RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINSTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ AMAR TELIDJI - LAGHOUAT

FACULTÉ DES SCIENCES

DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE

MÉMOIRE DE MASTER

DOMAINE : MATHÉMATIQUES ET INFORMATIQUE

FILIÈRE : INFORMATIQUE

OPTION : RÉSEAUX, SYSTÈMES ET APPLICATIONS RÉPARTIES (RESAR)

Thème

Impact de la signature numérique sur les protocoles de communication dans les VANETs

Présenté par :

DJARBOUA SAIDA HASSANI SOUMIA

Soutenu devant le jury composé de :

Mr. L.BENSAAD	PRÉSIDENT	U. AMAR TELIDJI, LAGHOUA
Mlle. Z. ABDELHAFIDI	EXAMINATRICE	U. AMAR TELIDJI, LAGHOUAT
Mr. L.OULAD DJEDID	EXAMINATEUR	U. AMAR TELIDJI, LAGHOUAT
Mr. M.B.YAGOUBI	ENCADREUR	U. AMAR TELIDJI, LAGHOUAT
Mr. N.CHAIB	CO-ENCADREUR	U. AMAR TELIDJI, LAGHOUAT

2012-2013

INTRODUCTION GENERALE

De nos jours, les véhicules prennent de plus en plus d'importance dans nos vies et pour le moment la voiture est le moyen de transport le moins sûr. Même si les technologies ont fait d'énormes progrès ces dernières années, aucun système de communication entre véhicules n'a encore été introduit pour diminuer le risque d'accident. La recherche dans ce domaine est devenue très active, et les constructeurs automobiles pensent à intégrer des systèmes de communication sans fils dans les véhicules.

Notre travail est orienté recherche sur les réseaux VANETs, où les nœuds sont des véhicules en mouvement sur les routes. Ce type de réseau est une version spécifique des réseaux mobiles ad-hoc MANET avec des spécificités supplémentaires. Le déploiement de ces réseaux nécessite l'assurance de sécurité de communication. La signature numérique est un élément de base pour assurer la sécurité de communication.

Notre projet consiste à évaluer l'impact de la cryptographie particulièrement les signatures numériques sur les communications véhiculaires.

Notre mémoire est organisé en trois chapitres comme suit :

Le premier chapitre, est une introduction générale aux réseaux Ad Hoc de véhicules, dans lequel nous avons abordé toutes les généralités liées à ce type de réseaux.

Le deuxième chapitre, présente la sécurité dans les réseaux ad hoc de manière générale et montre les mécanismes de sécurité utilisés dans les VANETs, et on termine par le routage sécurisé dans les réseaux Ad Hoc.

Dans le troisième chapitre, nous avons porté notre attention sur la simulation d'un protocole dans les VANETs, résultant de l'adaptation du protocole de routage géographique GPSR. Nous avons présenté les différents paramètres utilisés pour la simulation, suivis des mesures de performances adoptées pour son évaluation. Ces résultats de simulations vont nous permettre de situer notre approche et de comprendre son comportement.

En fin nous terminons ce mémoire par donner une conclusion générale et tracer des axes pour des futurs travaux.

Chapitre1

Introduction aux réseaux VANETs

1.1 INTRODUCTION

Un réseau VANET (Vehicular Ad Hoc Network) est un réseau sans infrastructure fixe, constitué d'un ensemble de véhicules dénommés nœuds mobiles. Les premières applications conçues pour les VANETs ont concerné la sécurité routière (systèmes de transports intelligents (STI)). L'objectif majeur de ces applications est de fournir aux véhicules présents dans le réseau, des informations utiles concernant l'état de la circulation routière pour aider à la conduite et proposer des services de sécurité actifs comme l'avertisseur d'accident, le trafic en temps réel et des systèmes actifs de diffusion de l'information.

En outre, ces réseaux ne sont pas conçus pour améliorer la sécurité sur les routes seulement, mais offrent également de nouveaux services de confort aux usagers de la route (internet, jeux,…etc).

Dans ce chapitre nous introduisons le concept des réseaux Ad Hoc et les caractéristiques inhérentes à ces réseaux. Ensuite nous définissons les réseaux VANETs et leurs caractéristiques, et enfin quelques domaines d'application d'un réseau VANET.

1.2 LES RESEAUX Ad-Hoc *:*

1.2.1 DEFINITION *:*

Les réseaux ad-hoc sont des réseaux mobiles sans infrastructure également appelés IBSS (Independent Basic Service Set) ne comporte pas l'entité, tous les sites du réseau sont mobiles et communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil. L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau. **[1]**

Les réseaux Ad Hoc, dans leur configuration mobile, sont connus sous le nom de MANET (pour Mobile Ad-hoc NETworks).

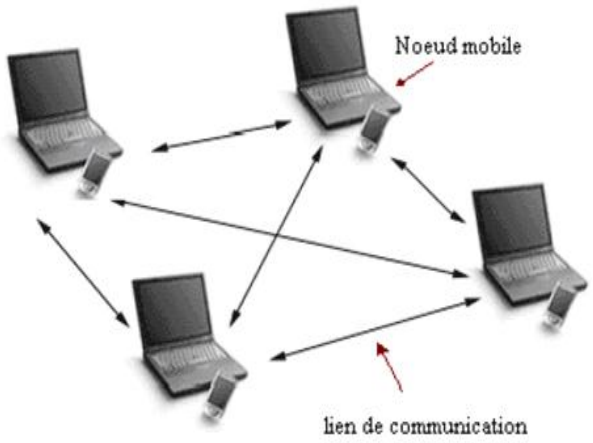

Figure 1.1 : ***Un exemple de réseau Ad Hoc*** **[2]** ***:*** Dans un réseau Ad Hoc les nœuds peuvent joindre ou quitter le réseau de manière totalement dynamique sans informer le réseau.

1.2.2 Les caractéristiques des réseaux Ad Hoc :

Les réseaux mobiles Ad Hoc sont caractérisés par ce qui suit:

- **L'absence d'infrastructure centralisée :**

Les réseaux Ad Hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.

- **Une topologie dynamique :**

Une particularité très importante qui distingue les réseaux mobiles Ad Hoc des réseaux filaires et la mobilité de ses nœuds. Les nouds sont libres de se déplacer arbitrairement, des routes peuvent être crées et disparaitre très souvent ce qui provoquent des changements fréquents dans la topologie du réseau. Ces modifications doivent être prises en compte par le protocole de routage, cette caractéristique rend la topologie de ce type de réseau sans fil très dynamique.

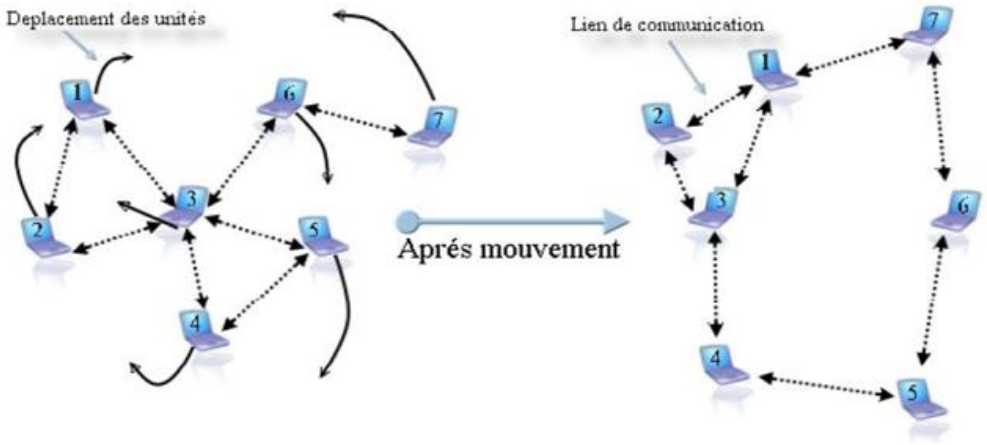

Figure 1.2 : ***Topologie dynamique des réseaux Ad Hoc.***

- **La contrainte d'énergie :**

Les équipements mobiles disposent de batteries limitées, sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité du routage. Cela limite les services et les applications supportées par chaque nœud.

- **Une bande passante limitée :**

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

- **L'hétérogénéité des nœuds :**

Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquence différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau.

- **Sécurité et vulnérabilité :**

Dans les réseaux Ad Hoc, le principal problème réside dans tous les nœuds équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont très grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'intrusions.

- **Communication Multi-sauts :**

Un réseau Ad Hoc est qualifiés par « multihops » car plusieurs nœuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires.

1.2.3 LES DIFFERENTS TYPES DE RESEAUX Ad Hoc : [3]

Nous avons plusieurs types de réseaux Ad Hoc on a choisi les deux types dont on aura dans notre recherche

a) MANET : Un réseau mobile Ad Hoc (MANET) est un système autonome composé de stations mobiles interconnectées par des liens sans fil sans l'administration d'une infrastructure centralisée.

Suivant les communications existantes dans le réseau, les stations (ou nœuds) mobiles peuvent jouer le rôle de routeur pour relayer les données.

b) Les réseaux véhiculaires ou VANETs : Sont une forme de réseau mobile Ad-Hoc permettant aux véhicules de communiquer entre eux ou avec l'infrastructure afin d'augmenter la sécurité et le confort des passagers.

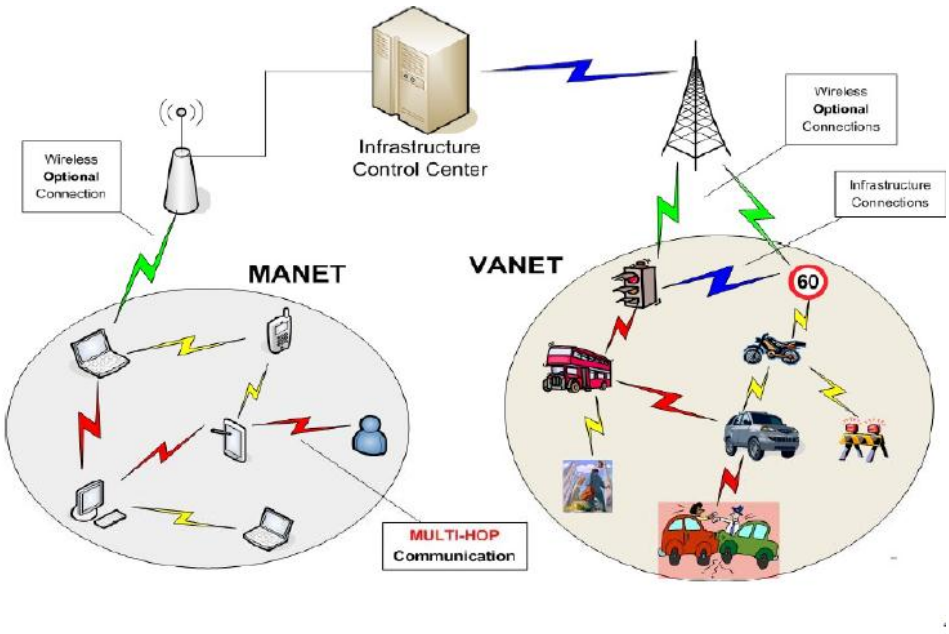

Figure 1.3 : ***Réseau MANET et VANET***

1.3 RESEAUX VEHICULAIRES Ad Hoc :

1.3.1 Définition d'un réseau VANET :

Les VANETs (Vehicular Ad Hoc NETworks) sont une catégorie des MANETs (Mobile Ad Hoc NETwork) permettant la communication entre les véhicules. En plus des caractéristiques des réseaux Ad Hoc mobiles classiques, les VANETs ont la particularité d'avoir une très grande mobilité c'est à dire les nœuds mobiles circulent à très grande vitesse. La topologie dynamique provoque de nombreuses reconfigurations (mise à jour des tables de routage, etc.), et soulevé par conséquent des problèmes de performances. **[4][2]**

1.3.2 Les technologies utilisées dans la communication véhiculaire :

Les réseaux véhiculaires par analogie à ce qui existe dans les réseaux sans fil peuvent être déployés suivant trois catégories : **[2]**

a) Communication de véhicule à véhicule (V2V) :

Dans cette catégorie, un réseau de véhicules est vue comme un cas particulier du réseau MANET (Mobile Ad Hoc NETwork) où les contraintes d'énergie, de mémoire et de capacité sont relaxées et où le modèle de mobilité n'est pas aléatoire mais prévisible avec une très grande mobilité.

