UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À

L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES

PAR

INES CHIHI

ÉTUDE DE L'ATTAQUE « Black Hole » SUR LE PROTOCOLE DE ROUTAGE VADD (Vehicule-Assisted Data Delivery)

JUILLET 2017

Ce mémoire a été évalué par un jury composé de:

- **Boucif Amar Bensaber**, directeur de recherche.

Professeur au département de mathématiques et d'informatique Université du Québec à Trois-Rivières.

- **François Meunier**, évaluateur.

Professeur au département de mathématiques et d'informatique Université du Québec à Trois-Rivières.

- **Ismail Biskri**, évaluateur.

Professeur au département de Mathématiques et d'informatique Université du Québec à Trois-Rivières.

À

Ma précieuse Yesmine,

Mon cher frère,

Mes parents,

Tous ceux qui me sont chers.

Remerciements

Je tiens à remercier mon directeur de recherche, Professeur Boucif Amar Bensaber, pour son aide et ses conseils, sans lui ce travail n'aurait pas vu le jour, il m'a donné l'opportunité de faire mon premier pas dans le domaine de la recherche scientifique.

J'adresse particulièrement, mes sincères remerciements au professeur Mhamed Mesfioui, pour ses qualités humaines et intellectuelles.

Je remercie les professeurs François Meunier et Ismail Biskri d'avoir accepté d'évaluer mon travail.

Je remercie tous mes professeurs à l'UQTR qui m'ont permis d'acquérir plus de connaissances durant mes études.

Je remercie tous mes collègues du Laboratoire de Mathématiques et Informatique appliquées (LAMIA).

Enfin, je remercie tous ceux qui de près ou de loin m'ont soutenu et encouragé pour réussir mes études.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

CA: Central Authority.

CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance.

DSR: Dynamic Source Routing.

DSRC: Dedicated Short Range Communication.

IDS: Intrusion Detection System.

GeOpps: Geographical Opportunistic Routing.

GPCR: Greedy Perimeter Coordinator Routing.

GPS: Global Positioning System.

GPSR Greedy Perimeter Stateless Routing.

IEEE: Institute of Electrical and Electronics Engineers.

MAC: Medium Access Control.

MANET: Mobile Ad hoc Network.

OBU: On Board Unit.

RSU: Road Side Unit.

STI: Systèmes de Transport Intelligents.

SUMO: Simulation of Urban Mobility.

VADD: Vehicle-Assisted Data Delivery.

VANET: Vehicular Ad hoc Network.

V2V: Vehicular-to-Vehicular.

V2I: Vehicular-to-Infrastructure.

WAVE: Wireless Access for the Vehicular Environment.

Wi-Fi: **W**ireless **F**idelity.

WiMAX : **W**orldwide **I**nteroperability **f**or **M**icrowave **A**ccess.

WLAN: **W**ireless **L**ocal **A**rea **N**etwork.

Résumé

La mise en œuvre des algorithmes de routage des réseaux véhiculaires sans fil (VANETs) est un problème complexe puisque l'environnement VANETs est dynamique et évolue au cours du temps ce qui implique un changement fréquent au niveau de la topologie du réseau. Afin de trouver une solution à ces problèmes, nous avons étudié dans un premier temps quelques protocoles de routage dédiés au réseaux véhiculaires sans fil pour sélectionner un protocole de routage d'informations qui garantit la transmission des paquets en utilisant la meilleure route, le moindre retard et la performance sur des routes denses. Nous choisissons le protocole VADD (Vehicle-Assisted Data Delivery) qui est unicast et adopte l'idée de stockage et de transmission (Carry-and-Forward). Pour VADD, le mécanisme de routage se base sur les positionnements courants des véhicules dans le voisinage et l'état de la circulation dans le réseau routier.

En se basant sur les résultats de simulation de l'algorithme de routage VADD, on a remarqué que c'est un protocole performant sur les routes denses, mais comme les réseaux VANETs sont un moyen de communication ouvert, cela peut construire une cible idéale pour les attaques qui pourraient intercepter les messages avant d'arriver à leurs destinations, ce qui implique que ce protocole de routage peut être vulnérable vis-à-vis des attaques. Pour tester les performances du protocole VADD en termes de sécurité, nous lui avons fait subir l'attaque « Black Hole » et nous avons étudié par la suite les impacts de cette attaque sur les performances du protocole VADD en termes de la quantité totale de données reçues par la destination. À la fin de notre travail, nous avons proposé des pistes de solutions pour rendre ce protocole plus performant.

Mot Clés : Algorithme de routage, sécurité, performance, Black Hole, attaque.

Abstract

The implementation of the Vehicular Ad-Hoc Network (VANET) routing algorithms is a complex problem since the VANETs environment is dynamic and evolves over time, which implies a frequent change at the level of the network topology. In order to find a solution to these problems, we first have to study some routing protocols dedicated to the vehicular networks in order to find an information routing protocol that guarantees the transmission of the packets using the best route, the shortest delay and the performance on dense routes. The protocol chosen is the Vehicle-Assisted Data Delivery (VADD) protocol. It is unicast and adopts the idea of storage and transmission. For VADD, the routing mechanism is based on the current positioning of vehicles in the vicinity and the state of traffic in the road network.

Based on the simulation results of the VADD routing algorithm, it has been observed that it is an efficient protocol on dense roads, but since VANET networks are an open mean of communication, this can build an ideal target for attacks that could intercept messages before arriving at their destinations, which implies that this routing protocol may be vulnerable to attacks. To test the performance of the VADD protocol in terms of security, we will make it undergo the « black hole » attack and thereafter we will study the impacts of this attack on the performance of the VADD protocol in terms of the total amount of data received by the destination. At the end of our work, we proposed solutions to make this protocol more efficient.

Keywords: Routing algorithms, security, performance, Black Hole, attack.

Chapitre 1 - Introduction générale

Le nombre croissant de véhicules aujourd'hui a conduit à un déséquilibre au trafic routier. En effet, ils entrainent des dégâts environnementaux ainsi qu'une mauvaise qualité de vie. Comme les systèmes de transport actuels fournissent très peu d'informations sur les conditions routières, de nombreux gouvernements, constructeurs automobiles et consortium d'industriels ont fixé la réduction des accidents de la route comme une priorité majeure. Afin d'aboutir à ce but, la première idée consistait à rendre les véhicules et les routes plus intelligents par le biais des communications sans fil, d'où la technique VANET s'est présentée et qui permet aux véhicules de communiquer via des messages envoyés entre eux.

Les réseaux véhiculaires sont une projection des systèmes de transports intelligents (STI) (ou ITS pour Intelligent Transportation System). Le but des systèmes de transport intelligents est de réduire les risques dans le domaine du transport de façon significative en travaillant simultanément sur quatre bases: la prévention des accidents; la réduction des dégâts en cas de collision; la gestion des secours et enfin la protection des utilisateurs [1] [2].

Puisque les réseaux véhiculaires ont comme caractéristique principale une forte mobilité, celle-ci entraine une topologie très dynamique, ce qui fait que la plupart des protocoles de routage dédiés pour MANETs sont inadéquate aux VANETs. En effet, dans les réseaux véhiculaires, la vitesse est élevée dans certains environnements de communication comme les autoroutes. Relativement à la vitesse, la distance entre deux nœuds peut augmenter très rapidement et être supérieure à la portée de transmission des nœuds, ce qui pourrait interrompre le lien entre les nœuds en question. Cela peut se produire fréquemment et affecter considérablement le bon acheminement des paquets dans le réseau. Une solution pour améliorer la connectivité du réseau consiste à utiliser les véhicules participants comme relais, établissant ainsi des communications multi-sauts [3].

Pour s'avérer efficace dans les VANETs, toute conception de protocole de routage prend en considération les contraintes suivantes :

- La minimisation de la charge du réseau en évitant les boucles de routage et la concentration du trafic autour de certains nœuds ou liens.
- L'évolution des chemins de transfert des données ne doit pas avoir des conséquences sur la circulation des paquets.
- La stratégie de routage doit assurer un maintien efficace des routes et avec des faibles couts.
- Lorsque la connectivité du réseau augmente la qualité du temps de latence et des chemins doit augmenter aussi.

En tenant compte de ces contraintes, nous proposons dans le cadre de notre mémoire une étude d'un protocole de routage d'informations qui garantit la transmission des paquets en utilisant la meilleure route, le moindre retard et la performance sur des routes denses. Le protocole choisi est le protocole VADD (Vehicle-Assisted Data Delivery).

L'étude du protocole VADD est faite sur deux étapes; la première étape consiste à une simulation de l'algorithme de routage du protocole VADD à l'aide du simulateur de trafic routier SUMO-O.15.0 et le simulateur réseau OMNET++ 4.2.2. La deuxième étape consiste à tester les performances du protocole VADD en termes de sécurité, donc, nous allons lui faire subir l'attaque « Black Hole » et nous allons étudier par la suite les impacts de cette attaque sur les performances du protocole VADD.

Le présent mémoire est structuré en sept chapitres. Le chapitre 2 porte sur la généralité des réseaux VANETs. Le chapitre 3 présente les résumés de quelques travaux de la littérature sur le routage et la sécurité des réseaux véhiculaires sans fil. L'étude des performances du protocole de routage VADD est présentée dans le chapitre 4. Le chapitre 5 décrit les résultats des simulations de notre étude. Le chapitre 6, présente notre idée de solution contre l'attaque « Black Hole » et finalement, le chapitre 7 conclut notre étude en présentant quelques perspectives.

Chapitre 2 - Réseaux véhiculaires sans fil: vue d'ensemble

2.1 Introduction

Les réseaux véhiculaires ad hoc (VANETs) sont un type particulier de réseaux mobiles ad hoc (MANETs), où les véhicules sont simulés comme des nœuds mobiles. Les réseaux MANETs et VANETs se diffèrent en quelques détails. Dans VANETs au lieu de se déplacer au hasard, les véhicules tendent à se déplacer d'une façon organisée. La communication avec les équipements de la route est caractérisée de manière assez exacte. De plus, la majorité des véhicules sont limités au niveau de leur mouvement, par exemple suivre une route bien définie. Les réseaux véhiculaires sans fil contiennent deux entités: les véhicules et les points d'accès. Les points d'accès sont fixés et connectés généralement à l'Internet, et ils pourraient participer en tant que point de distribution pour les véhicules.

Dans cette première partie de notre mémoire, nous détaillerons en premier l'architecture et les caractéristiques des réseaux véhiculaires sans fil. Par la suite, nous présenterons les technologies d'accès ainsi que les standards de communication. À la fin de ce chapitre, nous aborderons l'aspect de la sécurité pour présenter les éléments, les services et les mécanismes de la sécurité dans ces réseaux.

2.2 Architecture et caractéristiques des réseaux véhiculaires sans fil

2.2.1 Architecture des réseaux véhiculaires sans fil

L'architecture des réseaux véhiculaires sans fil (VANETs) peut être décrite par plusieurs entités. Trois principales entités permettent d'établir la communication dans les réseaux VANETs [2] :

a. RSU

Les «RSUs» (Road Side Unit) sont des équipements externes aux véhicules installés au bord des routes. Ils diffusent vers les véhicules des informations liées à l'état du trafic, l'état de la route, ainsi que des informations météorologiques. Ils sont d'ailleurs utilisé comme des routeurs entre les véhicules.

b. OBU

Les «OBUs» (On-Board Unit) sont donc des équipements radio installés dans les véhicules qui permettent à ces derniers de se localiser et qui garantissent l'envoie et la réception des données sur l'interface réseau. Les «OBUs» utilisent les signaux DSRC (Dedicated Short Range Communication) pour communiquer avec les « RSU ».

c. Autorité centrale

L'autorité centrale ou l'autorité de confiance est un tiers de confiance qui a comme rôle de signer et délivrer les certificats numériques. L'autorité centrale (Central Authority: CA) peut aussi dans certaines circonstances révéler l'identité de l'expéditeur d'un message [4].

2.2.2 Modes de communication pour les réseaux VANET

Dans les réseaux de véhicules, on peut distinguer deux modes de communication, les communications Véhicule-à-Véhicule (V2V) et les communications Véhicule-à-Infrastructure (V2I) comme les montre la figure 1. Les véhicules peuvent choisir un de ces deux modes ou bien les combiner en cas d'échec de communication directe avec les infrastructures. Dans cette partie, nous présentons le principe et l'utilité de chaque mode :

a. Mode de communication Véhicule-à-Véhicule (V2V)

C'est un mode de communication qui ne nécessite pas d'infrastructure pour son fonctionnement. Dans ce mode de communication qui fonctionne en environnement décentralisé, chaque véhicule par l'intermédiaire de son OBU, communique directement avec les véhicules situés à sa portée (exemple 800 m de portée) ou bien peut jouer le rôle de relayeur de message dans le but de transmettre des messages aux autres véhicules. Ce mode de communication est très efficace pour la diffusion rapide des informations liées à la sécurité routière et autres données du trafic routier par contre la connectivité n'est pas permanente entre les véhicules [2].

b. Mode de communication Véhicule à Infrastructure (V2I)

Ce mode de communication offre une meilleure connectivité et permet l'accès aux divers services (par exemple : accès à Internet, échange de données de voiture à domicile, information météorologique, ...etc.) grâce à un échange d'informations entre les véhicules et les entités fixes (RSU et CA) disposées le long de la route.

Le mode V2I est inadéquat pour les applications liées à la sécurité routière puisque il n'est pas performant par rapport aux délais d'acheminement des paquets qui sont plus longs, ce délai est lié au fait que les entités fixes (RSU et CA) prennent plus de temps pour le traitement des paquets avant de les diffuser [4].

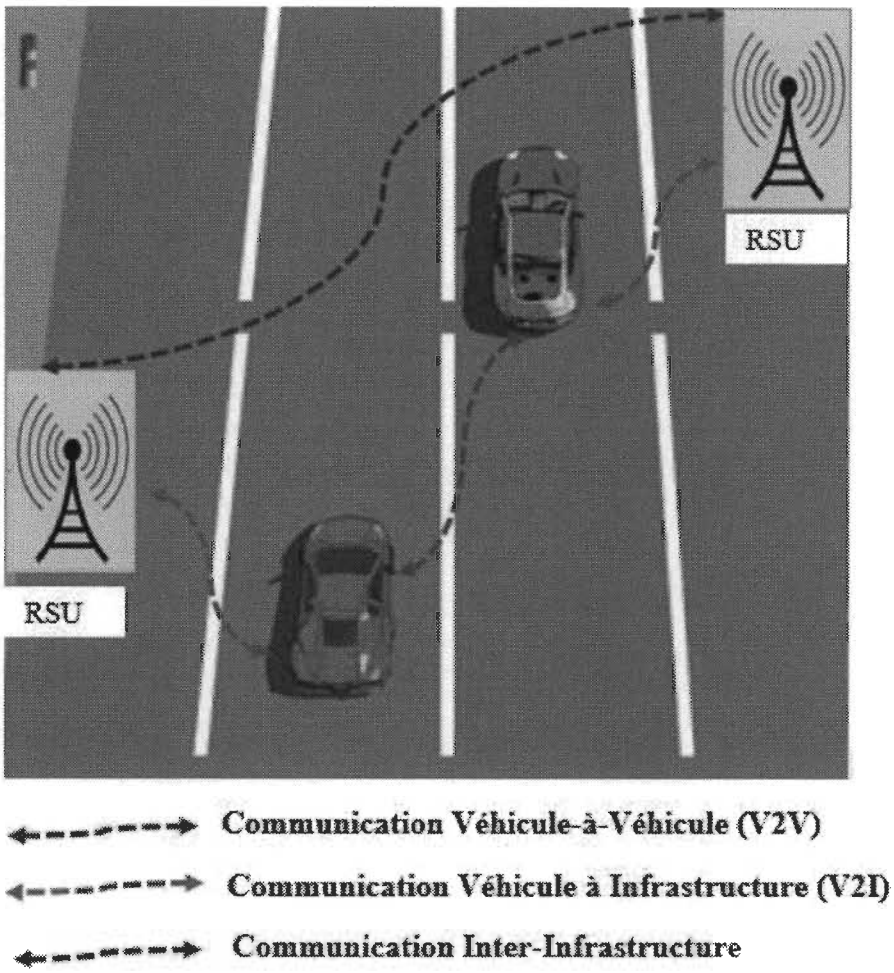

Figure 1: Modes de Communication dans les réseaux VANETs.

