réseaux VANET sont basés sur des protocoles de routage. Le véhicule se comporte comme un routeur dans le réseau pour participer au processus de routage ; par conséquent, cette caractéristique rend l'AOMDV vulnérable à plusieurs attaques, telle que blackhole. Dans cette dernière, les voisins du noeud malveillant considèrent qu'il a le chemin le plus court vers le noeud de destination en recevant un faux paquet RREP. En conséquence, les paquets de données seront détournés et supprimés par ce noeud malveillant au lieu d'être transmis aux noeuds intermédiaires ou de destination.

Dans ce chapitre nous exposons une simulation de l'attaque blackhole dans AOMDV avec notre solution propsée en utilisant le simulateur NS2 et le générateur des scénarios de mobilité SUMO. Le but principal de notre nouvelle solution c'est la détection et l'ignorance de tout comportement malicieux dans le réseau.

4.1 Etat de l'art

Cette section présente les différentes solutions proposées par plusieurs chercheurs dans le domaine des VANETs et des MANETs. Ces solutions reposent sur le mécanisme de détection et d'isolation qui peut soit utiliser une méthode basée sur la cryptographie, soit améliorer le processus de découverte de route.

Tamilselvan and Sankaranarayanan (Tamilselvan & Sankaranarayanan 2007) proposent une technique qui améliore le protocole de routage AODV pour éviter l'attaque par trou noir "black-hole" en calculant un chemin sécurisé vers la destination. Dans cette solution, le noeud source définit une valeur de temporisateur "timer" pour collecter les paquets RREP entrants. Ensuite, il stocke l'identité de l'auteur du paquet RREP, le noeud de saut suivant "next hop" vers la destination et l'heure de réception dans une table CRRT (Collect Route Reply Table) jusqu'à l'expiration de la temporisation "timer". En outre, le noeud source vérifie les chemins dans CRRT et transmet les paquets de données par le chemin qui contient le next hop (noeud de "saut suivant") répété vers la destination. Sinon, il choisit un chemin au hasard dans CRRT pour transmettre les paquets de données. Par conséquent, la probabilité que le chemin malveillant soit sélectionné est réduite.
Bien que cette méthode perfectionne AODV contre les noeuds malicieux, elle risque de tomber sur un noeud malicieux lors de ses choix aléatoires en cas d'absence de noeud de saut suivant répétés. Elle provoque également l'augmentation du délai et la surcharge de routage en raison du processus de collecte de plusieurs paquets RREP jusqu'à l'expiration de la minuterie.

Un système d'apprentissage dynamique connu sous le nom de DPRAODV (Detection, Prevention and Reactive AODV) a été proposé (Raj & Swadas 2009) pour sécuriser le protocole de routage AODV contre les attaques par trou noir. Ce système utilise une valeur du "seuil" qui est dynamiquement mise à jour dans chaque intervalle de temps comme présenté dans (Kurosawa *et al.* 2007). Le noeud source doit d'abord comparer le numéro de séquence du RREP entrant avec la valeur du seuil pour décider si ce noeud est un noeud de confiance ou non. Si le numéro de séquence du RREP reçu est supérieur à la valeur du seuil, le noeud est considéré comme un noeud blackhole, et son identité est stockée dans la liste noire du noeud source. De plus, un message "ALARM" est envoyé à ses noeuds voisins pour révéler l'identité du noeud malveillant et l'isoler. Tous les paquets RREP entrants provenant du noeud blackhole seront bloqués, et les paquets de données seront transmis par un chemin sécurisé.
Selon les résultats obtenus dans cette solution, DPRAODV améliore le taux de livraison des paquets. Cependant, elle peut augmenter le délai moyen de bout en bout et de l'overhead de routage en raison de la mise à jour de la valeur du seuil dans chaque intervalle de temps et à la transmission du paquet de contrôle supplémentaire ALARM.

Mistry et al. (Mistry *et al.* 2010) améliorent la sécurité du protocole de routage AODV contre les attaques par trou noir. Ici, le noeud source exige une fonction supplémentaire Pre_ReceiveReply (paquet P), dans laquelle il accepte tous les messages de contrôle RREP entrants au lieu du premier RREP frais seulement. Tous les paquets RREP collectés sont stockés dans la table Cmg_RREP_Tab jusqu'à l'expiration du temporisateur MOS_WAIT_TIME. Le noeud source extrait de la table Cmg_RREP_Tab le RREP avec un numéro de séquence plus élevé pour identifier le noeud malveillant et maintient l'identité de ce noeud comme Mali_node, rejetant ainsi tout RREP provenant

du noeud trou noir. Enfin, le noeud source sélectionne le RREP ayant le numéro de séquence de destination le plus élevé dans la table Cmg_RREP_Tab et poursuit le processus normal d'AODV ; de ce fait, la table Cmg_RRE_Tab sera vidée.
Ce schéma améliore le taux de livraison des paquets et n'utilise pas de paquet de contrôle supplémentaire. Néanmoins, il provoque la surcharge de routage et prolonge le délai moyen de bout en bout en raison de l'attente et de l'acceptation de tous les messages de contrôle RREP entrants au lieu seulement du premier RREP frais.

Huang et al. (Huang *et al.* 2011) ont adopté une méthode de sécurisation des messages (T-AOMDV) pour sécuriser le protocole de routage AOMDV contre l'attaque blackhole. Cette approche utilise un routage AOMDV multivoie basé sur la confiance combinée à un chiffrement doux "soft encryption". Le processus du schéma de sécurisation des messages est composé de quatre étapes. Dans la première, le noeud source calcule les chemins appropriés en utilisant la méthode du degré de secret des données "data degree of secrecy method" (Lou *et al.* 2004) pour transférer les paquets. Dans la seconde, le message est segmenté en trois parties, qui sont impliquées dans le cryptage du message entier pour réaliser une technique de cryptage doux. Dans la troisième, les trois morceaux chiffrés sont transférés de manière sécurisée en utilisant différents chemins multiples basés sur la confiance. Enfin, dans la dernière, le noeud de destination décrypte les trois parties codées pour récupérer le texte en clair.
Il est clair que ce type de méthode assure une sécurité efficace contre les attaques blackhole. Par contre elle peut échouer dans une attaque interne et augmente également les frais généraux de routage et les coûts de calcul en raison de leur grand nombre.

Rani and Kumar (Rani & Kumar 2013) quant à eux, ils ont suggéré une approche qui améliore le protocole de routage AOMDV pour éviter les attaques blackhole et minimiser l'overhead de routage. Cette amélioration consiste à ajouter plusieurs champs supplémentaires dans tous les paquets de contrôle (RREQ, RREP et HELLO) et à utiliser un paquet supplémentaire de changement de route. Dans cette solution proposée, chaque noeud maintient une table de légitimité afin de déterminer si le noeud est un noeud de confiance. En outre, la confiance à un noeud pour exécuter une fonction correcte est plus faible lorsque la valeur de légitimité est basse. Ainsi, ce noeud sera considéré comme un noeud malveillant.
Cette approche diminue la surcharge de routage dans le cas d'un réseau statique. Toutefois, la transmission des paquets de changement de route supplémentaires implique une augmentation du délai moyen de bout en bout et de la surcharge de routage.

Une nouvelle méthode de détection de black-hole dans les VANET est présentée dans (Almutairi *et al.* 2014) en utilisant le protocole de routage géographique gourmand " Greedy Geographic Routing Protocol". Chaque véhicule maintient une table de routage de confiance (TRT), qui stocke tous les voisins de confiance. Le processus de choix du prochain voisin de confiance vers la destination est déclenché et répété par le noeud source jusqu'à ce qu'il reçoive un accusé de réception de la destination. Par conséquent, les paquets de données sont transmis par un chemin sécurisé.
Ce type de solution détecte et ignore idéalement les noeuds de type " Blackhole " dans un réseau à faible mobilité. Cependant, et là, est le problème : il augmente la surcharge de routage due au processus de transmission du paquet d'accusé de réception supplémentaire.

(Pandikumar *et al.* 2017) appliquent une technique mesurable pour atténuer l'attacque

black-hole dans les MANETs avec le protocole AOMDV. Dans le processus de découverte de route, la chose qui distingue très clairement le comportement du noeud malveillant d'un noeud légitime est l'envoi de RREP immédiatement avec le numéro de séquence le plus élevé, qui est 2^{32}. Le rôle du noeud source dans cette technique est de vérifier si le numéro de séquence dans la table de routage est supérieur ou inférieur au numéro de séquence du RREP entrant. Par conséquent. A la réception de chaque paquet RREP le noeud source procède comme suit :

— Si le nouveau RREP est supérieur au numéro de séquence maximal, le nœud émetteur rejette le nouveau RREP.

— Si le numéro de séquence du RREP est inférieur au numéro de séquence maximal, il vérifie d'abord la table de routage. cette table est actualisée si elle est vide.

— Si le numéro de séquence du nouveau RREP est supérieur ou égale au numéro de séquence maximal et possède un nombre de sauts qui est inférieur au nombre de sauts minimal dans la table de routage, il effectue une mise à jour de la table de routage avec la nouvelle route.

Cependant dans ce schéma la détection des noeuds blackhole réside seulement au niveau du noeud source. Les autres du réseau n'ont aucune information sur l'identité des noeuds malveillants.

Un schéma fiable est proposé (Dhyani *et al.* 2017) pour améliorer la sécurité du protocole de routage AOMDV contre les attaques blackhole dans les VANET. Cette solution vise à trouver un chemin sécurisé entre une source et sa destination. Dans la méthode proposée, à la réception du paquet RREP, le noeud source sélectionne deux noeud avec le premier et le deuxième numéro de séquence de destination le plus élevé. De plus, pour détecter le noeud blackhole, la valeur du "seuil" (Th) (Chauhan *et al.* 2015) est calculée et comparée à la "valeur de confiance" (TV), qui est la différence entre le nombre de paquets transmis et ceux abandonnés par le noeud. Par conséquent, si la TV est inférieure à Th, ce noeud est déclaré comme noeud blackhole par le noeud source. Ses informations sont stockées dans la table de la liste noire, et son identité est révélée à tous les noeud du réseau en utilisant un paquet ALARM. Ensuite, la source envoie un paquet de données au second noeud. A défaut, elle l'envoie au premier noeud, qui est un noeud légitime.
Cette amélioration de la sécurité du protocole AOMDV détecte et ignore les noeuds de type " Blackhole " mais en même temps, elle augmente le délai moyen de bout en bout en raison de la période de temps pendant laquelle le noeud malveillant est notifié à tous les autres noeuds à l'aide du paquet flare.

Une technique de chiffrement à clé publique connue sous le nom de cryptographie à courbe elliptique "Elliptic Curve Cryptography" (ECC) est présentée dans (Sultana & Ahmed 2018) pour sécuriser les paquets contre les attaques par trou noir dans AOMDV avec une taille de clé plus petite. L'approche proposée se compose de quatre étapes. D'une part, le noeud source utilise AOMDV pour calculer plusieurs chemins sans boucle et sans lien vers la destination. D'autre part, une paire de clés publique et privée est générée. Ensuite, le noeud source crypte les paquets de données en utilisant la clé secrète de cryptage ECC. Enfin, le texte crypté est déchiffré par la destination pour récupérer le paquet de données original. Ainsi, même avec la présence du noeud trou noir, le paquet de données est transmis en toute sécurité puisque ce noeud malveillant ne sera pas en mesure de révéler le texte en clair sans les clés secrètes partagées.
La technique proposée dans ce travail donne une meilleure détection du noeud malveillant externe. Quoiqu'elle ne convient pas en cas d'attaques internes en raison des

clés partagées. Elle augmente également la surcharge de routage, la communication et le coût de calcul.