Cette architecture peut être utilisée dans la diffusion d'alerte ou pour la conduite coopérative. Aucune infrastructure est utilisée, aucune installation n'est nécessaire sur les routes et tous les véhicules sont équipés pour communiquer directement entre eux n'importe où que ce soit sur les autoroutes, des routes de montagne, ce qui donne une communication couteuse et plus flexible.

Cette approche soufre de certains inconvénients dont nous citons :

- Les délais de communication qui sont élevés, étant donné que la communication se fait en utilisent le multi sauts.
- Les déconnections fréquentes dues au fait que les véhicules sont mobiles.
- La sécurité réseau est très limitée.

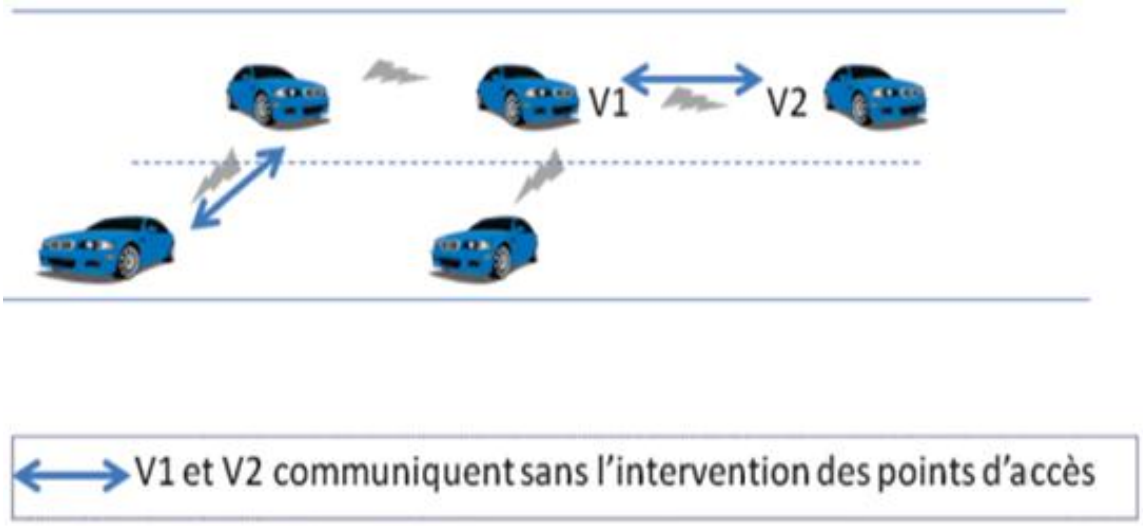

Figure 1.4 : ***Communication véhicule à véhicule***

b) Communication de véhicule avec utilisation d'infrastructures (V2I)

Dans cette catégorie, on ne se concentre pas seulement sur de simples systèmes de communications inter véhicules mais aussi ceux qui utilisent des stations de bases ou points d'infrastructure RSU (road side units). Cette approche repose sur le modèle client/serveur où les véhicules sont les clients et les stations installées sur la route sont les serveurs. Ces serveurs sont connectés entre eux via une interface filaire ou sans fil. Toutes communication doit passer par eux. Ils peuvent aussi offrir aux utilisateurs plusieurs services. Concernant le trafic, accès à l'internet échange de donnée de voiture-à-domicile et même la communication de voiture-à-garage pour le diagnostic distant.

L'inconvénient majeur de cette approche est que l'installation des stations sur les routes est une tache couteuse et prend beaucoup de temps, sans oublier les couts relatifs à la maintenance des stations.

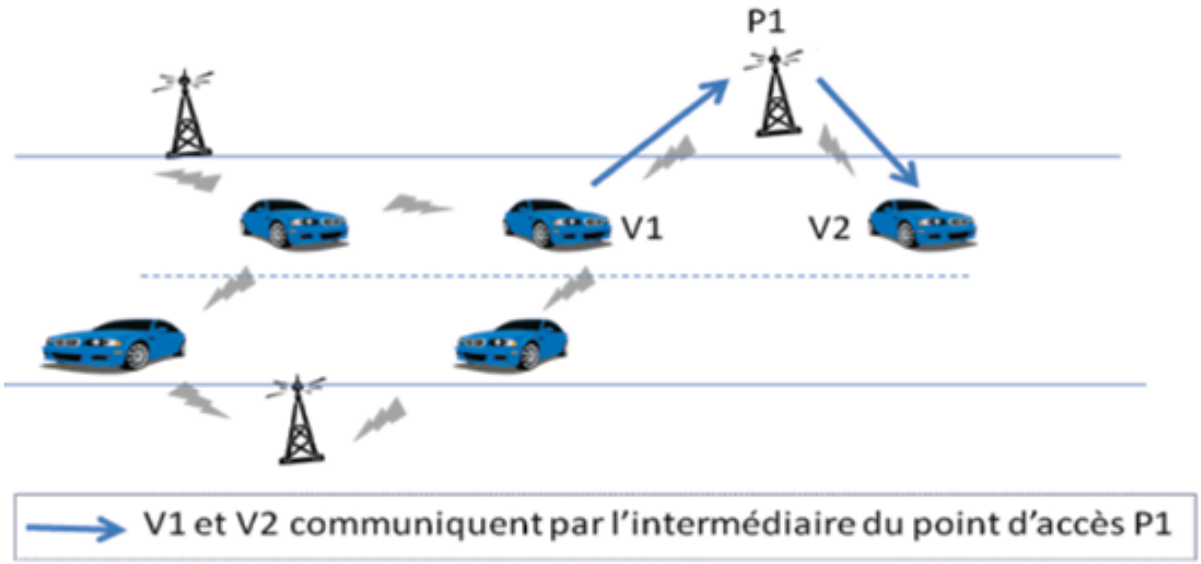

Figure 1.5 : ***Communication véhicule à infrastructure***

c) Communication hybride

La combinaison des communications V2V avec V2I permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures (station de bases) étant limité, l'utilisation des véhicules comme relais permet d'étendre cette distance. Dans un but économique et afin d'éviter la multiplication des stations de bases à chaque coin de rue, l'utilisation des sauts par véhicules intermédiaires prend toute son importance.

1.3.3 Les caractéristiques des réseaux VANET :

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des réseaux Ad Hoc, à savoir : **[2]**

a) La collecte d'informations et la perception de l'environnement proche

La collecte d'informations se fait par l'utilisation des différents capteurs de toutes catégories (caméras, capteurs de pollution, capteurs de pluies, capteurs de l'état de la voiture, etc.…) qui permet au conducteur à bord de son véhicule de disposer d'un certain nombre d'informations et d'une meilleure visibilité pour pouvoir réagir d'une manière adéquate aux changements de son environnement proche.

b) capacités de traitement, d'énergie et de communication

Contrairement au contexte des réseaux Ad Hoc où la contrainte d'énergies à des problématiques traitées, les éléments du réseau VANET n'ont pas de limite en terme d'énergie et disposent d'une grande capacité de traitement et peuvent avoir plusieurs interfaces de communication (wifi, Bluetooth et autres).

c) Environnement de déplacement et modèle de mobilité

Les environnements pris en compte par les réseaux Ad Hoc sont limités à des espaces complètement ouverts et sans obstacle ou indoor (le cas d'une conférence à l'intérieur d'un bâtiment), les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale.

Les contraintes imposées par ce type d'environnements, à savoir les obstacles radio et les effets de la propagation à trajets multiples (multipath), affectent considérablement le modèle de mobilité et la qualité des transmissions radio à prendre en compte dans les protocoles de routage. En plus la mobilité est un facteur lié directement au conducteur de véhicule.

d) Forte mobilité, topologie du réseau et connectivité

A la différence des réseaux Ad Hoc, les réseaux VANETs sont caractérises par la forte mobilité des nœuds (véhicules), liée à la vitesse des voitures qui est très importante dans les autoroute , par conséquent un nœud peut rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquents. De plus, des problèmes peuvent apparaitre quand le système IVC (INTER Véhicule Communication) n'est pas équipé dans la majorité des véhicules.

e) Type de l'information transportée et diffusée

Un des objectifs des réseaux VANETs étant la sécurité routiére. Les types de communication s'axeront sur les diffusions de messages d'une source vers plusieurs destinataires. Nénmoins, les véhicules sont concernées par la diffusion d'information en fonction de leurs positions géographiques et leurs degrés d'implication dans l'evenement déclanché. Dans de telles situation, les communications sont principalement unidirectonnelles.

1.3.4 Les applications des réseaux VANET : [2] [5]

a) Application dans la prévention et la sécurité routière

La sécurité routière devienne une priorité dans la plupart des pays développées, qui est motivée par le nombre croissant d'accident sur ses routes associé à un parc de véhicules de plus important.

Les VANETs permettant de prévenir les collusions(figure 1.6) et les travaux sur les routes, de détecter les obstacles (fixes ou mobile) et de distribuer les information métrologiques par envoi de messages d'alerte par exemple alerter un conducteur en cas d'accidents permet d'avertir les véhicules qui se dirigent vers le lieu de l'accident que le condition de circulation se modifier et qu'il est nécessaire de redoubler de vigilance (figure 1.7). Les messages d'alertes et de sécurité doivent être de taille réduite pour être transmis le plus rapidement possible et doivent être émis à des périodes régulières.

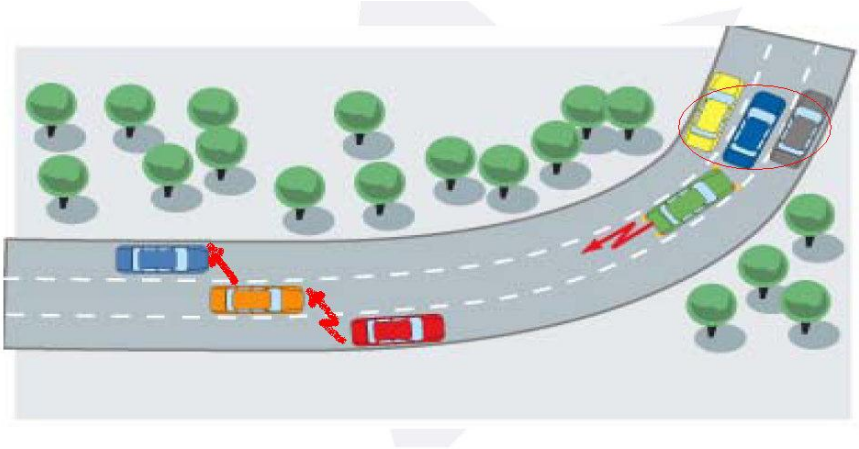

Figure 1.6 : Risque de collision

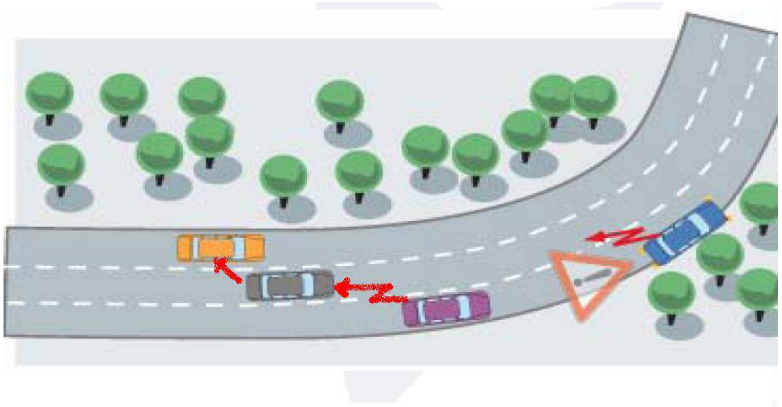

Figure 1.7 : Véhicule en panne

Il est nécessaire, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission. Les messages de sécurité devront être émis à des périodes régulières. Ainsi le ou les nœuds désignés pour la retransmission des messages émettront des alertes à instants réguliers.

b) Application au confort du conducteur et des passagers

Parmi les applications des réseaux véhiculaires, l'amélioration du confort des conducteurs et des passagers. Ce confort est illustré par l'accès à internet, la messagerie, le chat inter véhicule, etc. les passagers dans la voiture peuvent jouer en réseaux, télécharger des fichiers MP3, envoyer des cartes à des amis (figure 1.8).