2.2.3 Les applications des réseaux VANET

Dans le réseau véhiculaire sans fil, on trouve plusieurs types d'applications ou services qu'on peut classer en 3 catégories [5] :

a. Applications liées au confort

Comme certains voyages peuvent parfois être longs, dû au trajet ou aux congestions sur la route, les réseaux VANETs contribuent également à l'amélioration du confort en permettant d'assurer le confort des véhicules et leurs occupants durant leurs voyages; ces services comprennent, entre autres l'accès à Internet, la messagerie, le chat inter – véhicule, etc.

L'utilisation de ce genre d'applications, permet aux passagers de s'échanger des musiques, vidéos ou d'accéder à des jeux. Aussi, on pourra procéder à la vérification à distance des permis de conduire, des plaques d'immatriculation par les autorités compétentes, le paiement électronique au niveau des points de péage afin de faire gagner du temps aux utilisateurs.

b. Applications d'optimisation et d'amélioration du trafic routier

Outre les services liés aux applications de confort, les réseaux sans fil véhiculaires contribuent également à l'optimisation et à l'amélioration du trafic routier en fournissant des informations sur l'état des routes. En effet, un véhicule peut être informé sur l'état de la circulation de son trajet actuel ou futur à partir des messages échangés par les différentes entités du réseau, ce qui donne la possibilité au conducteur de décider quelle route il peut suivre lorsque le trafic est dense sur un trajet et éviter ainsi la congestion. De plus et grâce à l'échange des informations entre les véhicules, il y aura la possibilité de créer le passage pour les voitures d'urgence, ou de proposer d'autres itinéraires aux véhicules qui sont dans une zone de congestion dans le but d'optimiser le trafic et de le rendre fluide [5] [6].

c. Applications de prévention et de sécurité du trafic routier

Comme les applications de préventions et de sécurité du trafic routier ont un impact direct sur la sécurité des personnes et des biens, les conducteurs peuvent être avertis des accidents ou autres situations dangereuses (alerte pour les travaux routiers, informations météorologiques) en recevant des messages d'alerte diffusés entre les différentes entités afin d'être plus vigilant et de réduire leur vitesse. Comme ces applications contribuent à

la diminution du nombre d'accidents sur les routes alors elles aident à préserver la vie humaine. Un service de ces applications qui est un service SOS en cas d'accident est déjà implémenté dans certaines voitures actuelles. Il consiste à envoyer un message afin de prévenir le secours le plus proche [5].

2.2.4 Types de messages

Trois types de messages s'échangent entre les différentes entités du réseau véhiculaire sans fil.

a. Les messages « beacon »

Aussi appelé message de contrôle ou d'identification, ils sont envoyés à intervalles réguliers, par convention. Un véhicule envoie un message « beacon » toutes les 100ms. Ils contiennent des informations personnelles sur les véhicules telles que: sa vitesse, sa position GPS (Global Positioning System), sa direction, etc. Grâce à ce type de message, les véhicules se font connaitre à leur entourage [5].

b. Les messages d'alerte

Ce sont des messages générés dans le cas d'un accident, de congestion, d'un obstacle sur la route, etc. Ils permettent d'améliorer la sécurité routière, et de gérer le trafic routier. Lorsqu'un accident survient dans une zone, un message d'alerte est émis, ce message doit être retransmis à intervalle régulier pour assurer que l'alerte est toujours valide. En effet grâce à ces messages, les nœuds mobiles peuvent réduire leurs vitesses ou trouver un autre itinéraire dans le cas d'un secteur à dense trafic routier. Le message de sécurité est généré lorsqu'un évènement qui mérite l'attention du conducteur est détecté. De plus, ces messages doivent être de taille réduite pour pouvoir être retransmis rapidement dans le réseau.

c. Les autres messages

Outre les messages « beacon » et d'alertes, les entités du réseau véhiculaire sans fil peuvent échanger des messages d'une application, de l'envoi de courriel, etc. Ces messages ne sont émis qu'une seule fois. De plus, les véhicules peuvent échanger des messages multimédias ce qui rend la route moins ennuyeuse et facile.

2.2.5 Environnement de déploiement

Les réseaux véhiculaires sans fil se distinguent principalement par plusieurs milieux de déploiement, on peut définir la circulation des voitures dans le réseau routier sur deux environnements:

a.Environnement urbain

Le milieu urbain est caractérisé par des intersections, des points d'arrêts (les panneaux Stop, le feu tricolore, etc.) et il exige une vitesse réduite jusqu'à un maximum de 50 km/h en ville [7]. C'est un environnement qui présente une forte perturbation des ondes radio causée par la présence des bâtiments, des maisons et autres [5]. De plus, dans ce milieu on peut avoir une bonne connectivité entre les véhicules et une communication ad hoc facile grâce au faible intervalle entre les nœuds. L'installation des infrastructures routières en milieu urbain reste un problème complexe (exemple : insuffisance de place).

b. Environnement autoroutier

Le milieu autoroutier est caractérisé par une vitesse qui varie entre 60 et 100 km/h au Québec [8], de longues routes avec des voies d'accélération et des points de sorties. Comme la vitesse de certains nœuds mobiles est excessive, alors l'écart entre les voitures est important, ce qui entraine une perte de connectivité des nœuds mobiles du réseau voire même une difficulté de la communication en mode ad hoc. L'utilisation les entités fixes (RSU et CA) peut garantir une meilleure connectivité dans cet environnement afin de permettre à toutes les entités mobiles de bénéficier de toutes les fonctionnalités du réseau.

2.2.6 Caractéristiques des VANETs

Les réseaux véhiculaires sans fil ont des caractéristiques propres même s'ils possèdent une spécificité des réseaux sans fil ad hoc mobiles. Les caractéristiques et contraintes techniques sont présentées ci-dessous.

a. Capacité d'énergie et stockage

Les réseaux véhiculaires sans fil disposent d'une source énergétique importante grâce au système d'alimentation véhiculaire qui se renouvèle dans le temps, ce qui implique que ce type de réseau ne souffre pas de problème d'énergie [9] [10].

b. Topologie très dynamique

La topologie des VANETs est très dynamique à cause de la vitesse de circulation des véhicules. Par exemple, pour deux véhicules qui roulent dans le sens opposé avec une vitesse de 25 m/s, s'il existe une liaison sans de fil de portée 250 m entre ces deux véhicules, alors la connectivité entre les deux voitures ne durera que 10 s [11]. On remarque donc que la réorganisation de la topologie du réseau est fréquente.

c. Connectivité

Comme les réseaux VANETs se caractérisent par la forte topologie dynamique, alors, la connectivité est de courte durée surtout lorsque la densité des véhicules est très faible. Afin d'améliorer la connectivité, il faut un déploiement de plusieurs nœuds relais ou points d'accès le long de la route, ce qui permettrait la retransmission de l'information sur de longues distances [11].

d. Modèle de communication

Les types de communication se basent sur la diffusion des messages d'une source vers plusieurs destinataires et on l'appelle communication broadcast. Aussi, une communication unicast peut être établie entre les entités [5].

e. Géolocalisation

Afin de localiser et de faciliter la communication entre les différentes entités du réseau, des systèmes de localisation par satellite comme les GPS sont utilisés dans les réseaux VANETs.

f.Mobilité

Les réseaux VANETs se caractérisent par une mobilité extrêmement élevée. Cette mobilité peut être affectée par plusieurs facteurs comme la vitesse des nœuds, le comportement des conducteurs sur les routes ainsi que les infrastructures routières (routes, panneaux de signalisation, etc.)[2].

2.3 Normes et standards

Diverses méthodes de communication sont disponibles dans les réseaux véhiculaires, tels que le WiFi , le WiMAX et le DSRC (Dedicated Short Range Communication) [4], dont la couche physique est basée sur la norme IEEE 802.11a.

2.3.1 DSRC

Dedicated Short Range Communication (DSRC) est considéré comme le standard le plus approprié pour les communications sans fil dans les réseaux véhiculaires [12]. Cette technologie a évolué à partir de la norme IEEE 802.11a vers la norme IEEE 802.11p afin de répondre aux caractéristiques des réseaux VANETs. Grâce au standard DSRC, il est possible d'établir une communication véhicule-à-véhicule ainsi qu'une communication véhicule-à-infrastructure. Le standard DSRC est compatible avec les contraintes des réseaux véhiculaires dynamiques. En effet, il offre une fiabilité de communication ainsi qu'une faible latence lors de l'établissement de la communication.

Les caractéristiques du DSRC sont [11] :

- Il supporte une vitesse des véhicules dépassant 200 km/h.
- Il offre une portée radio variant entre 300 et 1000 mètres.

- Il garantit un temps de latence pour l'établissement de la communication ne dépassant pas 50 ms.
- Il permet un débit théorique (bande passante) atteignant 6 Mbps.

2.3.2 IEEE 802.11 p

En 2003, le groupe de travail IEEE a défini un nouveau standard dédié aux communications inter-véhicules, nommé WAVE (Wireless Ability in Vehicular Environments) et aussi connu sous le nom 21 de IEEE 802.11p [13]. Cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité et les autres services du Transport Intelligent.

IEEE 802.11p est généralement une variante personnalisée de IEEE 802.11a avec une couche physique adaptée pour permettre un fonctionnement à faible charge dans le standard DSRC [13].

La norme IEEE 802.11p est capable d'offrir un débit entre 6 et 27 Mbps (pour des distances jusqu'à 1000 mètres) [13]. De plus, la couche MAC du 802.11p reprend le principe du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) développé dans le protocole MAC de l'IEEE 802.11, pour gérer la qualité de service et le support du protocole de marquage de priorité [13] [9].

2.4 Les exigences de la sécurité

Il est primordial que les exigences de la sécurité doivent toujours respecter le bon fonctionnement d'un système afin de garantir la sécurité de ce dernier. Lorsqu'un requis n'est pas respecté, celui-ci présente un problème de sécurité. Les requis que doivent respecter les réseaux véhiculaire VANET ont été discuté dans [14] [15] [16] [17], il s'agit donc de: l'authentification, l'intégrité, la confidentialité, la non-répudiation, le contrôle d'accès, les contraintes de temps réels et la protection de la vie privée. Dans la suite nous détaillons ces différents requis.

2.4.1 L'authentification

L'authentification est un requis principal de tout système. Pour les VANETs, il est nécessaire de connaitre les informations liées aux nœuds émetteurs tels que son identifiant, sa position géographique, son adresse et ses propriétés. Cette exigence a pour objectif principal de contrôler les niveaux d'autorisation du véhicule dans le réseau. Dans les VANETs, l'authentification aide à la prévention des attaques telle que l'attaque Sybil en spécifiant un identifiant unique pour chaque véhicule et de cette manière ce dernier ne pourra pas réclamer d'avoir plusieurs identifiants afin de provoquer le mauvais fonctionnement du réseau [14] [18].

Plusieurs types d'authentifications ont été présentés dans [14] [19] :

- **L'authentification de l'ID :** Un nœud doit être capable d'identifier les transmetteurs d'un message donné de façon unique. A partir de cette authentification, un véhicule émetteur peut accéder au réseau.

- **L'authentification de la propriété :** Ce type d'authentification peut déterminer si le type d'équipement qui est en communication est un autre véhicule, un « RSU » ou encore d'un autre équipement.

2.4.2 L'intégrité

L'intégrité assure le non changement du message entre l'émission et la réception. Le récepteur du message vérifie le message reçu en s'assurant que l'identifiant de l'émetteur n'a pas changé au cours de transmission, et que le message reçu est bien celui qui a été envoyé [14] [20]. L'intégrité protège contre la modification, la duplication, la réorganisation et la répétition des messages pendant la transmission. L'intégrité des messages est gérée par des mécanismes qui reposent sur des fonctions mathématiques à sens unique tels que les fonctions de hachage et le code d'authentification de message MAC [5].

2.4.3 La confidentialité

La confidentialité des messages dans les VANETs dépend de l'application et du scénario de communication. Elle permet aux différents nœuds d'avoir confiance dans les messages diffusés dans le réseau. Il existe deux types d'authentification: une pour les messages et l'autre pour les entités. L'authentification des messages permet de retracer la source du message alors que celle des entités permet d'identifier les nœuds du réseau. La confidentialité peut être mise en place en utilisant la clé public/privé pour les cryptages du message durant la communication [5] [15]. Par exemple dans les communications V2I, les « RSU » et le véhicule se partagent une clé de session après avoir effectué une authentification mutuelle, aussi tous les messages sont cryptés avec la clé de session et attachés avec un code d'authentification du message [14] [19].

2.4.4 La non répudiation

Le but de la non-répudiation est de collecter, de maintenir et de rendre disponibles toutes les informations liées à la certitude de l'entité diffusant des messages, afin d'éviter les conséquences néfastes que peuvent présenter les applications de sécurité routière sur les biens et les personnes. La non-répudiation dépend donc de l'authentification. Dans ce cas, la mise en place de la politique de non-répudiation dans les réseaux VANETs permet au système d'identifier l'entité qui diffuse un message malveillant [14] [28]. Pour les messages des applications de sécurité et de gestion du trafic routier généralement, c'est la signature numérique qui est utilisée pour garantir le non répudiation. Quant aux messages des applications de gestion de confort, la non-répudiation n'est pas aussi nécessaire sauf pour les messages impliquant des transactions financières [10].

2.4.5 La disponibilité

Le principe de la disponibilité repose sur le fait que toutes les entités du réseau ont un accès permanent à des services ou des ressources, donc les services des applications de gestions du trafic routier, de sécurité et de confort doivent être toujours disponibles pour les véhicules. Afin d'assurer cette permanence des services, les réseaux véhiculaires

doivent empêcher les attaques de déni de service en utilisant certaines techniques comme le saut de fréquence et le changement de technologie [5] [21].

2.4.6 Le contrôle d'accès

Le contrôle d'accès a pour rôle de déterminer les droits et les privilèges dans les réseaux. Plusieurs applications se différencient en fonction des niveaux d'accès accordés aux entités du réseau. Par exemple, les applications de contrôle des feux tricolores peuvent être installées dans les voitures de police, de secours afin de faciliter le déplacement de ces dernières. Aussi certaines communications comme celles de la police ou d'autres autorités ne doivent pas être écoutées par les autres usagers. Il est donc primordial de mettre en place un système qui permet de définir toutes ces politiques d'accès pour garantir le contrôle d'accès dans le réseau [22].

2.5 Conclusion

Dans ce chapitre, nous avons décrit l'architecture et les caractéristiques des réseaux véhiculaires sans fil et présenté aussi les requis de sécurité que doivent respecter un réseau VANET. En raison du dynamisme et de l'évolution l'environnement VANETs au cours du temps, la mise en œuvre des algorithmes de routage des réseaux véhiculaires sans fil demeure un problème complexe. Donc, il faut trouver un protocole de routage qui garantit la transmission d'information en tenant compte de la complexité de l'environnement VANET.

Avant d'étudier notre protocole de routage d'information qui répond aux contraintes des réseaux véhiculaire, nous allons présenter dans le prochain chapitre, quelques travaux de la littérature qui sont liés aux protocoles de routage des réseaux VANETs.