Une nouvelle solution est présenté par (Delkesh & Jabraeil Jamali 2019) pour identifier les noeud malveillants et maintenir un chemin court et sécurisé de la source vers le noeud de destination en envoyant de faux paquets de routage. Dans le processus de découverte de route, le noeud source envoie un faux RREQ, qui inclut l'adresse de la destination irréelle. Après avoir reçu ce faux RREQ, le noeud malveillant répond pratiquement directement avec un faux RREP. Suite à cet état de faits, le noeud source peut détecter les noeud malveillants, qui sont tous des noeuds qui répondent par un faux RREP. Donc, la source enregistre leur identité à la liste des trous noirs et alerte les autres noeuds pour les isoler.
Cette solution améliore les données délivrées par rapport à l'algorithme du système de détection d'intrusion (IDS). Par contre, elle augmente l'overhead de routage et le délai de bout en bout en raison de la transmission des paquets de contrôle RREQ falsifiés.

Une nouvelle méthode basée sur la carte de contrôle variable est proposée (Cherkaoui *et al.* 2020) pour identifier le noeud malveillant dans les VANETs. Dans cette méthode, un système de surveillance est déployé dans chaque noeud récepteur du réseau pour surveiller le débit et le délai de bout en bout. Chaque noeud utilise une carte de contrôle pour observer et surveiller les deux métriques. Enfin, on suppose que le réseau sera attaqué si de fortes déviations sont présentes.
Ce contrôle peut détecter les mauvais comportements dans le réseau. Cependant, une forte déviation n'est pas forcement un signe exact d'une présence d'une attaque. Il détecte également la présence d'un noeud malveillant sans pour autant connaître son identité.

Kumar et al. (Kumar *et al.* 2021) ont proposé une nouvelle méthode pour détecter et supprimer les noeuds blackhole dans les VANETs. Cette solution est une version améliorée du protocole de routage standard AODV. De plus, des fonctions de cryptage et de décryptage sont incluses pour vérifier les noeuds source et destination. Le processus de la méthode proposée peut être classé en trois étapes. La première étape vise à connaître l'état des voisins en transmettant un message. Dans la deuxième étape, un paquet crypté est généré et le message est transmis à tous ses voisins connus en utilisant la clé secrète. Dans la troisième, la clé secrète est transmise aux noeuds connus, et dans la dernière, les types de paquets RREQ et RREP sont vérifiés et le paquet est transmis. La solution évoquée ci-dessus détecte et supprime avec succès les noeuds blackhole. De plus le pourcentage des paquets perdus est bien meilleur à celui du protocole de routage AODV existant. Néanmoins, elle ne convient pas en cas d'attaques internes en raison des clés partagées. Elle augmente également la surcharge de routage, la communication et le coût de calcul.

4.2 Modèle de l'attaque blackhole contre le protocole AOMDV

Une attaque par trou noir est un type d'attaque par déni de service, où le noeud malveillant exploite le concept d'avoir la route la plus récente vers une destination spécifique en termes de numéro de séquence plus élevé. Et cela en répondant immédiatement au RREQ avec un RREP corrompu contenant un numéro de séquence plus élevé dans le processus de découverte de route. Le noeud source supposera que ce noeud blackhole possède la route la plus récente vers la destination, et qu'il n'est pas nécessaire

d'accepter les RREP des autres. Ainsi, la source enverra tous les paquets de données à ce noeud malveillant, qui les supprimera au lieu de les relayer (Naib *et al.* 2021).

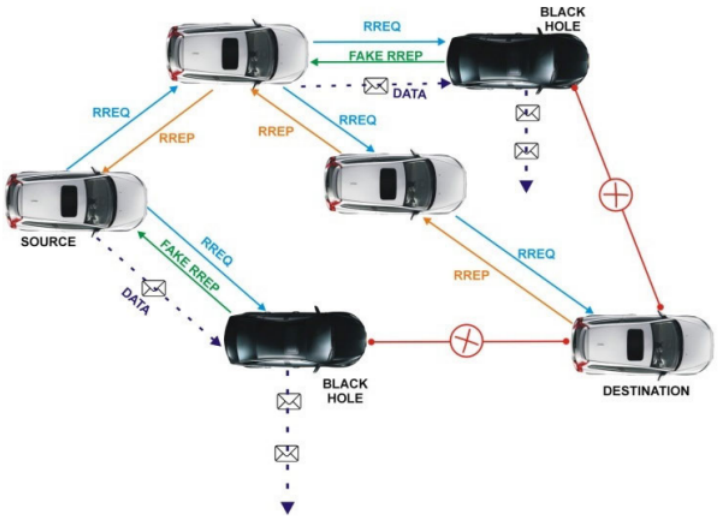


FIGURE 4.1 – *L'attaque Blackhole (Hassan et al. 2020)*

Dans la figure 4.1, le noeud source "SOURCE" veut envoyer des paquets de données au noeud "DESTINATION". Pour ce faire, "SOURCE" diffuse RREQ aux noeuds voisins. Le noeud blackhole "Blackhole" répond directement avec un paquet FAKE RREP avec un numéro de séquence plus élevé. Ce faisant, "Blackhole" oblige la source "SOURCE" à le sélectionner comme prochain saut vers la destination pour la transmission des paquets de données. Le noeud malveillant "Blackhole" supprime à son tour tous les paquets de données reçus.

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

4.3 Motivation et solution proposée

Dans cette section, les contributions et les motivations de cette recherche seront présentées et suivies d'une nouvelle approche CRAOMDV à couches croisées pour sécuriser les VANET contre les attaques par trou noir.

4.3.1 Contributions et motivations

Les principales contributions de cette recherche peuvent être divisées en trois parties importantes. Dans la première, nous mettons en œuvre et simulons l'attaque blackhole dans un réseau adhoc véhiculaire pour démontrer le niveau de dégradation des performances du réseau et les principaux problèmes de sécurité qui rendent la communication indisponible en raison de cette attaque. Dans la deuxième partie, nous visons à sécuriser le VANET contre les attaques blackhole en identifiant et en ignorant tout noeud malveillant qui pourrait supprimer ou détourner des informations sensibles. Bien qu'à tout moment, les véhicules échangent de nombreux messages comprenant des informations sensibles, telles que des informations d'urgence et de congestion. La principale raison d'isoler les véhicules malveillants est de surmonter le problème de disponibilité dans les VANET, car les paquets de données sont abandonnés par ces

noeuds et, tout Ça pour éviter les accidents, améliorer la sécurité routière et réduire le taux de mortalité.

Plusieurs études ont proposé des solutions pour traiter ce type d'attaque. Contrairement à notre méthode, les solutions proposées sécurisent les VANETs contre les attaques blackhole sans se concentrer sur la contrainte de temps limite importante pour la prise de décision dans les VANETs. Par conséquent, ces solutions ne peuvent pas être adaptées à des scénarios VANET réels. Dans la troisième partie, notre objectif est de sécuriser le VANET contre l'attaque blackhole dans une période opportune, en faisant cela nous respectons la contrainte de temps limite pour la prise de décision et rendons notre méthode efficace et adaptée dans un scénario VANET réel.

4.3.2 La solution proposée

Dans cette sous-section nous présentons un nouveau schéma inter-couche "cross-layer" pour protéger les VANET contre les attaques par trou noir en utilisant le protocole de routage multichemin AOMDV. Notre solution inter-couches utilise l'interaction entre la couche MAC et la couche réseau pour trouver un chemin sécurisé vers la destination en identifiant et en isolant les noeuds malveillants. Chaque noeud maintient une "liste de trous noirs" (liste BHN) qui stocke toutes les informations sur les noeuds malveillants, et une vérification supplémentaire inter-couches est déclenchée avant d'accepter tout paquet RREP entrant. Le noeud source diffuse un paquet RREQ aux noeuds voisins pendant le processus de découverte de route afin de trouver une nouvelle route vers une destination spécifique. La réponse avec un paquet RREP émanera soit du noeud intermédiaire avec une nouvelle route vers la destination (IN) soit la destination elle même. Cette procédure d'envoi de RREP se compose de deux étapes. Dans la première, le noeud intermédiaire et la destination au niveau de la couche réseau préparent le paquet RREP. Dans la deuxième étape, un échange de paquets RTS / CTS est nécessaire au niveau de la couche MAC puisque RREP est un paquet unicast. Dans cette étape, la couche MAC obtient les informations sur le noeud de confiance de la couche réseau et utilise ensuite la variable XMIT_REASON pour informer la couche de routage si ce RREP reçu provient d'un noeud de confiance ou non. Ensuite, le RREP est envoyé vers le noeud source. contrairement au noeud intermédiaire et le noeud de destination, le noeud blackhole répond immédiatement par un RREP corrompu à la source contenant le numéro de séquence le plus élevé pour prétendre qu'il a une nouvelle route vers la destination.

Après la réception du RREP, le noeud source procède à un contrôle supplémentaire pour décider s'il accepte ou non le RREP entrant. Ce contrôle consiste à vérifier la valeur de XMIT_REASON. Si la valeur de XMIT_REASON est égale à X_R_IN ou à X_R_DST, qui signifie respectivement XMIT_REASON_INTERMEDIATE NODE ou XMIT_REASON DESTINATION NODE , alors le RREP est accepté et les paquets de données seront envoyés par ce noeud de confiance. Sinon, ce RREP est considéré comme un faux RREP provenant d'un noeud malveillant. Par conséquent, la source procède comme suit :

- Identifie le noeud malveillant.
- Ajoute le noeud trou noir "BHN" à la liste des trous noirs.
- Supprime les chemins qui transitent par le BHN.
- Choisit un autre chemin parmi les multiples chemins calculés.
- Supprime le paquet RREP falsifié.

Les algorithmes suivants (Algorithme 1, Algorithme 2, Algorithme 3) détaillent le comportement du noeud malveillant, du noeud source et du noeud de confiance (noeud

de destination ou noeud intermédiaire avec une nouvelle route).