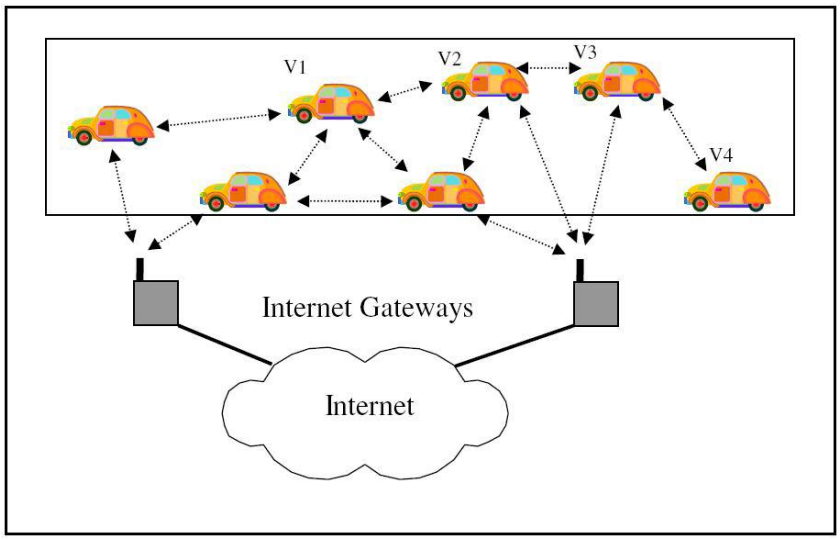

Figure1.8 : Accès à Internet

c) Application pour l'optimisation du trafic et aide dans la conduite

Le trafic automobile peut être amélioré grâce à la collecte et au partage de donnée collectées par les véhicules, ce qui devient un support technique pour les conducteurs. Une voiture peut par exemple, être avertie en cas d'un ralentissement anormal (bouchon, embouteillage, éboulement de rochers ou travaux).

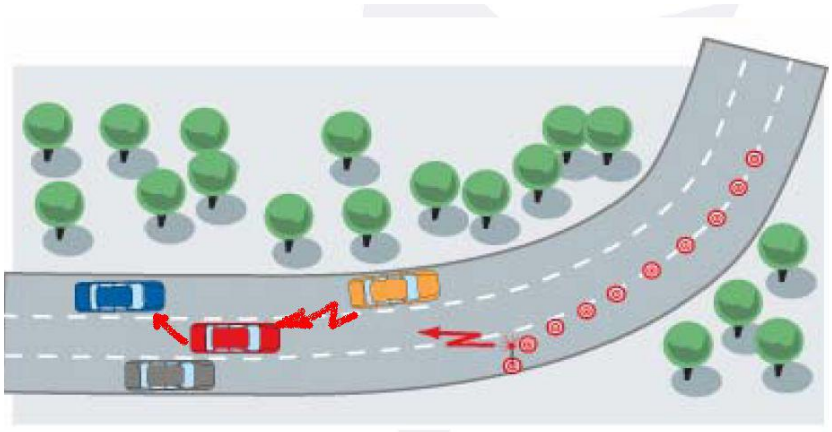

Figure1.9 : Travaux sur les routes

CONCLUSION :

Dans ce chapitre nous avons présenté les réseaux mobiles Ad Hoc ainsi que les réseaux véhiculaires Ad Hoc VANETs qui ne sont qu'un cas particulier des réseaux MANET. Nous avons décrit également leurs caractéristiques, leurs applications et leurs contraintes.

Une des contraintes des réseaux VANETs est le problème d'acheminement des données entre les nœuds mobiles du réseau .dans le but d'assurer la connectivité du réseau, malgré l'absence d'infrastructure et le changement de la topologie, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination : chaque nœud joue ainsi le rôle de routeur.

CHAPITRE 2 : Notions et mécanismes de sécurité

2.1 Introduction

Les applications de sécurité du trafic routier, présentées dans le premier chapitre utilisent les messages d'alerte pour informer le conducteur de situations potentiellement dangereuses (conditions de route dégradées, freinage d'urgence d'un autre véhicule, obstacle, etc.). Si ces alertes sont envoyées à tort, ou à outrance, alors l'utilisateur n'y prêtera plus attention. L'alerte elle-même peut devenir une menace, et provoque des accidents à cause des réactions des utilisateurs.

Pour cela il faut protéger et sécuriser les informations concernant les véhicules et leurs conducteurs pour assurer le bon fonctionnement d'un système de transport intelligent. La sensibilité des données véhiculées par un réseau VANET démontre un besoin fort en sécurité. En effet, l'importance de la sécurité dans ce contexte est cruciale vue les conséquences critiques qui résultent d'une violation ou d'une attaque.

En plus, pour pouvoir sécuriser un VANET, il est nécessaire de connaitre les menaces possibles, liée à la sécurité. Ainsi, nous détaillons dans ce chapitre les modèles d'attaquants et les attaques possibles.

2.2 Notions et mécanismes de base de la sécurité

A cause de l'importance de l'information envoyée aux équipements embarqués dans les véhicules, la sécurité des communications dans les VANETs permet d'assurer d'autres objectifs. Dans cette section, nous présentons des les mécanismes de base qui ont été mis en œuvre pour la sécurité de ces réseaux. **[6] [4]**

- **La cryptographie** :

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en employant souvent des secrets ou des clés. Elle consiste à appliquer des transformations sur le contenu d'un message à l'aide des algorithmes de chiffrement (afin de l'en rendre incompréhensible) et de déchiffrement (afin de reconstruire le message original).

- **La cryptographie symétrique** (ou cryptographie à clé secrète)

Le principe du chiffrement symétrique consiste pour l'expéditeur et le destinataire à utiliser la même clé secrète pour le chiffrement et le déchiffrement. Ils doivent au préalable partager cette clé identique de manière sûre.

- **La cryptographie asymétrique**(ou cryptographie à clé publique) :

Elle utilise deux clés, une clé publique pour le chiffrement, Cette clé peut être connue de tous par exemple ; disponible dans un répertoire accessible publiquement. Et une clé privée (secrète) pour le déchiffrement. Cette clé est liée (mathématiquement) à la clé publique correspondante, elle permet de déchiffrer tout message chiffré avec la clé publique correspondante.

- **Le certificat numérique:**

C'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'**autorité de certification** (AC).

- **Fonctions d'hachage :**

La fonction d'hachage permet d'extraire une empreinte qui caractérise les données. Cette empreinte a une taille fixe indépendamment de la taille des données. Il est pratiquement impossible de trouver deux données ayant la même empreinte.

- **Les fonctions de hachage à sens unique** :

Il est aisé de calculer l'empreinte d'une chaine donnée, mais il est difficile d'engendrer des chaine qui ont une emprunte donnée, et donc de déduire la chaine initiale à partire de l'emprinte .on demande géneralement en plus à une telle fonction d'être sans collusion, c'est à dire qu'il soit impossible de trouver deux messages ayant la même empreinte. On utilise souvent le terme fonction de hachage pour désigner, en fait, une fonction de hachage à sens unique sans collusion.

- **La signature numérique**:

La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier. Son implémentation fait appel aux fonctions de hachage et la clé privée du signataire.

- **Les systèmes de la signature numérique**

Le système RSA

L'algorithme RSA, introduit par Rivest, Shamir et Adlemanest, est le premier algorithme de chiffrement asymétrique. Son principe est de générés des clés publique, et publier librement les clés de cryptage. N'importe qui peut alors crypter un message, mais seul son destinataire, qui possède la clé de décodage, pourra le lire. L'algorithme RSA est très utilisé dans le domaine du numérique (pour les payements en ligne, lors des transactions avec des cartes bancaires. . .) et repose sur des propriétés arithmétique relativement simples.

Le système ECDSA (Elliptic Curve Digital Signature Algorithm)

L'algorithme ECDSA assure la génération des paires de clés (clé privée et clé publique) nécessaire aux signatures.

L'algorithme ECDSA fait la génération d'une paire de clés, par la fabrication d'une signature avec la clé privée et la vérification de cette signature avec la clé publique.

Le système DSA (Digital Signature Algorithm)

Le système DSA est une variante du système El Gamal-Schnorr. DSA sert uniquement comme système de signature et ne permet pas de chiffrer un message. La clé secrète opère sur le message généré par SHA-1. La longueur de la clé varie entre 512 et 1024 bits.

- **Le MAC** (Message Authentification Code MAC) Un code d'authentification de message est le résultat d'une fonction de hachage à sens unique dépendant d'une clef secrète : l'empreinte d'épand à la foi de l'entrée et de la clé. On peut construire un MAC à partir d'une fonction de hachage ou d'un algorithme de chiffrement par blocs. Il existe aussi des fonctions spécialement conçues pour faire un MAC.

2.2.1 Les objectifs de la sécurité

La sécurisation des communications dans les réseaux sans-fil comme dans les réseaux filaires nécessite la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent **[4] :**

- **L'authentification**:

Les applications déployées dans les réseaux Ad Hoc ont besoin d'avoir confiance en l'information. Cette confiance est assurée par l'authenticité. Par exemple, dans le cas d'un message (un signal d'alerte), la fonction du service d'authenticité est d'assurer au destinataire que le message a bien pour origine la source dont il prétend être issu.

- **La non-répudiation** :

Toute entité, après avoir émis un message, ne doit pas pouvoir ensuite nier cette action. Assurer la non-répudiation pour les applications de sécurité routière va donc minimiser la possibilité d'injecter des informations erronées.

- **La confidentialité**:

Elle consiste à garantir que les données échangées ne sont dévoilées qu'aux personnes voulues, alors la confidentialité est la protection des données transmises contre les attaques passives (écoute clandestine).

- **L'intégrité**:

Est de garantir que les données échangées ne sont pas altérées intentionnellement ou non. Donc, il permet aux destinataires de détecter les manipulations de données effectuées par les entités non autorisées et de rejeter les paquets correspondants.

- **La disponibilité:**

L'objectif de la disponibilité est de garantir un accès permanent à un service ou a des ressources.

2.3 La sécurité dans les réseaux sans-fil Ad Hoc [7]

Comme les réseaux VANETs peuvent être considérés comme une sous classe des réseaux sans-fil Ad Hoc, ils en héritent les problèmes de sécurité. En raison de la sensibilité des domaines d'utilisation des VANETs, une intrusion d'un véhicule malicieux aurait des conséquences graves sur l'ensemble des véhicules interconnectés, c'est pour cette raison que beaucoup de travaux de recherche ont été réalisés pour développer un mécanisme de sécurité instituant. Les relations de confiance entre les nœuds communicants et garantissant le contrôle d'accès aux services, pour assurer le bon fonctionnement d'un système de transport intelligent.

Dans cette section, nous nous intéressons à la sécurité des réseaux sans-fil Ad Hoc de manière générale, nous présentons quelques exemples d'attaques sur ces réseaux, ensuite nous en décrivons les objectifs de sécurité.