Chapitre 3 -Revue de littérature

3.1 Introduction

Le routage est un élément crucial dans les réseaux véhiculaires. Bien qu'il existe dans la littérature des protocoles pour étendre les réseaux MANET, la plupart des protocoles existants ne s'adaptent pas bien aux VANETS [22] [23]. Ceci est dû à l'environnement très dynamique dans les réseaux véhiculaires ce qui implique des changements fréquents au niveau de la topologie du réseau. Afin de garantir la transmission continue des messages dans le réseau véhiculaire, il faut que le protocole de routage prenne en considération les caractéristiques du réseau VANET. Et comme les réseaux VANETs sont un moyen de communication ouvert, cela peut construire une cible idéale pour les attaques qui pourraient intercepter les messages avant d'arriver à leurs destinations, ce qui implique que le protocole de routage peut être vulnérable vis-à-vis des attaques.

Dans le présent chapitre, nous présentons quelques travaux sur les protocoles de routage et sur les menaces dans les réseaux VANETs.

3.2 Le routage dans VANET

3.2.1 Problèmes de routage dans VANET

En raison de la nature dynamique des nœuds mobiles dans le réseau, la découverte et le maintien des routes semblent une tâche très difficile en VANETs. Pour cela, il faut que toute conception de protocole de routage prenne en considération les problèmes suivants :

- La minimisation de la charge du réseau en évitant les boucles de routage et en empêchant la concentration du trafic autour de certains nœuds ou liens.
- L'évolution des chemins de transfert des données ne doit pas avoir des conséquences sur la bonne circulation des paquets.

- La stratégie de routage doit assurer un maintien des routes efficace et avec des faibles coûts en créant des chemins optimaux tout en prenant en compte la bande passante, les nombres des liens, etc.

- Lorsque la connectivité du réseau augmente la qualité du temps de latence et des chemins doit augmenter aussi.

3.2.2 Quelques protocoles de routage

3.2.2.1 Le protocole de routage GeOpps (Geographical Opportunistic routing)

GeOpps [24] [25] est un protocole qui réduit les délais de transmission d'un paquet entre les nœuds capables de router le plus rapidement possible les paquets vers une région géographique prédéfinie. Les auteurs dans [24] [25] ont montré aussi que pour GeOpps chaque véhicule connait l'adresse de la destination du paquet ainsi que sa propre trajectoire récupérée par un système de géo-positionnement. En utilisant ces informations, chaque véhicule calcule les coordonnées du point le plus proche de la destination par rapport à sa trajectoire ainsi que la durée nécessaire pour atteindre la destination. Le mécanisme de retransmission et la sélection du nœud relais suivant, se base essentiellement, sur la durée minimale estimée pour arriver au point de destination.

3.2.2.2 Le protocole de routage GPSR (Greedy Perimeter Stateless Routing)

GPSR (**G**reedy **P**erimeter **S**tateless **R**outing) est un protocole de routage réactif qui utilise la position géographique des nœuds pour l'acheminement des paquets de données ou de contrôle. Dans GPSR, les nœuds diffusent dans le réseau un paquet de signalement (messages « beacon») contenant la position et un identifiant (par exemple, son adresse IP). L'échange périodique de ces paquets de contrôle permet aux nœuds de construire leur table de positions. La période d'émission des messages « beacon » dépend du taux de mobilité dans le réseau ainsi que de la portée radio des nœuds. En effet, lorsqu'un nœud ne reçoit pas de message « beacon » d'un voisin après un temps T, il considère que le voisin en question n'est plus dans sa zone de couverture et l'efface de sa table de positions. Il faut donc adapter le temps d'émission des paquets de contrôle. GPSR permet au nœud d'encapsuler sur quelques bits leur position dans les paquets de données qu'il envoie. Dans ce cas, toutes les interfaces des nœuds doivent être en mode promiscuité afin de recevoir les paquets s'ils se trouvent dans la zone de couverture de l'émetteur.

Dans [26] [27], les auteurs ont montré que l'acheminement des paquets par GPSR se fait selon deux modes suivant la densité du réseau : le « GreedyForwarding » et le « PerimeterForwarding » appelés respectivement GF et PF.

- **GreedyForwarding:**

Le GF construit un chemin parcourant les nœuds de la source à la destination où chaque nœud qui reçoit un paquet l'achemine en faisant un saut vers le nœud intermédiaire le plus proche de la destination dans sa zone de couverture.

- **PerimeterForwarding:**

Cet algorithme utilise la règle de la main droite: Lorsqu'un paquet arrive à un nœud x du nœud y, le chemin à suivre est le prochain qui se trouve dans le sens inverse des aiguilles d'une montre en partant de x et par rapport au segment [xy] tout en évitant les routes déjà parcourue.

3.2.2.3 Le protocole de routage GPCR (Greedy Perimeter Coordinator Routing)

Les auteurs Marwa Altayeb et Imad Mahgoub [28] ont montré que l'idée principale de GPCR est de profiter du fait que les rues et les carrefours forment un graphe planaire naturelle, sans utiliser l'information globale ou externe comme une carte de rue statique.

GPCR englobe deux parties : Une procédure « restricted greedy forwarding » et une stratégie de réparation qui est basée sur la topologie des rues et les carrefours du monde réel et donc ne nécessite pas un algorithme graphique d'aplanissement qui est un algorithme qui utilise le graphe planaire qui a la particularité de pouvoir se représenter sur un plan sans qu'aucune arête n'en croise une autre.

- **Restricted Greedy Forwarding**

C'est une forme particulière de « Greedy Forwarding », elle est utilisée pour transmettre un paquet de données vers la destination dans lequel les carrefours sont les seuls endroits où les décisions de routage sont prises. Par conséquent les paquets doivent toujours être transmis à un nœud sur un carrefour plutôt que d'être transmis à travers un carrefour.

3.2.3Classification des protocoles de routage

L'objectif principal pour le protocole de routage est de fournir des chemins optimaux entre les nœuds du réseau.

Selon les auteurs Marwa Altayeb et Imad Mahgoub [28] de nombreux protocoles de routage ont été développés pour l'environnement VANETs, qui peuvent être classés de plusieurs façons et selon différents aspects; tels que: les caractéristiques des protocoles, des techniques utilisées, les informations de routage, la qualité des services, les structures de réseau, des algorithmes de routage, et ainsi de suite.

Certaines recherches ont classé les protocoles de routage VANETs en cinq classes: la topologie, la position, la transmission « geocast », la transmission broadcast et les protocoles de routage basés sur les « clusters » [29] [30] [31].

Aussi, dans d'autres travaux, les protocoles de routage VANETs ont été classés selon les structures de réseau, en trois classes: routage hiérarchique, routage plat, et routage basée sur la position. Selon Vijayalaskhmi M. et al. dans [32], les protocoles de routage pour VANETs peuvent être classés en deux catégories en fonction des stratégies de routage: proactif et réactif.

D'autre chercheurs ont classé les protocoles de routage en deux catégories: à base de la position géographique et à base topologique selon les informations de routage utilisé dans la transmission des paquets [33].

Dans [28] deux types de classification sont présentés, la première est basée sur l'information de routage utilisé dans la transmission des paquets et la deuxième classification est basée sur les stratégies de transmission, qui présente un impact significatif dans la conception du protocole et sur les performances du réseau.

3.2.4Comparaison entre les protocoles de routage dédiés pour VANETS

3.2.4.1 Comparaison entre les protocoles de routage basés sur la stratégie de transmission

La transmission de l'information à partir d'une source vers une destination peut être classée en quatre types: unicast, broadcast, multicast et Geocast [28]. On peut considérer que la transmission multicast et la transmission geocast peuvent être fusionnées dans une seule classe puisque la transmission « geocast » est habituellement un type spécial de transmission multicast.

Le routage unicast se réfère à la transmission de l'information à partir d'une source unique vers une destination unique en utilisant une communication multi-sauts, où les nœuds intermédiaires ont comme rôle la transmission des données de la source à la destination, ou bien en utilisant la stratégie de stockage et transmission. Toujours dans [28], les auteurs ont montré que c'est la classe la plus utilisée dans les réseaux ad hoc; selon cette stratégie, le véhicule source conserve ses données pendant un certain temps, puis les transmet. Il existe de nombreux protocoles de routage unicast proposées pour VANETs. La plupart des protocoles de routage basés sur la topologie appartiennent à une classe unicast; comme VADD, DSR (Dynamic Source Routing) et beaucoup d'autres.

Pour le routage broadcast, les chercheurs dans [28] ont expliqué que les paquets se diffusent dans le réseau et vers tous les nœuds disponibles à l'intérieur du domaine de diffusion. Le routage broadcast est largement existant dans VANETs, il est principalement utilisé dans le processus de découverte de routes et certains protocoles autorisent les nœuds de retransmettre les paquets reçus. Cette stratégie de routage permet l'envoie des paquets par l'intermédiaire des nœuds qui peuvent réaliser une transmission fiable des paquets, mais il y a un risque de consommer la bande passante du réseau en envoyant des paquets répétés.

Le tableau 3.1 présente une comparaison entre les différentes stratégies de transmission

Stratégies de transmission	Méthodes utilisé	Avantages	Limitations	Commentaires	Exemples
Unicast	-Transmission de l'information à partir d'une source unique vers une destination unique	-Moins de surcharge de réseau -Plus de confidentialité -Moins de retard pour envoyer le paquet	-Les liens doivent être fréquemment configurés et maintenu -Moins de fiabilité -Perte des paquets	-Avoir plus de recherches pour améliorer la fiabilité, de retransmission de paquets, l'évolutivité et éviter la collision	-GPSR (Greedy Perim eter Stateless R outing) -GPCR (Greedy Perimeter Coordinator Routing) -DSR(Dynamic Source Routing)
Broadcast	-Diffusion des paquets à tous les nœuds de réseau à l'intérieur du domaine de diffusion	-Transmission des données plus fiables -Moins de perte des paquets	-Consomme la bande passante -Problème des boucles -Encombre ment du réseau -Faible débit du réseau -Plus de retard -Collisions des paquets	-Nécessité de réduire la consommation de bande passante -Pourrait être utile pour les messages d'alerte	-DADCQ (Disribution Adaptative Distance with Channel Quality) -DVCAST (Disribution Vehicular Broadcast)

Multicast	-Transmission Geocast des paquets à partir d'une source à un groupe de destinations en utilisant des adresses géographiques. -Division du réseau en clusters, chaque cluster a un « cluster head » qui gère la communication à l'intérieur et à l'extérieur du cluster.	-Un routage efficace en envoyant une copie à plusieurs nœuds -Moins de consommation du réseau -Moins de retard lors de transmission de paquet -Facile à mettre en œuvre -Transparent à des adresses variables (aucune exigence à l'adresse du destinataire)	-Consomme la bande passante -Plus de surcharge en divisant les nœuds du réseau en cluster -Problème de boucle	-Contrôle de l'évolutivité pour les clusters dynamiques -Le cluster peut ne pas très efficace car le « cluster head » change fréquemment	-ROVER (Robust Vehicular Routing) -MOBICAST(Mobile Multicasting Protocol)

Tableau 1 : Comparaison entre les différentes stratégies de transmission

3.2.4.2 Comparaison entre les protocoles de routage basé sur la topologie et le routage basé sur la position

Dans [28], ont présenté les inconvénients et les avantages de ces deux types de routage. Le principal inconvénient des protocoles de routage basé sur la topologie est l'instabilité de la route. En effet, une route établie se compose d'un ensemble de nœuds entre la source et la destination et la communication échoue fréquemment à cause de la grande mobilité des véhicules.

Le second inconvénient est la surcharge élevée au niveau du routage qui est due aux messages « beacon » et aux messages « Hello » utilisés pour découvrir et confirmer les routes de transmission des paquets et pour maintenir les chemins trouvés.

Une autre limitation de la catégorie basée sur la topologie est le délai de transmission élevé surtout quand le réseau est moins dense et un retard important suite aux mises à jour des itinéraires découverts. Les protocoles de routage à base topologique souffrent du problème de perte des paquets causé par la nature dynamique de l'environnement VANET. Toutes ces limitations ne se trouvent pas au sein des protocoles basés sur la position qui offrent une stabilité au niveau des routes découvertes mais qui présentent au même temps d'autres inconvénients [28].

Concernant le routage basé sur la position, plusieurs chercheurs ont montré que ce type de routage présente aussi quelques limitations, le premier inconvénient est la difficulté de trouver le nœud suivant optimale lors de la recherche de destination, en particulier dans le scénario de ville.

Le deuxième inconvénient est dû aux boucles inhérentes causées par la mobilité du véhicule et de ses positions strictes lors de la découverte ou du maintien des routes. Ces boucles peuvent conduire à la perte de la capacité de mémoriser l'historique du trafic passé, ce qui peut aider à prévenir le lancement d'un nouvel itinéraire de découverte. Un autre inconvénient des algorithmes de routage basé sur la position est l'utilisation d'un dispositif

GPS qui peut échouer à cause de diverses raisons telles que la présence d'obstacles ou les conditions atmosphériques qui pourraient bloquer le signal GPS. Le tableau 3.2 présente une comparaison entre le routage basé sur la topologie et celui basé sur la position.

Les protocoles de routage VANETs	Méthodes utilisées	Avantages	Limitations	Commentaire	Exemples
Routage basé sur la topologie	-Les informations de liaison sont stockées dans la table de routage en tant que base pour la transmission d'un paquet.	-La route la plus courte de la source vers la destination est la route choisie pour la transmission du paquet -Support des messages unicast, multicast et broadcast -Moins de consommation de ressource -L'utilisation des messages « beacon » -Économise de la bande passante	-Plus de surcharge de réseau -Retard au niveau de la découverte et le maintien des routes -Échec lors de la découverte de chemin de transmission	-Ces protocoles sont généralement proposés pour les MANET -Peut être utile pour les petits réseaux (moins de la surcharge)	-ZRP (Zone Routing Protocol) -FSR (Fisheye State Routing) -OLSR (Optimized Link State Routing)

Routage basé sur la position	-Il se base sur les informations de position des véhicules -Utilise les messages « Beacon » -Utilise les services de positionnement global	-Pas besoin de créer et de maintenir des routes globales -Plus stable dans un milieu à haute mobilité -Plus approprié pour les nœuds de réseau distribué -Moins de surcharge -Plus évolutive	-Obstacles dans le scénario de la ville -Problème de blocage dans le serveur de localisation -Services de position peuvent échouer dans le tunnel ou à la présence des obstacles (manque signal satellite)	-Plus approprié pour VANETs, avec une amélioration au niveau de contrôle de la congestion	MOVE (Motion Vector Routing) GeOpps (Geographical Opportunistic Routing) HLAR (Hybrid Location -Based Ad Hoc Routing)

Tableau 2 : Comparaison entre le routage basé sur la topologie et le routage basé sur la position.

3.3 Les attaques dans les réseaux VANETs

Pour assurer une communication efficace dans les réseaux véhiculaires, plusieurs protocoles de routage ont été conçus, mais ces réseaux sont vulnérables à plusieurs menaces en présence de nœuds malveillants. Donc les réseaux véhiculaires ad hoc ont besoin de sécurité pour mettre en œuvre l'environnement sans fil et servir les utilisateurs avec des applications sécurisées. Sans les mesures de sécurité adéquates dans le réseau, les informations peuvent ne jamais arriver à destination, ou devenir des menaces et devenir la cause d'accident.

Dans cette section, nous examinons quelques attaques de routage dans les réseaux VANETs.

a. L'attaque Déni de Service (DoS) :

Selon Sumra, I.A., et al [34], le but de ce type d'attaque est de rendre le réseau dysfonctionnel. L'attaque Déni de Service (DoS) consiste à rendre les différentes ressources et les services indisponibles pour les utilisateurs dans le réseau VANETs. Dans ce type d'attaques, l'entité malveillante peut bloquer le canal après la transmission des messages falsifiés et donc, interrompre la connexion réseau. L'attaque Déni de service peut être générer en diffusant à plusieurs reprises des faux messages avec des signatures non valides pour consommer la bande passante ou d'autres ressources du véhicule ciblé. L'impact de cette attaque est que, le réseau VANET perd sa capacité à fournir des services aux véhicules légitimes. La figure 2 illustre l'attaque déni de service dans laquelle un véhicule malveillant transmet un message erroné à un RSU et également un véhicule légitime derrière lui afin de créer un bourrage dans le réseau.