Algorithme 5 : Algorithme du noeud source

```
CRAOMDV.cc
Index    the address of this node;
S_REP    the sender of RREP packet;
Ih_daddr    the destination of the RREP packet;
BH_V    the black-hole list;
X_R_DST    Destination Xmit_Reason cross-layer value;
X_R_IN    Intermediate node Xmit_Reason cross-layer value;

.....
CRAOMDV.cc
SEND RREQ;
Receive RREP ;
 MAC-802_11.cc
recv(P) /* do nothing at the receive packet procedure concerning
 XMIT_REASON_*/;
if Ih_daddr == Index then
    /* the RREP packet is intended for me */
    if FIND(BH_V,S_REP)==TRUE then
        /* this received packet is coming from a BH node */
        Remove paths that transit through clack-hole node;
        Delete RREP;
    else
        /* Cross-Layer processus to find a secure path */
        if (XMIT_REASON_ == X_R_DST) or (XMIT_REASON_ == X_R_IN) then
            /* The received RREP is coming from trusted node */
            Go to FINISH;
        else
            /* The received RREP is coming from black-hole node */
            /* identify the sender of RREP as malicious node*/
            ADD S_REP to BH_V;
            Remove paths that transit through Black-Hole node from routing table;
            Choose a new alternative path from the routing table;
            Delete RREP;
        end
    end
end;
FINISH;
```

Algorithme 6 : Algorithme du noeud de destination ou intermédiaire possédant une route fraîche

```
MAC-802_11.cc;
Dst_Cross_V   cross-layer information about destinations;
IN_Cross_V   cross-layer information about the intermediate nodes that own the
 freshet route to the destination;
Tr    the transmitter of the packet;
Ra    the receiver of the packet;
CRAOMDV.cc
Receive RREQ ;
Prepare RREP ;
MAC-802_11.cc
recv(P) /* receive packet procedure at the mac layer */;
if packet_type==PCRAOMDV then
    /* the received packet is of type CRAOMDV*/
    if Ra!=MACBROADCAST then
        /*it's a RREP packet */
        if FIND(Dst_Cross_V,Tr) == TRUE then
            XMIT_REASON_= X_R_DST ;
        else if FIND(IN_Cross_V,Tr) == TRUE then
            XMIT_REASON_= X_R_IN ;
        else
            /*Transmitter not found in both of destination list and IN list that's
             own the fresh route*/
    end
end
CRAOMDV.cc
SEND RREP ;
FINISH;
```

Algorithme 7 : Algorithme du noeud malveillant

```
CRAOMDV.cc
Receive RREQ ;
Prepare the RREP packet ;
MAC-802_11.cc
recv(P) /* do nothing at the receive packet procedure concerning
 XMIT_REASON_*/;
XMIT_REASON_ == 0 ;
CRAOMDV.cc
SEND immediately a forged RREP with higher sequence number and
 minimumm number of jumps ;
FINISH;
```

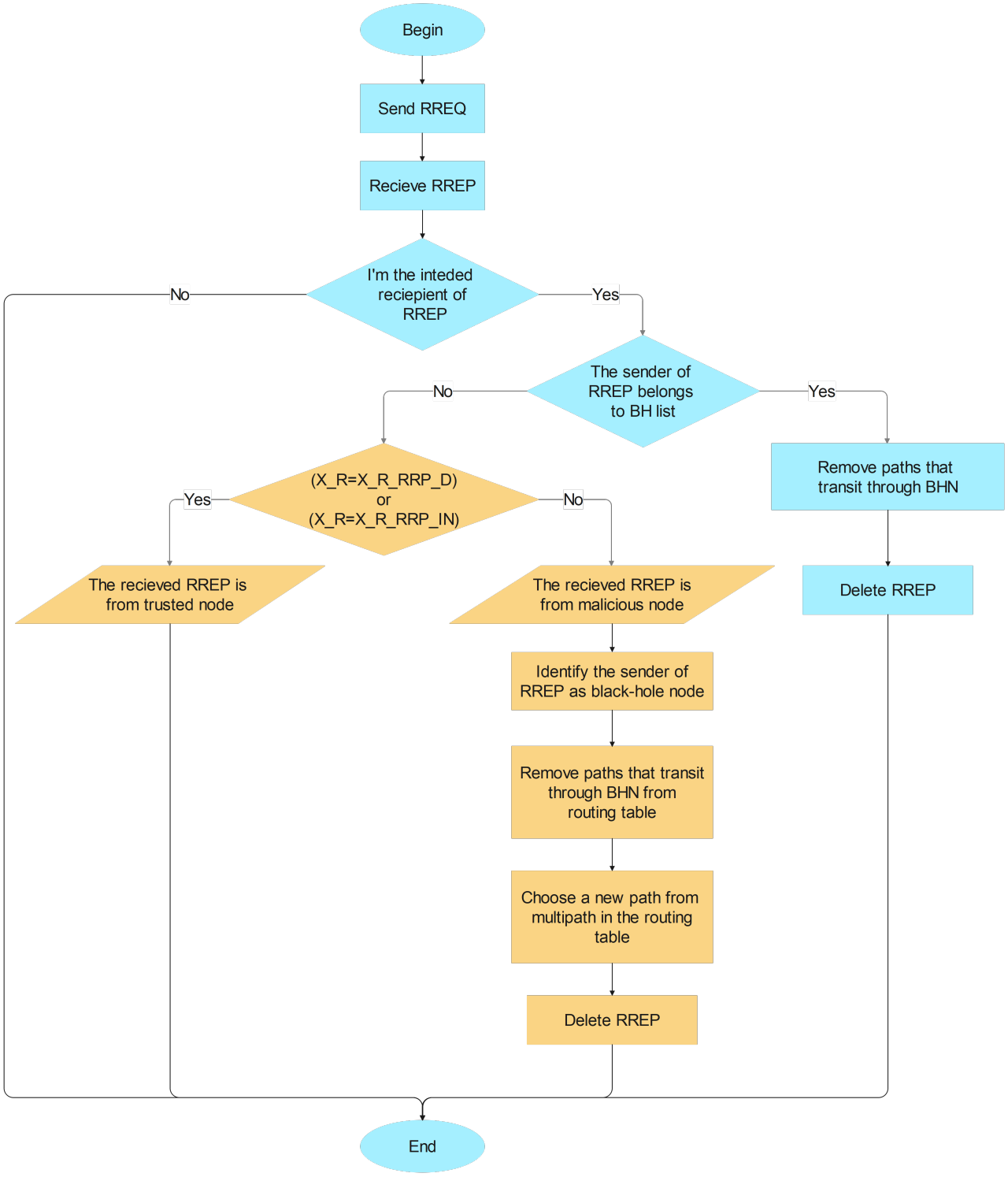


FIGURE 4.2 – *Diagramme pour le noeud source*

La figure 4.2 montre le processus de notre solution multicouche CRAOMDV dans un organigramme.

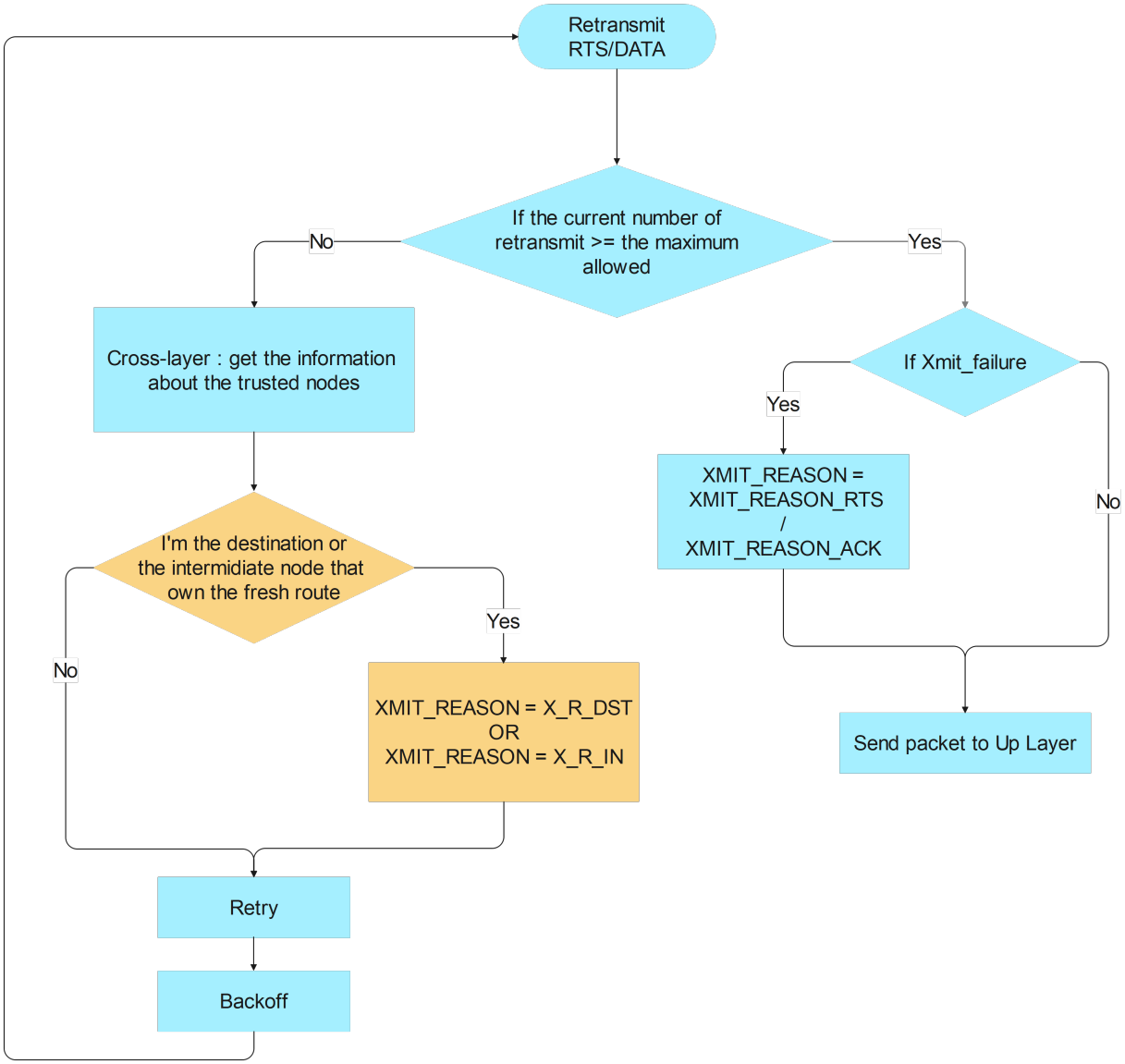


FIGURE 4.3 – *Le Diagramme inter-couche*

L'approche proposée utilise la variable X_R_ qui signifie XMIT_REASON_, illustrée ici (4.3). Ce diagramme montre également comment la couche MAC informe la couche de routage lorsque plusieurs tentatives de communication avec le noeud récepteur ont échoué.

TABLE 4.1 – *Comparaison entre notre solution et les méthodes proposées dans l'état de l'art.*

No.	Références	Protocole	Base de données	Simulateur	Avantages	Incovénients
1	(Tamilselvan & Sankaranarayanan 2007)	AODV	Simulation	NS2	Amélioration de l'AODV contre l'attaque blackhole	Augmenter le délai et la surcharge de routage
2	(Raj & Swadas 2009)	AODV	Simulation	NS2	Améliorer le taux de livraison des paquets	Augmenter le délai moyen de bout en bout et de l'overhead
3	(Mistry *et al.* 2010)	AODV	Simulation	NS2	Améliorer le taux de livraison des paquets	Augmenter la surcharge de routage et du délai moyen de bout
4	(Huang *et al.* 2011)	AOMDV	Simulation	NS2	Assurer une sécurité efficace contre les attaques par blackhole	Peut échouer dans une attaque interne
5	(Rani & Kumar 2013)	AOMDV	Simulation	NS2	Diminuer la surcharge de routage dans le cas d'un réseau statique	Augmenter le délai moyen de bout en bout et la surcharge de routage
6	(Almutairi *et al.* 2014)	GGRP	Simulation	SUMO-NS2	Détecter idéalement les noeuds malicieux dans un réseau à faible mobilité	Augmenter la surcharge de routage

Continued

Table 4.1 – *Comparaison entre notre solution et les méthodes proposées dans l'état de l'art.*