2.3.1 Les caractéristiques de la sécurité dans les réseaux Ad Hoc

Lors de l'analyse de la nature des communications dans les réseaux Ad Hoc, des propriétés spécifiques liées à la sécurité et la confidentialité doivent être prises en compte pour la conception des protocoles de communications, à savoir : **[8]**

a. Les communications multi-sauts :

Les protocoles de communications multi-sauts sont obligatoires pour avoir des communications sans-fil à longue portée dans les réseaux Ad Hoc, ce qui signifie que tous les nœuds doivent coopérer pour assurer le fonctionnement du réseau. Malheureusement les nœuds malveillants peuvent exploiter ce principe et de compromettre la sécurité du réseau, donc des mécanismes de sécurité appropriés doivent être mis en œuvre.

b. La diffusion d'information de la position géographique:

Avec certains protocoles dans les réseaux Ad Hoc mobiles, les nœuds sont supposés envoyer périodiquement des messages (balises) indiquant leurs positions courantes ou éventuellement d'autres données nécessaires pour des services spécifiques. Par conséquent, les attaquants peuvent créer un profil sur les trajectoires des nœuds et donc les utilisateurs du réseau.

c. Un support de transmission partagé:

Comme avec tout système de communication sans-fil, l'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés ou bien d'injecter de faux messages dans le réseau.

d. Les opérations autonomes:

Les nœuds eux mêmes déterminent leurs états et décident des informations à envoyer de manière autonome. Par conséquent, il est facile pour les entités malveillantes qui ont le contrôle sur un ou plusieurs nœuds d'envoyer des informations falsifiées. Les systèmes de sécurité, à leur tour, doivent employer des mécanismes qui détectent et empêchent l'utilisation de ces informations.

2.3.2 Les modèles d'attaquant : [4]

Pour éviter les attaques possibles sur un réseau Ad Hoc, il faut d'abord définir les modèles d'attaquant possibles. Les critères de classification d'attaquant sont come suivante :

- **Actif ou Passif** :

Un attaquant passif ne peut qu'écouter clandestinement le canal de transmission. Il est généralement indétectable mais une prévention est possible.

Un attaquant actif peut générer, modifier, rejeter ou rejouer des messages afin de dissimuler de fausses informations, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. De plus, généralement il n'y a pas de prévention possible pour ces attaques, bien qu'elles soient détectables.

- **Interne ou Externe**:

Un attaquant interne est un membre authentifie du réseau qui peut communiquer avec les autres membres du réseau. Comme il fait partie du réseau, il possède déjà quelques avantages comme les clés publiques utilisées par les autres véhicules. Un attaquant interne peut causer plus de dommages au réseau que l'attaquant externe qui a un accès limite au système.

- ***Malicieux* ou *Rationnel***:

Un attaquant malicieux cherche à détecter des zones de vulnérabilité et à les exploiter pour perturber le système, ou blesser des membres du réseau. Des attaquants qui causent délibérément des accidents de la route sont considères comme malicieux, ce dernier prêt à tout pour arriver à ses fins quels que soient les couts et les conséquences. Par opposition, l'attaquant rationnel vise l'accomplissement d'une tache spécifique sur le réseau en défaveur d'une personne identifiée. Les attaques rationnelles sont plus prévisibles que les attaques malicieuses.

2.3.3 Les attaques dans les réseaux sans-fil Ad Hoc

Un réseau sans-fil qui n'est pas bien sécurisé est exposé à de plusieurs types d'attaques ; nous en citons : **[4] [9]**

a. ***Subversion de la responsabilité***:

Lors d'un accident, un attaquant peut vouloir porter de fausses accusations contre un usager de la route ou permettre aux autres attaquants de rester non identifies.

b. ***Dépréciation de la vie privée*** **:**

A partir des informations de vitesse et de temps contenues dans un message d'alerte, un attaquant peut générer un profil de déplacement. Il pourra alors revendre l'information ou

l’utiliser à des fins malveillantes. Un attaquant pourra par exemple traquer les déplacements d’un convoyeur de fonds afin de lui tendre un piège.

***c. Contrôle à distance de véhicule* :**

A long terme, on peut supposer une automatisation de la conduite. C’est pourquoi en exploitant les vulnérabilités existantes, il sera possible de prendre le contrôle à distance d’un véhicule. Cela est théoriquement possible.

2.4 La sécurité dans les réseaux de véhicules

Les réseaux de véhicules utilisent des communications sans fil, les données sont donc diffusées sur un medium partagé et non sûr. Il est alors très simple pour un nœud malicieux d'intercepter et de modifier des données, ou d'injecter de faux messages. Pour cela il faut protéger et sécuriser les informations concernant les véhicules et leurs conducteurs pour assurer le bon fonctionnement d'un système de transport intelligent. La sensibilité des données véhiculées par un réseau VANET démontre un besoin fort en sécurité. En effet, l'importance de la sécurité dans ce contexte est cruciale vue les conséquences critiques qui résultent d'une violation ou d'une attaque. **[10]**

2.4.1 Les attaques spécifiques sur les VANETs

Dans cette section, nous passons en revue quelques attaques spécifiques sur les VANETs. Ces attaques comprennent : **[4]**

a. Attaque sur la vie privée:

Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou des informations personnelles d'un utilisateur du réseau. Pour identifier et tracer une victime, l'attaquant peut utiliser toute chaine de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaine de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat…etc.

b. Attaque sur la cohérence de l'information :

Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées.

L'intention de l'attaquant est d'altérer la perception qu'ont ses victimes des conditions de circulation (position, vitesse, direction). Ce faisant, l'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes.

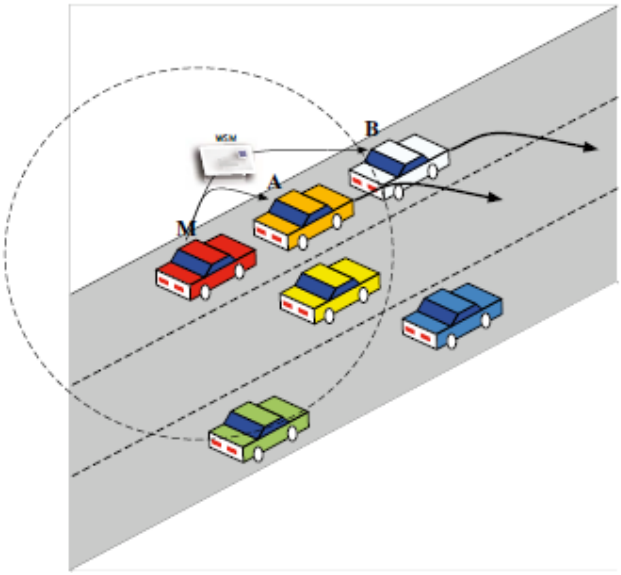

Figure 2-1. ***Attaque sur l'incohérence de l'information :*** un attaquant (M) diffuse des informations de trafic erronées amenant les victimes A et B a changer de voie.

c. Déni de service (DoS) :

Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau, en surchargeant ou en épuisant les ressources du réseau par des requêtes abondantes.

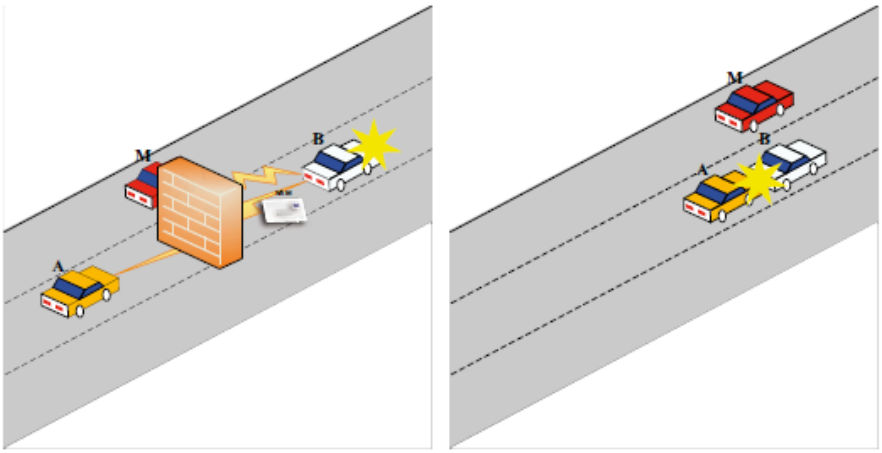

Figure 2-2: ***Attaque Déni de service*** : illustre une attaque par déni de service aboutissant à une collision, car l'attaquant M empêche l'échange de messages critiques entre le véhicule accidente B et le véhicule A.

d. Ecoute clandestine du réseau :

Dans cette attaque, l'entité malveillante collecte les données transmises dans le réseau par les véhicules victimes afin d'en extraire une information dont elle pourrait tirer profit.

Un exemple d'attaque est un attaquant qui espionne une transaction commerciale, typiquement un paiement électronique à un péage, en vue d'en extraire les informations bancaires.

e. Usurpation d'identité ou de rôle :

Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière.

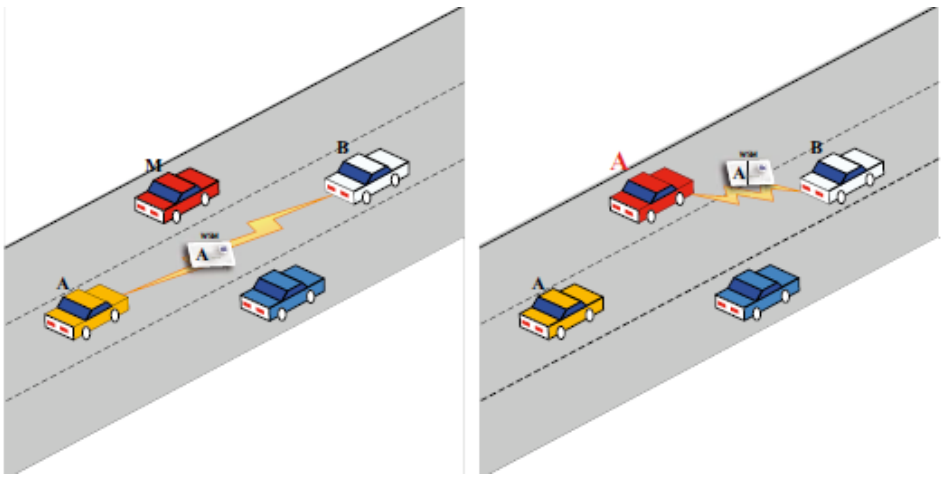

Figure 2-3. ***Usurpation d'identité ou de*** rôle : un cas ou l'attaquant M usurpe l'identité du véhicule A pour récupérer des données du véhicule B.

2.5 Le routage sécurisé dans les réseaux Ad Hoc :

Vue l'impotence de l'opération de routage dans les communications IVC, il constitue un cible idéal pour les attaques. Dans ce qui suit, nous décrirons brièvement la difficulté de routage dans les réseaux Ad Hoc et les différents mécanismes de routages.

2.5.1 Définition :

Le routage est une méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœud appartenant au réseau, ce qui assure l'échange des messages d'une manière continue. **[5]** Vu les limitations des réseaux Ad Hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante.

2.5.2 Les classification des protocoles de routage dans les réseaux AdHoc :

Actuellement il existe plusieurs protocoles de routage pour les réseaux ad-hoc, chacun ayant des propriétés différentes, en distingue deux grandes familles **[11]**

A. Protocoles de routage basés sur la topologie :

Les protocoles de routage basés sur la topologie utilisent les informations sur les liens qui existent entre les nœuds pour l'acheminement des paquets. Cette famille de protocoles peut être divisée en trois catégories suivant la manière dont ils créent et maintiennent les routes lors de l'acheminement des données : les protocoles proactifs, réactifs et hybrides.

En général, les protocoles basés sur la topologie ne supportent pas les réseaux qui dépassent quelques centaines de nœuds [8].

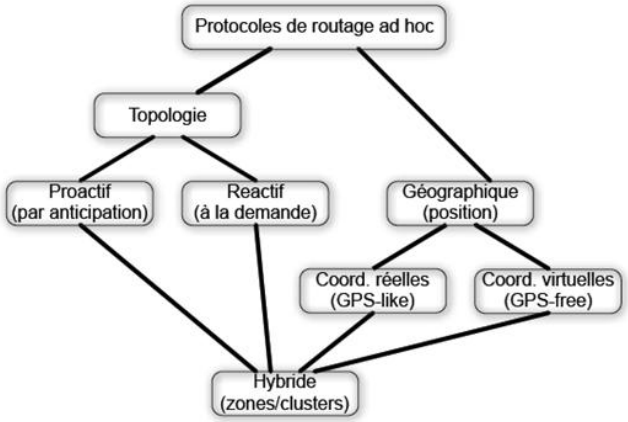

Figure 2.4 : ***Classification des protocoles de routage Ad Hoc*** **[12]**

A1. Protocoles de routages réactifs

Les protocoles réactifs, ne gardent que les routes en cours d'utilisation pour le routage. A la demande, le protocole va chercher à travers le réseau une route pour atteindre une nouvelle destination. Ce protocole est basé sur deux mécanismes "Découverte de route" et "Maintenance de route".