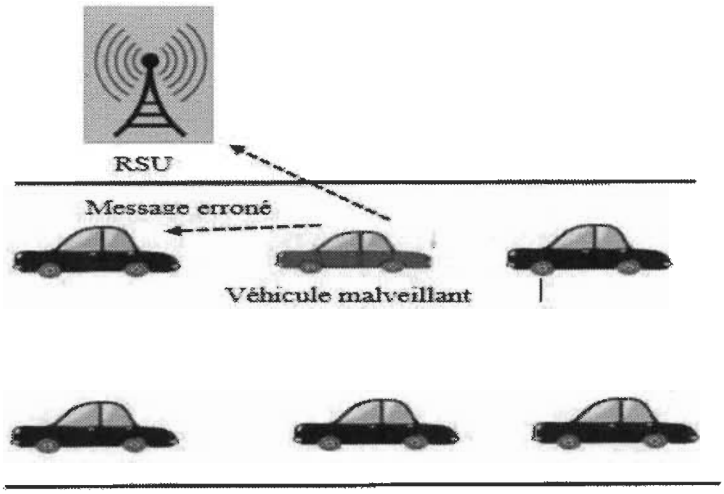

Figure 2 : L'attaque Déni de Service.

b. L'attaque Black Hole (Trou noir) :

Selon Al-kahtani [35], l'attaque « Black Hole » est dû à un nœud malveillant qui prétend avoir une route optimale pour la destination et qui indique que le paquet devrait être acheminé par lui en transmettant de fausses informations de routage. L'impact de cette attaque est que le nœud malveillant peut soit détruire ou utiliser improprement les paquets interceptés sans les transmettre. La figure 3 illustre une attaque « Black Hole » où une région « Black Hole » est créée par un certain nombre de véhicules malveillants et qui refusent de diffuser les messages reçus des véhicules légitimes pour les autres véhicules légitimes derrière eux.

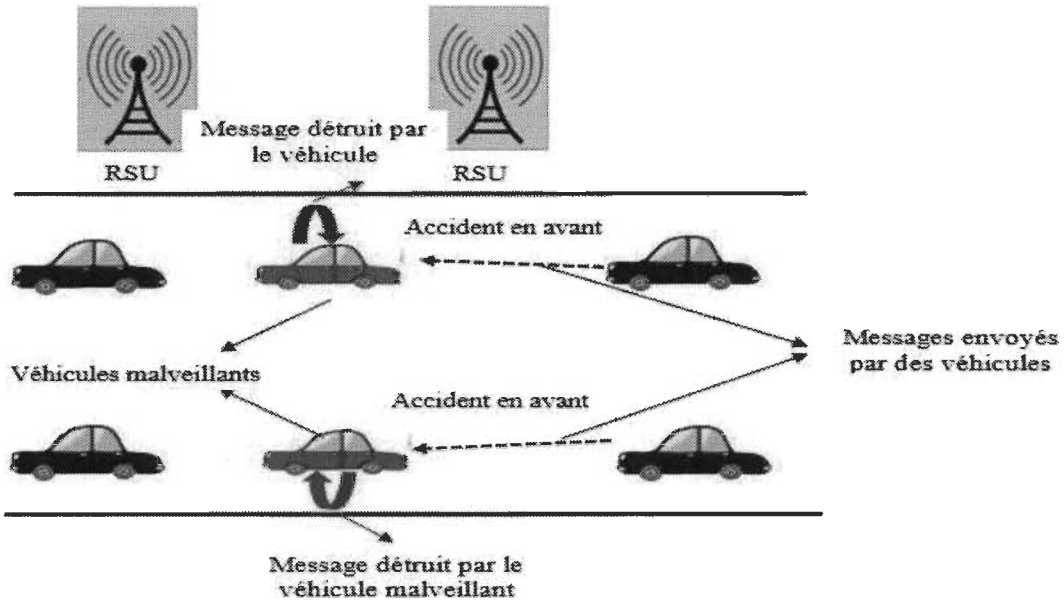

Figure 3 : L'attaque « Black Hole ».

c. L'attaque « Wormhole » (Trou de vers)

Dans l'attaque « Wormhole » et selon Hu, Y.-C., A. Perrig [36], un véhicule malveillant reçoit les paquets de données à un point dans le réseau et les retransmet à un autre véhicule malveillant en utilisant un lien « wormhole » à haut débit (tunnel) et par conséquence la communication de la source vers la destination passe par ces véhicules malveillants. L'impact de cette attaque est qu'elle empêche la découverte de routes valides et menace la sécurité de la transmission de paquets de données. La figure 4 illustre une attaque « Wormhole » où deux véhicules malveillants utilisent un tunnel pour diffuser des informations privées.

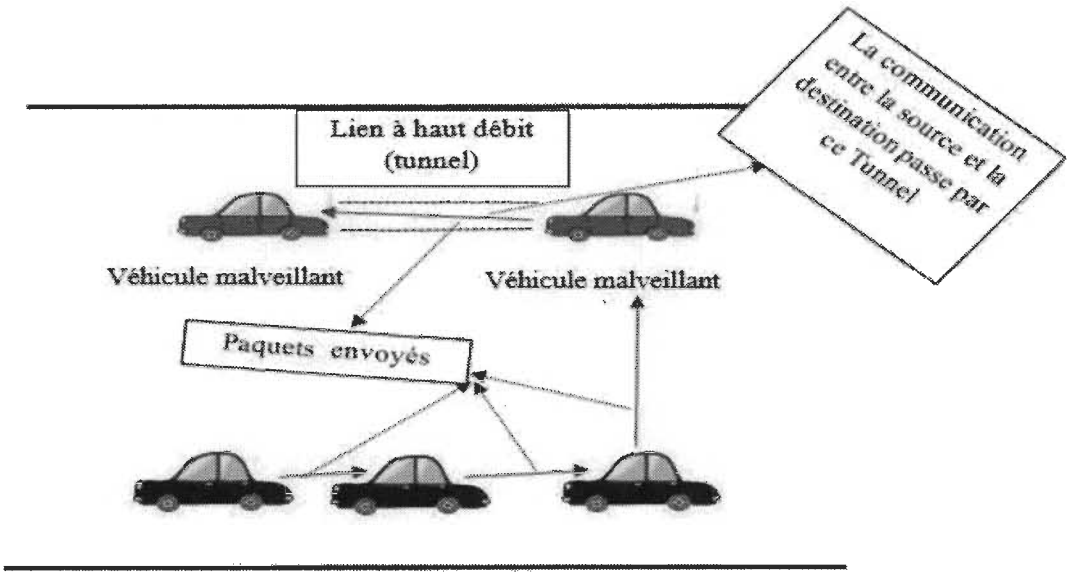

Figure 4 : L'attaque « Wormhole ».

d. L'attaque « Sinkhole »

Ngai, E.C.H., L. Jiangchuan, et M.R. Lyu [37] ont définit l'attaque « Sinkhole » comme un véhicule malveillant qui diffuse des fausses informations de routage de sorte qu'il peut facilement attirer tout le trafic réseau vers lui. L'impact de cette attaque est qu'elle rend le réseau compliqué et dégrade les performances du réseau, soit en modifiant les paquets de données ou en les détruisant.

La figure 5 illustre une attaque « Sinkhole » dans laquelle un véhicule malveillant supprime les paquets de données reçus à partir d'un véhicule légitime et diffue de fausses informations de routage pour les véhicules légitimes derrière lui.

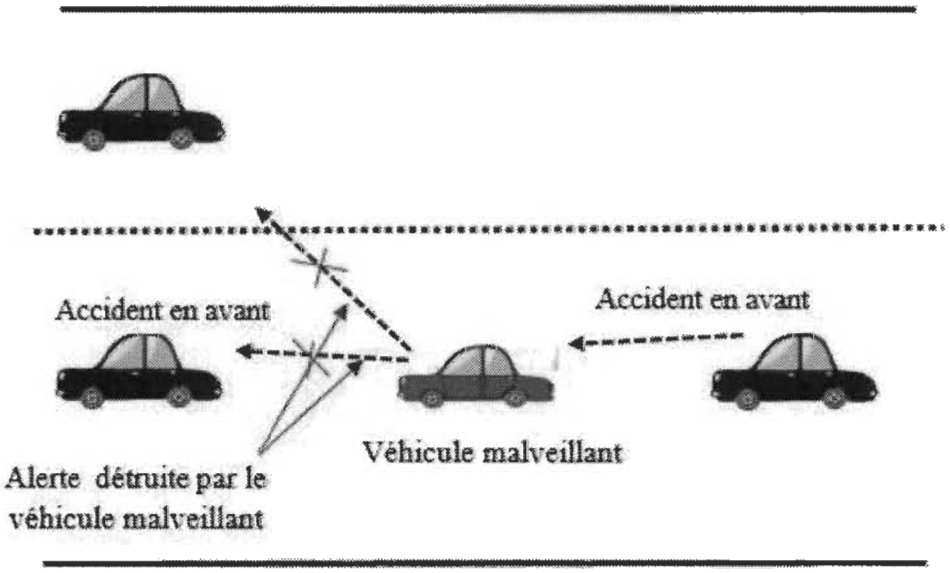

Figure 5 : L'attaque « Skinhole ».

e. L'attaque Illusion

Al-kahtani [35], a décrit cette attaque de cette manière : l'attaquant tente volontairement de manipuler ses lectures de capteur pour donner des informations falsifiées au sujet de son véhicule. En conséquence, il sera capable de diffuser des faux messages d'avertissement de trafic aux voisins.

L'impact de cette attaque est qu'il peut facilement changer le comportement du conducteur en diffusant des informations de trafic erronées et ça peut causer des accidents, des embouteillages et réduire l'efficacité du réseau véhiculaire en détruisant la consommation de la bande passante. Selon Lo, N.-W et H.-C. Tsai [38], les approches de l'intégrité et de l'authentification des messages existants ne peuvent pas sécuriser les réseaux contre cette attaque, parce que l'attaquant provoque une manipulation directement sur le véhicule visé pour rapporter de fausses informations.

La figure 6 illustre une attaque Illusion où un véhicule malveillant diffuse les messages d'avertissement de trafic erronés aux véhicules de leur quartier.

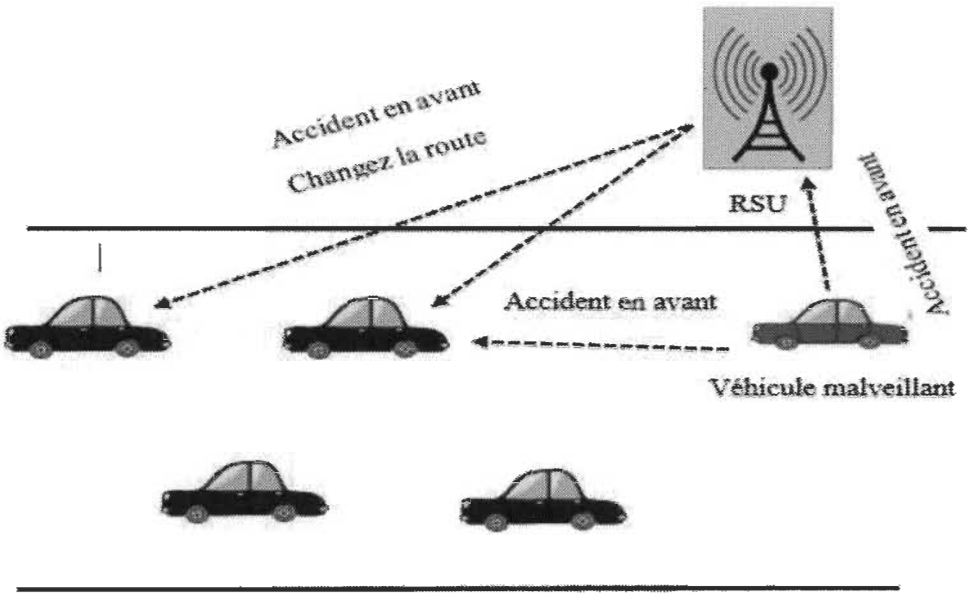

Figure 6 : L'attaque Illusion.

f.L'attaque Sybil

Pour le chercheurs Douceur [39], une attaque Sybil est un véhicule malveillant qui crée un grand nombre de fausses identités afin de prendre le contrôle de tout le réseau VANET et injecte de fausses informations dans le réseau afin d'endommager les véhicules légitimes. L'attaque Sybil a un fort impact sur la performance de VANET en créant une illusion sur l'existence de plusieurs véhicules dans le réseau. L'impact de cette attaque est que, après la falsification des identités ou des positions des autres véhicules en réseau véhiculaire, cette attaque peut conduire à d'autres types d'attaques. La figure 7 illustre une attaque Sybil dans laquelle un véhicule malveillant crée un certain nombre de fausses identités de véhicules et produit une illusion d'un nombre supplémentaire de véhicules sur la route.

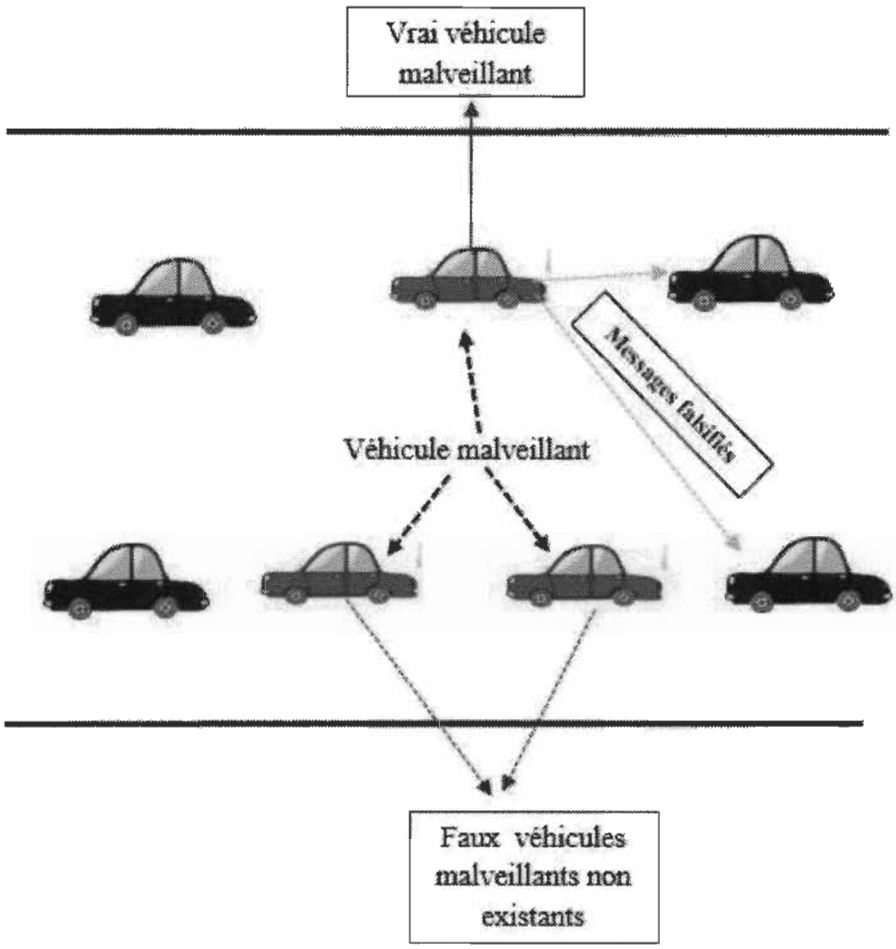

Figure 7 : L'attaque Sybil.