No.	Références	Protocole	Base de données	Simulateur	Avantages	Incovénients
7	(Dhyani *et al.* 2017)	AOMDV	Simulation	SUMO-NS2	Détecter et ignorer les noeuds de type" Black-hole"	Augmenter le délai moyen de bout en bout
8	(Pandikumar *et al.* 2017)	AOMDV	Simulation	NS2	Détecter et ignorer les noeuds de type"blackhole "	Detection seulement par le noeud source
9	(Sultana & Ahmed 2018)	AOMDV	Simulation	NS2	Meilleure détection du noeud malveillant externe	Il ne convient pas en cas d'attaques internes
10	(Delkesh & Jabraeil Jamali 2019)	AODV	Simulation	NS2	Améliorer les données délivrées	Augmenter l'overhead de routage et le délai de bout en bout
11	(Cherkaoui *et al.* 2020)	AODV	Simulation	SUMO-NS2	Détecter les mauvais comportements dans le réseau	Constater la présence du noeud malveillant mais pas son identité
12	(Kumar *et al.* 2021)	AODV	Simulation	SUMO-NS2	Le pourcentage des paquets perdus est bien meilleur que celui du protocole de routage AODV existant	Il ne convient pas en cas d'attaques internes et Augmente la surcharge de routage

Continued

Table 4.1 – *Comparaison entre notre solution et les méthodes proposées dans l'état de l'art.*

No.	Références	Protocole	Base de données	Simulateur	Avantages	Incovénients
13	(Naib *et al.* 2021)	AOMDV	Simulation	SUMO-NS2	Détecter efficacement les attaques externes et internes et améliorer le taux de livraison des paquets, le délai moyen de bout en bout et l'overhead de routage	

Le tableau 4.1 présentent une étude comparative entre divers schémas proposés pour fournir une communication sécurisée contre l'attaque blackhole. Ces schémas sont classés selon une méthode basée sur la cryptographie (Huang *et al.* 2011; Kumar *et al.* 2021; Sultana & Ahmed 2018) et des méthodes de modification du protocole de routage (Almutairi *et al.* 2014; Cherkaoui *et al.* 2020; Delkesh & Jabraeil Jamali 2019; Dhyani *et al.* 2017; Mistry *et al.* 2010; Pandikumar *et al.* 2017; Raj & Swadas 2009; Rani & Kumar 2013; Tamilselvan & Sankaranarayanan 2007).

Comme on peut le constater dans le tableau 4.1 , l'avantage commun des schémas proposés c'est la sécurisation du protocole de routage contre les attaques par trou noir. Cependant, l'inconvénient majeur des méthodes basées sur la cryptographie parait dans l'augmentation des coûts de calcul et de communication due à la génération et à l'échange de clés. Ces défauts rendent ce type de méthodes inadaptés à une attaque interne et à un réseau avec une grande vitesse de noeuds comme les VANETs. En outre, les méthodes de modification du protocole de routage augmentent l'overhead de routage et le délai moyen de bout en bout en raison soit de l'attente d'un **"timer"** pour collecter de nombreux paquets RREP soit de la transmission de paquets de contrôle supplémentaires, comme : **"ALARM, Accusé de réception, faux RREQ, échange de route et paquet Flar"**. Ces flux les rendent inefficaces dans les réseaux VANETs, où les noeuds se déplacent à grande vitesse et le temps de prise de décision est limité.

Les résultats de la simulation soulignent que notre solution CRAOMDV est meilleure et plus efficace contre les attaques blackhole dans les VANETs par rapport aux méthodes citées ci-dessus, et cela en améliorant le PDF et en diminuant l'overhead (NRL) et le délai moyen de bout en bout (AE2ED). En même temps, CRAOMDV n'utilise pas de paquet de contrôle supplémentaire et un coût de calcul élevé, ce qui le rend approprié pour les réseaux dynamiques comme les VANETs.

4.4 Evaluation de la performance

4.4.1 L'environnement de simulation

Afin d'évaluer les performances de notre approche, différentes expériences ont été réalisées à l'aide du simulateur de réseau NS2 (Raja Kumar *et al.* 2021). Dans nos expériences, nous avons utilisé des scénarios de mobilité basés sur des données réelles générées par SUMO (Raja Kumar *et al.* 2021). Ces scénarios réalistes se composent de trois scénarios VANETs urbains différents nommés U1, U2, et U3 (voir la figure 4.4) qui couvrent trois tailles différentes de la même zone métropolitaine de la ville de Malaga (Espagne) avec un nombre différent de véhicules en mouvement (Toutouh & Alba 2011).

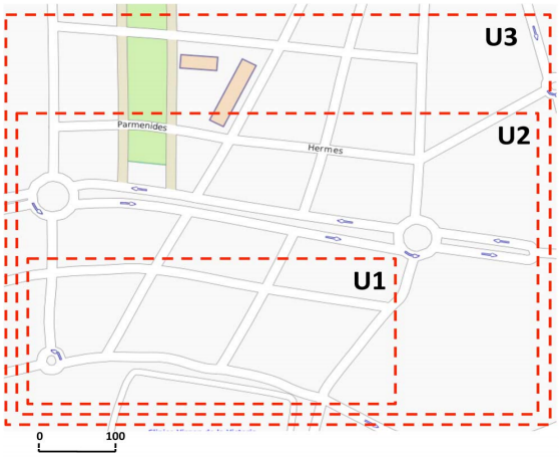


FIGURE 4.4 – *Sélection de trois différentes zones de Malaga de la topologie du réseau (Toutouh & Alba 2011)*

✓Présentation du SUMO (Simulation of Urban Mobility)

SUMO est un générateur de mobilité (Deshmukh & Dorle 2016) qui permet de simuler le trafic réel d'un réseau véhiculaire. Ce simulateur de trafic routier (Toutouh *et al.* 2012) est utilisé pour résoudre le problème des simulateurs réseaux à usage général comme NS2, qui ne permet pas de définir directement des simulations réalistes de VANETs. SUMO génére des modèles de mobilité réalistes, où les noeuds suivent : Le comportement des véhicules sur une route, les feux de signalisation, les panneaux de signalisation, etc. La génération des modèles de mobilité réalistes ce fait en sélectionnant automatiquement des zones réelles à partir de cartes numériques librement disponibles comme le montre la figure 4.5

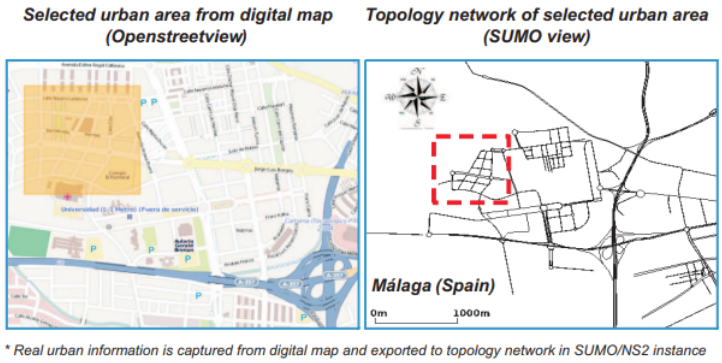


FIGURE 4.5 – *Scénario VANET urbain réel de Malaga (Toutouh et al. 2012)*

Les principales caractéristiques des scénarios VANET (U1, U2 et U3) et les paramètres de simulation sont décrits respectivement plus en détail dans les tableaux ci-dessous 4.2 4.3.

Sénarios	**La taille de la zone**	**Nombre de véhicules**	**Nombre de connexions**
U1	120 000 m^2	60	15.
U2	240 000 m^2	60	a)20. b)40.
U3	360 000 m^2	60	a) 30. b) 45. d)60.

TABLE 4.2 – *Détails des scénarios VANETs.*

paramètre	Valeur
Le modèle de propagation	Nakagami
Fréquence de la porteuse	5.89 GHz
Largeur de bande du canal	6 Mbps
PHY Layer	IEE 802.11p
MAC Layer	IEE 802.11p
La couche réseau	AOMDV - BH_AOMDV - CRAOMDV
La couche de transport	UDP
Taille des paquets CBR	1024 bytes
Débit de données CBR	1Mbps
Temps CBR	15s
Le temps de simulation	180s
Nombre des noeuds malveillants	3

TABLE 4.3 – *Paramètres de simulation*

4.4.2 Mesures des performances de la simulation

Nous avons utilisé les mesures très connues, pour évaluer les performances de l'AOMDV normal, soumis à une attaque par trou noir (BH_AOMDV) et de notre solution Cross-Layer AOMDV (CRAOMDV).

Ces métriques sont : La fraction de livraison de paquets (PDF), le délayage de bout en bout (AE2ED), la charge de routage normalisée (NRL) et BHN (Paquets supprimés par un noeud black-hole) pour voir l'impact du noeud blackhole dans la suppression des paquets. Ces mesures sont étudiées avec différents nombres de noeuds communicants.

✓PDF (Packet Delivery Fraction) :

Cette métrique représente le rapport entre tous les paquets de données livrés à leurs destinations et les paquets de données envoyés par la source dans le réseau. Un protocole de routage est performant lorsque la valeur du Packet Delivery Fraction (PDF) est plus élevée, ce qui signifie que les paquets de données ont atteint avec succès la couche d'application du noeud de destination.

$$PDF = \frac{\sum Paquets\ reçus}{\sum paquets\ envoyés} \times 100 \tag{4.1}$$

✓AE2ED (Average end-to-end delay) :

Cette métrique est définie comme le temps moyen nécessaire pour transmettre avec succès le paquet de données d'une source à sa destination.

$$AE2ED = \frac{E2ED}{\sum paquets\ reçus} \tag{4.2}$$

Avec :

E2ED= $\sum TR_{(i)} - TS_{(i)}$

$TR_{(i)}$: Moment où le paquet de données est reçu par la destination.
$TS_{(i)}$: Moment où le paquet de données est émis par la source.

✓Normalized routing load :

Il est calculé comme le rapport entre la somme des paquets de routage transmis et la somme des paquets de données reçus.

$$NRL = \frac{\sum Paquets\ de\ routage}{\sum paquets\ reçus} \tag{4.3}$$

✓Paquets supprimés par un noeud black-hole (BHN) :

Elle est calculée comme étant la somme de tous les paquets de données supprimés par les noeuds blackhole dans le réseau.

$$BHN_Drop = \sum \text{ paquets de données supprimés par les noeuds malicieux} \tag{4.4}$$

4.4.3 Discussions et comparaisons des résultats de simulation

Dans cette partie, nous avons d'abord exposé les résultats de simulation de l'AOMDV normal, de l'AOMDV sous attaque blackhole (BH_AOMDV), et de notre solution cross-layer (CRAOMDV) dans les trois scénarios (U1, U2, et U3) de la ville de Malaga, comme le montre le tableau 4.2. Ensuite, nous avons comparé l'évaluation des performances de notre solution CRAOMDV avec AOMDV normal et AOMDV sous attaque blackhole. Enfin, nous avons fait une étude comparative entre nos résultats et toutes les méthodes proposées dans les travaux connexes.

✓Les graphes du PDF :

La figure 4.6 présente une variation du taux de délivrance "PDF" pour AOMDV, BH_AOMDV et CRAOMDV par rapport à celle du nombre de véhicules communicants dans chaque scénario : U1 avec 15 véhicules communicants, U2 avec 20 et 40 véhicules communicants et U3 avec 30, 45 et 60 véhicules communicants. Malgré la présence des noeuds blackhole dans notre solution cross-layer, le PDF est presque égal à l'AOMDV normal dans la plupart des cas. Cette performance démontre l'efficacité de notre méthode à détecter, isoler les noeuds blackhole et à délivrer avec succès les paquets de données au point final.