Nous allons décrire dans ce qui suit, les protocoles les plus importants de cette classe : **[13]**

- **AODV** (Ad Hoc On Demand Distance Vector) C'est-à-dire établissement d'une route (un chemin) si un nœud demande (*On-Demand*). Il permet de réduire les charges de réseau en permanent. Par conséquent, il s'adapte mieux à la dynamique de topologie par rapport aux routages proactifs. Il utilise un numéro de séquence crée par la destination, ceci permet de choisir un «meilleur chemin» entre la source et la destination et il peut également éviter des chemins infinis. Dans ce protocole 3 messages sont échangés entre les nœuds pour créer un chemin de source vers la destination :

RREQs -(Route Requests): requête de recherche de chemin.

Quand un nœud demande une route, il fait une requête RREQ. Pour éviter une diffusion «innondable», la recherche de chemin est limitée par le temps TTL (la durée de vie de RREQ qui se trouve dans l'en-tête' IP)

RREPs (Route Replies):

Quand la destination reçoit une RREQ, un paquet de réponse de route doit être envoyé à la source (RREP : Route REPly)

Les nœuds appartenant au chemin de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse.

RERRs (Route Errors): RERR est envoyé à la source si un nœud détecte une rupture de lien (connexion)

- **DSR** (**Dynamic source routing**) :

Fondé sur le principe du routage par la source, Les nœuds n'ont pas besoin de tables de routage, dans cette technique lorsqu'une source veut initier un flux vers une destination il envoi une requête spéciale : ROUTE REQUEST (par inondation)

Cette requête parvient au destinataire en plusieurs exemplaires via différentes routes.

Dans ce cas il choisira la route la plus optimal.

Si une route est trouvée, un paquet Route Reply contenant la séquence de nœuds appropriée pour atteindre la destination est renvoyé en unicast au nœud source. DSR ne prend pas en compte la bidirectionnalité des liens puisque le paquet Route Reply est envoyé au nœud source selon une route déjà stockée dans la « cachette de routes » d'un nœud intermédiaire ou à l'aide d'une réponse du nœud destinataire. **[11]**

A2. Protocoles de routages proactifs

Les protocoles proactifs consiste à établir les routes à l'avance en se basant sur l'échange périodique des tables de routage, ce protocole est base sur deux méthodes sont : La méthode Etat de Lien ("Link State") et la méthode du Vecteur de Distance ("Distance Vector"), les deux méthodes exigent une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau.

Nous allons décrire dans ce qui suit, les protocoles les plus importants de cette classe :

- **OLSR: (Otimized Link State Routing) [12]**

Est un protocole à état de liens qui fabrique des routes de plus court chemin.

Dans ce protocole, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints. Ces relais multipoints sont des nœuds qui n'ont la

connaissance que de nœuds considérés pertinents. Les nœuds considérés comme redondants pour le calcul des plus courts chemins ne font pas parti de la liste de nœuds connus par ces relais multipoints. Les nœuds pertinents sont sélectionnés de façon à pouvoir atteindre tout le voisinage à deux sauts.

Cet ensemble est appelé l'ensemble des relais multipoints.

Le rôle des relais multipoints est de :

- ✓ diminuer le trafic engendré par la diffusion des messages de contrôle dans le réseau,
- ✓ diminuer le nombre de liens diffusés à tout le réseau puisque les routes sont construites à base des relais multipoints

A3. Les protocoles hybrides

Les protocoles hybrides combinent les deux approches. Ils utilisent un protocole proactif, pour apprendre le proche voisinage (voisinage à deux ou trois sauts) et un protocole réactif pour atteindre les nœuds situés au-delà de cette zone prédéfinie de voisinage. **[12]**

Les protocoles hybrides font appels aux techniques des protocoles réactifs pour chercher des routes.

B. Les protocoles de routage géographique

Les protocoles de routage géographiques sont les plus adaptés pour les réseaux Ad Hoc de véhicules, puisque le mécanisme de routage se base sur les données géographiques des nœuds. **[14]**

Ces protocoles se basent sur le fait que tous les nœuds connaissent leur position, par exemple, grâce à un équipement GPS (Global Positioning System) ou grâce à un système logiciel, afin de trouver un chemin vers la destination, Les protocoles de routage géographiques comportent deux étapes : la première consiste à retransmettre le paquet sur un chemin de routage construit à l'intérieur d'une zone déterminée, appelée zone de retransmission (Forwarding Zone). La **deuxième** étape consiste à diffuser le paquet aux nœuds à l'intérieur de la région cible (Geocast Region). **[14]**

Nous allons décrire dans ce qui suit, les protocoles les plus importants de cette classe : **[15]**

- GPSR Greedy Perimeter Stateless Routing, est un protocole de routage efficace pour les réseaux Ad Hoc véhiculaires. Contrairement aux algorithmes de routage mis en place avant, qui utilisent des notions de théorie des graphes du chemin le plus courts et l'accessibilité transitive pour trouver des routes, GPSR exploite la correspondance entre la position géographique et la connectivité dans un réseau sans fil, en utilisant les positions des nœuds afin de prendre des décisions de transfert de paquets.

Alternativement, le protocole 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.

L'acheminement des paquets par GPSR se fait selon deux modes suivant la densité du réseau : le « Greedy Forwarding » et le « Perimeter Forwarding » (appelés respectivement GF et PF dans la suite).

Greedy Forwarding:

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. La figure 2.5 montre un exemple de ce mode d'acheminement.

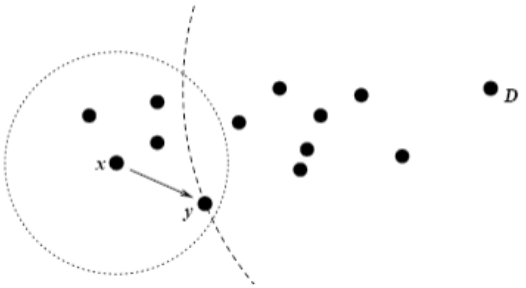

Figure 2.5 : **Greedy Forwarding**

Cet algorithme d'acheminement offre un taux de réussite assez proche des réseaux filaires dans le cas où la mobilité de la destination n'est très forte. Lorsqu'un paquet de données atteint une région où le GF échoue, alors le PF est utilisé

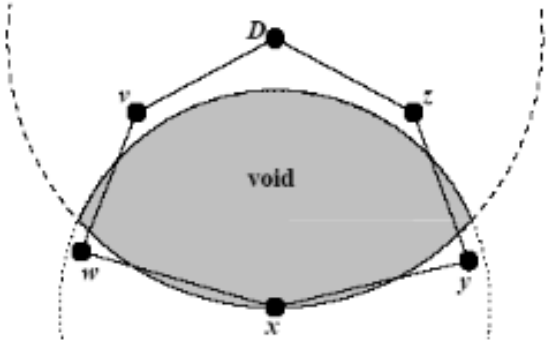

Figure 2.6 : **Explication de la méthode *Greedy Forwarding***

Périmètre Forwarding:

Cet algorithme utilise la règle de la main droite qui est définie comme suit : 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 « crossing links » (route déjà parcourue). La figure 2.7 montre un exemple plus précis de ce mode.

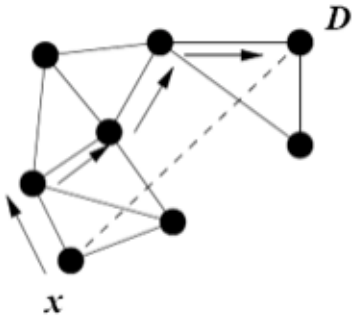

Figure 2.7 : Passage au mode PR

- ✓ **Les avantages du GPSR sont les suivants :**

-Il marche mieux sur les grandes routes avec un partage égal des nœuds, car sans obstacles il obtient de très bonnes performances.

-Le résultat de la comparaison de la simulation du GPSR est généralement considéré comme meilleur que celle du DSR.

- ✓ **Les inconvénients du GPSR sont les suivants:**

- le "Greedy Forwarding" est restreint à cause des obstacles.

-Les performances de routages se dégradent à cause de la longueur des chemins résultant des longs délais d'attente.

-La mobilité des nœuds peut inciter des boucles de routages.

-Les paquets sont parfois envoyer dans de mauvaises directions, ce qui augmente les délais.

2.6 Exemples d'attaques contre les protocoles de routage

Dans cette session, nous décrivons quelques attaques connues sur les protocoles de routage dans les réseaux Ad Hoc:

2.6.1 Attaque Flooding : [18]

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille (paquets de demande de route, de formation de groupes...etc.) La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

2.6.2 Attaque Rushing : [12]

Cette attaque n'affecte que les protocoles réactifs. Le but est de faire passer un maximum de messages par l'attaquant. Dans lesquels un nœud ne transmet que le premier message de type ***Route Request*** reçu et rejette les autres (pour une même demande). En effet, s'il reçoit deux fois la même Route Request, la deuxième est forcément moins bonne car plus longue (sinon il l'aurait reçue en premier). L'attaquant va donc se dépêcher de transmettre toutes les Route Requests qu'il reçoit pour avoir le plus de chances d'être le premier et donc plus de chances que la route passe par lui. Pour cela il peut profiter des temporisations avant l'envoi de message que vont supporter ses voisins (et concurrents).Ces temporisations ont deux origines :

- Le MAC (Medium Access Control) impose souvent un délai entre le moment ou le paquet est délivré à l'interface pour envoi et le moment ou il est effectivement envoyé.
- Même si le MAC n'impose pas de délai, la majorité des protocoles réactifs le font pour éviter Les risques de collusion entre ***Route Requests***.

Il est évident que le détournement de la majeure partie du trafic présente un avantage non négligeable pour réaliser ensuite les attaques citées précédement.

2.6.3 Attaque Sybil : [16]

L'attaquant pratique ici une ***usurpation d'identités multiples***. Cette attaque est en fait une réponse aux solutions de routage multi-routes et probabiliste. Ici l'attaquant ne se contente pas d'usurper une identité mais se fait plutôt passer pour plusieurs nœud différents Dés lors, il est possible pour l'attaquant d'intercepter l'ensemble du trafic même s'il est repartie sur plusieurs routes (l'attaquant aura juste à être présent sur l'ensemble des routes). Cette attaque est très dangereuse sur le routage géographique, car un nœud peut prétendre être sur plusieurs positions stratégiques à la fois, afin d'être choisi comme relai pour l'acheminement de leurs paquets.