3.4 Les systèmes de détection d'intrusion dans les VANETs

Puisque les réseaux VANETs sont un moyen de communication ouvert, alors comme nous l'avons vu précédemment cela peut constituer une cible idéale de nombreuses attaques. Les IDS (systèmes de détection d'intrusion) sont des systèmes capables de repérer n'importe quel type d'attaque dans le réseau, dans [40][41][42] les auteurs ont montré que les IDS peuvent être classifiés selon les techniques de détection utilisées telles que les systèmes de détection d'anomalie qui détectent tout comportement qui n'est pas normal et déclenchent une réponse et les systèmes qui sont basé sur les signatures et qui possèdent une base de données de certaines attaques avec laquelle il

compare tout comportement anormal détecté. Les chercheurs dans [40] [41] [42] ont aussi parlé de système basé sur des spécifications ou il définit un ensemble de conditions qu'un protocole doit satisfaire. Dans ce cas l'attaque sera détectée si le programme ou le protocole ne respecte pas les conditions établies pour le bon fonctionnement. Dans [43] les chercheurs ont montré que les IDS peuvent être classés selon leurs architectures : des IDS autonomes, distribués et coopératifs et hiérarchiques.

Dans [44], les auteurs ont présenté un IDS basé sur «l'immunocomputing» et sur les systèmes immunitaires artificiels. L'IDS proposé fonctionne en trois modes: le mode d'entrainement, le mode de surveillance et le mode d'adaptation. Le dernier est responsable de l'adaptation de l'IDS au trafic réseau, ce qui améliore les performances de détection d'intrusion.

Un autre système de détection d'intrusion basé sur le niveau de confiance des voisins appelé « Watchdog » a été proposé par Hortelano et al. [45]. Cette méthode consiste en effet, à surveiller le comportement de tous les nœuds d'une part, et choisir la route la plus sécuritaire d' autre part. Stern et al. [46] ont proposé un IDS clustérisé qui est basé sur la signature d'attaques qui peut être structuré en plusieurs niveaux là où les chefs de cluster doivent au début effectuer la fusion, l'intégration et la réduction des données, par la suite, il passe à la détection d'intrusions et finalement la gestion de la sécurité. Buchegger et le Boudec [47] ont proposé une solution qui s'appelle CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks), une extension du protocole de routage DSR et similaire au mécanisme «Watchdog», là où grâce à un système de réputation, chaque nœud malicieux détecté sera exclu de tout le réseau et ensuite un message d'alerte sera envoyé aux autres nœuds du réseau. CONFIDANT utilise le module Monitoring, dans le cas de détection d'un comportement malicieux, ce module envoie une notification au système de réputation qui, à son tour, fait une mise à jour de sa table de réputation en fonction des notifications reçus. Si la valeur de réputation dépasse un seuil prédéfini, une alarme est envoyée aux autres nœuds ainsi qu'au Path Manager qui supprime toutes les routes contenant le nœud malicieux [42].

3.5 Conclusion

Les réseaux véhiculaires sont par nature plus sensibles aux problèmes de sécurité. L'intrusion sur le support de transmission est plus facile en menant des attaques qui peuvent brouiller les bandes de fréquences utilisées. D'autre part, la communication véhicule à véhicule augmente aussi le nombre de failles de sécurité potentielles. En plus, on remarque que le routage pose des problèmes spécifiques tel que la possibilité d'être exposée à des attaques qui peuvent détourner le trafic en transit.

Pour garantir une transmission efficace des paquets et au même temps pallier à l'inconvénient de la sécurité, nous proposons dans le chapitre suivant l'étude du protocole de routage VADD en premier temps et par la suite nous allons étudier d'une manière détaillée l'attaque « Black Hole » afin de pouvoir tester les performances du protocole de routage VADD en termes de sécurité.

Chapitre 4 - Étude des performances de protocole de routage VADD

4.1 Introduction

La transmission multi-sauts des données dans les réseaux VANETs est compliquée du fait que les réseaux véhiculaires sont très mobiles. La densité du réseau est liée à la densité du trafic, qui est affectée par l'emplacement et le temps. Par exemple, la densité du trafic est faible dans les zones rurales et pendant la nuit, mais elle est très élevée dans les grandes zones peuplées et pendant les heures de pointe. En outre, un véhicule en mouvement peut transporter le paquet et le transmettre au véhicule suivant. Grâce au stockage et à la transmission, le message peut être transmis vers la destination sans une communication multi-saut.

Après avoir étudier quelques protocoles de routage dédiés au réseaux véhiculaire sans fil dans le but de trouver un protocole qui garantit la transmission des paquets en utilisant la meilleure route, le moindre retard et la performance sur des routes denses, nous avons remarqué que le protocole de routage d'information VADD (Vehicle-Assisted Data Delivery) répond assez bien à ces contraintes.

Dans ce chapitre, nous allons étudier le comportement du protocole de routage VADD, par la suite nous allons lui faire subir l'attaque « Black Hole » et voir les impacts de cette attaque sur ses performances.

4.2 Le protocole de routage VADD (Vehicule-Assisted Data Delivery)

Le protocole VADD est un protocole de routage unicast basé sur la position et conçu pour gérer les problèmes des déconnexions fréquentes et de mobilité extrême de réseau

véhiculaire. Il implémente la stratégie de « stockage et transmission », tandis qu'un nœud se déplace, il stocke les paquets jusqu'à ce qu'un nouveau nœud arrive à sa région et il lui transmet les paquets stockés.

Ce protocole prévoit la mobilité des nœuds en fonction de deux facteurs: le trafic réseau et le type de la route; ce qui permet à un nœud de découvrir le prochain nœud de transmission. Le problème le plus important est de choisir un chemin de transmission avec le plus court délai de transmission et c'est pour cette raison que le protocole VADD envoie habituellement le paquet suivant trois grands principes:

- Continuer d'utiliser le canal sans fil disponible ;
- Envoyer le paquet au nœud avec la plus grande vitesse dans la voie de transport ;
- Comme VANET est un environnement de haute mobilité, il est donc difficile d'estimer la transmission des paquets par un chemin optimal prédéfini, ce qui peut conduire à continuer la découverte d'une nouvelle route optimale pour transmettre un paquet.

Pour éviter la boucle de routage, chaque nœud ajoute des informations sur ses anciens saut /sauts avant de transmettre le paquet, qui contient aussi ses propres informations en tant qu'ancien saut : Une fois le paquet reçu par un nœud, le nœud regarde les informations concernant les sauts précédents pour éviter de les retransmettre et essaye de trouver d'autres sauts disponibles, de sorte qu'il peut éviter le problème de boucle au niveau du routage [25] [48].

4.2.1Mode de transmission des paquets pour VADD

Le protocole VADD possède trois modes de paquets : Intersection, chemin droit et destination, basés sur l'emplacement du porte-paquet (c'est à dire, le véhicule qui transporte le paquet). En passant entre ces modes de paquets, le porte-paquet choisi le meilleur chemin de transfert des paquets.

Mode intersection : Optimise la direction d'acheminement des paquets.

Mode chemin droit : Transmission géographique des paquets vers la prochaine intersection cible.

Mode destination : Diffusion des paquets vers la destination.

Parmi les trois modes, le mode intersection est le plus critique et le plus complexe, car les véhicules ont plus de choix à l'intersection [48].

La transmission des données en mode chemin droit est beaucoup plus simple que le scénario d'intersection, puisque le trafic est généralement bidirectionnel. Pour ce mode, on peut tout simplement spécifier l'intersection à venir, qui est reliée par la route actuelle, comme la cible, puis on applique le protocole GPSR vers l'emplacement de la cible.

Pour le mode chemin droit, s'il n'y a pas de véhicule disponible pour recevoir le paquet et le retransmettre, le porte-paquet courant continue à transmettre le paquet. Certes, il peut y avoir de meilleures solutions. Par exemple, lorsqu'un véhicule qui transmet un paquet trouve un autre véhicule dans la direction opposée, le retard estimé à partir de la position actuelle du véhicule peut être différent lorsque l'autre véhicule dans l'autre direction reçoit le paquet.

La transmission de paquet change vers le mode de destination lorsque sa distance à la destination est inférieure à un seuil prédéfini. L'emplacement de la destination devient connu et le protocole GPSR sera utilisé pour délivrer le paquet à la destination finale.

4.2.2 Mécanisme de transmission des paquets pour VADD

Pour transférer un paquet, le protocole VADD met en œuvre quatre méthodes différentes [28] :

- Location first Probe (L-VADD): il permet de délivrer le paquet au nœud le plus proche de la destination sans tenir compte de la direction du mouvement. L'inconvénient dans cette méthode est le problème de boucle au niveau du routage.

- Direction first Prob (D-VADD): la sélection du saut suivant est basée sur le nœud qui a le même sens de déplacement que la destination, ce qui peut aider à éviter la boucle au niveau du routage.
- Multi-Path Direction First is the Probe VADD (MD-VADD): il offre un chemin d'accès multiples plutôt qu'une seule voie, mais il consomme de la bande passante à cause des paquets de redondance.
- Hybride Probe VADD (H-VADD): il s'agit d'un système hybride qui prend les avantages de la L-VADD et D-VADD, pour délivrer un paquet, il utilise d'abord la L-VADD, mais si une boucle de routage est identifiée, il change à D-VADD. Par conséquent, ce système fonctionne mieux que les méthodes L-VADD et D-VADD.

Le mécanisme de routage se base, d'une part sur les positionnements courants des véhicules dans le voisinage et d'autre part, sur l'état de la circulation dans le réseau routier. Dans VADD, les routes les plus denses en véhicules sont considérées comme les chemins optimaux pour le routage des paquets.

La figure 8 explique le fonctionnement de VADD [25] [48]:

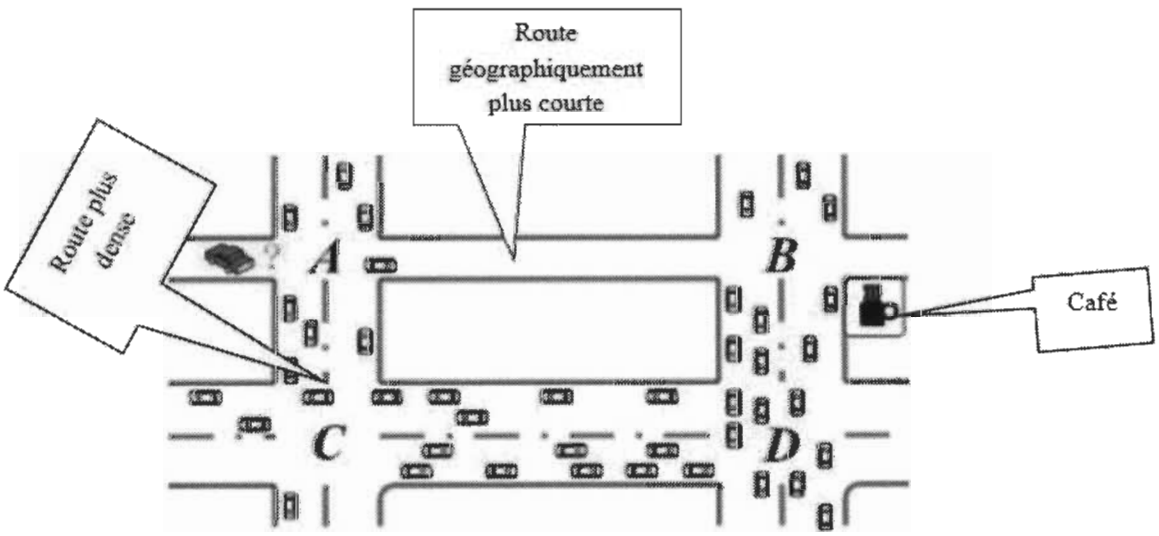

Figure 8 : Mécanisme de routage utilisant le protocole VADD

Supposons qu'un conducteur se rapproche de l'intersection A et il envoie une demande au café situe dans le coin de l'intersection B pour faire une réservation. La transmission de la demande à travers A → C, C → D et D → B serait plus rapide que par A →B même si ce dernier fournit le chemin géographiquement le plus court. La raison est que, qu'en cas de déconnexion, le paquet doit être porté par d'autres véhicules.

Toutefois, il n'est pas toujours possible de savoir à l'avance le changement de comportement des véhicules ainsi que les changements de l'état de la circulation dans un réseau routier, les nœuds peuvent changer de direction et sortir du chemin à tout moment et pour cette raison, le véhicule doit garder le paquet et chercher un nœud retransmetteur capable de délivrer le paquet avec succès [28].

4.2.3Algorithme de transmission des paquets en mode chemin droit

Dans ce qui suit, nous allons étudier ce protocole en mode chemin droit.

Les notations utilisées dans cette partie sont expliquées dans le tableau 3.

Terme	Explication
V_{Src}	Véhicule source
D_{fx}	La destination
D_{sd}	La distance entre la source et la destination
R	La portée de communication
V_{vd}	Le voisin direct

Tableau 3 : Termes utilisés dans l'algorithme.

- **Hypothèse pour le mode chemin droit ou « StraightWay »**
  - Chaque véhicule connait la position de ses voisins par l'échange des messages « beacon ».
  - Un **message « beacon »** contient :
    - La vitesse des véhicules
    - La direction des véhicules
    - La position des véhicules
  - Chaque véhicule connait les informations routières et les statistiques du trafic à partir d'une carte digitale.
- **Description de l'algorithme de transmission du paquet en mode <<staightway>>:**

Procédure 1 : Lorsqu'un véhicule souhaite envoyer un message, comme un message de réservation pour un restaurant, il compare tout d'abord la distance qui reste pour arriver au restaurant et la portée de communication. Si cette distance est inférieure à la portée de communication alors il envoie le paquet directement à la destination.

Procédure 2 : Dans le cas contraire et si la distance est supérieure à la portée de communication alors le véhicule cherche un voisin direct à partir de l'échange des messages beacon. S'il trouve un voisin direct et avant de lui envoyer le paquet, il doit vérifier d'abord au niveau de sa table de routage si l'identifiant de ce voisin est enregistré comme un ancien saut :

- ✓ Si ce voisin est enregistré comme un ancien saut alors le véhicule continu à porter le paquet, chercher un autre voisin ou transporter le paquet jusqu'à la destination dans le cas où aucun voisin n'est trouvé.
- ✓ Si le voisin direct n'est pas enregistré alors le véhicule enregistre son identifiant en tant qu'ancien saut et lui envoie le paquet.

- **Les procédures 1 et 2 seront répéteés jusqu'à la réception du paquet par la destination.**
- **Algorithme d'envoi du paquet « DATA » dans le protocole de routage VADD en mode chemin droit ou « StraightWay »:**

Début :

Initialisation des paramètres :

Paramètres d'entrées :

Un paquet du type « DATA ».

Une destination fixe (coffee shop, restaurant, station …etc)

Envoi de paquet « DATA » de $V_{\_Src}$ à $D_{\_fx}$:

$D_{\_sd}$ est la distance entre la source et la destination

R est la portée de communication

Si $d_{\_sd}<R$

Si $d_{\_sd}<R$ alors on change de mode chemin droit au mode destination

{

Envoyer le paquet « DATA » directement de $V_{\_Src}$ à $D_{\_fx}$

}

Sinon

{

Stocker le paquet et chercher le voisin direct $V_{\_vd}$

Si le voisin direct $V_{\_vd}$ existe (1)

{

Mettre à jour la table de routage

Répéter (1) jusqu'à la réception du paquet par la destination $D_{\_fX}$

}

Sinon

{

Stocker et transporter le paquet jusqu'à la destination

Mettre à jour la table de routage

}

Fin

- **Format du paquet « DATA » :**

On suppose que le paquet « DATA » dans cette approche contient les informations présentées dans le tableau 4.

Tableau 4 : Message Data

Nom de la variable	Type de donnée	Taille en octet	Description de la variable
Source_ID	int	4	Identifiant de la source où le message est émis.
Source_location	Coord	12	Coordonnées X, Y, Z du véhicule émetteur
Time_gen_paq	int	4	Temps d'envoi du paquet
Time_récep_paq	int	4	Temps de réception du paquet
Destination_ID	int	4	Identifiant de la destination où le message sera reçu
Destination_location	Coord	12	Coordonnées X, Y, Z de la destination.
TTL	int	4	Durée de vie du paquet
Former_hops_ID	int	4	Identifiant des anciens véhicules émetteurs

4.2.4Modèle de propagation pour le protocole VADD

Le modèle de propagation pour le protocole VADD est le modèle «Shadwing» (modèle d'ombre). Ce modèle ne tient pas compte des phénomènes imprévisibles que peut subir le réseau car il n'exige pas l'existence d'un chemin direct entre l'émetteur et le récepteur [49].