Tandis que pour AOMDV, sous l'attaque du trou noir, le PDF généré est plus petit que pour AOMDV normal et CRAOMDV. Cette diminution du PDF est due au fait que les paquets de données étant supprimés ne parviennent pas à leur destination, par conséquent, le nombre de paquets de données reçus sera très réduit. Lorsque le nombre de véhicules augmente, les PDF dans : AOMDV, BH_AOMDV et CRAOMDV diminuent ; cela peut être expliqué par l'augmentation du nombre de connexions avec le changement rapide de la topologie du réseau. Cette situation produit une saturation des files d'attente et donc une probabilité d'augmentation de perte de paquets. Le PDF dans notre schéma cross-layer est significativement amélioré de 2% par rapport à l'AOMDV normal et considérablement amélioré de 52% par rapport à l'AOMDV sous attaque blackhole BH_AOMDV. Ce dernier a une diminution du PDF à 53.20%.

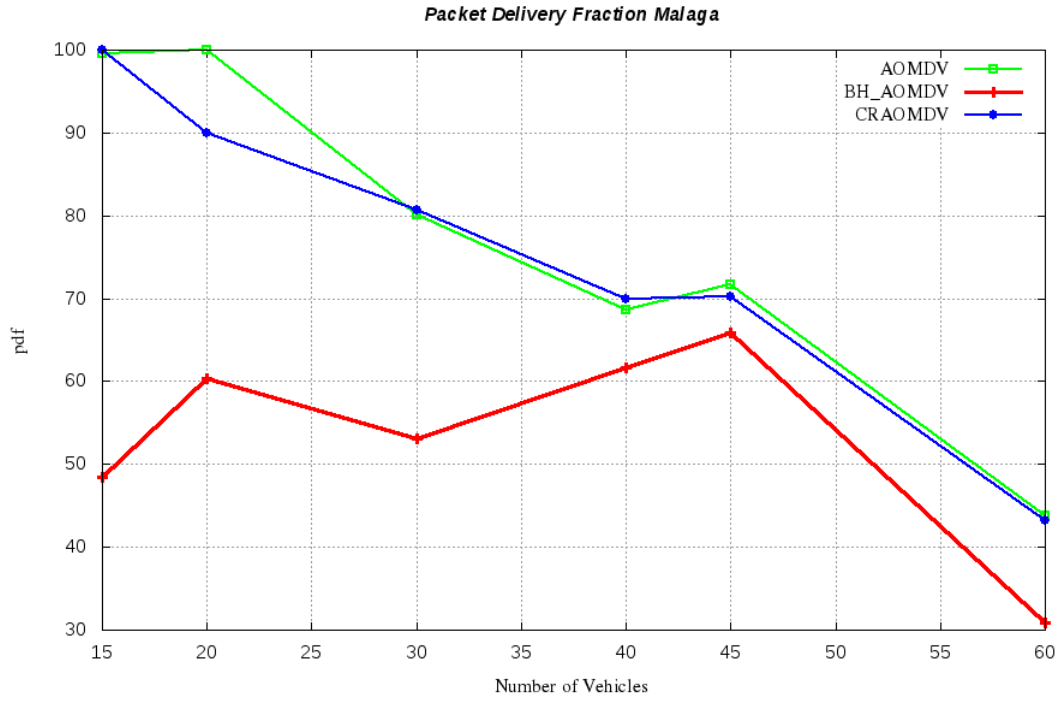


FIGURE 4.6 – *Packet Delivery Fraction*

✓Les graphes du AE2ED :

La figure 4.7 montre que l'AE2ED des protocoles de routage augmente lorsque le nombre de véhicules augmente en raison de la congestion du réseau. Le délai moyen de bout en bout est presque le même pour le protocole AOMDV standard et pour notre solution CRAOMDV, ce qui signifie que notre schéma inter-couche CRAOMDV protège le protocole AOMDV contre les attaques par trou noir avec le même délai et un délai inférieur dans les cas : 15, 40, 45 et 60 véhicules.

Ces résultats prouvent l'efficacité de notre nouvelle solution CRAOMDV cross-layer par rapport à AOMDV normal et AOMDV sous l'attaque (BH_AOMDV). Notre solution CRAOMDV diminue en moyenne l'AE2ED d'environ 23,43% par rapport à AOMDV sous attaque (BH_AOMDV). De plus, le BH_AOMDV enregistre moins de retard avec 30 véhicules communicants par rapport à l'AOMDV normal et le CRAOMDV. Ce constat s'explique par l'absence de saturation des files d'attente due à la suppression directe des paquets par les noeuds malveillants.

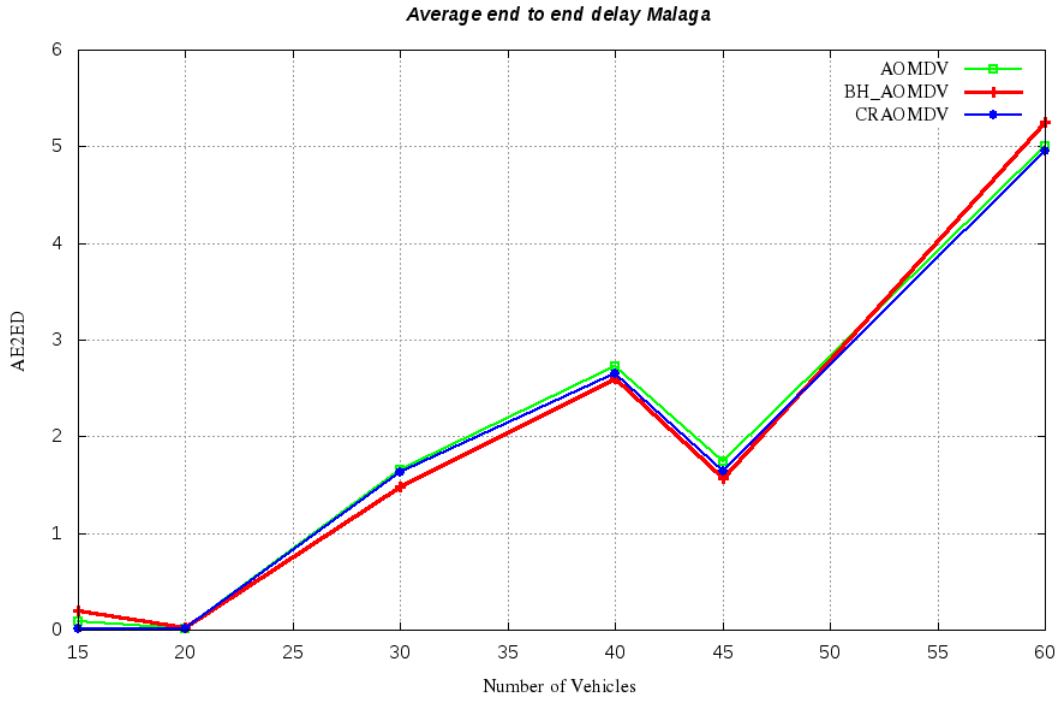


FIGURE 4.7 – *Average End-To-End Delay*

✓Les graphes du NRL :

Les résultats de simulation de la figure 4.8 montrent que le NRL des protocoles de routage est plus élevé lorsque le nombre de véhicules augmente pour les deux raisons suivantes : Le nombre élevé de paquets de routage générés par un grand nombre de connexions et le changement rapide de la topologie du réseau. Notre solution CRAOMDV diminue le NRL d'environ 51,34%, et le NRL de CRAOMDV est inférieur à celui d'AOMDV en cas d'attaque blackhole et presque égal à celui d'AOMDV normal. Comme le montre la figure 4.8, la charge de routage normalisée du CRAOMDV enregistre une augmentation avec 45 véhicules communicants ; cela peut s'expliquer par les paquets de routage générés dans le processus de découverte de route après avoir supprimé tous les chemins passants par le noeud malveillant pour calculer un nouveau chemin sécurisé.

Cette constatation confirme l'efficacité de notre nouveau système inter-couches par rapport à l'AOMDV normal et à l'AOMDV en cas d'attaque par blackhole, où les noeuds trouvent un chemin sécurisé avec des paquets de routage optimaux pendant le processus de découverte de route.

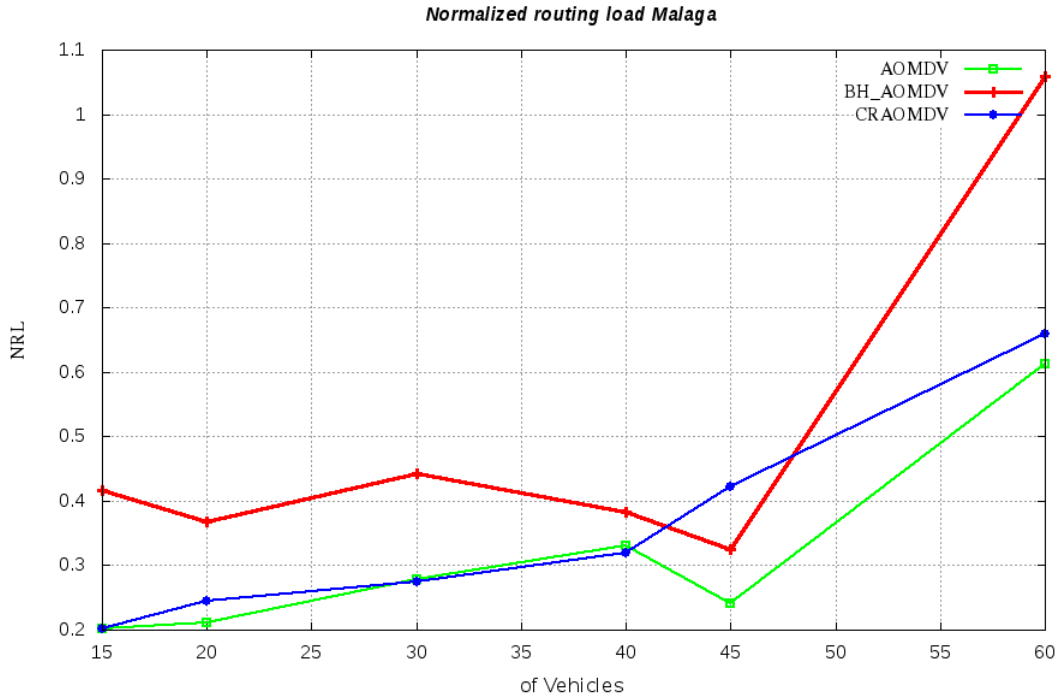


FIGURE 4.8 – *Normaized Routing Load*

✓Les graphes du BHN_Drop :

Comme le montre la figure 4.9, le nombre de paquets de données supprimés par le noeud malveillant est significativement plus élevé dans BH_AOMDV par rapport à l'AOMDV et à notre solution inter-couches CRAOMDV. Ce résultat valide la dégradation des performances d'AOMDV sous l'attaque blackhole où les noeuds malveillants suppriment tous les paquets de données reçus. De plus, le nombre de paquets de données supprimés dans notre solution et dans l'AOMDV normale est de zéro, ce qui indique que notre solution inter-couche atteint une meilleure performance même en présence de noeuds blackhole. La perte de paquets dans le cas de BH_AOMDV est d'environ 65%. De plus, le nombre de paquets de données supprimés dans CRAOMDV a diminué de 100% par rapport à BHAODV et est égal à celui d'AOMDV standard.