2.7 Les protocoles de routage Ad Hoc sécurisés

Pour résoudre les problèmes liés à la sécurité plusieurs protocoles ont été développés. Dans cette section nous présentons quelques protocoles de routage sécurisés :

2.7.1 SRP

Le protocole SRP (*Secure Routing Protocol*) est proposé comme une solution contre les comportements malveillante dont l'objectif est la découverte des informations de topologie ou l'injection de fausses informations de routage .SRP à été conçu pour fournir des informations de rouge correcte .Il nécessite une association de sécurité pré existante entre le nœud source et le nœud destination. Les auteurs proposent dans le même papier un mécanisme qui permet de détecter des comportements malveillants (*Neighbor Lookup Protocol*) et un protocole de sécurisation des données SMT (*Secure Message Transmission protocol*) qu'ils proposent d'utiliser en complémentarité avec SRP. Une analyse a été faite démontrant les vulnérabilités de ce protocole en affirmant principalement que la source ne peut assurer que la route qu'elle a choisie est non corrompue. **[16]**

2.7.2 SAODV

SAODV c'est une extension de sécurité pour le protocole AODV nommée Secure AODV, l'idée principale de SAODV consiste à utiliser une extension cryptographique pour assurer l'authenticité et l'intégrité des messages de routage, et pour éviter les manipulations de la valeur de nombre de sauts (HOP-COUNT). **[17]**

SAODV se propose de sécuriser les données modifiables des informations de routage. Le mécanisme sécurise principalement le champ modifiable *hop count*, qui peut être par exemple décrémenté volontairement par un attaquant, et authentifie à l'aide d'une signature les champs ne devant pas être modifiés. SAODV permet principalement de faire en sorte qu'un nœud malveillant puisse au mieux soit ne pas retransmettre les paquets, soit mentir sur lui même. **[18]**

2.8 Les protocoles de routage existants dans les réseaux VANET

Il existe plusieurs protocoles de routage proposés pour les réseaux VANET; la plupart de ces protocoles ont en commun ou l'utilisation de l'information géographique dans le

routage ou les informations indiquant des distances géographiques entre les nœuds de manière indirecte (par exemple : les techniques basées sur les mesures d'énergie de signal de trames transmises). Les premières tentatives de définition d'un protocole de routage ont commencé par l'adaptation des protocoles de routage topologiques sur les réseaux VANET, en ajoutant généralement des extensions aux protocoles topologiques, parmi les protocoles destinés aux réseaux VANET, nous citons : **[8]**

2.8.1 AODV+PGB :

Afin d'adapter le protocole AODV aux VANETs Naumov et al. ont proposé la stratégie PGB (*Preferred Group Broadcasting*) qui est destinée à être utilisée conjointement avec le protocole AODV pour un double objectif:

- Eviter le problème de *Broadcast storm7* et réduire la consommation de la bande passante lors de la découverte de routes.
- Etablir des routes à durée de vie plus longue.

Selon le PGB, en mesurant la quantité d'énergie du signal, les nœuds recevant la requête de découverte de route peuvent connaitre s'ils appartiennent ou non au groupe préféré, et qui doit rediffuser cette requête. Comme elle doit être rediffusée seulement par un seul nœud qui n'est pas nécessairement le plus proche de la destination, les routes construites seront plus stables.

2.8.2 GPSR+AGF :

Naumov et al. Ont aussi proposé la stratégie AGF basée sur le rafraichissement périodique des informations géographiques dans la table de voisins pour adapter le protocole GPSR aux VANETs. Dans cette stratégie, en utilisant les techniques de localisation, chaque nœud doit intégrer sa vitesse, sa direction et sa position géographique dans les balises afin de permettre à ses voisins de prédire ses futures positions géographiques; donc ces voisins peuvent savoir si ce nœud est dans la portée de leurs zones de couverture radio.

2.8.3 CAR (*Connectivity-Aware Routing*) :

C'est un protocole conçu spécifiquement pour l'environnement véhiculaire, l'avantage principal de ce protocole est qu'il ne se base pas sur un service de localisation indépendant, ce qui lui permet d'optimiser les opérations de découverte de route avec le service de localisation.

Conclusion :

Dans ce chapitre nous avons présenté quelques mécanismes de base de la sécurité dans Les réseaux véhiculaires, les modèles d'attaquant, les attaques possibles et quelques protocoles de routage Ad Hoc sécurisés avec leurs performances dans les réseaux à haute mobilité.

En effet, tous ces protocoles n'assurent pas la sécurité des communications à cent pour cent contre les différentes attaques.

Donc, d'autres mécanismes doivent être mis en œuvre afin d'améliorer sécurité de routage et la disponibilité de réseau.

CHAPITRE3:

LA PERFORMANCE DE GPSR SECURISE

3.1 INTRODUCTION:

Comme les protocoles de routage géographiques, sont préconisés à être utilisés dans les réseaux VANETs, on a envisagé d'utiliser le protocole GPSR qui est un protocole géographique plus connu.

Dans la littérature, il existe plusieurs mécanismes proposés pour sécuriser ce protocole. Nous avons choisi d'utiliser deux mécanismes avec des niveaux de sécurité différents. Bien sur ces mécanismes n'assurent pas une sécurité parfaite mais leur objectif est de minimiser les attaques externes.

Pour étudier l'impact de la cryptographie des protocoles de routage dans les réseaux véhiculaires, le protocole GPSR sera utilisé. Comme ce protocole est un protocole de routage géographique ce dernier est préconisé pour les réseaux véhiculaires.

Dans ce chapitre nous présentons les variantes de GPSR sécurisé et ensuite nous décrivons notre approche pour sécuriser ce protocole.

3.2 Les variantes de GPSR sécurisé :

Dans notre étude, on a constaté qu'il ya plusieurs attaques visant ce protocole, l'information de la position géographique peut être falsifiée ou l'attaquant peut aussi lancer l'attaque Sybil et avoir plus de chance pour contrôler le trafic dans le réseau.
Plusieurs solutions ont été proposées pour sécuriser le GPSR, les plus connues sont:

3.2.1 GPSR protégé contre les nœuds Sybil : [19]

Les auteurs ont proposé ce protocole pour minimiser l'impact de l'attaque Sybil sur le réseau, en minimisant la chance de choisir un nœud Sybil en choisissant des relais minimisant la distance vers la destination de manière aléatoire.

Le mécanisme de défense existant contre l'attaque Sybil doit vérifier et confirmer l'unicité d'identité pour ce nœud physique. En utilisant les signatures numériques qui doivent être générées et vérifiés par les membres du réseau.

- **Critique de cette technique** :

  Dans cette technique, il n'existe pas un mécanisme pour détecter tous les nœuds Sybil notamment dans le cas d'un attaquant interne.
  De plus, les auteurs ne donnent pas une description détaillée de la variante modifiée, ce qui rend ce protocole difficile à implémenter et à évaluer (mesure de performance).

3.2.2 GPSR sécurisé avec clés de session : [20]

Ce protocole utilise la méthode de **Diffie-Hellman** pour l'échange de la clé secrète, cette clé est utilisée par la suite, pour sécuriser les communications entre les deux nœuds.

L'auteur utilise l'algorithme AES pour le chiffrement de données.

- **Critique de cette technique** :

  Dans cette technique, la non-répudiation n'est pas garantie à cause de la clé secrete partagée.

3.2.3 Les variantes de GPSR sécurisé proposées :

Pour étudier l'impact de la cryptographie sur les communications véhiculaires, nous avons besoin d'une variante sécurisée de ce protocole. Vu que les approches trouvées sont limitées et les concepteurs n'ont pas donné les détails de leurs propositions. Dans cette section, nous proposons deux variantes de GPSR sécurisé qui se basent sur deux techniques d'authentification.

a. Variante 1 de GPSR sécurisé :

Dans cette section, nous présentons la première variante de protocole GPSR sécurisé, cette variante n'est qu'une version modifiée de GPSR **[21].**

- **Format de paquet GPSR de la variante1**

Packet Type	**Subtype**	**TTL**	**Flags**
Length		**Protocol**	**Priority**
Sequence Number		**Souirce Timestamp**	
Source ID			
Destination ID			
Source Position (Latitude /Longitude)			
Sender ID			
Sender Position (Latitude /Longitude)			
Sender Time stamp		**Next hop**	
Signature			

Figure 3.1 : Format de paquet GPSR de la variante1

Nous avons ajouté un champ qui comporte la signature numérique du dernier relais, ce champ doit aussi être vérifié avant de regénérer une autre signature numérique

b. Variante 2 de GPSR sécurisé :

Afin d'assurer l'authenticité et l'intégrité des messages de routage du protocole GPSR, les champs d'un paquet sont divisés en deux types de données:

1. **Information immutable:** ce qui ne devrait pas être modifiée sur le chemin de la source à la destination comme adresse source.

   Générée par la source et vérifiée par tous les nœuds intermédiaires.

2. **Information mutable:** ce qui doit être changé sur le chemin de la source à la destination.

   Générée par un nœud source ou intermédiaire et vérifiée par un nœud destination ou intermédiaire.

- **Format de paquet GPSR de la variante 2**

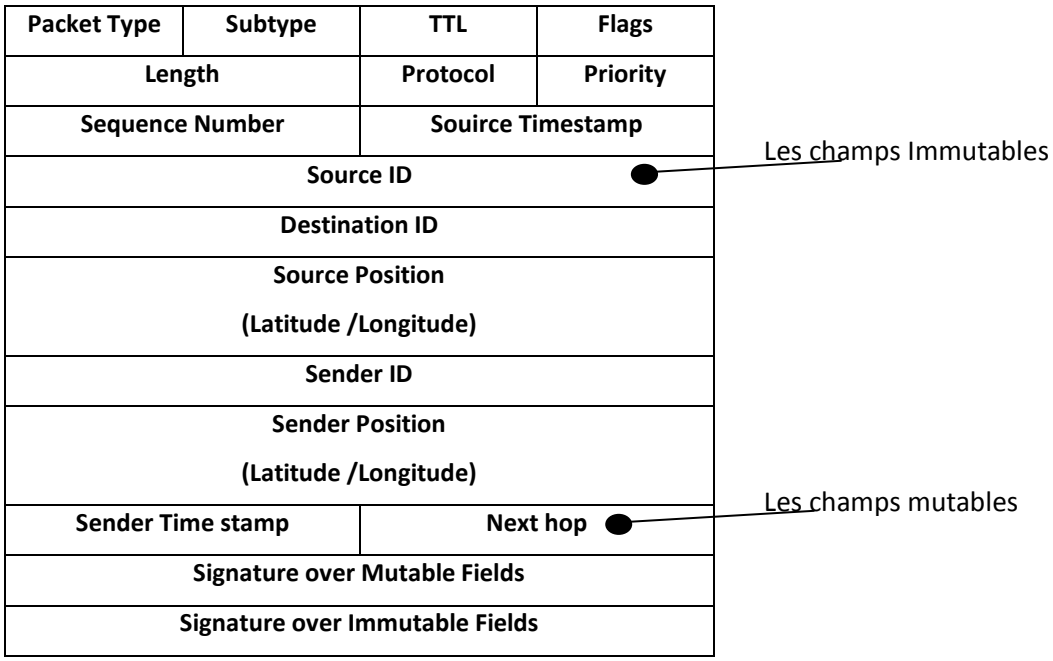

Figure3.2 : **Format de paquet GPSR de la variante 2**

- **Le principe de cette approche est :**

Le nœud source génère une signature numérique sur les champs immutables et une autre sur les champs mutables.

La première signature numérique est vérifiée par les nœuds intermédiaires et ne subit pas de changement au cours d'acheminement du paquet, alors que le champ de la deuxième signature numérique est modifié par chaque nœud intermédiaire après la vérification de la validité de la signature numérique.

Dans ce protocole, le nœud intermédiaire doit :

- •Vérifiez le time stamps.
- •Vérifier les deux signatures numériques.
- • Mise à jour des tables de localisation.
- •Vérifier si S ne dépasse pas le taux d'émission maximale autorisée.
- •Remplacer la signature des champs mutables.

Et le nœud destinataire doit :

- • Vérifier le time stamps.
- •Vérifier les deux signatures numériques.
- • Mise à jour des tables de localisations.