Le phénomène «Shadwing» est constitué de deux sous modèles, le premier est le modèle de perte de trajet. Pour ce modèle la puissance moyenne du signal reçu à une distance d notée $P_r(d_0)$ est :

$$\left[\frac{\overline{P_r(d)}}{P_r(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d0}\right) \quad (1)$$

β est l'exposant de l'affaiblissement du chemin.

Le deuxième sous modèle est la variation de la puissance du signal reçue à une certaine distance.

L'ensemble du modèle « Shadowing » est représenté alors par :

$$\left[\frac{\overline{P_r(d)}}{P_r(d_0)}\right]_{dB} = -10\beta \log(\frac{d}{d0}) + X_{dB} \quad (2)$$

X_{dB} est une variable aléatoire gaussienne avec moyenne nulle et écart-type σ [49].

4.3 L'attaque «Black Hole» sur le protocole de routage VADD

L'attaque trou noir (Black Hole) a été brièvement expliquée dans la section des attaques dans le réseau VANETs dans le chapitre précédent. Dans cette partie, nous allons l'expliquer plus en détail vis-à-vis du protocole VADD.

Dans une attaque de trou noir [50], un nœud malveillant refuse de transmettre des paquets de données vers le nœud suivant dans une route reliant une source et une destination. Pour effectuer son attaque, le nœud malveillant doit tout d'abord être un membre du

réseau sur la route de transmission des données, puis il passe à l'action qui est de détruire tous les données qui passent à travers lui.

Deux types des attaques du trou noir peuvent être décrits afin de les distinguer :

a. L'attaque du trou noir interne :

Pour ce type d'attaque, un véhicule malveillant interne s'intègre dans la route reliant la source vers la destination, dès qu'il a la chance, ce nœud malveillant devient un élément de la route des données actif. A ce stade, il devient désormais capable de commencer l'attaque dès le début de la transmission des données.

b. L'attaque du trou noir externe

Pour l'attaque de trou noir externe, l'attaquant reste physiquement en dehors de la région du réseau véhiculaire à attaquer. L'attaque « Black Hole » externe peut devenir une sorte d'attaque interne quand il prend le contrôle d'un véhicule malveillant situé sur la route entre la source et la destination et le contrôle pour attaquer les autres nœuds dans le réseau. Ce type d'attaque peut bloquer l'accès au trafic réseau, créer de la congestion ou perturber l'ensemble du réseau.

4.4 Scenario de l'attaque « Black Hole » sur le protocole de routage VADD

Le scénario de l'intégration de l'attaque « Black Hole » passe par les étapes suivantes :

1. Un nœud malveillant « Black Hole » détecte qu'un véhicule actif qui porte le paquet cherche un voisin pour lui transmettre le paquet.
2. Le nœud malveillant prend note de l'adresse de destination.
3. Le nœud malveillant envoie des messages « beacon » contenant des informations falsifiées qui montre que c'est lui le voisin direct.
4. Une fois que le véhicule qui porte le paquet reçoit ces messages « beacon » du nœud malveillant, il lui envoie le paquet.

5. Dès que le nœud malveillant reçoit le paquet alors il peut le détruire et ne le retransmet jamais.

La figure 9 explique le déroulement du scénario de l'attaque trou noir.

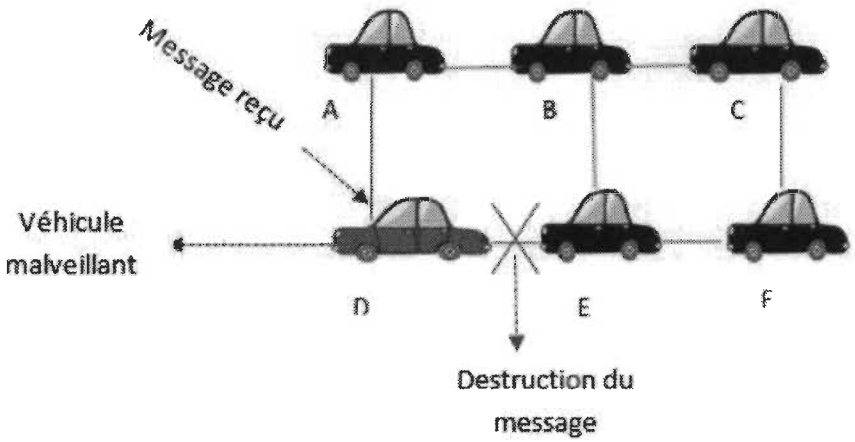

Figure 9 : Scénario de l'attaque trou noir « Black Hole ».

La figure 9 illustre un exemple où le nœud A souhaite envoyer des paquets de données au nœud F, mais il n'est pas familier avec l'itinéraire vers F. Par conséquent, A lance le processus de découverte d'itinéraire. En tant que nœud malveillant, D affirme qu'il a une route active vers F et agit comme un nœud voisin direct. Si A veut envoyer des paquets à F alors une route à travers le nœud « Black Hole » serait choisie par le nœud D.
Une fois le nœud D «Black Hole » a pris le contrôle du chemin de rouage vers F, il peut supprimer les paquets de données qu'il reçoit.

4.5 Conclusion

L'étude conceptuelle du protocole de routage VADD ainsi que l'analyse de la sécurité de ce protocole vis-à-vis de l'attaque « Black Hole » ont été réalisées dans ce chapitre. Dans le chapitre suivant, nous allons présenter et analyser les résultats de simulations de notre protocole de routage VADD en mode chemin droit avec et sans l'attaque « Black Hole ».

Chapitre 5 -Évaluation des performances

5.1 Introduction

Dans les réseaux véhiculaires, l'étude du comportement des différentes entités du réseau nécessite l'utilisation de simulateurs performants.

Pour ce faire, nous allons décrire dans ce chapitre l'environnement de simulation de notre étude et ensuite nous allons discuter des différents résultats de simulation.

5.2 Environnement de la simulation

Pour analyser la performance du protocole de routage VADD et étudier l'attaque « Black Hole » sur ce protocole, nous avons utilisé le simulateur de trafic routier SUMO-O.15.0 et le simulateur réseau OMNET++ 4.2.2. Pour évaluer le protocole de routage VADD avec et sans l'attaque « Black Hole » à partir du simulateur OMNET ++, nous avons utilisé le Framework Veins-2.0 [49] (Vehicles in network Simulation) qui permet d'assurer la réunion des simulateurs OMNET ++ et SUMO. Le protocole VADD est évalué dans un milieu urbain et les propriétés de l'environnement de simulation sont décrites dans le tableau 5.

Paramètres	Valeurs
Simulateur réseau	OMNET++ 4.2.2
Simulateur de trafic routier	SUMO-O.15.0
Modèles de propagation	Shadowing
Nombre des nœuds	30, 50, 150
Temps de simulation	100s
Portée de transmission	300m
Carte routière Manhattan City	1200m*1200m
Vitesse des véhicules	20 m/s
Nombre des paquets	40
Taille du paquet	1024 bits
Intervalle_msg_beacon	0,5 s

Tableau 5 : Propriétés de l'environnement de simulation

5.3 Les métriques utilisées dans les simulations

L'évaluation des performances du protocole de routage VADD avec et sans l'attaque « Black Hole » a été faite en utilisant les métriques suivantes:

1. Taux de transmission des paquets :

$$\frac{\text{Total des paquets reçus par la destination}}{\text{Total des paquets émis par la source}}$$

2. La moyenne du délai de transmission EE (End to End) (de la source vers la destination) :

$$\frac{1}{n}\sum_{i=1}^{n}(\text{Tri} - Tsi) * 1000 \quad \text{en ms.} \qquad (3)$$

Avec :

i = identification du paquet

Tri = temps de réception

Tsi= temps d'envoie

n = Nombre des paquets reçu avec succès

3. Taux de perte de paquets :

$$\frac{\text{Nombre de paquets envoyé-Nombre de paquets reçu par la destination}}{\text{Nombre des paquets envoyés}}$$

Nous présenterons dans ce qui suit, les résultats de simulations du protocole VADD dans les deux approches (sans l'attaque « Black Hole » et avec l'attaque « Black Hole ») en tenant compte des métriques mentionnées ci-dessus.

5.4 Les résultats des simulations

5.4.1 Simulation du protocole de routage VADD sans attaque « Black Hole »

a. Taux de transmission des paquets

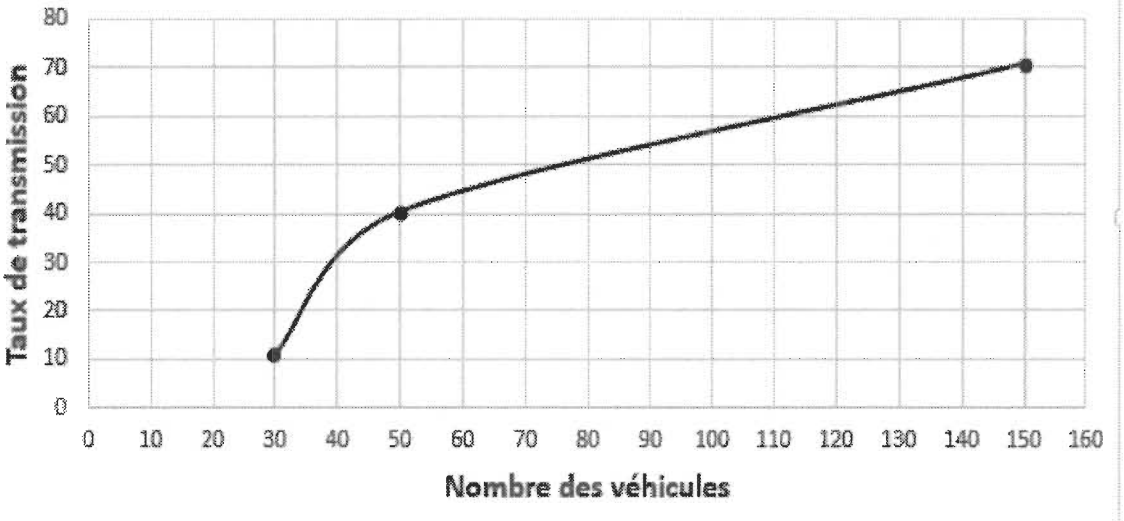

Figure 10 : Taux de transmission de 40 paquets pour 30, 50 et 150 nœuds.

La figure 10 montre que le taux de transmission de 40 paquets envoyés augmente quand on augmente le nombre de véhicules. Pour la première simulation de 30 véhicules, nous remarquons que le taux de transmission est aux alentours de 10% alors que pour 150 véhicules le taux de transmission monté à 70%.

Cette augmentation nous prouve que le protocole VADD est plus performant dans les milieux denses, c'est à dire, plus le nombre de véhicules augmente plus le taux de transmission augmente aussi.

b. Délai de transmission des paquets

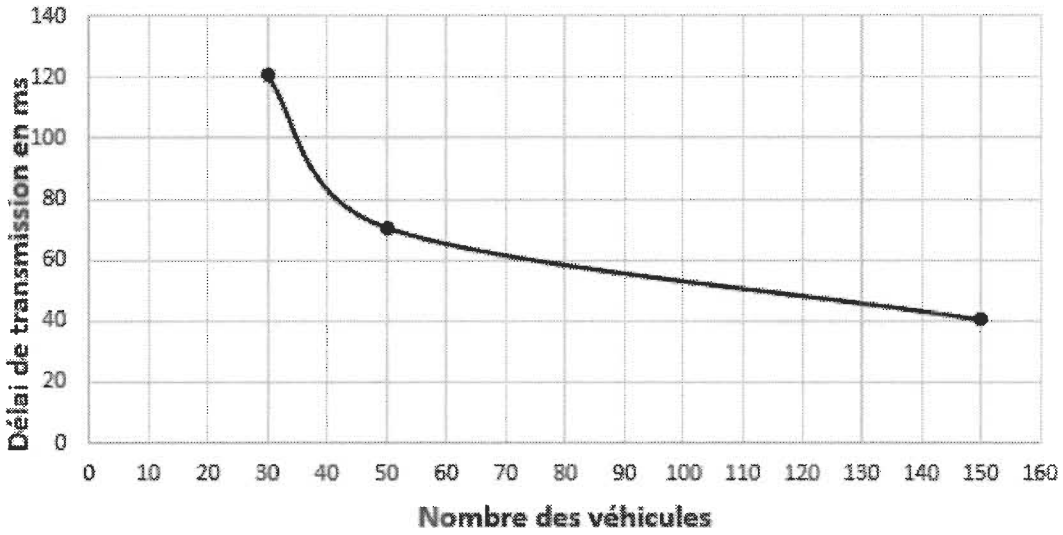

Figure 11 : Délai de transmission de 40 paquets pour 30, 50 et 150 nœuds

La figure 11 montre la variation du délai de transmission des 40 paquets envoyés. Le délai diminue de 120 ms pour la première simulation de 30 véhicules à 70 ms pour la deuxième simulation de 50 véhicules. Pour la troisième simulation de 150 véhicules, le délai de transmission est de 40 ms. On remarque donc qu'à chaque fois qu'on augmente le nombre de véhicules, le temps nécessaire à la transmission des paquets entre la source et la destination diminue.

On conclut alors que pour avoir un délai minimum de transmission, il faut toujours choisir les routes les plus denses en termes de nombre de véhicules.

c. Taux de perte des paquets

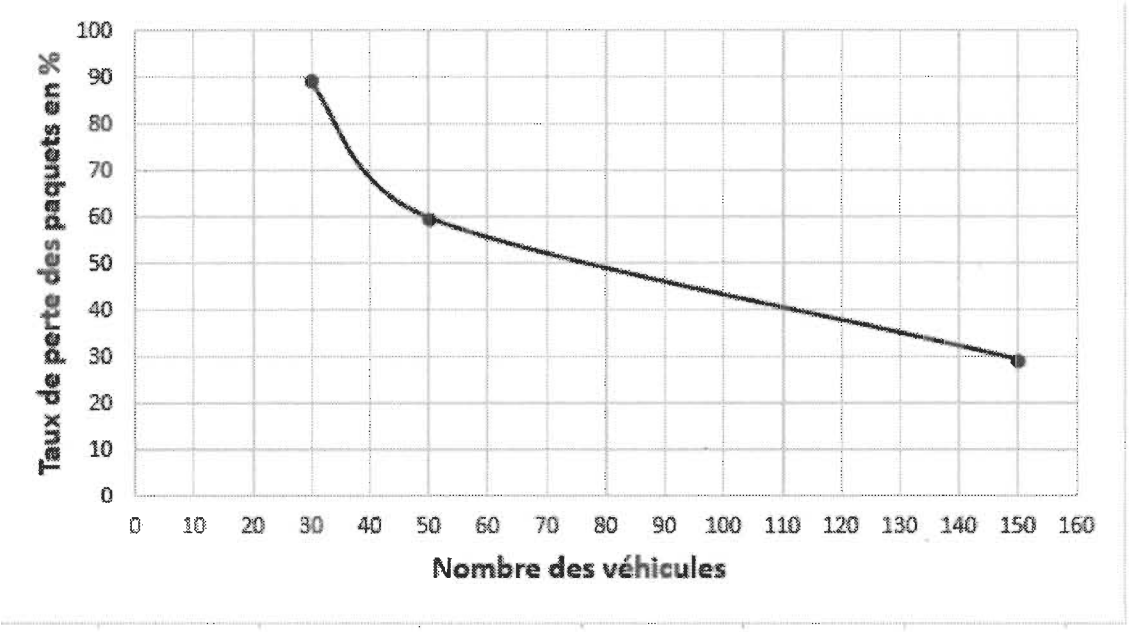

Figure 12 : Taux de perte des paquets pour 30, 50 et 150 nœuds

Pour la figure 12, si on compare le taux de perte des paquets entre les trois scénarios, on constate qu'il y a une diminution remarquable entre le premier (30 nœuds) et le troisième scénario (150 nœuds).