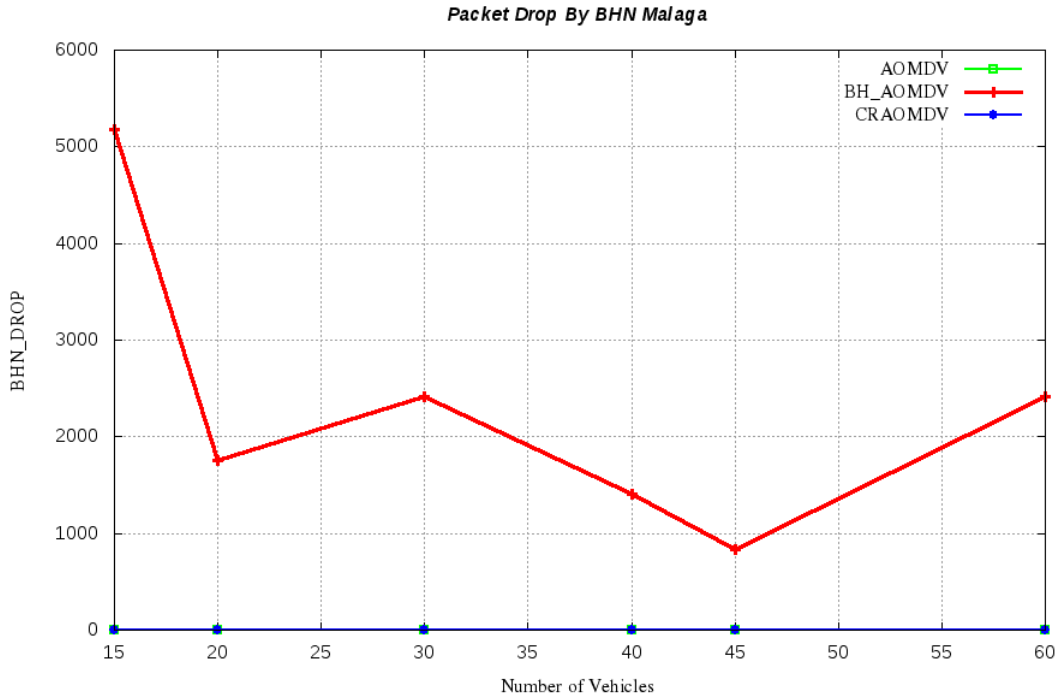


FIGURE 4.9 – *Paquets supprimées par les noeuds Black-Hole*

CONCLUSION DU CHAPITRE

Dans ce chapitre, nous avons abordé le comportement du noeud blackhole et décrit les plusieurs solutions proposées pour sécuriser les VANETs contre ce type d'attaque. Ces méthodes suggérées sont classées comme suit : Méthodes basées sur la cryptographie et Méthodes de modification du protocole de routage. Une solution efficace pour sécuriser la communication dans un réseau aussi dynamique avec des noeeuds plus rapides consiste à réduire le délai de routage en optimisant le temps nécessaire pour décider si le noeud intermédiaire est fiable ou non et pour trouver un chemin sécurisé. L'objectif principal de notre solution est de faire en sorte que les couches réseau et MAC coopèrent pour trouver un chemin sécurisé entre chaque paire source/destination avec un temps de décision réduit. Notre méthode a été évaluée et comparée à AOMDV normal et à AOMDV sous attaque blackhole (BH_AOMDV). Les résultats confirment que la solution proposée est performante par rapport à AOMDV sous attaque blackhole, où le chemin de confiance est trouvé avec une amélioration de la valeur du PDF et avec un minimum de délai et d'utilisation de la surcharge de routage. Dans nos futurs travaux, nous nous concentrerons sur la sécurité des VANETs contre les attaques par trou noir coopératif en proposant une nouvelle méthode inspirée de notre solution proposée pour ignorer les noeuds trou noir coopératifs.

Conclusion et perspective 5

Sommaire

5.1 Conclusion 83
5.2 Perspectives 84

5.1 Conclusion

Dans notre thèse, nous nous sommes focalisés sur la sécurité des réseaux véhiculaire VANETs et en particulier, la sécurité des protocoles de routages multichemin comme AOMDV contre l'attaque blackhole. Le travail a été concentré sur le protocole de routage AOMDV. Malgré ses avantages qui consistent à réduire la saturation du réseau, AOMDV est aussi sujet à différenntes attaques spécialement des attaques de type déni de service telle l'attaque blackhole. En outre, pour atteindre son objectif, le noeud malveillant exploite les caractéristiques des MANETs/VANETs et également la situation où chaque noeud/véhicule joue le rôle d'un routeur dans les procedures de recherche de chemin. Pour résoudre ce problème on a en premier lieu, intérprété et exposé le comportement du noeud malicieux en détail puis, nous avons présenté les différentes méthodes proposées dans la litérature ces quinze dernière s années pour sécuriser les protocoles de routage contre l'attaque blackhole dans les MANETs/VANETs.

En nous basant sur les deux étapes sus-cités, nous avons proposé une nouvelle thechnique inter-couche pour détécter et ignorer les noeuds blackhole du réseau. Notre but est de trouver une solution efficace. Cette efficacité c'est qu'elle soit d'une part, une solution plus performante en terme de PDF, AE2E et NRL et BHN. Et d'autre part, adéquate à un réseau MANET/VANET tout en respectant le changement imprévisible de la topologie, la grande vitesse des véhicules et le temps opportun pour prendre une décision.

Dans notre recherche nous avons utilisé un mécanisme inter-couche afin d'excéder les limites de celui à couche unique et d'améliorer les performance du réseau. Dans cette tecnique,les couches : MAC et réseau s'entraident pour détecter le comportement malicieux tout en utilisant une variable partagée XMIT_REASON.

Ce mecanisme inter-couche consiste à ajouter une phase de vérification optimisée au niveau du noeud source pour l'accéptation du RREP et pour l'envoie des paquets de données. Si la variable du XMIT_REASON contient le noeud de confiance le RREP sera accépté et les données seront envoyées. Sinon le processus de détection du noeud malicieux se déclanchera. Cette technique est appliquée dans les réseaux adhoc mobiles MANETs comme première contribution. Par rapport à la deuxième contribution cette méthode inter-couche sera utilisée avec une optimisation dans un environnement VANETs.

Enfin, en utilisant le simulateur NS2 et le générateur de mobilité SUMO, nous avons évalué les performances de notre solution CRAOMDV par papport à L'AOMDV dans une situation normale par contre AOMDV avec une attaque blackhole. les résultats des simulations montrent l'efficacité de notre solution en augmentant considérablement le taux des paquets de données qui atteignent avec succès la couche d'application du noeud de destination sans augmenter la surcharge du réseau.

5.2 Perspectives

En résumé, les travaux de cette thèse se sont focalisés sur la sécurité du protocole AOMDV contre l'attaque blackhole dans les VANETs. L'impact important de cette attaque qui peut dégrader les performances d'un tel réseau et les caractéristiques des VANETs augmentent la complexité pour trouver une solution efficace.

Comme première perspective, c'est évaluer la solution que nous avons proposée (CRAOMDV) dans ce domaine avec les autres. Ensuite, étant donné que ce que nous avons suggéré dans cette thèse vise à sécurisé AOMDV contre l'attaque blackhole avec un seul noeud (responsable du comportement malveillant), nous viserons dorénavant dans nos futurs recherches la sécurité des VANET contre les attaques par trou noir coopératif là où les noeuds malveillants coopèrent pour perturber les services de la couche réseau. Le résultat de cette attaque est bien plus sévère que l'attaque blackhole simple (single blackhole attack).

Enfin, quant aux simulations des trois protocoles suivants : BHAOMDV, CRAOMDV et l'AOMDV normale, ils ont été effectués en utilisant le simulateur NS2 et SUMO, le fournisseur des modèles de mobilité des véhicules en temps réel. Les résultats de ces simulations prouvent l'efficacité de la solution que nous avons envisagée. Comme une dernière perspective, et pour valider l'efficacité de notre mécanisme inter-couche, il est judicieux d'appliquer notre solution dans un réseau véhiculaire réel.

Liste des publications

Journal internationale

Naib Rabiaa, Ali Cherif Moussa et Boukli Hacene Sofiane. A Cross-layer Method for Identifying and Isolating the Blackhole Nodes in Vehicular Ad-hoc Networks. Information Security Journal : A Global Perspective, pages 1–15,2021, DOI : 10.1080/19393555.2021.2007316

Naib Rabiaa, Ali Cherif Moussa et Boukli Hacene Sofiane. A NEW CROSS LAYER MECHANISM TO SECURE AOMDV AGAINST THE BLACK-HOLE ATTACK. International Journal of Advancements in Electronics and Electrical Engineering – IJCNS, vol. 8, no. 2, 2019.

Conference internationale

Naib Rabiaa, Ali Cherif Moussa et Boukli Hacene Sofiane., A NEW CROSS LAYER MECHANISM TO SECURE AOMDV AGAINST THE BLACK-HOLE ATTACK, Eighth International Conference on Advances in Computing, Communication and Information Technology CCIT,April 23-24 2019, Birmingham City University, Birmingham, United Kingdom.

Bibliographie

[Ahmed & Khalifa 2017] Diaa Eldein Mustafa Ahmed et Othman O Khalifa. *An overview of MANETs : applications, characteristics, challenges and recent issues*. PhD thesis, University of Science and Technology, 2017.

[Al-Kahtani 2012] Mohammed Saeed Al-Kahtani. *Survey on security attacks in Vehicular Ad hoc Networks (VANETs)*. In Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, pages 1–9. IEEE, 2012.

[Ali & Kulkarni 2015] Abdalftah Kaid Said Ali et U Kulkarni. *Characteristics, applications and challenges in mobile Ad-Hoc networks (MANET) : overview*. Wireless Networks, vol. 3, no. 12, pages 6–12, 2015.

[Almutairi *et al.* 2014] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri et Dima Alotaish. *A new black hole detection scheme for VANETs*. In Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems, pages 133–138, 2014.

[Arif *et al.* 2020] Muhammad Arif, Guojun Wang, Tao Peng, Valentina Emilia Balas, Oana Geman et Jianer Chen. *Optimization of communication in VANETs using fuzzy logic and artificial Bee colony*. Journal of Intelligent & Fuzzy Systems, vol. 38, no. 5, pages 6145–6157, 2020.

[Association *et al.* 2010] IEEE Standards Association*et al. 802.11 p-2010-IEEE standard for information technology-local and metropolitan area networks-specific requirements-part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6 : Wireless access in vehicular environments*. URL http ://standards. ieee. org/findstds/standard/802.11 p-2010. html, 2010.

[Awang *et al.* 2017] Azlan Awang, Khaleel Husain, Nidal Kamel et Sonia Aissa. *Routing in vehicular ad-hoc networks : A survey on single-and cross-layer design techniques, and perspectives*. IEEE Access, vol. 5, pages 9497–9517, 2017.

[Beijar 2002] Nicklas Beijar. *Zone routing protocol (ZRP)*. Networking Laboratory, Helsinki University of Technology, Finland, vol. 9, pages 1–12, 2002.

[Bhardwaj & Singh 2014] Neetika Bhardwaj et Rajdeep Singh. *Detection and avoidance of blackhole attack in AOMDV protocol in MANETs*. International Journal of Application or Innovation in Engineering & Management (IJAIEM), pages 376–383, 2014.

[Chauhan *et al.* 2015] RK Chauhan*et al. An assessment based approach to detect black hole attack in MANET*. In International Conference on Computing, Communication & Automation, pages 552–557. IEEE, 2015.

[Cherkaoui *et al.* 2020] Badreddine Cherkaoui, Abderrahim Beni-hssane et Mohammed Erritali. *Variable control chart for detecting black hole attack in vehicular ad-hoc*

networks. Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 11, pages 5129–5138, 2020.

[Chihi 2017] Ines Chihi. *Étude de l'attaque «Black Hole» sur le protocole de routage VADD (Vehicule-Assisted Data Delivery)*. PhD thesis, Université du Québec à Trois-Rivières, 2017.

[Clausen & Jacquet 2003] Thomas Clausen et Philippe Jacquet. *Optimized link state routing protocol (OLSR)*. Rapport technique, Internet Engineering Task Force (IETF), 2003.

[Delkesh & Jabraeil Jamali 2019] Taher Delkesh et Mohammad Ali Jabraeil Jamali. *EAODV : Detection and removal of multiple black hole attacks through sending forged packets in MANETs*. Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 5, pages 1897–1914, 2019.

[Deng *et al.* 2002] Hongmei Deng, Wei Li et Dharma P Agrawal. *Routing security in wireless ad hoc networks*. IEEE Communications magazine, vol. 40, no. 10, pages 70–75, 2002.

[Deshmukh & Dorle 2016] AR Deshmukh et SS Dorle. *Simulation of Urban Mobility (Sumo) For Evaluating Qos Parameters For Vehicular Adhoc Network*. IOSR J. Electron. Commun. Eng. Ver. I, vol. 11, no. 1, pages 2278–2834, 2016.

[Dhyani *et al.* 2017] Isha Dhyani, Neha Goel, Gaurav Sharma et Bhawna Mallick. *A reliable tactic for detecting black hole attack in vehicular ad hoc networks*. In Advances in Computer and Computational Sciences, pages 333–343. Springer, 2017.

[Engoulou *et al.* 2014] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre et Alejandro Quintero. *VANET security surveys*. Computer Communications, vol. 44, pages 1–13, 2014.

[19] European Telecommunications Standards Institute (ETSI). *Intelligent Transport Systems (ITS) ; Vehicular Communications ; Basic Set of Applications ; Part 2 : Specification of Cooperative Awareness Basic Service. ETSI TS 102 637-2*, 2011.

[Fu *et al.* 2020] Xiuwen Fu, Giancarlo Fortino, Pasquale Pace, Gianluca Aloi et Wenfeng Li. *Environment-fusion multipath routing protocol for wireless sensor networks*. Information Fusion, vol. 53, pages 4–19, 2020.

[Gupta *et al.* 2018] Aditya Gupta, Prabal Verma et Rakesh Singh Sambyal. *An Overview of MANET : Features, Challenges and Applications*. NCRACIT) Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, pages 2456–3307, 2018.

[Hamdi *et al.* 2020] Mustafa Maad Hamdi, Lukman Audah, Sami Abduljabbar Rashid, Alaa Hamid Mohammed, Sameer Alani et Ahmed Shamil Mustafa. *A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs)*. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pages 1–7. IEEE, 2020.

[Hasrouny *et al.* 2015] Hamssa Hasrouny, Carole Bassil, Abed Ellatif Samhat et Anis Laouiti. *Group-based authentication in V2V communications*. In 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), pages 173–177. IEEE, 2015.

[Hassan *et al.* 2020] Zohaib Hassan, Amjad Mehmood, Carsten Maple, Muhammad Altaf Khan et Abdulaziz Aldegheishem. *Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles*. IEEE Access, vol. 8, pages 199618–199628, 2020.

[He *et al.* 2015] Debiao He, Sherali Zeadally, Baowen Xu et Xinyi Huang. *An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks*. IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pages 2681–2691, 2015.

[Hota *et al.* 2021] Lopamudra Hota, Biraja Prasad Nayak, Arun Kumar, GG Ali, Peter Han Joo Chong*et al. An Analysis on Contemporary MAC Layer Protocols in Vehicular Networks : State-of-the-Art and Future Directions*. Future Internet, vol. 13, no. 11, page 287, 2021.

[Huang *et al.* 2011] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S Obaidat, Ting-Yun Chi et Sanjay K Dhurandher. *Multi-path trust-based secure AOMDV routing in ad hoc networks*. In 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, pages 1–5. Ieee, 2011.

[Ilyas 2017] Mohammad Ilyas. The handbook of ad hoc wireless networks. CRC press, 2017.

[isi.edu 2022] isi.edu. *Information Sciences Institute*. https://www.isi.edu/nsnam/nam/, 2022. Accessed : 2022-06-05.

[Kabir *et al.* 2014] Mohammed Humayun Kabir, Syful Islam, Md Javed Hossain et Sazzad Hossain. *Detail comparison of network simulators*. International Journal of Scientific & Engineering Research, vol. 5, no. 10, pages 203–218, 2014.

[Karp & Kung 2000] Brad Karp et Hsiang-Tsung Kung. *GPSR : Greedy perimeter stateless routing for wireless networks*. In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243–254. ACM, 2000.

[Kenney 2011] John B Kenney. *Dedicated short-range communications (DSRC) standards in the United States*. Proceedings of the IEEE, vol. 99, no. 7, pages 1162–1182, 2011.

[Kim *et al.* 2018] Jin-Woo Kim, Jae-Wan Kim et Dong-Keun Jeon. *A Cooperative Communication Protocol for QoS Provisioning in IEEE 802.11 p/Wave Vehicular Networks*. Sensors, vol. 18, no. 11, page 3622, 2018.

[Kumar *et al.* 2021] Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, VD Ambeth Kumar, Bijaya Ketan Panigrahi et Kalyana C Veluvolu. *Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm*. Microprocessors and Microsystems, vol. 80, page 103352, 2021.

[Kurosawa *et al.* 2007] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour et Yoshiaki Nemoto. *Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method*. IJ Network Security, vol. 5, no. 3, pages 338–346, 2007.

[Laouiti *et al.* 2017] Anis Laouiti, Amir Qayyum et Mohamad Naufal Mohamad Saad. Vehicular ad-hoc networks for smart cities : Second international workshop, 2016, volume 548. Springer, 2017.

[Lee & Atkison 2021] Michael Lee et Travis Atkison. *Vanet applications : Past, present, and future*. Vehicular Communications, vol. 28, page 100310, 2021.

[Li & Wang 2021] Wei Li et Xin Wang. *Construction of Modularized English Teaching Platform for Multimedia Wireless Network Based on NS2 Simulation Software*. Mobile Information Systems, vol. 2021, 2021.

[Liang *et al.* 2015] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang et Rongfang Bie. *Vehicular ad hoc networks : architectures, research issues, methodologies, challenges, and trends*. International Journal of Distributed Sensor Networks, vol. 11, no. 8, page 745303, 2015.

[Lou *et al.* 2004] Wenjing Lou, Wei Liu et Yuguang Fang. *SPREAD : Enhancing data confidentiality in mobile ad hoc networks*. In IEEE INFOCOM 2004, volume 4, pages 2404–2413. IEEE, 2004.

[Ma *et al.* 2020] Mengyuan Ma, Kai Liu, Xiling Luo, Tao Zhang et Feng Liu. *Review of MAC protocols for vehicular ad hoc networks*. Sensors, vol. 20, no. 23, page 6709, 2020.

[Marina & Das 2001] Mahesh K Marina et Samir R Das. *On-demand multipath distance vector routing in ad hoc networks*. In Network Protocols, 2001. Ninth International Conference on, pages 14–23. IEEE, 2001.

[Meddeb Makhlouf & Guizani 2019] Amel Meddeb Makhlouf et Mohsen Guizani. *SE-AOMDV : Secure and efficient AOMDV routing protocol for vehicular communications*. International Journal of Information Security, vol. 18, no. 5, pages 665–676, 2019.

[Mistry *et al.* 2010] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri*et al. Improving AODV protocol against blackhole attacks*. In Proceedings of the international multi conference of engineers and computer scientists, volume 2. Citeseer, 2010.

[Moghraoui 2015] Kahina Moghraoui. *Gestion de l'anonymat des communications dans les réseaux véhiculaires Ad hoc sans fil (VANETs)*. PhD thesis, Université du Québec à Trois-Rivières, 2015.

[Mokhtar & Azab 2015] Bassem Mokhtar et Mohamed Azab. *Survey on security issues in vehicular ad hoc networks*. Alexandria Engineering Journal, vol. 54, no. 4, pages 1115–1126, 2015.

[Naib *et al.* 2019a] Rabiaa Naib, Moussa Ali Cherif et Sofiane Boukli Hacene. *A NEW CROSS LAYER MECHANISM TO SECURE AOMDV AGAINST THE BLACK-HOLE ATTACK*. International Journal of Advancements in Electronics and Electrical Engineering – IJCNS, vol. 8, no. 2, pages 22–29, 12 2019.

[Naib *et al.* 2019b] Rabiaa Naib, Moussa Ali Cherif et Sofiane Boukli Hacene. *A NEW CROSS LAYER MECHANISM TO SECURE AOMDV AGAINST THE BLACK-HOLE ATTACK*. In Eighth International Conference on Advances in Computing, Communication and Information Technology CCIT, pages 32–39, 2019.

[Naib *et al.* 2021] Rabiaa Naib, Ali Cherif Moussa et Boukli Hacene Sofiane. *A Cross-layer Method for Identifying and Isolating the Blackhole Nodes in Vehicular Ad-hoc Networks*. Information Security Journal : A Global Perspective, pages 1–15, 2021.

[Naik *et al.* 2017] Gaurang Naik, Jinshan Liu et Jung-Min Jerry Park. *Coexistence of dedicated short range communications (DSRC) and Wi-Fi : Implications to Wi-Fi performance*. In IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pages 1–9. IEEE, 2017.

[Nampally & Raghavender Sharma 2017] Venkata Nampally et Mamillapally Raghavender Sharma. *Tool Command Language for VANET*. International Journal of Scientific Research in Computer Science Applications and Management Studies, vol. 6, 07 2017.

[Nguyen *et al.* 2018] Vandung Nguyen, Oanh Tran Thi Kim, Chuan Pham, Thant Zin Oo, Nguyen H Tran, Choong Seon Hong et Eui-Nam Huh. *A survey on adaptive multi-channel MAC protocols in VANETs using Markov models*. IEEE Access, vol. 6, pages 16493–16514, 2018.

[Obidike *et al.* 2018] GC Obidike, CA Nwabueze et VC Onuzulike. *Concept and Characteristics of Mobile Ad-hoc Network*. International Journal of Innovative Engineering, Technology and Science, vol. 2, 2018.

[Ogundoyin 2020] Sunday Oyinlola Ogundoyin. *An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks*. International Journal of Computers and Applications, vol. 42, no. 2, pages 196–211, 2020.

[Pandikumar *et al.* 2017] T Pandikumar, Biruk Zewdie et Capt Zinabu Haile. *Mitigating black hole attack on MANET with AOMDV protocol*. International Journal of Engineering Science, vol. 12666, 2017.

[Quyoom *et al.* 2020] Abdul Quyoom, Aftab Ahmad Mir et Abid Sarwar. *Security attacks and challenges of VANETs : a literature survey*. Journal of Multimedia Information System, vol. 7, no. 1, pages 45–54, 2020.

[Raj & Swadas 2009] Payal N Raj et Prashant B Swadas. *Dpraodv : A dyanamic learning system against blackhole attack in aodv based manet*. arXiv preprint arXiv :0909.2371, 2009.

[Raja Kumar *et al.* 2021] K Raja Kumar, Nagarjuna Karyemsetty et Badugu Samatha. *Performance Analysis of Vehicular Network Scenarios Using SUMO and NS2 Simulators*. In Data Engineering and Communication Technology, pages 337–344. Springer, 2021.

[Rana & Gupta 2015] Anuj Rana et Sandeep Gupta. *Review on MANETs characteristics, challenges, application and security attacks*. International Journal of Science and Research, vol. 4, no. 2, 2015.