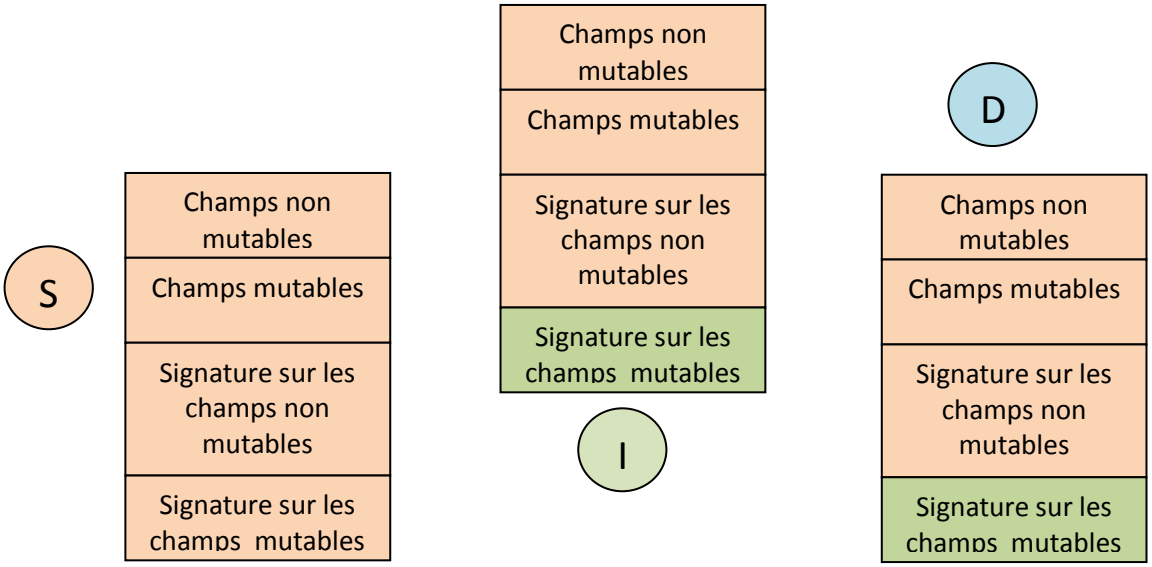

Figure 3.3 : Génération et vérification de la signature numérique pendant l'acheminement d'un paquet.

3.3 Analyse de performance du protocole GPSR :

Dans cette section, nous analysons la performance de notre protocole.

3.3.1 Le simulateur utilisé

Pour analyser la performance de nos algorithmes, nous avons utilisé l'outil NS2. Ce dernier est un simulateur open source utilisé dans les recherches liées aux réseaux de communication d'ordinateurs [**8].** Il est très populaire car il est à accès libre et la majorité des protocoles de réseaux ont été implémenté sous ce simulateur.

3.3.2 Le générateur des modèles de mobilité : IMPORTANT

Pour le modèle de mobilité, nous avons particulièrement étudié le cas des autoroutes, car ces derniers sont plus contraignants en termes de durée de connectivité à cause de haute mobilité. A cet effet, nous avons utilisé l'outil « IMPORTANT » pour générer les fichiers traces définissant des scénarios de mobilité, cet outil a été proposé par l'université de Californie du Sud afin que les simulations liées aux réseaux véhiculaires soient plus réalistes, la documentation et le code source sont téléchargeables depuis le site web**. [8]**

- modèle de mobilité (freeway)

Le modèle Freeway est l'un des modèles qui peut être généré par IMPORTANT, il simule le comportement de mouvement des véhicules sur une autoroute. Il peut être aussi utilisé dans l'échange de trafic ou dans le suivi d'un véhicule sur une autoroute.

3.3.3 paramètres de simulation

Durant la simulation on a utilisé les paramètres suivants :

Paramètre	Valeur
Simulateur	NS-2 version 2.35
La portée de transmission(m)	300m
Le nombre de nœuds	100
Le générateur de la mobilité	IMPORTANT
Le modèle de mobilité	Freeway
Les caractéristiques de l'autoroute	5Km/4 voies pour chaque sens
L'intervalle de temps minimum entre deux messages hello	1 seconde
Vitesse de véhicule (m/s)	[20..30]

Table 3.1 : ***Paramètres de simulation***

3.3.4 Les métriques d'évaluation :

Pour évaluer la performance du protocole simulé, nous considérons les métriques suivantes : délai de bout en bout moyen, le taux des paquets perdus.

- **Délai de bout en bout moyen :**

C'est le temps moyen écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Il comprend les retards générés par les attentes aux files d'attente et les retransmissions sont inclus dans le délai de bout en bout, par contre les paquets de données qui sont perdus en route ne sont pas considérés.

- **Le taux des paquets perdus :**

Le taux de paquets perdus permet de mettre en évidence la qualité de la réception.

Il est possible d'avoir un délai élevé mais un taux de paquets perdus également élevés.

Pour simuler le temps de génération et le temps de vérification nous avons ajouté des timers pour calculer le délai de génération et de vérification de la signature numérique au niveau de chaque nœud.

Pour ce premier scénario, deux paramètres nous ont permet d'obtenir le graphe ci dessous (figure3.4) le délai d'acheminement des paquets (s) et Δ(t): qui représente la durée séparant deux messages hello.

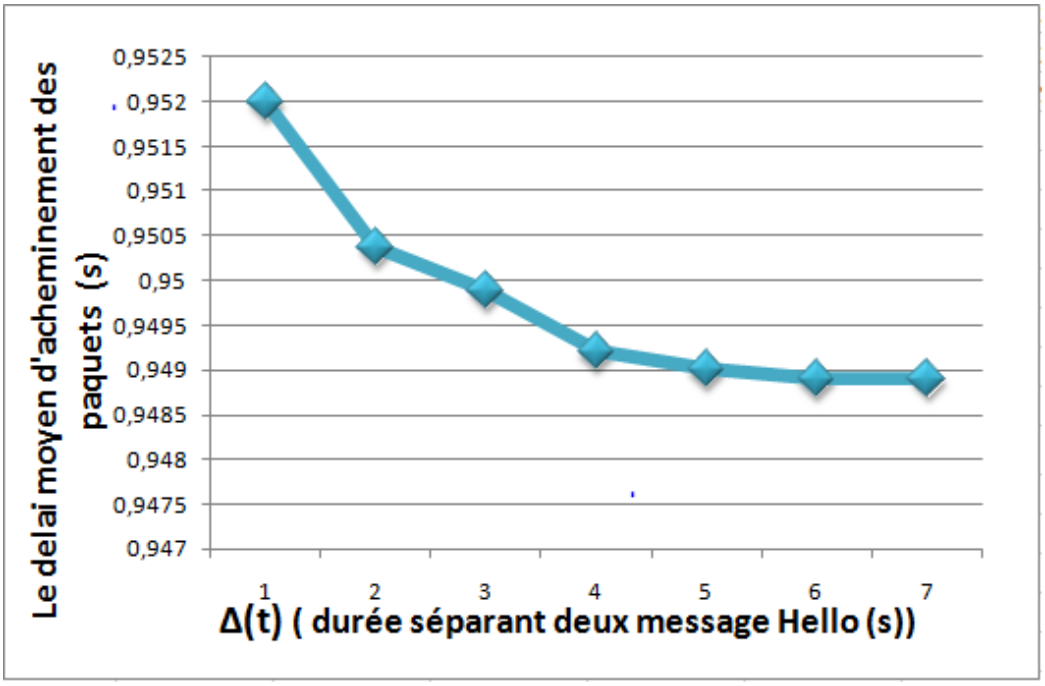

Figure3.4 ***: Délai moyen d'acheminement des paquets***

La figure 3.4 est un graphe qui représente le délai moyen d'acheminement des paquets de bout en bout avec cryptage des paquets conformément à la durée Δ(t) séparent deux messages hello qui est changer chaque fois.

Les résultats obtenus montrent que le délai moyen diminue avec l'augmentation de la durée Δ(t).

Le taux de paquets perdus en fonction de la durée Δ(t) est représenté dans la figure 3.5

.

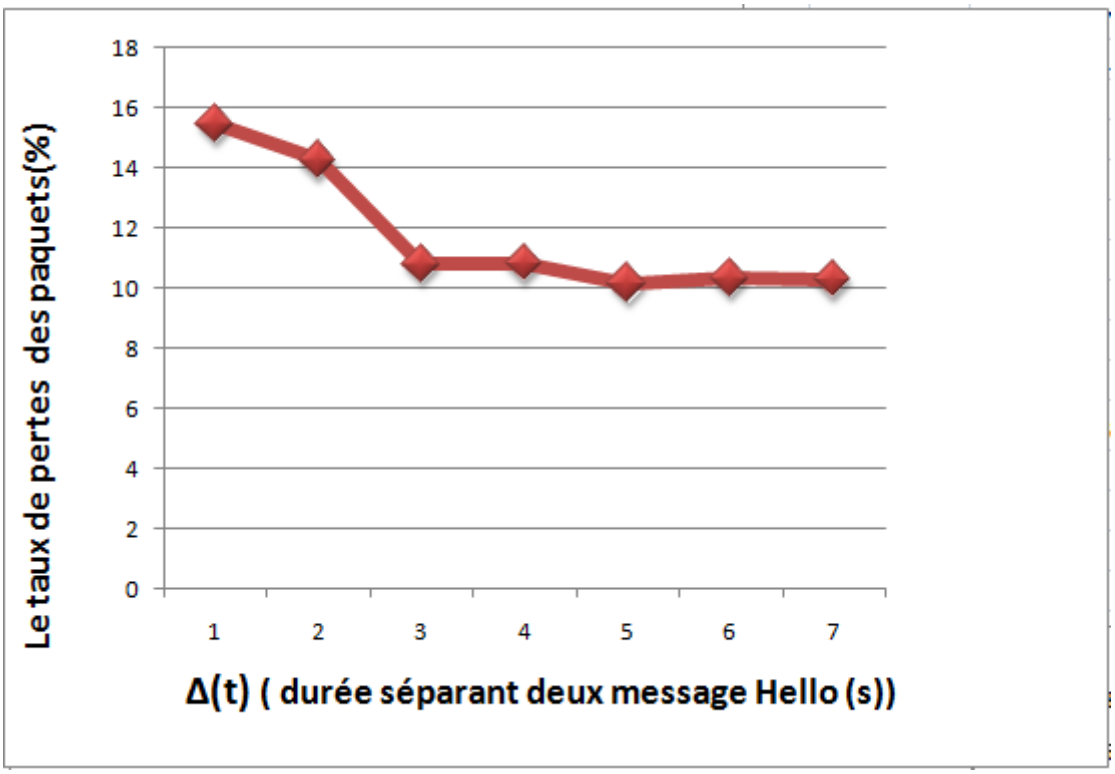

Figure3.5 ***: Les pertes des paquets***

La figure3.5 est un graphe qui représente le taux de perte des paquets conformément à la durée Δ(t). Nous avons changé à chaque fois la durée Δ(t).

Les résultats obtenus montrent que le taux de perte des paquets diminue avec l'augmentation de la durée Δ(t). Par conséquent, la probabilité de collusion regresse, à cause de :

- la consommation élevée de la bande passante.
- nombre de message hello échange.

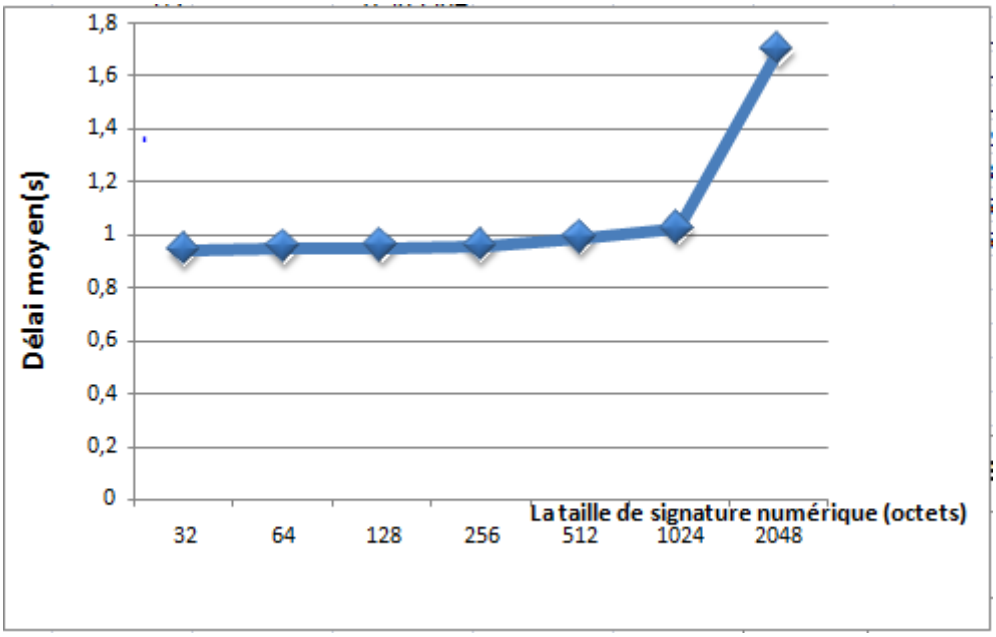

Figure3.6 *: Délai moyen d'acheminement des paquets*

Le graphe de la figure 3.6 représente le délai moyen d'acheminement des paquets de bout en bout avec cryptage en fonction de la taille de la signature numérique car le temps de vérification dépend de la taille de la signature numérique.