Le taux de perte des paquets diminue plus que 50% entre la simulation avec 30 véhicules (taux de perte est 89%) et la simulation avec 150 véhicules (taux de perte est 29%).

Ces résultats montrent que la perte des paquets augmente quand on diminue le nombre de véhicules, cela peut être dû à la courte durée de connectivité surtout lorsque la densité des véhicules est très faible comme dans le cas de la première simulation.

Afin de baisser le taux de perte des paquets, il faut un déploiement de plusieurs nœuds relais ou points d'accès le long de la route, ce qui permettrait la retransmission de l'information sur de longues distances.

5.4.2 Simulation du protocole de routage VADD avec l'attaque « Black Hole »

Dans cette partie, nous avons défini en premier temps 3 attaques « Black Hole » pour chacun des scénarios (30, 50 et 150 véhicules), par la suite, nous avons augmenté le nombre d'attaque « Black Hole » et nous avons effectué une simulation avec 5 attaques « Black Hole » pour les trois scenarios aussi.

a. Simulation avec 3 attaques « Black Hole »

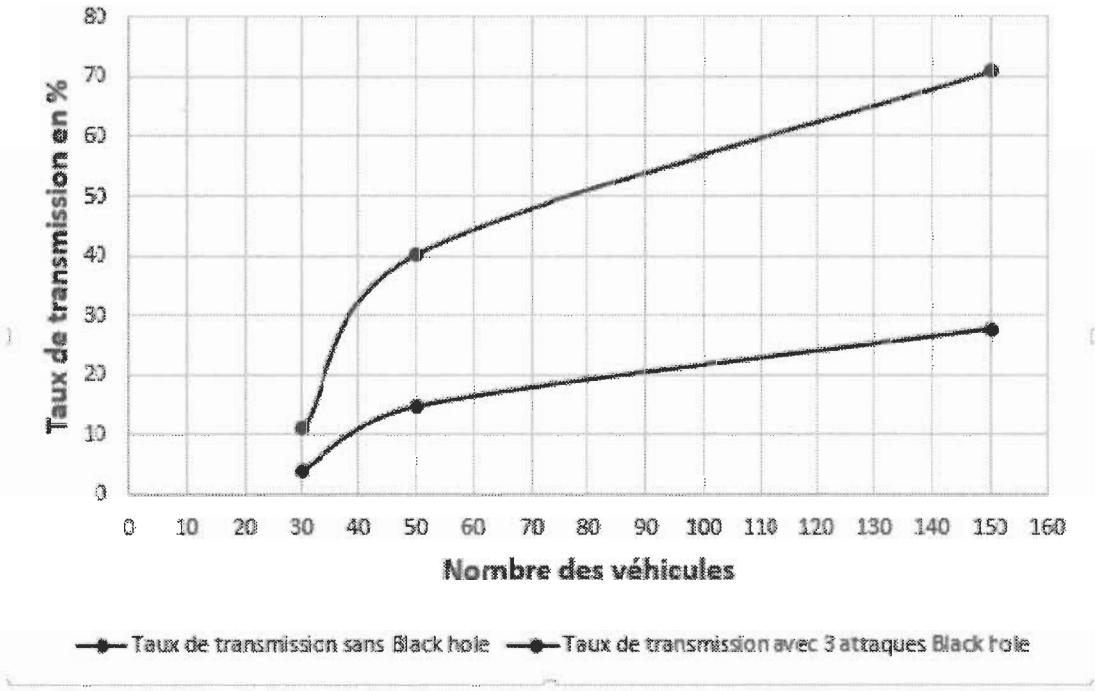

Figure 13 : Taux de transmission de 40 paquets avec 3 attaques « Black Hole » pour 30, 50 et 150 nœuds.

Pour chaque simulation (30, 50 et 150 véhicules), si on compare entre le scénario normal et le scénario avec la présence de trois attaques, on remarque que le taux de transmission

diminue énormément, par conséquent il y a plus de perte des paquets. Ceci est dû au comportement de l'attaquant qui détruit tous les paquets qui passe par lui.

Pour le scénario anormal, on constate que même avec la présence de 3 attaques « Black Hole » plus le nombre des véhicules dans le voisinage est grand, meilleur est le taux de transmission.

On peut conclure alors que même dans un scénario anormal le protocole VADD garde l'une de ses caractéristiques qui est la performance dans les milieux denses.

b. Simulation avec 5 attaques « Black Hole »

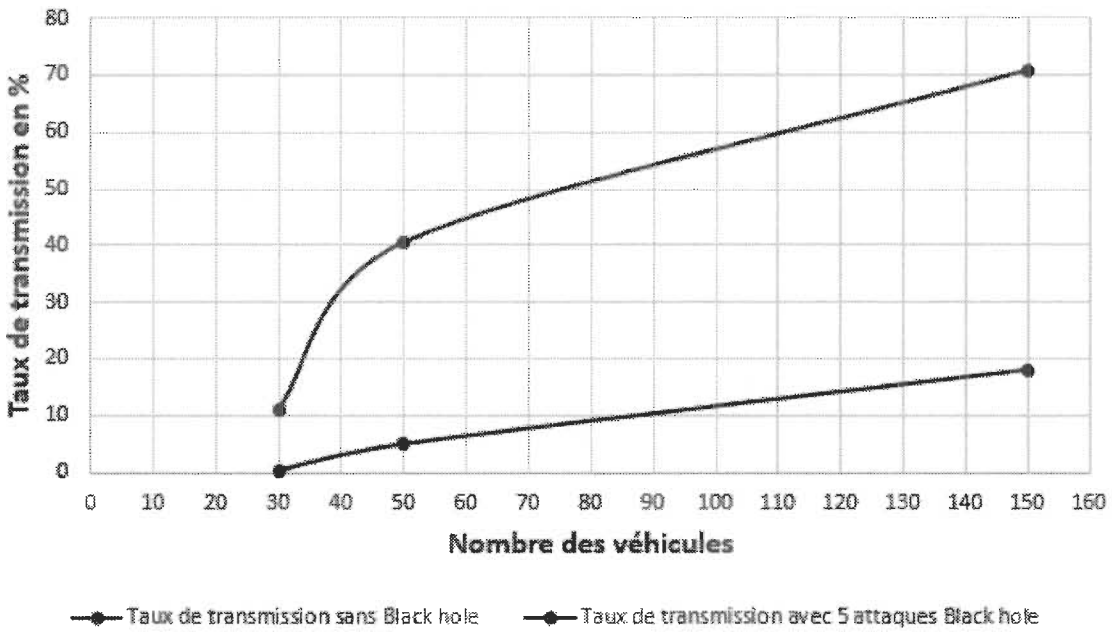

Figure 14 : Taux de transmission de 40 paquets avec 5 attaques « Black Hole » pour 30, 50 et 150 nœuds.

La figure 14 montre qu'avec 5 attaques « Black Hole », le taux de transmission pour la simulation avec 30 véhicules est proche de 0% alors que pour celle avec 50 véhicules, on

remarque que le taux de transmission est inferieur a 10%. Quant à la simulation avec 150 véhicules le taux de transmission n'arrive pas à atteindre le 20%.

On constate alors qu'avec ce nombre d'attaques, le taux de transmission des paquets diminue d'une manière remarquable et que tous les paquets qui passent par les attaquants n'ont jamais été retransmis. Donc, on aura un taux de perte a 100% et un délai de transmission infini.

5.5 Conclusion

L'évaluation des performances du protocole de routage VADD a été réalisée dans ce chapitre. Eu égard aux différents résultats des simulations, nous avons constaté que la simulation avec 150 véhicules présente un avantage considérable au niveau du taux de transmission, du taux de perte et du délai de transmission, ce qui prouve que notre choix de protocole de routage qui garantit la transmission des paquets en utilisant la meilleure route, le moindre retard et la performance sur des routes denses était réussi. Aussi, nous avons étudié notre protocole de routage en termes de sécurité en lui faisant subir 3 attaques « Black Hole » puis 5 attaques « Black Hole ». Nous avons remarqué que du taux de perte des paquets est proportionnel au nombre d'attaquants présents pour chaque scénario. En se basant sur les résultats des simulations, nous avons remarqué que l'attaque « Black Hole » a des impacts qui sont illustrés par la grande diminution de taux de transmission en présence des nœuds malveillants et donc tous les paquets qui passent par l'un des nœud malveillant ont été détruit et n'ont jamais était retransmis .Suite à ces résultats, on peut conclure que le protocole de routage VADD est vulnérable vis-à-vis de l'attaque « Black Hole ».

Afin de pallier ces inconvénients et faire face aux impacts de l'attaque « Black Hole » sur le protocole de routage VADD, nous proposons dans le chapitre suivant une piste pour améliorer le fonctionnement du protocole de routage VADD en cas d'attaque « Black Hole ».

Chapitre 6 - Détection de l'attaque « Black Hole » à l'aide de système du détection d'intrusions « Watchdog »

6.1 Introduction

Comme les réseaux VANETs sont un moyen de communication ouvert, ceci peut constituer une cible idéale pour les attaques qui pourraient intercepter les messages avant d'arriver à leurs destinations. Suite à l'étude du protocole de routage VADD dans le chapitre précédent, nous avons remarqué que ce dernier est vulnérable vis-à-vis de l'attaque « Black Hole ». Dans VANETs, il existe de nombreuses méthodes, architectures, protocoles et algorithmes qui ont été proposés pour la sécurisation des VANETs et la détection des attaques. Des recherches ont été réalisées sur la sécurisation des protocoles de routage, d'autres recherches se sont concentrées sur la sécurisation des messages transmis par les méthodes de cryptage par certificat et clé public/privé. Une autre catégorie de recherche s'est focalisée sur la sécurisation par la méthode de détection d'intrusion IDS. Un IDS contient trois étapes : une étape de collection de données suivie d'une étape d'analyse et enfin une étape de réponse pour prévenir ou minimiser l'impact sur le système. L'implémentation de système IDS se différencie en fonction du type protocole et de l'architecture de l'IDS. Dans ce chapitre, nous allons élaborer une solution de détection de l'attaque « Black Hole » au niveau du protocole de routage VADD à l'aide d'un système de détection d'intrusions « Watchdog » [53].

6.2 Principe d'un système de détection d'intrusions « Watchdog »

Le « Watchdog » est un agent de détection d'intrusions. C'est un processus de contrôle exécuté par chaque voiture du réseau.

Chaque véhicule implémentant « Watchdog » enregistre chaque paquet de données qu'il émet, et vérifie ensuite si le nœud à qui il a envoyé le paquet le retransmet correctement. Chaque nœud est capable d'écouter tous les paquets que son voisin émet grâce au mode « promiscuous ». Selon cette technique, un nœud capture les paquets transitant dans le réseau qui ne lui sont pas destinés, et par conséquent, il peut vérifier si le nœud voisin retransmet les paquets qu'il a reçus au bon destinataire [2] [52] [53].

Cette vérification se fait en comparant chaque paquet envoyé par son voisin avec l'ensemble des paquets qu'il possède dans son buffer. Si un paquet dans son buffer correspond à celui que vient d'envoyer son voisin, alors, le nœud supprime le paquet de son buffer et estime que son voisin a fait suivre correctement son paquet. Si après une période de temps T, il n'a toujours pas entendu son voisin retransmettre le paquet, il efface le paquet de son buffer et incrémente le compteur d'échecs de son voisin. Si le compteur d'échecs d'un voisin est supérieur à un certain seuil préétabli, l'agent «Watchdog » considère que ce dernier est un nœud malveillant et une alerte est diffusée au voisinage [51] [52].

Les informations collectées grâce au système « Watchdog » sont alors exploitées par le système de réputation qui attribue des poids ou des scores pour un certain ensemble de nœuds. Au début, les nœuds sont assignés à un score dit neutre, ce score est réévalué suivant le nombre de paquets retransmis. Le système de réputation est responsable du calcul des évaluations et de la sélection des chemins les plus fiables en évitant les nœuds les moins coopératifs. Ce système isole et / ou punisse les nœuds ou itinéraires mal comportés en se basant sur le niveau de confiance du nœud en question. Si le niveau de confiance est inferieur a 0.5 alors le système de réputation conclu que c'est une attaque [51] [52] :

- ***Niveau de confiance = Totale des paquets retransmis/ Totale de paquet reçu***

Le niveau de confiance du voisin idéal est de 1 (100%), ce qui est difficile à atteindre en raison de la collision et du bruit du signal.

6.3 Algorithme de détection d'attaques « Black Hole » à l'aide du système « Watchdog »

a. Hypothèse

Pour que cette méthode soit applicable pour la détection de l'attaque « Black Hole » on suppose que :

- Chaque véhicule est équipé avec un IDS « Watchdog ».
- Le réseau doit être mis en mode promiscuité pour écouter tous les paquets qui circule dans le voisinage en tenant compte de la portée.
- Chacun des agents « Watchdog » détecte de manière individuelle les attaques, ensuite l'information est transmise aux autres agents « Watchdog ».
- L'agent « Watchdog» isole les véhicules attaquants en les mettant dans une liste noire.
- On applique un seuil de tolérance pour éviter la confusion entre une attaque « Black Hole » ou bien une collision ou perte de paquet.
- Pour le niveau de confiance, on ne l'applique pas parce que on aura toujours 0 comme résultat. Au fait, l'attaque « Black Hole » ne retransmet jamais les paquets reçus, donc le nombre des paquets retransmis est toujours égal à 0.

b. Format du message « Alerte » :

On suppose que le message « Alerte » dans cette approche contient les informations présenté dans le tableau 6 :

Nom de la variable	**Description de la variable**
ID_ veh_ émetteur	Identité du véhicule émetteur de l'alerte
ID _Watch_detectant	Identité du l'agent « Watchdog» qui a détecté l'attaque
ID_attaquant	Identité de véhicule attaquant
TTL	Durée de vie du paquet.
ID_Watch_dest	Identifiants des agents «watchdog» où l'alerte sera reçu
Detection_Time	Temps auquel l'attaque a été détectée.

Tableau 6 : Message d'alerte.

c. Algorithme de détection d'une attaque « Black Hole » pour le protocole de routage VADD

Les notations utilisées dans cette partie sont expliquées dans le tableau 7 suivant:

Terme	Explication
V_{Src}	Le véhicule source
D_{fx}	La destination
D_{sd}	La distance entre la source et la destination
R	La portée de communication
V_{vd}	Le voisin direct
T	Temps d'écoute prédéfini
$C_{échec}$	Compteur d'échec
S	Seuil de tolérance prédéfini

Tableau 7 : Termes utilisés dans l'algorithme du système « Watchdog ».

Début

Initialisation des paramètres :

Paramètres d'entrées :

Un paquet du type « DATA ».

Une destination fixe (coffee shop, restaurant, station …etc)

Envoi de paquet « DATA » de V_{Src} (La source) à D_{fx} (destination) :

D_{sd} est la distance entre la source et la destination

R est la portée de communication

Si $d_{sd}<R$

Si $d_{sd}<R$ alors on change de mode chemin droit au mode destination

{

Envoyer le paquet « DATA » directement de V_{Src} à D_{fx}

}

Sinon

{

Stocker le paquet et chercher le voisin direct V_{vd}

Si le voisin direct V_{vd} existe Alors

{

Envoyer le paquet au voisin direct V_{vd}

L'agent « Watchdog » de V_{Src} garde une copie de paquet

L'agent « Watchdog » écoute si V_{vd} retransmet le paquet ou non

Si V_{vd} retransmet le paquet {

Alors l'agent « Watchdog » de $V_{\_Src}$ supprime le paquet de son buffer

Mise à jour de la table de routage}

Sinon {

Si T écoule et $V_{\_vd}$ ne retransmet pas le paquet

{

L'agent « Watchdog » de $V_{\_Src}$ incrémente $C_{échec}$ avec l'identifiant de $V_{\_vd}$

L'agent « Watchdog » de $V_{\_Src}$ diffuse un message d'échec aux autres agents « Watchdog » du voisinage

Les autres agents « Watchdog » du voisinage, incrémentent $C_{échec}$ de $V_{\_vd}$

Si pour un agent « Watchdog » d'un véhicule donné V_n

$C_{échec}$ de $V_{\_vd}$ > S {

L'agent « Watchdog » considère le véhicule $V_{\_vd}$ comme une attaque « Black hole »

L'agent « Watchdog » insère l'identifiant de $V_{\_vd}$ dans une liste noire

L'agent « Watchdog » diffuse un message d'alerte aux autres agents « Watchdog » du voisinage

Mise à jour de la liste noire de tous les agents « Watchdog » du voisinage

}

}

}

}

} **Fin**

6.4 Conclusion

Dans ce chapitre, nous avons présenté la méthode de détection d'intrusions « Watchdog » afin de pouvoir détecter l'attaque « Black Hole » dans le cas du protocole de routage VADD.

Cette solution théoriquement proposée est spécialement conçue pour éviter l'attaque « Balck Hole » qui peut détruire ou utiliser improprement les paquets interceptés sans les transmettre. Selon le scénario du protocole VADD avec l'attaque « Black Hole », on peut déduire que cette méthode peut être performante car dans le cas de cette attaque aucun des messages reçu ne sera retransmis, donc en écoutant le voisinage, l'agent « Watchdog » peut conclure facilement que c'est une attaque à travers l'incrémentation du compteur d'échec chaque fois que le nœud malveillant ne retransmet pas le paquet.

Dans nos travaux futurs, afin de prouver que la solution proposée de détection de l'attaque « Black Hole » est performante, nous allons passer à l'étape de simulation de système de détection d'intrusion « Watchdog » dans le cas de détection de l'attaque « Black Hole » pour le protocole VADD.

Chapitre 7 - Conclusion générale et perspectives

Le routage dans les réseaux VANETs est un problème très difficile puisque l'environnement VANETs est évolutif et dynamique, ce qui implique un changement fréquent au niveau de la topologie du réseau. Le routage est en quelque sorte le mécanisme clé des réseaux véhiculaires. C'est grâce au mécanisme de routage que les véhicules ont la possibilité de communiquer entre eux. Afin de garantir une transmission continue des messages dans le réseau véhiculaire, il faudrait que le protocole de routage prenne en considération les caractéristiques des réseaux véhiculaires. Pour ce faire, nous avons étudié dans le cadre de ce mémoire le protocole de routage VADD (Vehicle-Assisted Data Delivery) qui est un protocole de routage unicast adoptant l'idée de stockage et de transmission. Pour VADD, le mécanisme de routage se base sur les positionnements courants des véhicules dans le voisinage et l'état de la circulation dans le réseau routier. À partir de l'analyse des résultats obtenus lors des simulations du protocole VADD, on retient que pour avoir un taux maximum de transmission des paquets et un moindre délai, il faut travailler dans un milieu dense en termes de véhicules. Mais comme les réseaux VANETs sont un moyen de communication ouvert, cela peut constituer une cible idéale pour les attaques qui pourraient intercepter les messages avant d'arriver à leurs destinations, ce qui implique que le protocole de routage VADD peut être vulnérable vis-à-vis des attaques. Pour tester la performance de notre protocole en termes de sécurité, nous avons fait subir à VADD l'attaque « Black Hole ». Après une analyse des résultats obtenus nous avons remarqué que l'attaque « Black Hole » avait des impacts sur le protocole VADD illustrés par la diminution du taux de transmission, ce qui a impliqué un énorme taux de perte des paquets. Afin de pallier à ce problème, nous avons proposé comme solution, l'utilisation du système de détection d'intrusions « Watchdog ». Après une étude théorique de cette solution, nous avons déduit que pour le scénario du

protocole VADD soumis à l'attaque « Black Hole », la méthode de détection « Watchdog » serait très intéressante.

Dans les travaux futurs, nous avons l'intention d'approfondir l'étude du système de détection d'intrusions « Watchdog » et de passer à l'étape de simulation de cette méthode pour confirmer qu'elle est capable de détecter les nœuds malveillants « Black Hole » et aussi garantir un bon fonctionnement du protocole de routage VADD.

Références bibliographiques

[1] Véhicules connectés et systèmes de transport intelligents, Rapport interne, Michelin Challenge Bibendum, 2011, Berlin.

[2] Noureddine CHAIB, "La sécurité des communications dans les réseaux VANET", Mémoire, Université ELHADJ LAKHDER-BATNA, faculté des sciences de l'ingénieur département d'informatique, 05 Septembre 2011.

[3] Amadou Adama Ba, Protocole de routage basé sur des passerelles mobiles pour un accès Internet dans les réseaux véhiculaires, Mémoire, Université de Montréal, Faculté des arts et des sciences, Avril, 2011.

[4] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri, "Short-lived Key Management for Secure Communications in VANETs", 11th International Conference on ITS Telecommunications (ITST), pp. 613-618, August 23-25, 2011- St. Petersburg, Russia. ISBN: 978-1-61284-668-2.

[5] Jonathan Petit, "Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", Thèse de Doctorat, Université de Toulouse, 13 Juillet 2011.

[6] GRICH Sofien, "Contribution à la Qualité de Service dans les réseaux VANET", Mémoire, Université d'Oran, département d'informatique, 04 Novembre 2015.

[7] https://securite-routiere.qc.ca/doc/aide-determination-limite.pdf (accédé le 10/12/2013).

[8] http://fr.wikipedia.org/wiki/Autoroutes_du_Québec(accédé le 10/12/2013).

[9] Moez JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections", Thèse de Doctorat, Université d'Évry Val d'Essonne, 06 Novembre 2008.

[10] Christian Tchepnda, "Authentification dans les Réseaux Véhiculaires Opérés", Thèse de Doctorat, École Nationale Supérieure des Télécommunications Spécialité : Informatique et Réseaux, 18 Décembre 2008, Paris- France.

[11] Fan Li and Wang, "Routing in Vehicular Ad Hoc Networks: A Survey", IEEE Vehicular Technology Magazine Volume 2, pp. 12-22, June 2007. Print ISSN: 1556-6072.

[12] Abdel Mehsen AHMAD, "Techniques de Transmission et d'Accès sans fil dans les Réseaux Ad Hoc Véhiculaires (VANETs) ", Telecom Sudparis et l'Université Pierre et Marie Curie en co-tutelle avec l'Université Libanaise, Spécialité : Informatique et Télécommunications, 09 Octobre 2012.

[13] Ahizoune Ahmed, " Un protocole de diffusion des messages dans les réseaux véhiculaires", Mémoire, Université de Montréal, Département d'informatique et de recherche opérationnelle, Faculté des arts et sciences, Avril 2011.

[14] Richard Engoulou, "Sécurisation des VANETS par la Méthode de Réputation des Nœuds", Mémoire, Université de Montréal, École Polytechnique de Montréal, Département de Génie Informatique et Génie Logiciel, Avril 2013.

[15] Wafaa A.H. Al-Salihy, R. Sures, Ghassan Samara, "Security Analysis of Vehicular Ad Hoc Networks (VANET) ", Network Applications, Protocols and Services, International Conference, pp.55-60, September 2010, Alor Setar, Kedah Malaysia. ISBN: 978-0-7695-4177-8.

[16] Praveen G Salagar, Shrikant S Tangade, "A Survey On Security In VANET", International Journal for Technological Research in Engineering, Volume 2, Issue 7, pp. 1397-1402, March-2015, Bangalore, India. ISSN: 2347 - 4718.

[17] Swapnil G. Deshpande, "Classification of Security attack in Vehicular Adhoc network: A survey ", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 2, pp. 371-377, March – April 2013, Amravati, Maharashtra, India. ISSN 2278-6856.

[18] B. Parno and A. Perrig, "Challenges in securing vehicular networks", in Workshop on Hot Topics in Networks (HotNets-IV), pp. 11-21, November 2005, College Park, Maryland, USA.

[19] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for VANETs", 4th Workshop on Embedded Security in Cars. (escar 2006), pp. 15-22, November 2006, Berlin, Germany.

[20] S. Biswas, J. Misic,"Proxy signature-based RSU message broadcasting in VANETs", 25th Biennial Symposium on, pp. 5-9, 12-14 May 2010, Kingston, ON, Canada. ISBN: 978-1-4244-5711-3.

[21] M. Raya, J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks", SASN '05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, , pp. 11-21, November 2007, Alexandria, VA, USA . ISBN: 1-59593-227-5.

[22] Q. Yi and N. Moayeri, "Design of secure and application-oriented VANETs", in Vehicular Technology Conference, 2008, VTC Spring 2008. IEEE, May 2008, pp. 2794-2799. Print ISBN: 978-1-4244-1644-8.

[23] F. Li, Y. Wang, "Routing in Vehicular Networks: A Survey", in the IEEE Vehicular Technology magazine, Vol. 2, No. 2, pp. 12-22, 2007.

[24] L. Ilias, M. Cecilia, "GeOpps: Geographical Opportunistic Routing for Vehicular Networks", IEEE International Symposium World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-6, June 2007, Espoo, Finland. ISBN: 978-1-4244-0992-1.

[25] Talar Atéchian, "Protocole de routage géo-multipoint hybride et mécanisme d'acheminement de données pour les réseaux ad hoc de véhicules (VANETs) ", Thèse de Doctorat, Institut National des Sciences Appliquées de Lyon, 24 septembre 2010.

[26] http://www.memoireonline.com/04/10/3394/m_Greedy-perimeter-stateless-routing-sur-omnet2.html (accédé le 15/01/2014).

[27] B. KARP, H.T. KUNG, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", In: 6th International Conference on Mobile computing and networking MobiCom, pp. 243-254, August 2000, Boston, Massachusetts, USA. ISBN: 1-58113-197-6.

[28] M. Altayeb and I. Mahgoub: "A Survey of Vehicular Ad hoc Networks Routing Protocols", International Journal of Innovation and Applied, Vol., pp. 829-846, 3 July 2013. ISSN: 2028-9324.

[29] Bijan Paul, Mohammed J. Islam, "Survey over VANET Routing Protocols for Vehicle to Vehicle Communication," IOSR Journal of Computer Engineering (IOSRJCE), vol. 7, Issue 5, pp. 01- 09, Nov-Dec 2012, ISSN: 2278-0661, ISBN: 2278-8727.

[30] Salim Allal and Saadi Boudjit, "Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal," Journal of Internet Services and Information Security (JISIS), vol. 3, no. 1/2, pp. 20-36, February 2013.

[31] R. Kumar and M. Dave, "A Comparative Study of Various Routing Protocols in VANET," International Journal of Computer Science Issues (IJCSI), vol. 8, Issue 4, no. 1, pp. 643-648, July 2011. ISSN: 1694-0814.

[32] Vijayalaskhmi M., A. Patel, L. Kulkarni, "QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network," Indian Journal of Computer Science and Engineering , vol. 1, no. 1, pp. 283-294, 2010. ISSN 0976-5166.

[33] Lee, Kevin C., Uichin Lee, and Mario Gerla. , "Survey of Routing Protocols in Vehicular Ad Hoc Networks," Chapter 8, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges reference, IGI Global, edition 2010, pp. 149-170, 25 March 2013.

[34] Sumra, I.A., et al. "Classes of attacks in VANET" In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International: IEEE, pp. 1-5, April 2011. Print ISBN: 978-1-4577-0068-2.

[35] Al-kahtani, M.S, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs) ", in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, pp. 1-9, December 2012, Gold Coast, Australia. Print ISBN: 978-1-4673-2392-5.

[36] Hu, Y.-C., A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, pp. 1976-1986, March 2003, San Francisco, CA, Print ISBN: 0-7803-7752-4.

[37] Ngai, E.C.H., L. Jiangchuan, and M.R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks in Communications", 2006. ICC '06. IEEE International Conference on, Vol. 8, pp. 3383 – 3389, June 2006. Print ISSN: 1550-3607.

[38] Lo, N.-W and H.-C. Tsai, "Illusion attack on VANET applications-A message plausibility problem", in Globecom Workshops, 2007 IEEE, pp. 1-8, November 2007 Print ISBN: 978-1-4244-2024-7.

[39] Douceur, J.R., "The sybil attack, in Peer-to-peer Systems", IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, March 2002, Springer-Verlag London, UK, ISBN: 3-540-44179-4.

[40] F. Anjum, D. Subhadrabandhu, S. Sarkar, "Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols." Vehicular Technology Conference, VTC 2003-Fall. 2003 IEEE 58th. Vol. 3, pp. 2152 – 2156, October 2003, Orlando, FL, USA. Print ISBN: 0-7803-7954-3.

[41] P C Kishore Raja, Dr. Suganthi M, R Sunder, "Wireless Node Behavior Based Intrusion Detection Using Genetic Algorithm", Ubiquitous Computing and Communication Journal, pp. 1-6, August 2006.

[42] Mohammed Erritali, Contribution à la sécurisation des réseaux ad hoc véhiculaires, thèse de doctorat, Université Mohamed V- Agdal Faculté des Sciences Rabat, 10 Octobre 2013.

[43] A. Mishra, K. Nadkarni et A. Patcha. "Intrusion detection in wireless ad hoc networks". IEEE Wireless Communications, vol. 11, no 1, p. 48-60, 16 August 2004. Print ISSN: 1536-1284.

[44] D. Kotov, Vladimir 1. Vasilyev, "Immune Model Based Approach for Network Intrusion Detection", SIN' 10 Proceedings of the 3rd international conference on Security of information and networks, ACM, pp. 233-237, September 2010, New York, USA. ISBN: 978-1-4503-0234-0.

[45] Jorge Hortelano, Juan Carlos Ruiz, Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETS", Communications Workshops (ICC), 2010 IEEE International Conference, pp. 1-5, May 2010, Cape town, South Africa, Print ISBN: 978-1-4244-6824-9.

[46] Sterne, Daniel, et al. "A general cooperative intrusion detection architecture for MANETs." Information Assurance, 2005. Proceedings. Third IEEE International Workshop on. IEEE, pp. 50-57, March 2005, College Park, MD, USA. Print ISBN: 0-7695-2317-X.

[47] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol", Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, pp. 226-236, June 2002, Lausanne, Switzerland. ISBN: 1-58113-501-7.

[48] ZHAO Jing, CAO Guohong, " VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks", Vehicular Technology, IEEE, pp. 1910-1922, May 2008. Print ISSN: 0018-9545.

[49] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, "Protocol of Change Pseudonyms for VANETs", 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on. pp. 162–7, ISBN: 978-1-4799-0539-3, 21–24 October 2013, Sydney, NSW.

[50] Ms Annu , Ms Sarul, " International Journal of Advanced Technology in Engineering and Science", Vol. No.3, Special Issue No. 01, pp. 2810-2821, September 2015, New Delhi, India. ISSN: 2348 75-50.

[51] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." International Conference on Mobile Computing and Networking: Proceedings of the 6 the annual international conference on Mobile computing and networking. Vol. 6. No. 11, pp. 255-265, August 2000, Boston, Massachusetts, USA. ISBN:1-58113-197-6.

[52] Juliette DROMARD, "Vers une solution de contrôle d'admission sécurisée dans les réseaux mesh sans fil ", Thèse, Université de Technologie de Troyes, 6 décembre 2013.

[53] R. Coussement, B. Amar Bensaber, and I. Biskri "Decision support protocol for intrusion detection in VANETs", DIVANet '13 Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications, pp. 31-38, November 2013, Barcelona, Spain. ISBN: 978-1-4503-2358-1.