[Rani & Kumar 2013] Jyoti Rani et Naresh Kumar. *Improving AOMDV protocol for black hole detection in Mobile Ad hoc Network*. In Control Computing Communication & Materials (ICCCCM), 2013 International Conference on, pages 1–8. IEEE, 2013.

[Rayamajhi *et al.* 2018] Anjan Rayamajhi, Zoleikha Abdollahi Biron, Roberto Merco, Pierluigi Pisu, James M Westall et Jim Martin. *The impact of dedicated short range communication on cooperative adaptive cruise control*. In 2018 IEEE International Conference on Communications (ICC), pages 1–7. IEEE, 2018.

[Razzaque *et al.* 2013] MA Razzaque, Ahmad Salehi et Seyed M Cheraghi. *Security and privacy in vehicular ad-hoc networks : survey and the road ahead*. Wireless Networks and Security, pages 107–132, 2013.

[Sakiz & Sen 2017] Fatih Sakiz et Sevil Sen. *A survey of attacks and detection mechanisms on intelligent transportation systems : VANETs and IoV*. Ad Hoc Networks, vol. 61, pages 33–50, 2017.

[Santa *et al.* 2014] José Santa, Fernando Pereñíguez, Antonio Moragón et Antonio F Skarmeta. *Experimental evaluation of CAM and DENM messaging services in vehicular communications*. Transportation Research Part C : Emerging Technologies, vol. 46, pages 98–120, 2014.

[Shah *et al.* 2019] Syed Sarmad Shah, Asad Waqar Malik, Anis U Rahman, Sohail Iqbal et Samee U Khan. *Time barrier-based emergency message dissemination in vehicular ad-hoc networks*. IEEE Access, vol. 7, pages 16494–16503, 2019.

[Sharma *et al.* 2021] Sparsh Sharma, Ajay Kaul, Suhaib Ahmed et Surbhi Sharma. *A detailed tutorial survey on VANETs : emerging architectures, applications, security issues, and solutions*. International Journal of Communication Systems, vol. 34, no. 14, page e4905, 2021.

[Singh & Agrawal 2014] Surmukh Singh et Sunil Agrawal. *VANET routing protocols : Issues and challenges*. In 2014 Recent Advances in Engineering and Computational Sciences (RAECS), pages 1–5. IEEE, 2014.

[Singh *et al.* 2016] Atinder Preet Singh, Avneet Singh Chawla et Surjeet Surjeet. *Performance issues and behavioral analysis of routing protocols in MANETs*. International Journal of Communications, Network and System Sciences, vol. 9, no. 11, pages 431–439, 2016.

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

[Taha *et al.* 2017] Aqeel Taha, Raed Alsaqour, Mueen Uddin, Maha Abdelhaq et Tanzila Saba. *Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function*. IEEE access, vol. 5, pages 10369–10381, 2017.

[Talpur & Gurusamy 2021] Anum Talpur et Mohan Gurusamy. *Machine learning for security in vehicular networks : A comprehensive survey*. IEEE Communications Surveys & Tutorials, 2021.

[Talukdar *et al.* 2021] Md Ibrahim Talukdar, Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar et Amjed Sid Ahmed. *Performance improvements of AODV by black hole attack detection using IDS and digital signature*. Wireless Communications and Mobile Computing, vol. 2021, 2021.

[Tamilselvan & Sankaranarayanan 2007] Latha Tamilselvan et V Sankaranarayanan. *Prevention of blackhole attack in MANET*. In The 2nd international conference on wireless broadband and ultra wideband communications (AusWireless 2007), pages 21–21. IEEE, 2007.

[Toh 2007] Chai K. Toh. *Future Application Scenarios for MANET-Based Intelligent Transportation Systems*. Future Generation Communication and Networking (FGCN 2007), vol. 2, pages 414–417, 2007.

[Toor & Jain 2017] Amanjot Singh Toor et AK Jain. *A survey on wireless network simulators*. Bulletin of Electrical Engineering and Informatics, vol. 6, no. 1, pages 62–69, 2017.

[Toutouh & Alba 2011] Jamal Toutouh et Enrique Alba. *An efficient routing protocol for green communications in vehicular ad-hoc networks*. In Proceedings of the 13th annual conference companion on Genetic and evolutionary computation, pages 719–726, 2011.

[Toutouh *et al.* 2012] Jamal Toutouh, José García-Nieto et Enrique Alba. *Intelligent OLSR routing protocol optimization for VANETs*. IEEE transactions on vehicular technology, vol. 61, no. 4, pages 1884–1894, 2012.

[Upadhyaya 2018] Ajay Upadhyaya. *Attacks on vanet security*. International Journal of Computer Engineering & Technology (IJCET), vol. 9, no. 1, pages 8–19, 2018.

[Uzcátegui *et al.* 2009] Roberto A Uzcátegui, Antonio Jose De Sucre et Guillermo Acosta-Marum. *Wave : A tutorial*. IEEE Communications magazine, vol. 47, no. 5, pages 126–133, 2009.

[Zaidi & Faisal 2018] Taskeen Zaidi et Syed Faisal. *An overview : Various attacks in VANET*. In 2018 4th International Conference on Computing Communication and Automation (ICCCA), pages 1–6. IEEE, 2018.

Notations

MANET	Mobile Ad Hoc Network
VANET	Vehicular Adhoc Network
OMS	Organisation Mondiale de la Santé
OBU	On Board Unit
RSU	Roadside Service Units
V2V	Vehicle-to-vehicle
V2I	vehicle-to-infrastructure
DSRC	Dedicated Short Range Communication
ITS	Intelligent Transportation Systems
ISO/ETSI	European Telecommunications Standards Institute
CAM	the Cooperative Awareness Message
DENM	the Decentralized Environmental Notification Message
DSRC	Dedicated Short Range Communication
IEEE	Institue of Electricol and Electronicol Engenies
Wi-Fi	Wireless Fidelity
PHY	Physical layer
MAC	Medium Access Control
FCC	Federal Communications Commission
ASTM	American Society for Testing and Materials
LAN	Local Area Network

ISM	industrial, scientific and medical
GPSR	Greedy Perimeter Stateless Routing
OLSR	Optimized Link State Protocol
DSDV	Destination-Sequenced Distance Vector
ZRP	Zone Routing Protocol
GSR	Global State Routing
AODV	Adhoc On Demand Distance Vector
AOMDV	Ad-hoc On-demand Multipath Distance Vector
DV-CAST	A distributed vehicular broadcast protocol for vehicular ad hoc networks
POCA	Position Aware Reliable Broadcast Protocol
DECA	Density Dependent Reliable Scattering in Vehicular Ad Hoc Networks
COIN	Clustering for Open IVC Network
LORA_CBF	Location routing algorithm with cluster-based flooding
ZOR	Zone of Relevance
IVG	Inter Vehicles Geocast protocol
DG-CASTOR	Direction-based geocast routing protocol for query dissemination in VANET
QoS	Quality Of Service
IP	Internet Protocol
DCF	Distributed Coordination Function
PCF	Point Coordinated Function
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
EDCA	Enhanced Distributed Channel Access
RREQ	Route Request Packet
RREP	Route Replay Packet

RERR	Route Error Packet
MAC	Medium Access Control
PMLE	Physical layer management entity
MLME	MAC layer management entity
WAVE	Wireless Access in Vehicular Environments
WSMP	WAVE Short messages protocol
OSI	Open Systems Interconnection
PHY	Physical layer
NET	Network Layer
TA	Trusted Agent
DOS	Denial Of Service
DDOS	Destributed Denial Of Service
T-AOMDV	Trust-based ad hoc on-demand multipath distance vector
ECC	Elliptic-curve cryptography
BHN	Black-Hole Node
CRAOMDV	Cross-layer ad hoc on-demand multipath distance vector
BH_AODMV	BlackHole ad hoc on-demand multipath distance vector
GGRP	Greedy Geographic Routing Protocol
NS	Netowrks Simulator
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
TCL	Tool Command Language
TclCL	Tcl with classes
TK	Tool kit

OTCL	Object Tool Command Language
NAM	Network Animator
GUI	Graphical User Interface
PDR	Packet delivery ratio
AE2ED	Average end-to-end delay
NRL	Normalized routing load
DPRAODV	Detection,Prevention and Reactive AODV
SUMO	Simulation of Urban MObility

الملخص

شبكة المركبات المخصصة هي مجموعة من المركبات الذكية التي تتواصل بدون بنية تحتية ثابتة. يتم الاتصال بين كل زوج مصدر / وجهة باستخدام بروتوكولات التوجيه. يُعد متجه المسافات متعدد المسارات عند الطلب أحد أكثر بروتوكولات التوجيه متعدد المسارات المخصصة المستخدمة في شبكات المركبات المخصصة. تجعل الطبيعة اللامركزية للشبكات المخصصة للمركبات هذا النوع من الشبكات عرضة لهجمات مختلفة ، مثل هجوم الثقب الأسود. في مثل هذا الهجوم ، تهدف السيارة الخبيثة إلى جعل الاتصال غير متاح. تقنع المركبة الخبيثة المصدر بإرسال حزم البيانات الخاصة به من خلالها لأن لديها أحدث طريق نحو الوجهة. يتم ذلك عن طريق تزوير معلومات التوجيه. بعد استلام حزم البيانات ، تقوم السيارة الخبيثة بحذفها بدلاً من إعادة توجيهها إلى وجهتها المقصودة. في أطروحتنا ، نركز على تأمين متجه المسافات متعدد المسارات عند الطلب ضد هذا النوع من الهجوم من خلال تقديم طريقة جديدة عبر الطبقات تعتمد على المعلومات المشتركة بين التحكم في الوصول المتوسط وطبقات الشبكة لاكتشاف المركبات الضارة وتجاهلها.

Résumé

Le réseau Adhoc véhiculaire (VANET) est un ensemble de véhicules intelligents qui communiquent sans infrastructure fixe. La communication entre chaque paire source/destination se fait à l'aide de protocoles de routage. Le vecteur de distance multivoie à la demande (AOMDV) est l'un des protocoles de routage multivoie Adhoc les plus connus utilisés dans les VANET. La nature décentralisée des réseaux VANET rend ce type de réseau vulnérable à différentes attaques, comme l'attaque par trou noir. Dans ce type d'attaque, le véhicule malveillant vise à rendre la communication non disponible. Le véhicule malveillant convainc la source d'envoyer ses paquets de données par lui parce qu'il a la route la plus récente vers la destination. Cela se fait en falsifiant les informations de routage. Dans notre thèse, nous nous concentrons sur la sécurisation d'AOMDV contre ce type d'attaque en introduisant une nouvelle méthode inter-couches (CRAOMDV) basée sur les informations partagées entre les couches MAC et réseau pour détecter et ignorer les véhicules malveillants dans les VANETs.

Abstract

Vehicular Adhoc Network (VANET) is a set of intelligent vehicles that communicate without a fixed infrastructure. The communication between each source/destination pair is done by using routing protocols. On-demand multipath distance vector (AOMDV) is one of the most known Adhoc multipath routing protocols used in VANETs. The decentralized nature of VANET makes this type of network vulnerable to various attacks, such as blackhole attack. In such attack, the malicious vehicle aims to make the communication unavailable. the malicious vehicle convinces the source to send its data packets through it because it has the freshest route towards the destination. This is done by forging routing information. After receiving the data packets the malicious vehicle deletes them instead of forwarding them to their intended destination. in our thesis, we are focused by securing AOMDV aginst this type of attack by introducing a new Cross-Layer method (CRAOMDV) based on the shared information between MAC and network layers to detect and ignore the malicious vehicles in VANETs.