Les résultats obtenus montrent que le délai moyen augmente avec la croissance de la taille de la signature numérique.

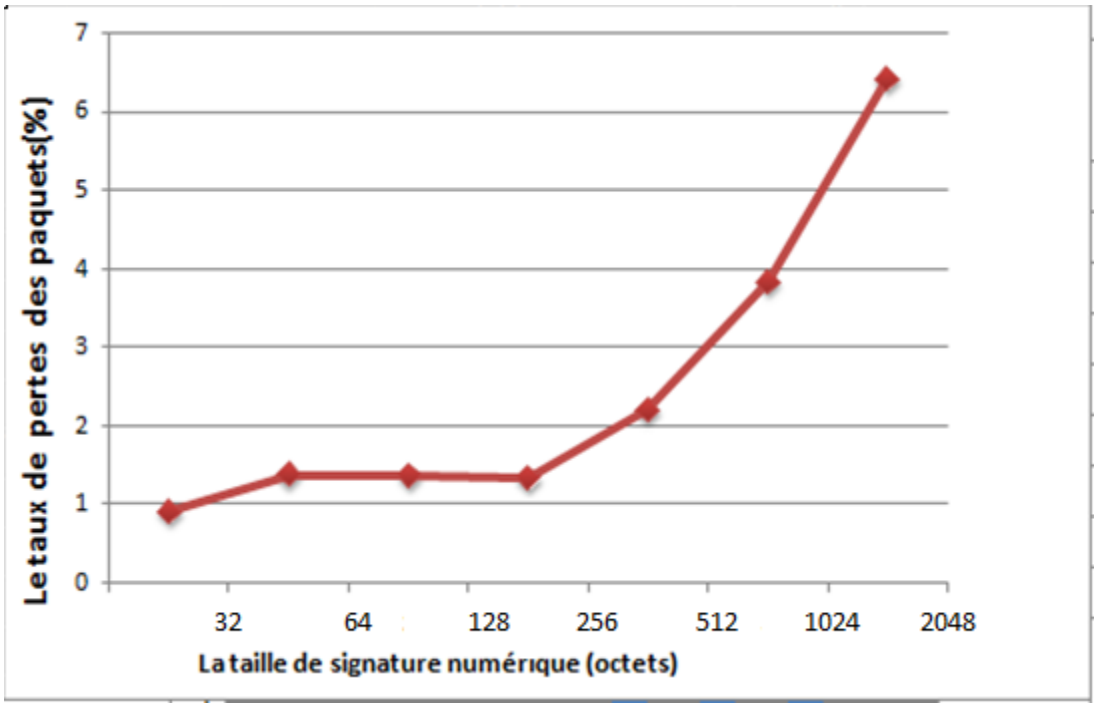

Figure3.7 ***: Les pertes des paquets***

Le graphe de la figure 3.7 représente le taux des paquets perdus en fonction de la taille de la signature numérique.

On remarque que le taux de perte des paquets augmente avec la croissance de la taille de signature numérique.

Pour étudier la performance de GPSR, on prend en considération les algorithmes DSA, RSA, ECDSA pour générer la signature numérique et le temps de génération et de vérification.

3.3.5 Comparaison des performances des trois techniques :

Avec les mêmes paramètres de simulation nous avons comparé la performance de notre protocole en utilisant les algorithmes précédents RSA, DSA, ECDSA.

Les paramètres utilises sont représentés dans la table suivante **[22]** :

	DSA	**RSA**	**ECDSA**
Temps de génération (ms)	0.45	6.05	10.62
Temps de vérification (ms)	0.52	0.16	12.80
Taille de signature (octets)	1024	1024	233
		2048	

Table 2 : Temps de génération et de vérification des signatures numériques

Dans cette partie, nous présentons et nous analysons les résultats de simulation que nous avons obtenus à travers les scénarios précédemment définis.

Avant l'analyse de performance de notre protocole GPSR sécurisé qui est utilisé avec RSA, DSA, ECDSA, on donne les équations qui représentent le délai moyen pour acheminer les paquets:

Equation 1: les paquets GPSR pour la variante 1

D= (n-1) (TV+TG)

Equation 2: les paquets GPSR pour la variante 2

D= (n-1) (2TV+2TG)

Avec

D : le délai moyen d'acheminements des paquets

n : nombre des nœuds intermédiaires +nœud source+ nœud destination

TV : le temps de vérification du message signé.

TG : le temps de génération de signature numérique.

- **Les résultats obtenus de la variante 1 de GPSR :**

	Taille de signature	**Délai moyen (ms)**	**Le taux de perte(%)**
RSA	1024	18.3695	27.44
	2048	19.2721	80.07
ECDSA	233	69.2508	12.45
DSA	1024	2.9038	26.57

Table 3.3: ***Délai moyen de bout en bout (une seule signature)***

- **Les résultats obtenus de la variante 2 de GPSR :**

	Taille de signature	**Délai moyen (ms)**	**Le taux de perte (%)**
RSA	1024	19.1641	27.44
	2048	20.0718	80.07
ECDSA	233	132.697	12.45
DSA	1024	5.4809	28.24

Table 3.4 : ***Délai moyen de bout en bout (double signature)***

Nous remarquons que les deux équations de signature numérique donnent toujours le même taux de perte des paquets même avec double signatures.

En comparent les trois systèmes dans les deux variantes, nous pouvons dire que le meilleur système est le système ECDSA par ce qu'il présente un taux de perte minimum (12.45), malgré que le délai de bout en bout était élevé par rapport aux autres systèmes (RSA, DSA).

Ce choix a été pris sur la base qu'il vaut mieux recevoir les paquets en retard (un grand délai) que de ne jamais les recevoir (ou avec une grande perte).

Conclusion :

Ce chapitre a été entièrement consacré à l'étude de l'impact de la cryptographie sur les protocoles de routage de réseaux VANETs. Nous nous sommes focalisés sur les algorithmes : RSA, DSA, ECDSA.

Nous avons trouvé pour le cas des VANETs que le système ECDSA est le meilleur système qui peut être utilisé dans les réseaux VANETs, car il assure un niveau de sécurité acceptable avec un taux de perte minimum.

CONCLUSION GENERALE ET PERSPECTIVES

Dans un futur proche, les véhicules sont appelés à devenir de plus en plus intelligents, grâce à l'ajout de communication sans fil.

Les réseaux véhiculaires sont en effet une classe émergente des réseaux mobiles Ad Hoc, permettant des échanges de données entre véhicules ou encore véhicule et infrastructure. Ils suscitent un intérêt certain dans le but d'améliorer la sécurité.

Pour cela, il faut déployer une multitude de services de sécurité (confidentialité, authentification, intégrité, respect de la vie privée, contrôle d'accès, disponibilité, non-répudiation).

Notre études est localisée sur l'étude des performances des algorithmes de génération et de vérification des signatures numériques et leur applicabilité dans les communications véhiculaires, particulièrement on a considéré les protocoles de routage.

Parmi les difficultés trouvées pendant la réalisation de ce projet on n'a pas trouvé des protocoles sécurisés implémentés, et pour cette raison on a modifié le protocole GPSR et on a proposé 2 variantes sécurisées, chacune avec un niveau de sécurité différent. Après l'implémentation et la simulation on a trouvé que le système ECDSA présente des performances élevés par rapport aux RSA et DSA.

Perspectives :

Les contributions de ce mémoire ont apporté des réponses à certains problèmes, mais il reste des pistes à explorer. Chacune de ces pistes est une perspective possible dans la continuité de ce travail.

Comme extensions futures à notre travail nous proposons :

- Utilisation des bibliothèques cryptographiques pour estimer les délais et les intégrer directement dans la simulation de notre protocole.
- Simuler des différents scenarios d'attaque pour notre protocole.
- Simuler notre protocole avec d'autres modèles de mobilité.

Bibliographie

[1] Daniel MABELE MONDONGA, "Etude sur les protocoles de routage d'un réseau en mode Ad Hoc et leurs impacts", Institut supérieur d'informatique Kinshasa, 2010.

[2] Meraihi yassine," routage dans les réseaux véhiculaires (vanet) cas d'un environnement type ville", Memoire de magister, Université M'hamed Bougara – Boumerdes , 2011.

[3] CATHERINE Loison, Thomas Ruocco, Camille Rives," Routage multicast dans les réseaux véhiculaires ", 2013.

[4] Jonathan Petit, " Surcoût de l'authentification et du consensus dans la sécurité des réseaux Sans fil véhiculaires", Thèse de doctorat, Université Toulouse III - Paul Sabatier, juillet 2011.

[5] Rabah Meraihi, Sidi-Mohammed Senouci, Djamal-Eddine Meddour, Moez Jerbi, "Communications véhicule à véhicule" Universite D'evry Val D'essonne, 2008.

[6] Samuel Galice, "Modèle Dynamique De Sécurité Pour Réseaux Spontanés", Thèse de doctorat, L'Institut National des Sciences Appliquées de Lyon, Octobre 2007.

[7] Valérie Gayraud, Loutfi Nuaymi, Francis Dupont, Sylvain Gombault, Bruno Tharon, " La sécurité dans les réseaux Sans Fil Ad Hoc", Thomson R&I, Security Lab, 2008.

[8] Noureddine CHAIB," La sécurité des communications dans les réseaux VANET " , Memoire de magister, Université Elhadj Lakhder – Batna, 2011.

[9] Stéphane Gill," Type d'attaques ", Université de franche-comte, 2003.

[10] Farid JADDI," CSR : une extension hiérarchique adaptative du protocole de routage ad hoc DSR", Ecole Doctorale d'Informatique et Télécommunications, 2006.

[11] Kamal Beydoun, "conception d'un protocole de routage hiérarchique pour les réseaux capteur", Université de franche-comte, 2009.

[12] Jean Carle, Olivier Flauzac, Bachar Salim HAGGAR, Florent NOLOT, "État de l'art sur les protocoles de routage dans les réseaux ad hoc", Université Libre de Bruxelles, 2007.

[13] C. Perkins, E. Belding-Royer et S. Das," Ad hoc On-Demand Distance Vertor (AODV) Routin", IETF, RFC 3561, juillet 2003.

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

[15] Hassan DKHIL, "Greedy perimeter stateless routing sur omnet++", école national Supérieur d'informatique, 2009

[16] Soufiene Djahel, Le routage OLSR et l'attaque du trou noir, Memoire de magister, Université Abderrahmane Mira, 2007.

[17] CELINE BURGOD," Contribution a la sécurisation du routage dans les réseaux ad hoc", Université de Limoges, octobre 2009.

[18] ADJIDO IDJIWA, BENAMARA Radhouane, BENZIMRA Rebecca, GIRAUD Laurent, "Protocole de routage ad hoc sécurisé dans une architecture clustérisée", Université Pierre et Marie Curie (Paris VI) Paris, France.

[19] Wu Hao Cheng,Chao Li, Cheng-shu,"Research on One Kind of Improved GPSR Secure Routing Protocol", Beijing Jiaotong University, 2007.

[20] Mohammed Erritali, Oussama Mohamed Reda, Bouabid El Ouahidi"A contribution to secure the routing protocol", University Morocco, 2011.

[21] F.Armknecht, A. Festag, A. Hessler, O. Ugus, "surcout Building Blocks for VANET Security", University Paul sabatier, 2011.

[22] Terence Chen, Olivier Mehani, Roksana Boreli," Trusted Routing for VANET", University of New South, September 2011.

TABLE DES MATIERES

Table des figures :

Liste des tableaux: