République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Larbi Tébessi
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : mathématique et informatique

MEMOIRE DE MASTER
Domaine: Informatique /mathématique
Filière: Informatique
Option: Réseaux et sécurité informatique

Thème:

DETECTION D'INTRUSION DANS LES RESEAUX VANETS

Présenté par:
DAOUADI zineb
ABBAS Assia

Devant le jury:

BENDJANNA Hakim	M.C.A	Université de Tébessa	Président
AOUINE Mohamed	M.A.B	Université de Tébessa	Rapporteur
DARDOUR Makhlouf	M.C.A	Université de Tébessa	Examinateur

Date de soutenance:29/05/2016

Note :……. Mention :……..

ملخص

العنوان: Détection d’intrusion dans les réseaux VANET

شبكة VANET (Vehicular Ad-hoc Network) هي تكنولوجيا جديدة من عائلة شبكات المحمول MANET وتستخدم هذه الشبكات لتلبية متطلبات الاتصالات على أنظمة الإرسال الخاصة بالنقل لتحسين القيادة و السلامة المرورية لمستخدمي الطريق.

خصائص VANETs تقدم تحديات كبيرة، مما يجعلها مفتوحة للعديد من المجالات البحثية. من بين هذه المجالات الأمنية وتبادل المعلومات. أنظمة كشف التسلل IDS : Intrusion Detection Systems، والتي هي أدوات للكشف عن محاولات الهجوم على الشبكة.

في هذا العمل أجرينا دراسة مقارنة لبعض أنظمة كشف التسلل IDS القائمة. ثم عرضنا أسلوبنا، الذي هو مزيج من اثنين من أنظمة كشف التسلل الموجودة (watchdog and pathrater , IDS clustred ....) لتحسين القدرة على كشف التسلل .

Abstract

Title: Intrusion Detection in VANET Networks

The VANET network (Vehicular Ad- hoc Network) is a new technology fonts part of the family of mobile networks MANET. These networks are used to meet the communication requirements applied to transmission systems to improve driving and road safety to road users.

VANETs properties offer significant challenges, making them open to several research areas; among these areas of information exchange security. Intrusion detection systems (IDS: Intrusion Detection Systems), which are tools for the detection of attempted attacks on a network.

In this work we make a comparative study of some existing IDS (watchdog and pathrater , IDS clustred ... ..) . Then we offered our method, which is a combination of two IDS existing to improve the intrusion detection capability.

Key words:

MANET, VANET, intrusion , watchdog and pathrater, IDS clustred, Zhang ET Lee IDS, CONFIDANT

Résumé

Titre : Détection d'intrusion dans les réseaux VANET

Le réseau VANET (Vehicular Ad-hoc Network) est une nouvelle technologie fonts parti de la famille des réseaux mobiles MANET. Ces réseaux sont utilisés pour répondre aux besoins de communication appliquée aux réseaux de transport pour améliorer la conduite et la sécurité routière aux utilisateurs de la route.

Les propriétés des VANETs offrent des challenges importants, ce qui les rend ouvertes à plusieurs domaines de recherche ; parmi ces domaines la sécurité des échanges des informations. Les systèmes de détection d'intrusions (IDS : Intrusion Detection Systems) qui sont des outils conçus pour la détection des tentatives d'attaques sur un réseau.

Dans ce travail nous nous faire une étude comparative entre quelques IDS existants (watchdog and pathrater , IDS clustred …..). Ensuite, nous avons proposé notre méthode, qui est une combinaison entre deux IDS existent, pour améliorer la capacité de détection d'intrusions.

Mots clés :

MANET, VANET, IDS, intrusion, watchdog and pathrater, IDS clustred, Zhang ET Lee IDS, CONFIDANT

Résumé

Dédicace

A mon Très cher père ***El Haddi,***

Pour leur encouragement qui n'ont jamais
cessés de me consentir durant les années d'études, je demande à Dieu de le protéger
Et leur réserver une longue vie.

A la plus chère au monde, ma mère ***Hafida*** *qui a toujours m'encouragé durant mes études.*
Je t'aime maman.
Je demande à Dieu les protéger et leur réserver une longue vie.
A mes grand- parents maternels et paternels.
A mes Très chère sœur ***Assia.***
Ma cher binôme ***Assia .***
A toue ma famille ***DAOUADI****.*
A tous mes enseignants.
A toute la promotion master 2015-2016 / Réseaux et sécurité informatique.
Appliquée du Département mathématique et informatique, Faculté des sciences exactes et sciences de la nature et de la vie et de l'Univers,
Université Larbi Tébessi tebessa.

A toute personne qui me connait de près ou de loin.

zineb

Dédicace

Je dédie ce modeste travail tout d'abord à :

Ma mère, qui a œuvrée pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude AKILA

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi ABDRRAHMAN

. Mon frère qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité ALI

Mes sœurs ABLA .KHAOULA.HASNA.TAKOUA et MOUFIDA et mon beau frère ABDALLAH

Ainsi que :

Ma cher binôme ZINEB

Ma cher amie et ma sœur KHAOULA

A mes chères amies surtout MUS

A tous ceux qui me sens chers

Assia

Remerciement

*Avant tout nous remercions "**Allah**" le tout puissant, le Miséricordieux, qui nous a donné le courage, la volonté, la force, la santé et la persistance pour accomplir ce modeste travail. Merci de nous avoir éclairé le chemin de la réussite.*

*Nous adressons nos plus vifs remerciements à Ms **AOUINE Mohamed**, monsieur assistant à la Faculté des Sciences de la Nature et de la Vie, Université Tebessa , pour nous avoir proposé ce sujet, pour son encadrement, ses encouragements, ses orientations, pour ses aides, sa patience, ses conseils scientifiques judicieux , sa compétence et sa gentillesse qui m'ont permis de bien mener ce modeste travail.*

*A Mr .**BENDJENNA.H**, nous adressons nos remerciements les plus sincères pour l'honneur qu'il nous fait en acceptant de présider ce jury.*

*A Mr. **DERDOUR.M**, pour avoir bien voulu siéger dans ce jury afin d'examiner ce mémoire et nous éclairer par ces précieux conseils*

Nos remerciements aussi vont à tous les enseignants et enseignantes qui nous ont fait former durant ces 5 années, en nous préparant pour cette dernière année de master. Merci pour vos encouragements et votre gentillesse.

Nous associons mes remerciements à toutes nos amies pour leur solidarité, leur aide, et leur disponibilité.

Table de matière

Liste de tableaux

Liste de figures

Glossaire des acronymes et notations

AAFID	**Autonomous Agent for Intrusion Detection**
ADAM	**Audit Data Analysis and Mining**
AP	**Point d'Accès**
BSS	**Basic Service Set**
CONFIDANT	**Cooperation of Nodes-Fairness in Dynamic Ad hoc NeTworks**
CSM	**Cooperating Security Manager**
DIDS	**Distributed Intrusion Detection System**
DS	**Distribution System**
DSRC	**Dedicated Short Range Communication**
DVB-S	**Digital Video Broadcasting Satellite**
EDR	**Event Data Recoreder**
ESS	**Extended Service Set**
HIDS	**Host-based IDS**
GACE	**Global Aggregation and Correlation Engines**
GrIDS	**Graph-Based Intrusion Detection System**
GSM	**Global System for Mobile Communication**
GSR	**Global State Routing**
GPRS	**General Packet Radio Service**
GyTAR	**Improved Greedy Traffic-Aware Routing protocol**
LACE	**Local Aggregation and Correlation Engines**
IBSS	**Independant Basic Service Set**
ICN	**Integrated Computing Network**
IDS	**Systèmes Detection Intrusion**
LTE	**Long Term Evolution**
MANET	**Mobile Ad-hoc Network**
MIDAS	**Multics Intrusion Detection and Alerting System**
NADIR	**Network Anomaly Detection and Intrusion Reporter**
NIDS	**Network-based Intrusion Detection System**
NIDES	**Next Generation Real time Intrusion Detection Expert System**
NS-2	**Network Simulator version 2**
OBU	**On Board Unit**
RSU	**Raad Side Unit**

UMTS	**Universal Mobile Telecommunications**
STAT	**State Transition Analysis Toolkit**
VANET	**Vehicular Ad-hoc Network**
V2I	**Véhicule à infrastructure**
V2V	**Véhicule-à-Véhicule**
WAVE	**Wireless access in vehicular network**
WiFi	**Wireless Fidelity**
WIMAX	**Worldwide Interoperability for Microwave Access**
WLAN	**Wireless Local Area Network**
WMAN	**Wireless Metropolitan Area Network**
WPAN	**Wireless Personal Area Network**
WWAN	**Wireless Wide Area Network**

Introduction générale

Le déploiement des réseaux VANET a considérablement augmenté les risques causés par les attaques sur les réseaux véhiculaires qui deviennent un réel problème pour La sécurité routière

Un système de détection d'intrusions (**IDS**, de l'anglais Intrusion Detection System) est un périphérique ou processus actif qui analyse l'activité du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un **IDS** détecte des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout **IDS** est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources.

Les **IDS** protègent le réseau contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus.

Les **VANETs** sont caractérisés par une forte mobilité, liée à la vitesse des voitures, qui est d'avantage importante sur les autoroutes. Par conséquent, un élément peut rapidement rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquents. Néanmoins, l'absence d'une gestion centrale des fonctionnalités du réseau crée d'autres contraintes tels que l'accès au canal, le routage et la dissémination des données, l'auto-organisation, l'adressage ou encore la sécurité.

watchdog and pathrater , IDS clustred ont tous les deux des limites et aucun d'eux ne peut remplacer l'autre, par contre ils peuvent se compléter pour constituer un système plus sécurisé. En effet, dans notre travail, nous proposons de faire collaborer les deux méthodes watchdog and pathrater, **IDS** clustred pour construire un système permettant d'améliorer la capacité de détection d'intrusions.

Notre travail est basé sur :

- Un état de l'art des **VANETs** et des attaques
- Synthèse sur les travaux de recherches liés aux domaines de la sécurité avec comparaison des quelques méthodes **IDS** existantes.
- Etude comparative entre quelques **IDS** connus dans les réseaux **VANETs**
- proposition notre méthode pour construire un système permettant d'améliorer la capacité de détection d'intrusions.

Notre mémoire est organisé en trois chapitres :

- **Chapitre I :** les réseaux sans fil et les réseaux **VANETs.**
- **Chapitre II :** la sécurité et les attaque dans les réseaux **VANETs**.
- **Chapitre III :** état de l'art et les IDS dans les réseaux **VANETs**.

CHAPITRE I :

LES RESEAUX SANS FIL ET LES RESEAUX VANETS

Introduction

Les réseaux **VANETs** (Vehicular Ad-hoc Network) constituent une nouvelle forme de réseaux MANET, les nœuds de réseau **VANET** sont des véhicules). Ils permettent d'établir des communications entre véhicules ou bien avec les véhicules et infrastructure située aux bords de routes.

Les réseaux **VANETs** sont caractérisés par une topologie dynamique et fort mobilité des nœuds.

Les réseaux **VANET** offerts services liés à la sécurité routière et des Services liés au confort.

Dans notre chapitre en va voire les réseaux sans fil, après le réseau **VANETs** leur modes de communications, leur caractéristiques, leur objectif .Ensuite, les services et les applications offres dans celtes réseaux et en fin citer les domaines de recherche dans ce réseau.

1. Les réseaux sans fil

1.1. Définition d'un réseau

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies. [1]

1.2. Définition d'un réseau informatique

Réseau informatique ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques. [1]

1.3. L'objectif d'un réseau

- ✓ Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- ✓ La communication entre personnes (courrier électronique, discussion en direct, etc.)
- ✓ La communication entre processus (entre des ordinateurs industriels par exemple)
- ✓ La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau) [1]

1.4. Classification des réseaux

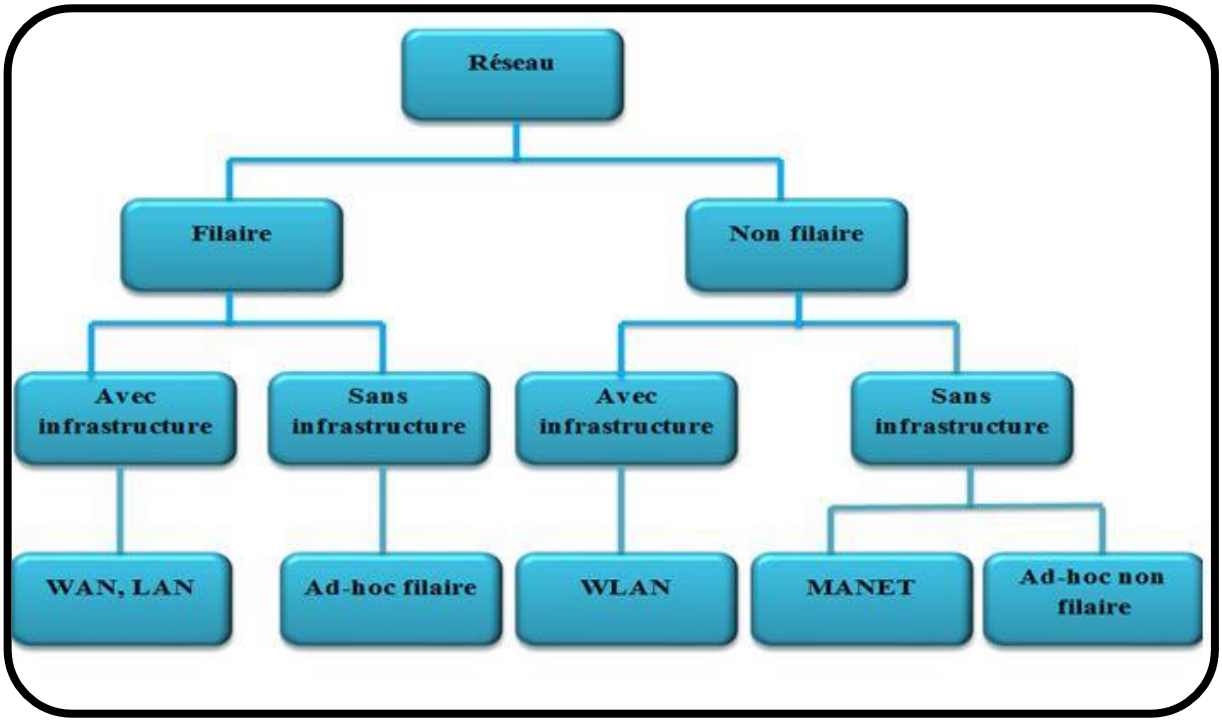

Figure I.1 : Classification des réseaux.

1.4. Définition de réseau sans fil

Un réseau sans fils (en anglais Wireless network) est un réseau dans lequel les différents éléments participants (ordinateur portable, téléphone portable…etc.) ne sont pas raccordés entre eux par un média physique. La transmission des données se fait via les ondes hertziennes (radio ou infrarouge). Ceci permet aux utilisateurs de se déplacer dans un périmètre de couverture pouvant aller d'une dizaine de mètres à quelques kilomètres [2]

1.5 Avantages et inconvénients de la communication sans fil

Nous citerons dans la section suivante les avantages liés à l'utilisation du médium radio dans les réseaux sans fil. Les contraintes liées à cet environnement seront également présentés. [3]

1.5.1. Les avantage

- **La mobilité :**

La mise en place d'un réseau sans fil entre les éléments portables permet d'éviter les fils de connexion au réseau et les fils d'alimentation, afin de permettre le mouvement libre des utilisateurs avec leurs terminaux portables. [3]

- **Faibles coûts :**

Contrairement au réseau filaire où le câblage représente un coût supplémentaire, le réseau sans fil s'affranchit de ce coût. Néanmoins, les protocoles de routage et de configuration doivent être repensés pour permettre la bonne gestion et l'acheminement des données dans le réseau. [3]

1.5.2. Les inconvénients

- **Dégradation de la qualité du signal :**

Cette contrainte est causée par l'affaiblissement de la puissance du signal avec la distance et les conditions atmosphériques. De plus, le bruit dû à d'autres signaux parasites cause une altération du signal. D'autres paramètres tels que l'absorption atmosphérique du signal par la vapeur d'eau et l'oxygène, la propagation multi trajet causée par les obstacles entre l'émetteur et le récepteur, font que le signal se dégrade davantage. [3]

- **Sécurité :**

La confidentialité des données circulantes sur les réseaux sans fil doit être assurée, car les transmissions radioélectriques sont sensibles aux interférences et sujettes à l'écoute par un utilisateur mal intentionné. Cet utilisateur peut se placer dans le périmètre des équipements du réseau afin de récupérer les informations qui lui permettront d'avoir accès au réseau. Ceci représente le plus grand problème des réseaux sans fil. [3]

- **Débit**

Le simple fait d'avoir un trop grand nombre d'utilisateurs dans un réseau sans fil peut entraîner une diminution importante de débit. Cette diminution de débit peut même conduire à une perte de connectivité ce qui est très contraignant. [3]

1.6. Architecture de réseau sans fil

1.6.1. Mode infrastructure

Ce mode de fonctionnement est très semblable au protocole Ethernet des réseaux filaires. Les machines se connectent à un point d'accès (AP), appelé aussi station de base, qui partage la bande passante disponible. Les stations de base sont munies d'une interface de communication sans fil avec les sites mobiles qui se trouvent dans sa zone géographique ou sa couverture radio. [2]

Cette topologie (figure I.2) est appelée BSS (Basic Service Set). [4]

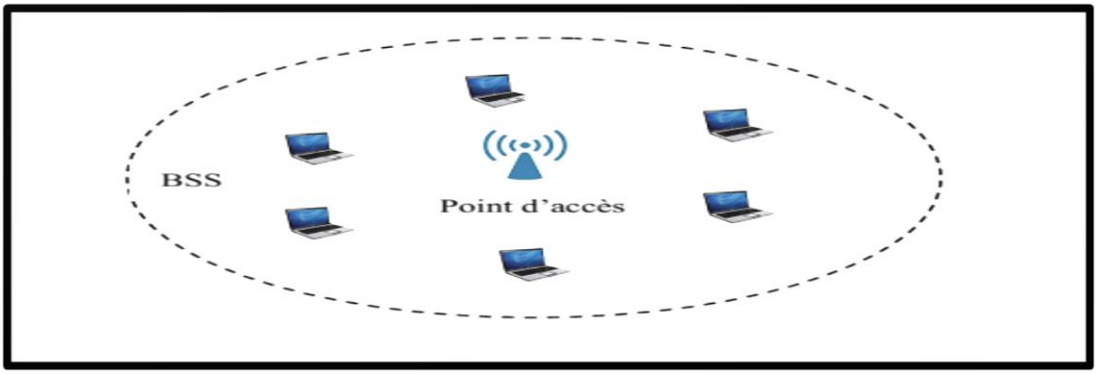

Figure I.2 : Basic Service Set. [4]

Plusieurs points d'accès peuvent être reliés entre eux grâce à un système de distribution DS (Distribution System) (figure 3) pour former un ensemble de services étendu ESS(Extended Service Set). [4]

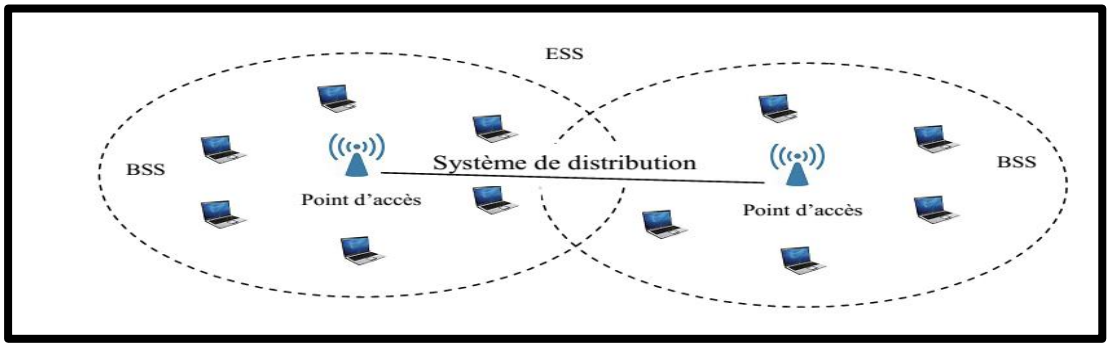

Figure I.3 : Ensemble de services étendu. [4]

1.6.2. Mode sans infrastructure ou réseau ad hoc

Ce mode n'a pas besoin de point d'accès pour fonctionner, ce sont les stations elles-mêmes qui entrent en communication sans s'appuyer sur un équipement extérieur. Tous les nœuds d'un réseau de ce type se comportent comme des routeurs et prennent part à la découverte et à la maintenance des chemins de communication entre les différentes machines. Ce type de réseau s'organise lui-même. [2]

Cette topologie est appelée IBSS (Independant Basic Service Set). [4]

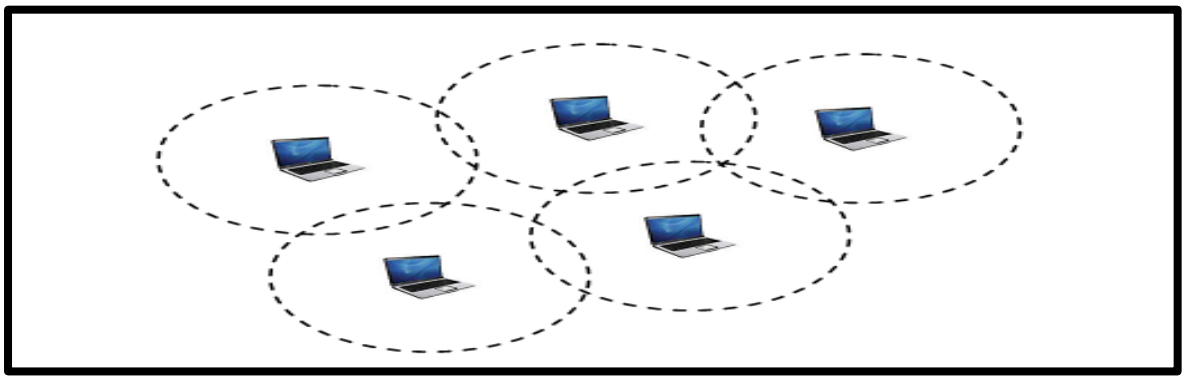

Figure 1.4: Independant Basic Service Set. [4]

1.6.3. Réseau ad hoc mobile MANET

Un réseau mobile ad hoc ou réseau MANET est un réseau sans fil capable de s'organiser sans infrastructure définie préalablement. Un tel réseau est composé de stations mobiles ou nœuds qui peuvent communiquer directement entre eux s'ils sont situés à portée radio. [5]

- **Caractéristique des réseaux MANETS :**

- **Mobile :**

Les stations ne sont pas fixes dans les réseaux MANETs. Elles peuvent se déplacer et sont entièrement indépendantes. A tout moment, de nouvelles stations peuvent joindre le réseau ou le quitter. Le changement de la topologie d'un réseau MANET dans le temps est un élément primordial. [5]

- **Sans fil :**

Les stations d'un réseau MANET utilisent un support sans fil pour communiquer entre elles. Elles partagent le même média lors des échanges d'informations. De fait, ce partage et ses conséquences (collisions, réservation de ressources...) sont autant d'éléments à prendre en compte. [5]

- **Sans infrastructure :**

Par nature, les réseaux MANETs ne dépendent pas d'une architecture fixe. Ils peuvent donc être facilement déployés. [5]

- **Auto-organisé et distribué :**

Les réseaux MANETs ne disposent pas de point central pour coordonner ou centraliser les échanges. De fait, ces réseaux doivent s'auto-organiser afin d'opérer. De plus, l'absence de centralisation demande à chaque acteur du réseau de participer au bon fonctionnement du réseau (distribution). [5]

- **Multi-saut :**

Comme la portée des stations est limitée, il peut s'avérer nécessaire que des stations agissent en tant que pont intermédiaire pour transmettre un paquet d'une source vers une destination. Par conséquent, les nœuds d'un réseau MANET agissent en tant que routeur et relayent les paquets qu'ils reçoivent pour participer au routage multi-saut.

- **Ressources limitées :**

Les ressources limitées touchent toute la chaîne de communication d'un réseau MANET en commençant par les nœuds jusqu'aux liens de communication. Les terminaux étant mobiles, ils fonctionnent principalement sur batterie. La mobilité contraint également la puissance embarquée. La capacité des liens sans fil s'avère aussi limitée comparativement aux réseaux filaires. De même, le taux d'erreur est bien plus élevé que dans un réseau filaire. [5]

- **Temporaire et rapidement déployable :**

Ce type de réseau est intrinsèquement temporaire et rapidement déployable. Il n'a pas pour but de remplacer un réseau à infrastructure mais de le compléter ou de le remplacer lorsque nécessaire. [5]

2. Réseau VANET

2.1. Définition

Un réseau **VANET** est une particularité des réseaux MANET où les nœuds mobiles sont des véhicules (intelligents) équipés de calculateurs, de cartes réseau et de capteurs. Comme tout autre réseau Ad hoc, les véhicules peuvent communiquer entre eux (pour échanger les informations sur le trafic par exemple) ou avec des stations de base placées tout au long des routes (pour demander des informations ou accéder à internet…). [5]

Par rapport à un nœud rendant la topologie du réseau fortement dynamique. [6]

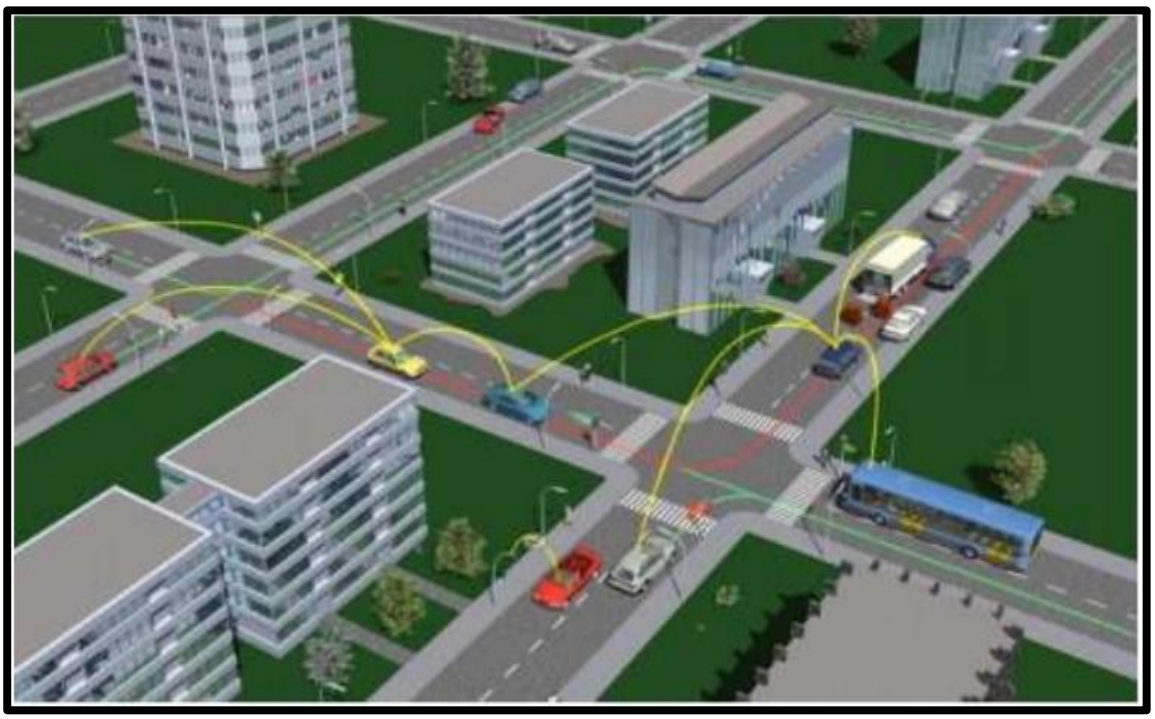

Figure I.5 : Réseau VANET. [42]

2.1.1. Paradigme de communication

- **Infrastructure**

- **En général fixe (RSU) :**

Les RSUs (Raad Side Unit) sont les bornes au bord de la route. Elles ont deux fonctions: dans un premier temps, elles diffusent les informations météorologiques, le trafic routier, etc. ; dans un second temps, elles permettent également de retransmettre l'information sur de longues distances entre les véhicules et vers les points d'entrée du réseau pour y connecter les véhicules aux différentes applications proposées. [6]

- **Peut-être mobile (véhicules policier dédié).**

- **véhicule**
- **Voiture**
- **peut inclure aussi les bus, trains,…etc.**

2.1.2. Les éléments constituant le véhicule intelligent

Les véhicules sont le centre des entités du réseau. Ils possèdent de nombreux capteurs et unités de calcul à bord permettant de gérer et traiter les informations reçues. Les véhicules sont équipés de bornes « On Board Unit» (OBU). L'OBU est l'interface de calcul, de localisation et d'émission/réception de messages dans le réseau. Le véhicule intelligent et son équipement, ainsi que l'intégralité des protocoles et des normes mise en place pour la communication sont appelés DSRC (Dedicated Short Range Communication). [7]

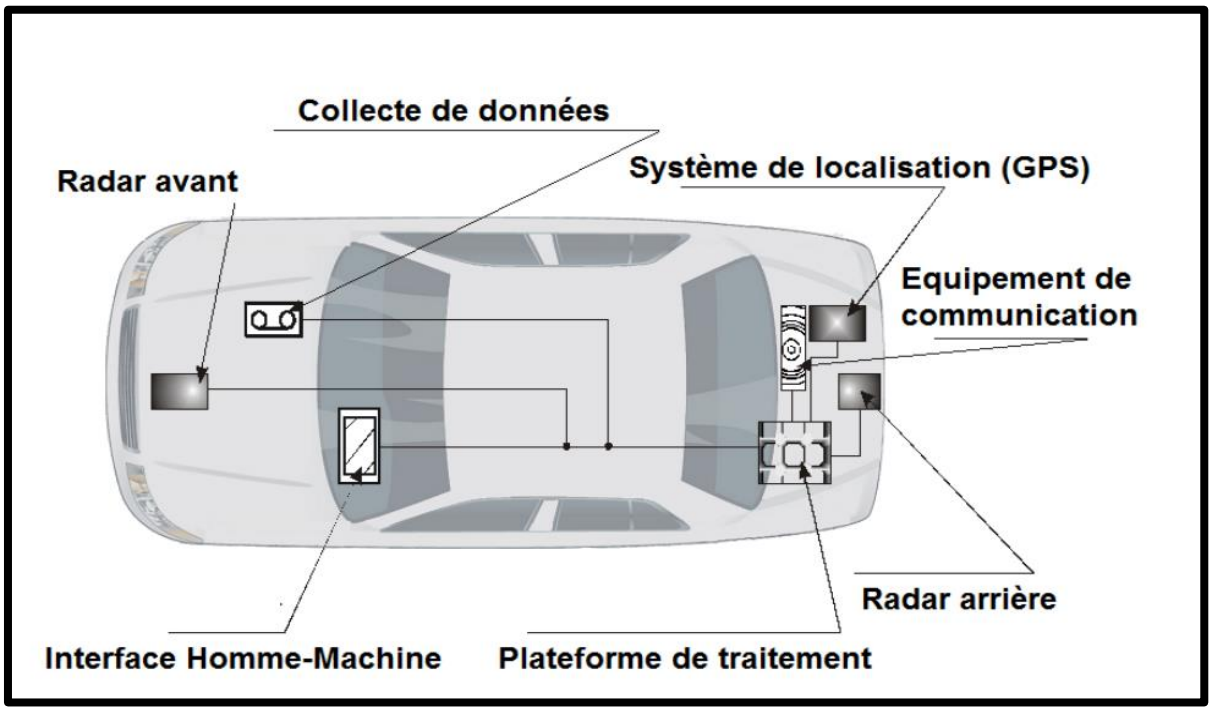

Figure I.6 : Les éléments constituant le véhicule intelligent. [9]

- **Collecte de données (Event Data Recoreder(EDR)) :** enregistre tous les paramètres importants (vitesse, accélération, événements importants comme les accidents.
- **Système de localisation GPS (positioning system) :** communique l'emplacement géographique de véhicule.
- **Les radars :** sont utilisés pour détecter des obstacles.
- **Plateforme de traitement (computing platforme) :** générer l'information utile à échanger avec les autres véhicules ou avec l'infrastructure.

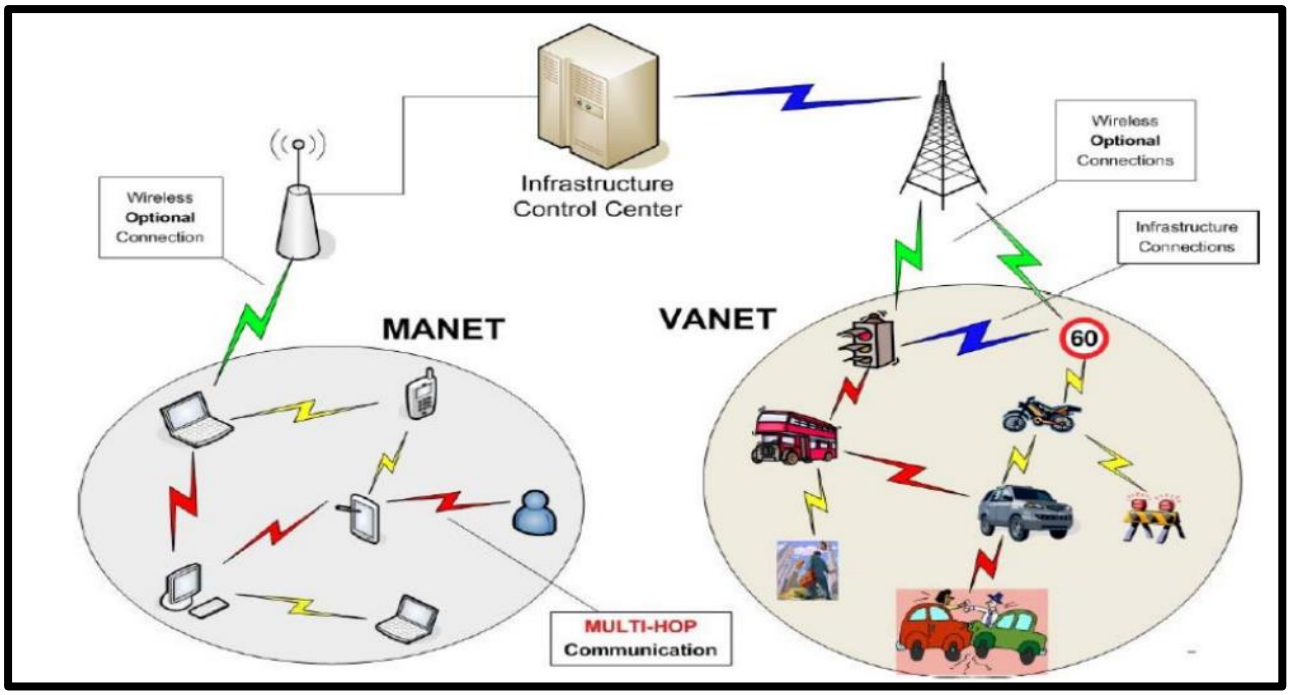

Figure I.7 : VANET vs MANET. [8]

2.2. Les objectifs

Les réseaux **VANET** sont basés sur la communication et l'échange d'information entre les véhicules, et entre les véhicules et des éléments de la route (Exemples : les panneaux de signalisations, les feux d'intersections…) ou des éléments de réseaux externes (Satellites, antennes, internet). [8]

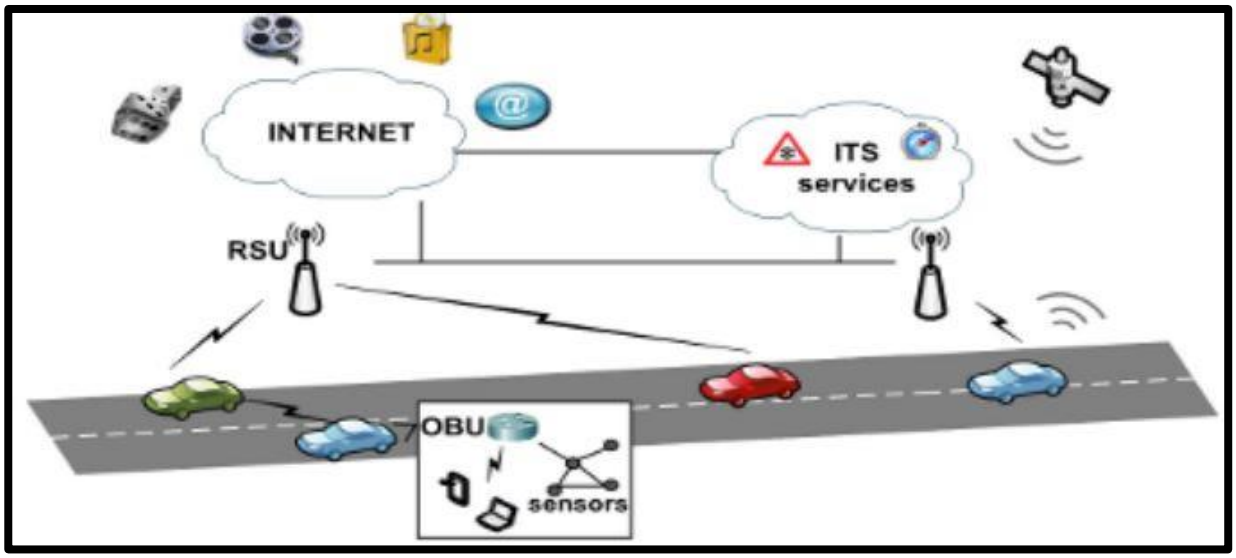

Figure I.8 : L'objectif de VANET. [8]

Les objectifs de ces échanges d'informations sont [8] :

- **Sécurité des usagés :**
  - ✓ Prévention sur les accidents : Les accidents deviennent plus rapidement détectables et l'intervention devient plus rapide, cela peut minimiser le risque de décès après un accident.
  - ✓ Anticipation du trafic : Les véhicules sont informés par les routes ou il y'a des embouteillages, ils peuvent donc emprunter un autre chemin, cela peut permettre de rendre les routes plus fluides.
  - ✓ Préventions d'un véhicules prioritaire : Permet d'avisé les conducteurs d'un passage de véhicules prioritaire (Exemple : ambulances, véhicules de police…).
  - ✓ Anticipation d'un danger quelconque : Les véhicules peuvent s'échanger entre eux des préventions de dangers liés aux routes pour mieux les anticipés.
- **Confort des usagés :**
  - ✓ Avoir une prévention sur l'itinéraire peut permettre de facilité la conduite et amoindrir les risques d'accidents.
  - ✓ Les réseaux **VANET** peuvent communiquer avec les infrastructures externes comme internet, donc la capacité d'accéder a des loisirs comme les téléchargements de flux multimédias, lecture des emails …etc.
  - ✓ Possibilité de jouer en réseau entre les passagers des voitures, téléchargement et partage de fichier tel que les cartes.
  - ✓ La régulation des flux de véhicules, permet de réduire le nombre d'embouteillages.
  - ✓ Le guidage par GPS permettant un déplacement plus facile, et l'auto-localisation qui permet de trouver les véhicules volés.

2.3. Les applications

Les principales applications des réseaux **VANET** peuvent être classées en trois catégories.

2.3.1. Application dans la prévention et la sécurité routière

La sécurité routière est devenue une priorité dans la plupart des pays développés, cette priorité est motivée par le nombre croissant d'accidents sur ses routes associé à un parc de véhicules de plus en plus important. Les **VANET** permettent de prévenir les collisions et les travaux sur les routes, de détecter les obstacles (fixes ou mobiles) et de distribuer les informations météorologiques par envoi de messages d'alerte. A titre d'exemple, alerter un conducteur en cas d'accidents permet d'avertir les véhicules qui se dirigent vers le lieu de l'accident que les conditions de circulations se trouvent modifiées et qu'il est nécessaire de redoubler de vigilance. 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. [3]

2.3.2. Application pour l'optimisation du trafic et aide dans la conduite

Le trafic automobile peut être grandement amélioré grâce à la collecte et au partage de données 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). [3]

2.3.3. Applications au confort du conducteur et des passagers

Les réseaux véhiculaires peuvent aussi améliorer le 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, etc. [3]

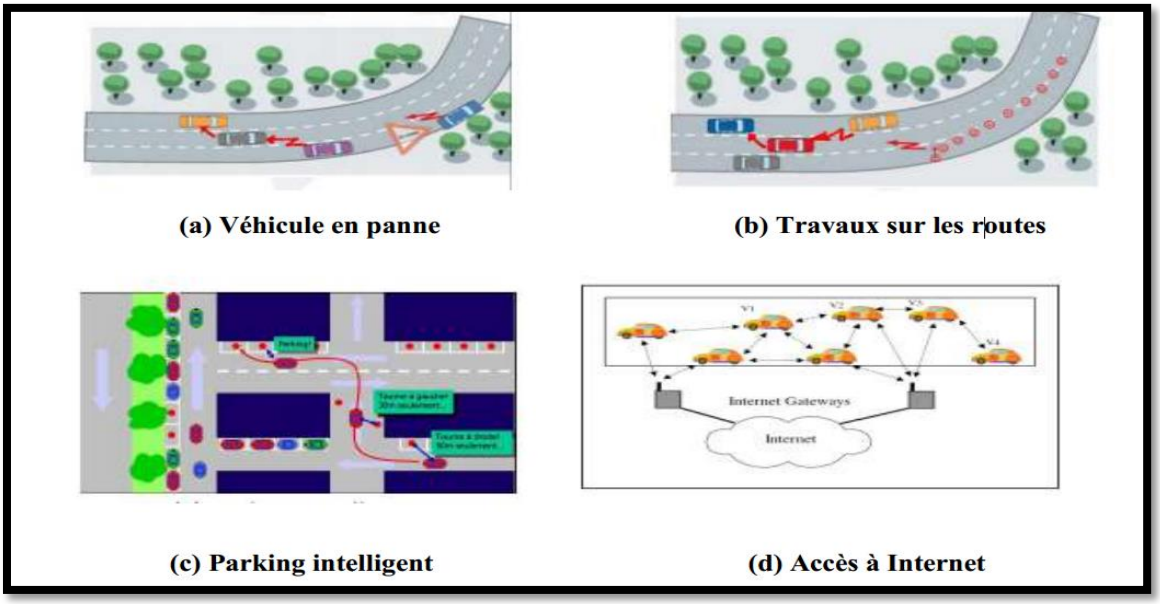

Figure I.9. Applications des réseaux de véhicules. [43]

2.4. Les avantages et les inconvénients des VANETs

2.4.1. Les avantage [8]

- **Topologie dynamique :**

Les nœuds des réseaux **VANET** (véhicules) se déplaçant très rapidement, la topologie du réseaux et a chaque fois modifiée, mais les caractéristiques de **VANET** permettent le maintien des communications et l'échange de flux d'informations en dépit des changements fréquents des positions des nœuds.

- **Echange entre nœuds hétérogènes :**

Les véhicules des réseaux **VANET** sont de différentes marques et les composants réseaux qui les constituants utilisent différents technique, mais ils peuvent tout de même aboutir à un bon échange d'informations grâce aux protocoles instaurés par les concepteurs du réseau.

- **Propagation par trajet multiple :**

Les infos partagées par un véhicule peuvent être reçus par tous les autres véhicules se trouvant dans son entourage.

- **Relais d'informations :**

Deux véhicules distants de plusieurs KM peuvent se partager une information, cette information envoyée depuis un nœud A est relié par plusieurs nœuds intermédiaires avant d'arriver au destinataire B.

2.4.2. Les inconvénients [8]

- **Canal radio partagé et limité :**

Un canal radio à fréquences précises est utilisé par tous les nœuds, le flux d'information est donc limité et le débit de transmission diminue surtout dans les centres villes.

- **Faible bande passante :**

Le partage du canal limite la bande passante dont dispose chaque nœud pour partager les informations.

- **Les interférences :**

Les réseaux **VANET** utilisent les transmissions radio pour transmettre l'information, ce qui rend les communications exposées aux interférences radio, ces derniers sont de nature diverse comme : le rapprochement des fréquences d'émission (interférences entre deux nœuds), les bruits de l'environnement (équipements électriques, moteurs), et les phénomènes de réflexion, atténuation et dispersion qui déforment le signal. Ces interférences font augmenter le taux d'erreurs de transmission, et le rendent incompréhensible par le récepteur.

2.5. Les caractéristiques

Les réseaux véhiculaires se distinguent des réseaux sans fil traditionnels par un certain nombre de caractéristiques spécifiques dont on peut citer [8] :

- **Le potentiel énergétique:**

À la différence des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de grandes capacités énergétiques qu'elles tirent du système d'alimentation des véhicules.

- **L'environnement de communication et le modèle de mobilité:**

Les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale. Du fait de la mobilité des véhicules, il est en effet possible de passer d'un environnement urbain caractérisé par de nombreux obstacles à la propagation des signaux, à un environnement périurbain ou autoroutier présentant des caractéristiques différentes. En plus de cette diversité environnementale, les réseaux véhiculaires se distinguent également des réseaux sans fil ordinaires par un modèle de mobilité dont une des traductions les plus évidentes est l'importante vitesse des nœuds qui réduit considérablement les durées de temps pendant lesquelles les nœuds peuvent communiquer.

- **Le modèle de communication:**

Les réseaux véhiculaires ont été imaginés principalement pour les applications liées à la sécurité routière (ex. diffusion de messages d'alerte). Dans ce type d'application, les communications se font presque exclusivement par reliages successifs d'une source vers une multiplicité de destinataires. Le modèle de transmission en Broadcast ou en Multicast est donc appelé à dominer largement dans les réseaux véhiculaires, ce qui n'est par exemple pas sans conséquence sur la charge du réseau et le modèle de sécurité à mettre en œuvre.

- **La taille du réseau:**

Etant donné les avancées importantes réalisées dans le domaine des communications sans fil et les bas coûts des équipements associés, les véhicules qui intègrent déjà massivement des systèmes GPS et des équipements Bluetooth, seront très probablement équipés et ce, tout aussi massivement, de plateformes de communication leur permettant de constituer de véritables réseaux. Ce faisant, et compte tenu de l'importance sans cesse grandissante de la densité et du parc des véhicules, on peut s'attendre à ce que la taille des réseaux véhiculaires dont les déploiements restent encore très confidentiels, soit d'une tout autre ampleur.

L'importance potentielle de la taille des réseaux véhiculaires constitue donc une caractéristique majeure à prendre en compte dans la conception de ces réseaux.

2.6. Les différents types de messages

Les entités membres des réseaux sans fil véhiculaires vont générer et s'envoyer des messages. Dans ces échanges, différents types de messages vont être identifiés en fonction de l'environnement et des types d'applications utilisées. Nous pourrons discerner les types suivants: message de contrôle, message de sécurité et les autres types de message. [7]

- **Message de contrôle**

Les messages de contrôle sont envoyés à intervalles réguliers, par convention. Chaque véhicule émet un message de contrôle toutes les 100 ms. Dans la littérature, ces messages sont aussi appelés message «beacon ». Ils contiennent des informations personnelles sur les véhicules telles que: sa vitesse, sa position GPS, sa direction, etc. [7]

Les messages de contrôle permettent à chaque véhicule d'avoir une vision locale de son entourage. Grâce à ce type de message, les véhicules se font connaitre de leur entourage. [7]

- **Message de sécurité**

Le message de sécurité est généré lorsqu'un événement qui mérite l'attention du conducteur est détecté. Ces messages sont générés dans le cas d'un accident, de congestion, d'un obstacle sur la route, etc. Lorsqu'un message d'alerte est émis, il doit être retransmis à intervalle régulier pour assurer que l'alerte est toujours valide. De plus, ces messages doivent être de taille réduite pour pouvoir être retransmis rapidement dans le réseau. Les messages contiennent les informations des coordonnées du lieu de l'accident et les paramètres sur sa zone de retransmission. [7]

- **Autres messages**

Les autres types de messages sont tous les messages qui ne sont pas des messages de contrôle ou des messages de sécurité. Il peut s'agir des messages d'une application, de l'envoi de courriel, etc. Ces messages ne sont émis qu'une fois. [7]

2.7. Les modes de communication

Les **VANETs** ont pour objectif d'être ouverts et connectés aux réseaux pour utiliser les services proposés. Nous présentons ici les différents modes de communication mis en place pour répondre à ce besoin. **[**7]

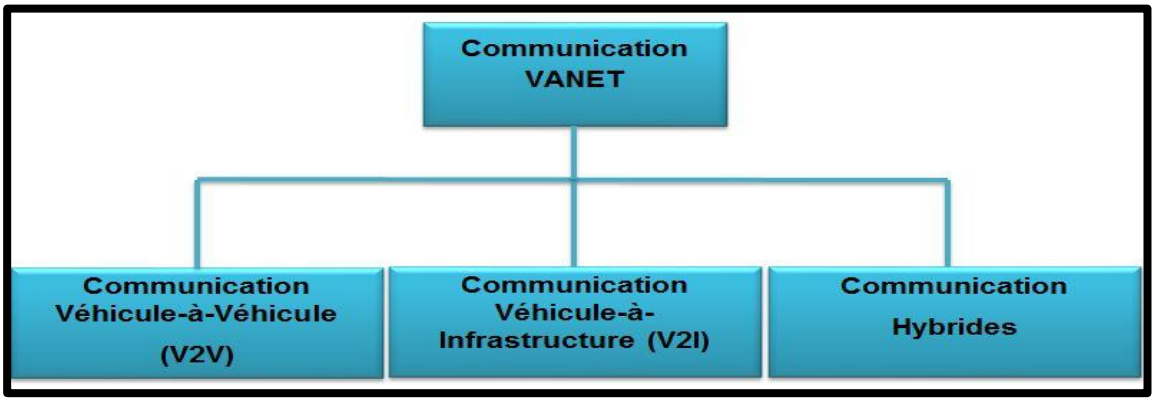

Figure I.10. Les déférentes modes de communication dans le réseau VANET.

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

Ce mode de communication fonctionne suivant une architecture décentralisée, et représente un cas particulier des réseaux ad hoc mobiles, Il est basé sur la simple communication inter-véhicules ne nécessitant pas une infrastructure. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds voisins qui les séparent comme des relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission. [11] **[**12]

Les communications V2V sont très efficaces pour le transfert des informations concernant les services liés à la sécurité routière, mais elles ne garantissent pas une connectivité permanente entre les véhicules. **[**9]

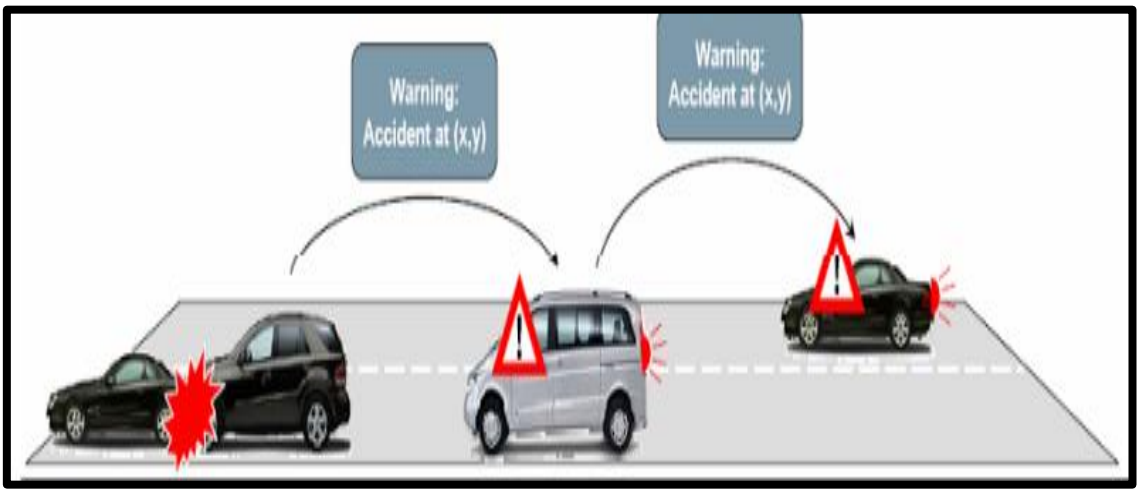

Figure I.11. Mode de communication V2V. [10]

2.7.3. Mode de communication de Véhicule à Infrastructure (V2I)

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (par exemple : accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostique distant, ...etc.) grâce à des points d'accès RSU (Road Side Units) déployés aux bords des routes; ce mode est inadéquat pour les applications liées à la sécurité routière car les réseaux à infrastructure ne sont pas performants quant aux délais d'acheminement. [13]

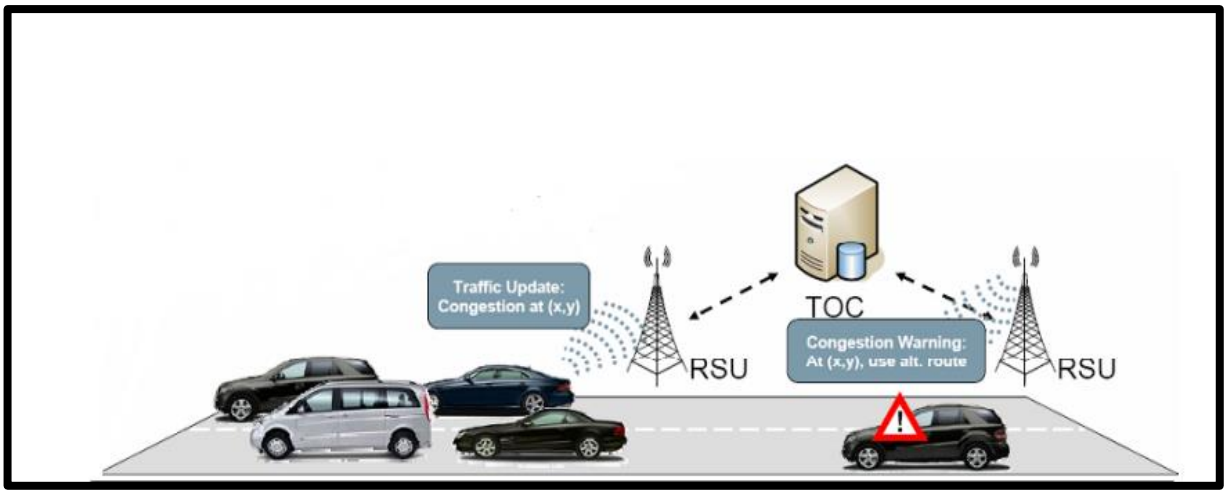

Figure I.12. Mode de communication V2I. [10]

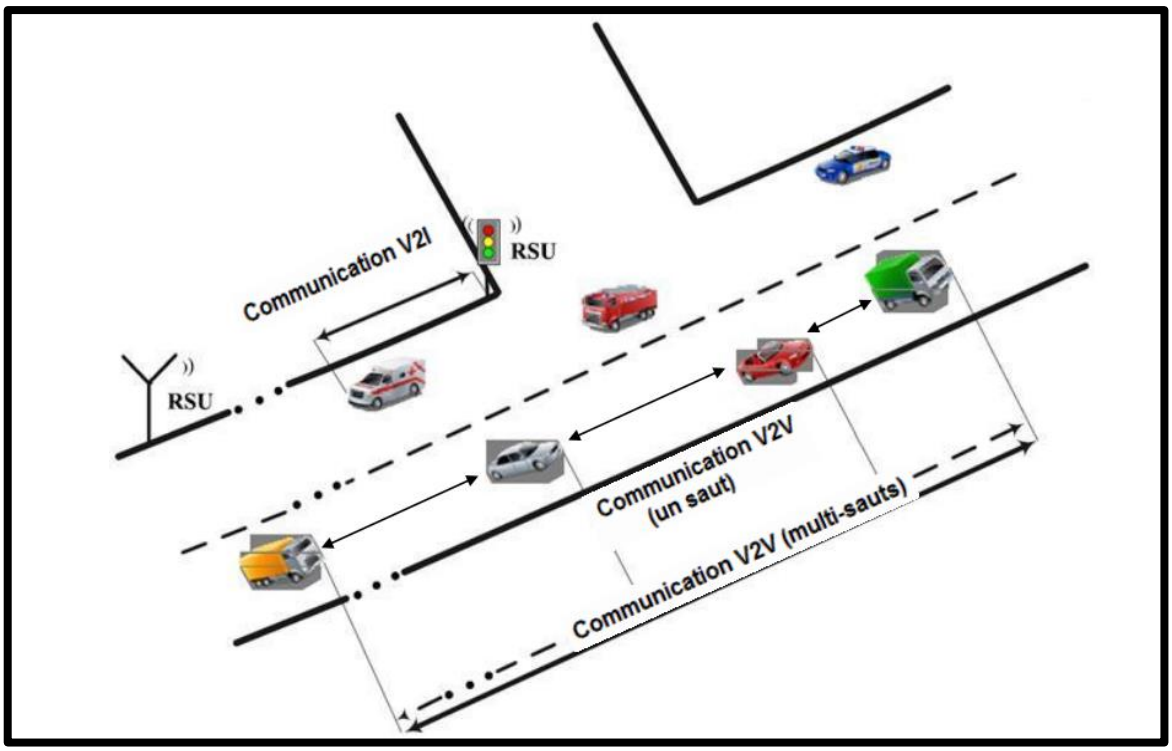

Figure I.13. Les Communications V2V et V2I. [14]

2.7.3. Mode de communication hybride

Les différents modes de communication présentés jusqu'à présent, qu'ils soient entre véhicules ou entre le véhicule et l'infrastructure sont des atouts majeurs. Néanmoins ceux-ci, pris séparément, présentent des limites dans les échanges d'informations des **VANETs**.

Les communications uniquement véhiculaires sont de faible portée. Elles ne permettent pas de joindre rapidement des véhicules distants ; tandis que les

communications uniquement véhicules à infrastructure permettent d'échanger des informations sur de longues distances, mais sans exploiter les forces de la topologie du réseau. L'utilisation des deux méthodes de communication simultanée est le point fort des **VANETs**. Ce mode hybride permet de diffuser efficacement les informations des applications sur courtes et longues portées en utilisant la topologie dynamique des **VANETs**. [7]

2.8. Les technologies utilisées dans Les réseaux VANETs

Les réseaux **VANETs** peuvent utiliser les technologies suivant :

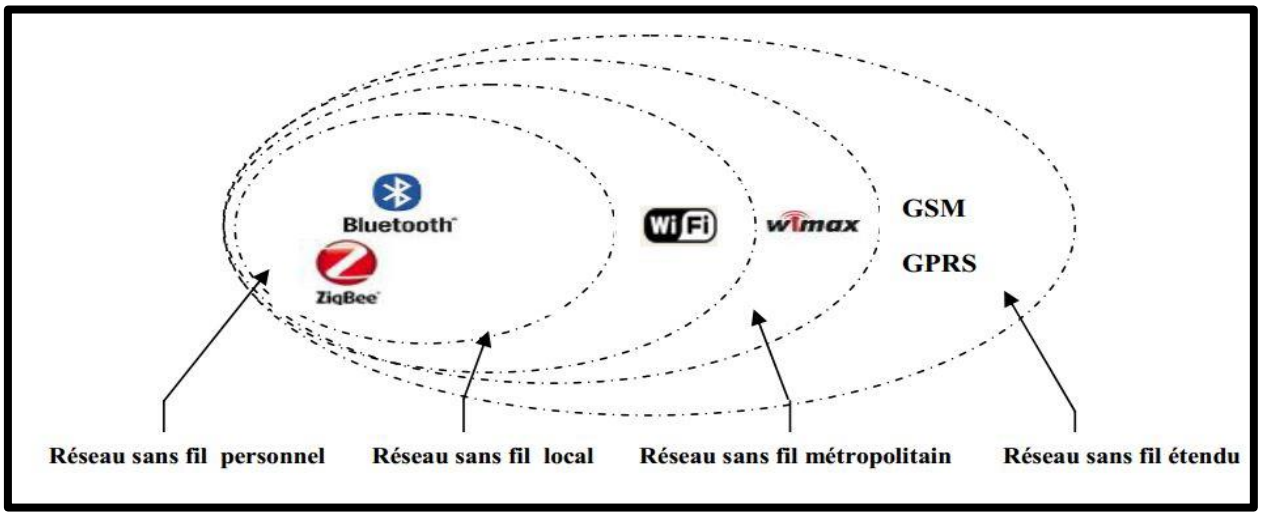

Figure I.14. Les technologies utilisées dans Les réseaux VANETs. [4]

2.8.1. WP AN (Wireless Personal Area Network)

Les réseaux personnels sans fil (appelés également réseaux individuels ou réseaux domestiques sans fil) sont des réseaux de faible portée, de l'ordre d'une dizaine de mètres. Ils servent à établir des liaisons sans fil entre des équipements peu distants ou à relier des périphériques comme des imprimantes.

La norme 802.15.1 aussi appelée Bluetooth est utilisée pour ces technologies. Elles sont peu gourmandes en énergie et offrent un débit théorique allant jusqu'à 1 Mbitls. Néanmoins l'échange de données peut être facilement perturbé par des obstacles. **[**7]

- **Le Bluetooth**

Le Bluetooth (ou "dents bleues") est un standard développe en 1994 par Ericsson et normalise par l'IEEE 802.15.1.Son débit théorique est de 1 Mb/s mais en pratique il atteint 720 Kb/s. Le Bluetooth a une portée de 10 a 20 mètres et permet l'interconnexion de huit terminaux simultanément. Son point fort réside dans sa faible consommation d'énergie. On le voit apparaitre de plus en plus dans de nombreux matériels, comme les téléphones mobiles. **[**44]

- **ZigBee**

ZigBee est basée sur la norme IEEE 802.15.4 .Cette technologie est utilisée dans les réseaux ad-hoc de capteurs (Wireless Sensor Networks). Elle offre une bande passante assez limitée allant à 250 Kbps et une couverture jusqu'à 75 m. La technologie ZigBee est utilisée principalement dans les systèmes où on transmit des petites quantités d'informations dans des petites distances. L'une des caractéristiques les plus importantes de ZigBee est la faible consommation d'énergie. **[**44]

2.8.2. WLAN (Wireless Local Area Network)

Les réseaux locaux sans fil (WLAN) font le pont entre le monde de la téléphonie et le monde informatique. Ils utilisent les normes 802.11 avec l'étiquette WiFi **[**15].La dernière norme mise en place permet un débit théorique jusqu'à 300Mbit/s (IEEE 802.11n) sur plus de 100 mètres [16]. Parmi les autres nombreux avantages que présentent les WLAN, ceux -ci permettent:

- ✓ De rendre mobiles les équipements informatiques.
- ✓ De rendre compatibles les applications informatiques actuelles avec les débits.
- ✓ L'utilisation des bandes de fréquences libres de droits.
- ✓ L'utilisation de peu, ou pas d'infrastructures. [7]

- **Wifi**

Le Wifi est un ensemble de fréquences radio qui élimine les câbles, partage une connexion Internet et permet l'échange de données entre plusieurs postes. **[**44]

2.8.3. WMAN (Wireless Metropolitan Area Network)

Les réseaux métropolitains sans fil (WMAN), connus également sous le nom WiMAX sont basés sur la norme 802.16e. Ils offrent un débit de l'ordre de 70 Mbitls pour une portée théorique allant jusqu'à 50 kilomètres. Ces réseaux peuvent fournir un point d'accès Internet aux **VANETs**. Néanmoins, le principal problème réside dans les délais importants lors des communications véhicule à véhicule (V2V). [7]

2.8.4. WWAN (Wireless Wide Area Network)

Les réseaux sans fil étendus (WWAN) regroupent plusieurs types de réseaux, notamment les réseaux cellulaires et les réseaux satellitaires. Parmi les réseaux cellulaires, on retrouve l'utilisation des technologies comme le GSM (Global System for Mobile), le GPRS (General Packet Radio Service) ;tandis que les réseaux satellitaires s'appuient sur des normes comme DVB-S (Digital Video Broadcasting Satellite) proposant des débits plus élevés. [7]

- **Le GSM**

Sigle signifiant Global System for Mobile Communications. Standard de téléphonie mobile défini par la "GSM association", il est utilisé principalement en Europe et en Asie et dans une moindre mesure aux Etats-Unis. **[**44]

- **Le GPRS**

Sigle signifiant Global Packet Radio Service.Evolution du standard de téléphonie mobile GSM qui permet des transferts de données par paquets, comme sur Internet. Avec un débit théorique de 128 kbps, il est permet notamment l'envoi de photo d'un téléphone a un autre. **[**44]

2.9. Travaux dans le domaine des VANETs

Les propriétés des réseaux véhiculaires offrent des challenges importants, ce qui rend les VANET s'ouvrent à plusieurs domaines de recherche dont nous citons les plus importants [17] [18] [19] [20] [21]:

2.9.1. Sécurité

La sécurité est un défi majeur ayant un grand impact sur le futur déploiement des réseaux véhiculaires ainsi que leurs applications. En raison de la sensibilité des domaines d'utilisation des **VANET**, 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.

2.9.2. L'accès au canal

Les réseaux véhiculaires utilisent des communications radio. Par conséquent, il est important de concevoir des solutions spécifiques aux réseaux **VANET** qui permettent d'apporter de la qualité de service et de gérer les priorités en résolvant les problèmes d'interférences radio, des problèmes de propagation à multi-trajets des ondes ainsi que les irrégularités électromagnétiques.

2.9.3. Localisation des véhicules

Si l'un des véhicules du réseau doit être localisé (dans le cas d'un accident par exemple), les autres doivent être informés de sa position. Le problème est que tous les véhicules ne sont pas équipés d'un système de repérage par satellite (GPS). Pour cette raison, un mécanisme de localisation sans utilisation de GPS est nécessaire.

2.9.4. Problèmes de congestion

L'un des problèmes des **VANET** est que chaque véhicule communique avec tous ceux qui sont dans sa zone de couverture. Ceci entraîne une dégradation de la qualité de service (QoS) avec l'augmentation du nombre de véhicules. Ce problème a fait l'objet de plusieurs études.

2.9.5. Mobilité dans la simulation des réseaux

Dans la simulation des **VANET**, le facteur mobilité a longtemps été négligé. On ne considérait pas la différence de mouvements entre les noeuds des **VANETs** et des MANET, ce qui pouvait biaiser les résultats de la simulation. Pour cette raison, de plus en plus d'équipes de recherche s'intéressent à l'étude de la mobilité dans les **VANET**. Avec un bon simulateur, plus le modèle de mobilité est réaliste, plus les résultats de la simulation sont proches de la réalité. D'où l'impact direct des modèles de mobilité sur la réussite d'une simulation.

2.9.6. Routage

Le routage dans les réseaux **VANET** est un problème très difficile à gérer et un axe de recherche pour beaucoup de chercheurs. Pour que les véhicules puissent communiquer entre eux, un protocole de routage doit être défini. En effet quand les terminaux ne sont pas à une portée de transmission radio directe, le routage est exigé pour établir la communication entre les véhicules.

Conclusion

Les VANETs est une particularité des réseaux MANET où les nœuds mobiles sont des véhicules (intelligents) équipés de calculateur.

Les objectifs des réseaux **VANETSs** sont : Sécurité des usagés et Confort des usagé.

Les applications dans les réseaux **VANETs** sont : application dans la prévention et la sécurité routière, application pour l'optimisation du trafic et aide dans la conduite et applications au confort du conducteur et des passagers.

Les modes de communication dans les réseaux sans fil sont : véhicule-véhicule (V2V), véhicule-infrastructure (V2I) et Hybride.

Les caractéristiques de réseaux **VANETs** sont : Echange entre nœuds, hétérogènes topologie dynamique, propagation par trajet et multiple Relais d'informations.

Les domaines de recherche dans les réseaux **VANETs** sont : Sécurité, l'accès au canal , localisation des véhicules ,Problèmes de congestion , mobilité dans la simulation des réseaux ,le routage .

Dans le chapitre en va voire la sécurité et les attaques dans les réseaux **VANETs** et comment évités ces attaques.

CHAPITRE II :

LA SECURITE ET LES ATTAQUES DANS LES RESEAUX VANETS

Introduction

Les réseaux **VANETs** comme tous les réseaux sans fil sont difficiles à sécuriser contre les attaques. Pour assurer la sécurité sur **VANET**, il y a des méthodes et techniques ont été développées.

Dans les réseaux traditionnels les solutions de sécurité est utilisent le cryptographique pour authentifier les nœuds et sécuriser les échanges de données. A contrario, les réseaux **VANETs** est utilisent mécanisme de sécurité les réseaux traditionnels et les systèmes de détection d'intrusions (**IDS**) pour assurer la sécurité de nœuds et la transmission des données contre les déférentes attaques existent.

Dans ce chapitre en va voir les objectifs de la sécurité dans un réseau **VANET** pour assurer une meilleure sécurité de transmission des données surtout les alertes liée à la sécurité routier ; après en citer les types et les déférentes attaques existent sur **VANET** et en fin l'**IDS** qui est utiliser pour surveillant les nœuds des **VANETs.**

1. La sécurité dans les VANETs

1.1. Les objectifs de la sécurité

1.1.1. L'authentification

Ce requis est l'un des principaux de tout système. Pour les **VANETs**, il très important de connaitre plusieurs informations sur le nœuds émetteur tel que son identifiant, son adresse, ses propriétés , sa position géographique. Il est donc important d'authentifier l'émetteur du message et le message qui circule sur le réseau. L'authentification a pour objectif principal de contrôler les niveaux d'autorisation du véhicule dans le réseau. Dans les **VANETs**, l'authentification peut aider à la prévention des attaques de Sybil en spécifiant un identifiants unique pour chaque véhicule. Grâce à cette technique, un véhicule ne pourra pas clamer d'avoir plusieurs identifiants et de faire croire qu'il s'agit de plusieurs véhicules et ainsi perpétrer une attaque sur le réseau. [22]

L'objectif de l'authentification dans les réseaux **VANETs** est assuré le bon nœud du réseau, il est très important pour connaitre les nœuds du réseau et leurs informations comme : position, priorité, id …etc.

Il y a deux types d'authentification sont [23]:

- ✓ L'authentification de l'ID, C'est le fait pour un nœud d'être capable d'identifier les transmetteurs d'un message donné de façon unique. C'est par cette authentification que passe l'accès au réseau du véhicule émetteur.
- ✓ L'authentification de la propriété, elle aide à déterminer le type d'équipement qui est en communication. Il peut s'agir d'un autre véhicule, d'un « RSU » ou encore d'un autre équipement.

1.1.2. L'intégrité

Elle s'assure que le message n'est pas altéré entre l'émission et la réception. Le récepteur du message vérifie le message reçu. Il s'assure que l'identifiant de l'émetteur reste le même tout au long de la transaction, et que le message reçu est bien celui qui a été émis .[24]

L'intégrité protège contre la destruction et l'altération du message pendant la transmission. Si un message corrompu est accepté, on considère qu'il y'a eu une violation de l'intégrité. Pour mettre en place l'intégrité, le système devrait prévenir les attaques contre l'altération des messages, car le contenu du message doit toujours être fiable . [25]

Certain protocoles de sécurité utilisent la signature électronique pour se rassurer que le message n'a pas été altéré Durant la transaction. Ainsi, à l'arrivé du message, la signature est vérifiée pour juger de l'intégrité du message. [26]

L'objectif est assuré que les données échangé ne sont pas altéré dans le temps de transmission, quelle que soit cette altération volontaire ou accidentelle.

1.1.3. La confidentialité

Le cryptage des messages permet d'empêcher à des véhicules n'ayant pas les autorisations nécessaire de lire les messages qui ne leurs sont pas destines. Cette mesure permet de respecter la confidentialité des échanges. [25] [27]

La confidentialité des messages dans les **VANETs** dépends de l'application et du scenario de communication. Par exemple les messages reliés à l'avertissement d'une situation d'urgence peuvent être lu par n'importe quel membre du réseau. Ce type de message n'a donc par besoin d'être crypté. Par contre pour une application de paiement en ligne, il est important que les messages soient cryptés pour ne pas divulguer des informations sensibles sur une carte de crédit par exemple. La confidentialité peut être mise en place en utilisant les clé public/privé pour le cryptages des messages Durant la communication. [28]

Dans les communications V2I, les « RSU » et le véhicule se partagent une clé de session après avoir effectué une authentification mutuelle. Ainsi tous les messages sont cryptés avec la clé de session et sont aussi attaché un code d'authentification du message pour l'authentification du message [23].

L'objectif est empêché l'accès aux données (information ou message) transmises dans le réseau par un nœud non autorisé.

1.1.4. La non-répudiation

Ce requis permet d'empêcher une entité de nier d'avoir participer à une communication. Il permet de protéger le système contre le déni d'un nœud qui indique n'avoir pas participé à une communication alors qu'il l'a fait. La non-répudiation permet donc au récepteur de prouver qu'il a reçu le message d'un tiers de communication. Ainsi, pour chaque message reçu, l'émetteur peut être clairement identifié. [29]

Le but général de la non-répudiation est de collecter, de maintenir et de rendre disponibles toutes les évidences à propos d'un évènement ou d'une action, afin de résoudre des disputes à propos d'une occurrence ou non d'une action.

La non-répudiation dépend donc de l'authentification. Le système peut ainsi identifier l'auteur d'un message malveillant. [22]

L'objectif est assurer que l'émetteur ne peut nier d'envoyer le massage à un autre nœud dans le réseau.

1.1.5. La disponibilité

Le réseau et les applications doivent rester disponibles même en présence de panne dans le réseau. Ce requis permet non-seulement de sécuriser le système mais rend aussi celui-ci tolérant aux fautes. Ainsi les ressources doivent rester disponibles jusqu'à ce que la faute soit réparée. [30]

Un protocole de routage adéquat est nécessaire pour atteindre tous les récepteurs d'un message envoyé. Certain messages doivent rester circonscrit à un moment ou à un endroit définie, pour ne pas induire en erreur les véhicules si l'information n'est plus pertinente. [31]

L'objectif est garantir aux nœuds d'accéder aux services de réseau, c'est-à-dire garantir disponibilité des applications et des services même le réseau est en panne.

1.2. Sécurité des VANETs vs Réseaux Traditionnels [6]

- **La mobilité :**

La mobilité des nœuds rend la topologie des **VANETs** instable. Il n'est donc pas facile pour un nœud de connaître correctement son voisinage. Les attaquants peuvent ainsi forger et diffuser des fausses informations de topologie [32] pour construire des routes qui passent par eux et réaliser ainsi des attaques qui visent à causer des accidents ou la congestion de routes. Par ce moyen, un protocole de routage ad hoc non-sécurisé peut facilement être attaqué. De plus, la mobilité des attaquants peut aussi les rendre plus difficiles à détecter ou la localiser.

En comparaison avec les réseaux traditionnels, il n'y a pas autant de mobilité dans les réseaux filaires, et dans les réseaux cellulaires ce sont des infrastructures qui gèrent la mobilité, donc il est nécessaire de construire des protocoles de routage spécialement pour les **VANETs** capables de découvrir correctement la topologie du réseau même sous attaques.

- **Le support sans fil partagé :**

La nature de transmission radio dans l'air, permet à un intrus d'écouter passivement. [33]Tous les messages échangés pourvu qu'il se trouve dans la zone d'émission.

L'adversaire, a donc accès au réseau et peut intercepter aisément les données transmises, sans même que l'émetteur ait connaissance de l'intrusion. L'intrus, en étant potentiellement invisible, peut brouiller le canal radio pour bloquer les transmissions, injecter massive de paquets visant à épuiser les ressources des nœuds, enregistrer, modifier, et ensuite retransmettre les paquets comme s'ils avaient été envoyés par un utilisateur légitime, donc les **VANETs** ont besoin de nouveau mécanismes afin de sécuriser l'accès au réseau.

- **Manque des serveurs centraux :**

Dans les **VANETs** puisqu'il n'y a pas forcément de serveur central [34] , la distribution et la gestion de clés peuvent être difficiles à réaliser. Dans les réseaux traditionnels les solutions de sécurité s'appuient souvent sur des relations de confiance préalablement établies ou des autorités de confiance tierces, et utilisent les primitives cryptographiques pour authentifier les nœuds et sécuriser les échanges de données. Afin d'utiliser ces moyens cryptographiques dans les **VANETs**, nous devons étudier comment établir des autorités de confiance ou des relations de confiance entre les nœuds sans l'aide d'aucune infrastructure.

- **Manque de coopération :**

Dans un réseau ad hoc il est difficile de détecter des nœuds égoïstes [35] qui peuvent tout simplement être silencieux et/ou refusent de transférer les données afin de préserver leur ressource. Quand de tels nœuds sont nombreux dans le réseau, la disponibilité du service de routage est touchée. Ce problème d'égoïsme n'existe pas dans les réseaux traditionnels où les nœuds reposent sur les routeurs dédiés pour assurer la fonctionnalité de routage. Donc, de nouveaux mécanismes doivent être désignés pour garantir la coopération des nœuds dans les réseaux **VANETs**.

- **Nœuds compromis :**

Les nœuds dans un **VANET** sont plus faciles à compromettre que ceux des réseaux traditionnels, parce qu'ils sont de nature mobile, en plus les **VANETs** peuvent être divisés et/ou fusionnés, les attaquants auront plus de chances d'attaquer (compromettre) des nœuds sans être aperçus. Dans les réseaux ad hoc il y a quelques attaques très sophistiquées, par exemple les attaques de type ‘’wormhole’’ ne peuvent être commises que par des nœuds compromis et sont difficiles à éviter.

L’utilisation de la cryptographie ne permet pas de résoudre le problème de ces nœuds compromis par une simple authentification, car ces nœuds ont été des participants légitimes au processus de routage avant d’être contrôler par des attaquant.

2. Les attaques dans les VANETs

2.1. Les Types d'attaquants dans les réseaux VANETs

2.1.1. Attaque interne vs attaque externe

L'attaquant interne est une entité dans le réseau, elle est les mêmes privilèges et les mêmes caractéristiques que les autres entités du réseau qui peut communiquer avec les autres membres du réseau. A contrario, L'attaquant externe n'est pas un nœud dans le réseau.

Généralement :

- ✓ les attaques internes sont difficiles à détecter para port à les attaques externes.
- ✓ l'attaquant externe est plus limité quant à la diversité des attaques que l'attaquant interne.

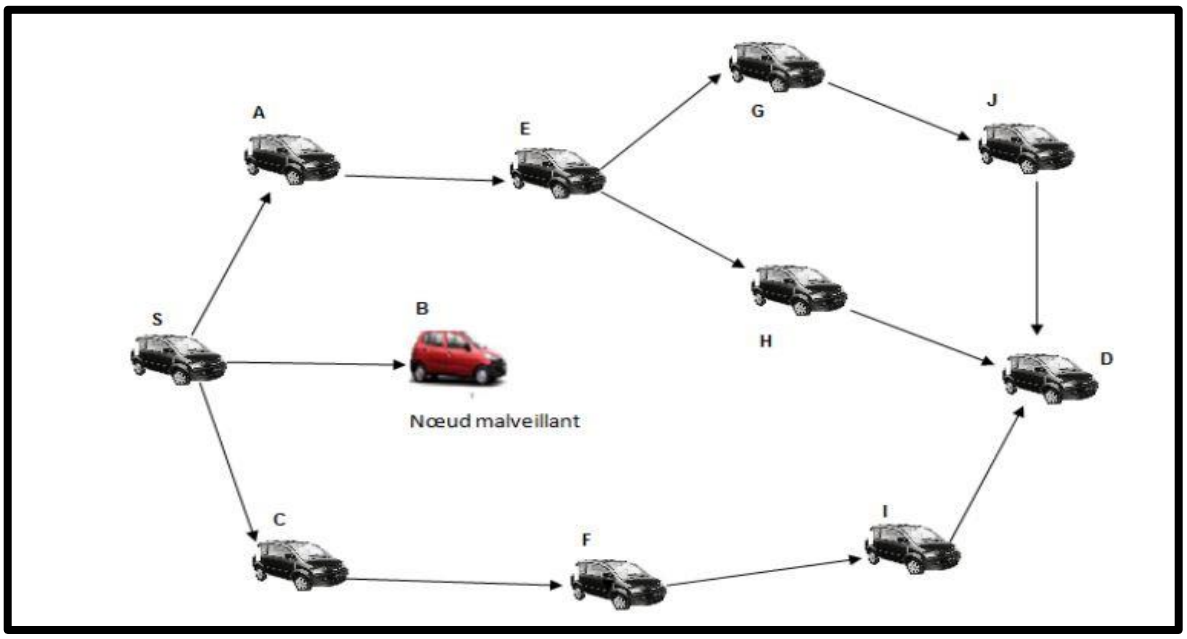

Figure II.1. Attaque interne. [6]

2.1.2. Attaquant malveillant vs attaquant rationnel

L'attaquant malveillant (ou Malicieux) cherche à prouver une prouesse personnelle à travers détecter les points faible dans le réseau pour blesser des nœuds du réseau ou attaquer le système, il n'est utilisé pas aucune structure. A contrario, L'attaquant rationnel est professionnel, il y'a un objectif précis.

L'attaquant malveillant est facile identifier que l'attaquant rationnel est très difficile à identifier.

2.1.3. Attaquant passif vs attaquant actif

L'attaquant passif écouter les messages transmis et attenté jusqu'à une information utile pour utiliser pour suivre son attaque. A contrario, L'attaquant actif agit sur les messages et les informations qui sont transmissent entre les nouds.il peut les modifier, supprimer,… etc.

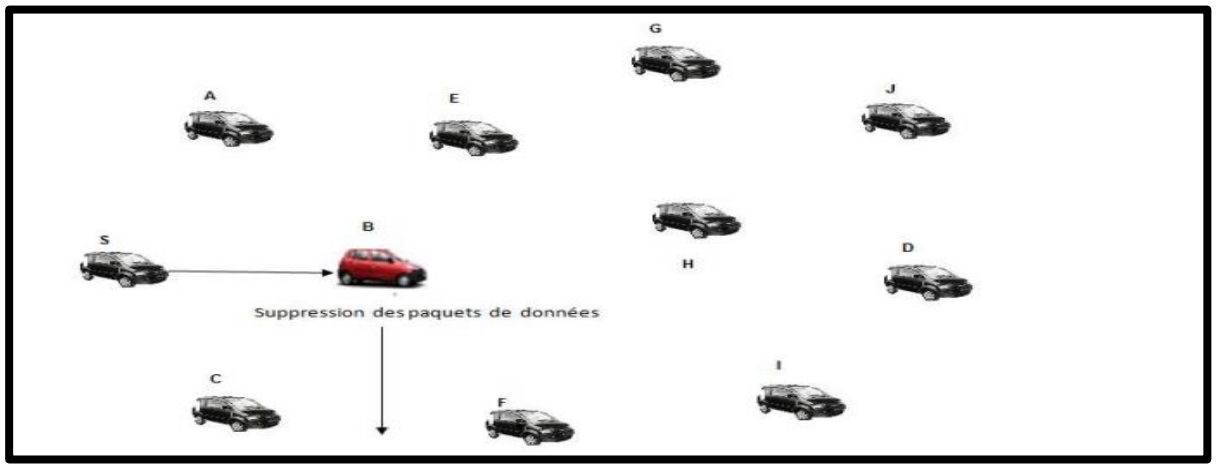

Figure II.2. Exemple attaque actif. [6]

2.2. Les différentes attaques dans les réseaux VANETs

2.2.1. Attaque sur la vie privée (tracking)

L'entité malveillante identifier un nœud du réseau pour récupérer le maximum des informations et on peut utiliser sons identité pour accédés à les données du réseau.

2.2.2. Attaque sur la cohérence de l'information (Bogus information)

L'entité malveillante injectée des fausses informations dans le réseau pour modifier l'itinéraire d'un nœud ou changer la topologie de réseau.

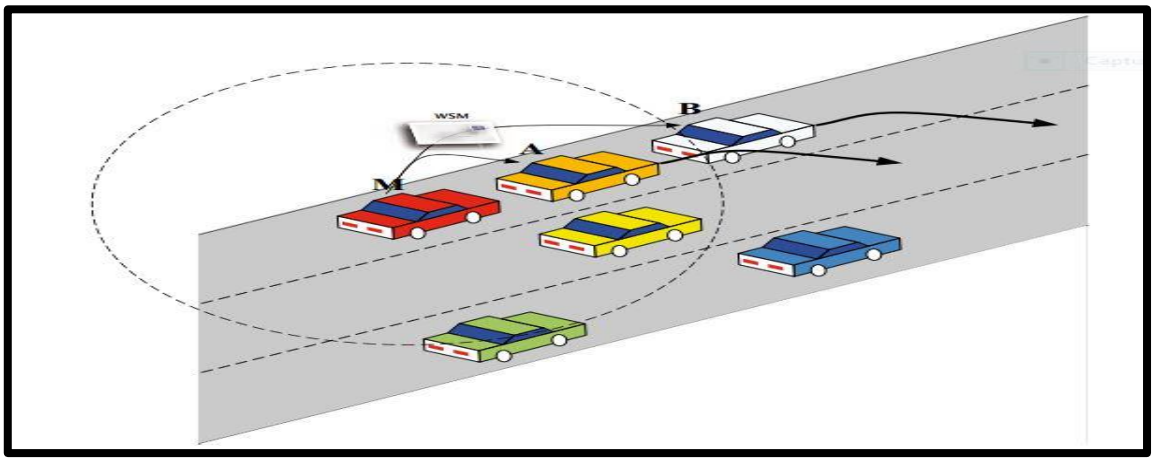

Figure II.3. Attaque sur la cohérence de l'information. [36]

2.2.3. Usurpation d'identité ou de rôle (Spoofing)

L'entité malveillante usurper l'identité d'une notre entité dans le réseau et jouer leur rôle comme passerelle. Donc tous les nœuds de réseau vont transmettre les informations à l'attaquant.

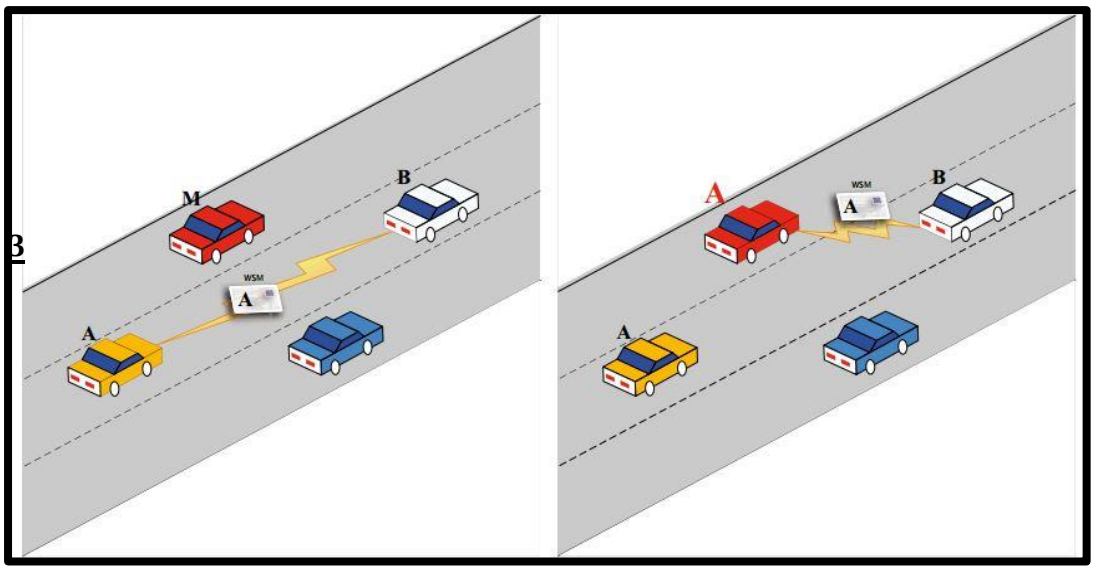

Figure II.4. Usurpation d'identité ou de rôle. [36]

3.2.4. Déni de service (Deny 0/ Services, DoS)

L'objectif de cette attaque est d'empêcher l'accès aux services et la communication entre les nœuds du réseau, en utilisant brouillage dans le canal radio.

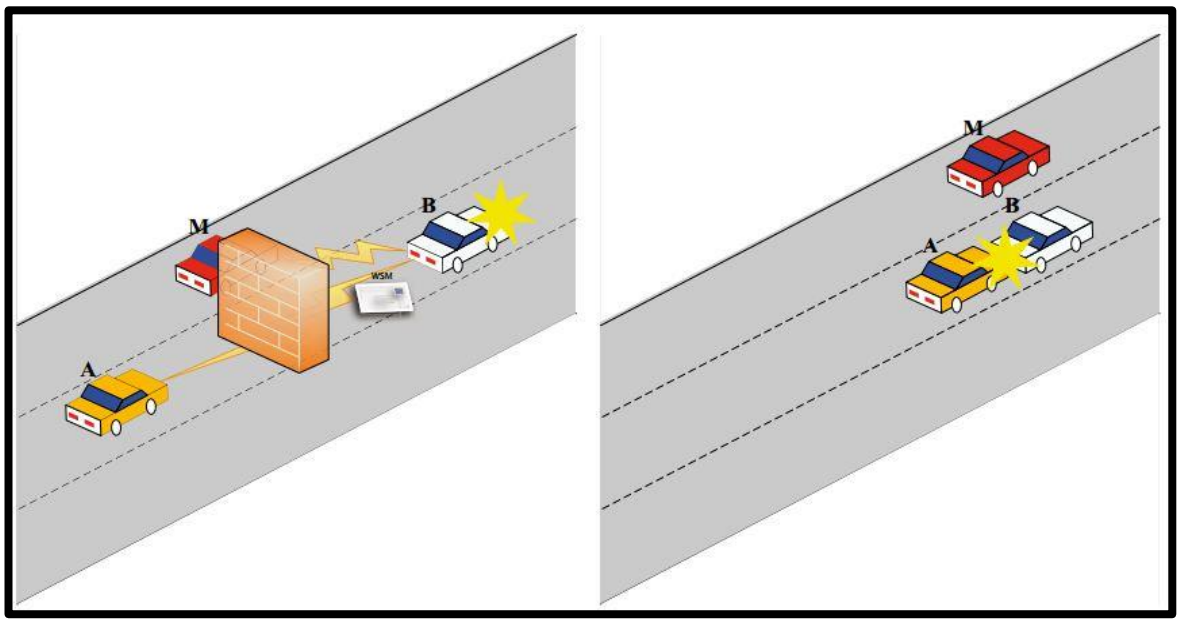

Figure II.5. Déni de service (Deny 0/ Services, DoS). [36]

2.2.5. Écoute de communication

Cette attaque combine les concepts de « spoofing » et de « tracking », l'attaquant cible un véhicule sachant par exemple que celui-ci va effectuer un paiement et se met à l'écoute de ses communications en vue d'extraire un mot de passe. [36]

2.2.6. Véhicule caché

L'attaquant génère de fausses identités de véhicules sur la route, ainsi que de fausse information de localisation de manière à être dans une position avantageuse. Son objectif est de s'octroyer de manière légitime des droits, en faisant penser aux vrais véhicules que sa localisation est la meilleure. L'attaquant peut alors émettre des alertes, prendre la tête d'un c1uster, générer de fausse congestion, etc. [36]

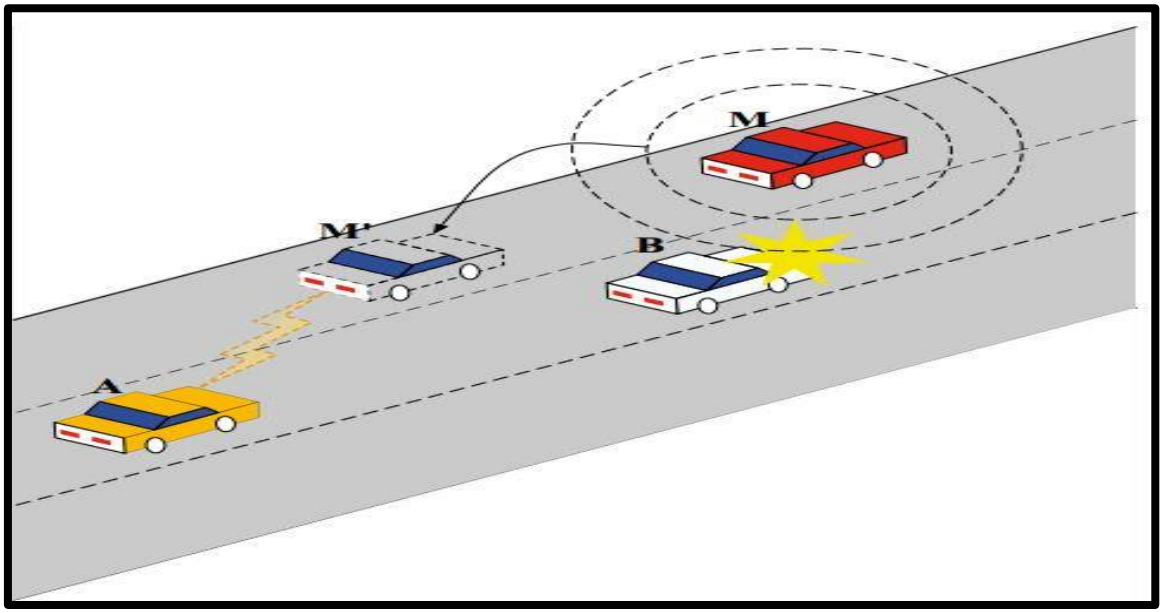

Figure II.5. Véhicule caché. [36]

2.2.7. Wormhole

Cette attaque suppose que l'attaque contrôle une autre entité plus loin dans le réseau ou qu'elle est effectuée de manière coopérative. L'objectif de l'attaquant est de modifier le routage et la topologie du réseau à grande échelle.

Les deux entités attaquantes créent un tunnel entres-elles et laissent pensée aux autres nœuds que le routage est plus rapide par elles. Les entités perturbent le routage et récupèrent les informations des nœuds. C'est une forme de « spoofing ». [36]

3. Mécanismes de sécurité de routage ad hoc existants

3.1. Les mécanismes de routage sécurisé

Garantissent l'authentification, la confidentialité, l'intégrité et finalement la non-répudiation dans les deux phases de routage : découverte de route et la transmission des données. [6]

3.2. Les mécanismes de gestion des clés

Qui traitent l'identification et toutes les questions concernant (création, la distribution, la révocation, le renouvellement et l'échange des clés). [6]

3.2.1. Gestion de clés asymétriques

Le déploiement des PKI traditionnelles dans les réseaux ad hoc est problématique, puisqu'un tel système a besoin d'une autorité de certification (CA) qui est un serveur central qui assure la livraison et la révocation de certificats en permanence, en plus le CA doit être toujours connecté et accessible par les nœuds. Ces contraintes font du PKI traditionnelle inadaptée à un environnement **VANET**. [6]

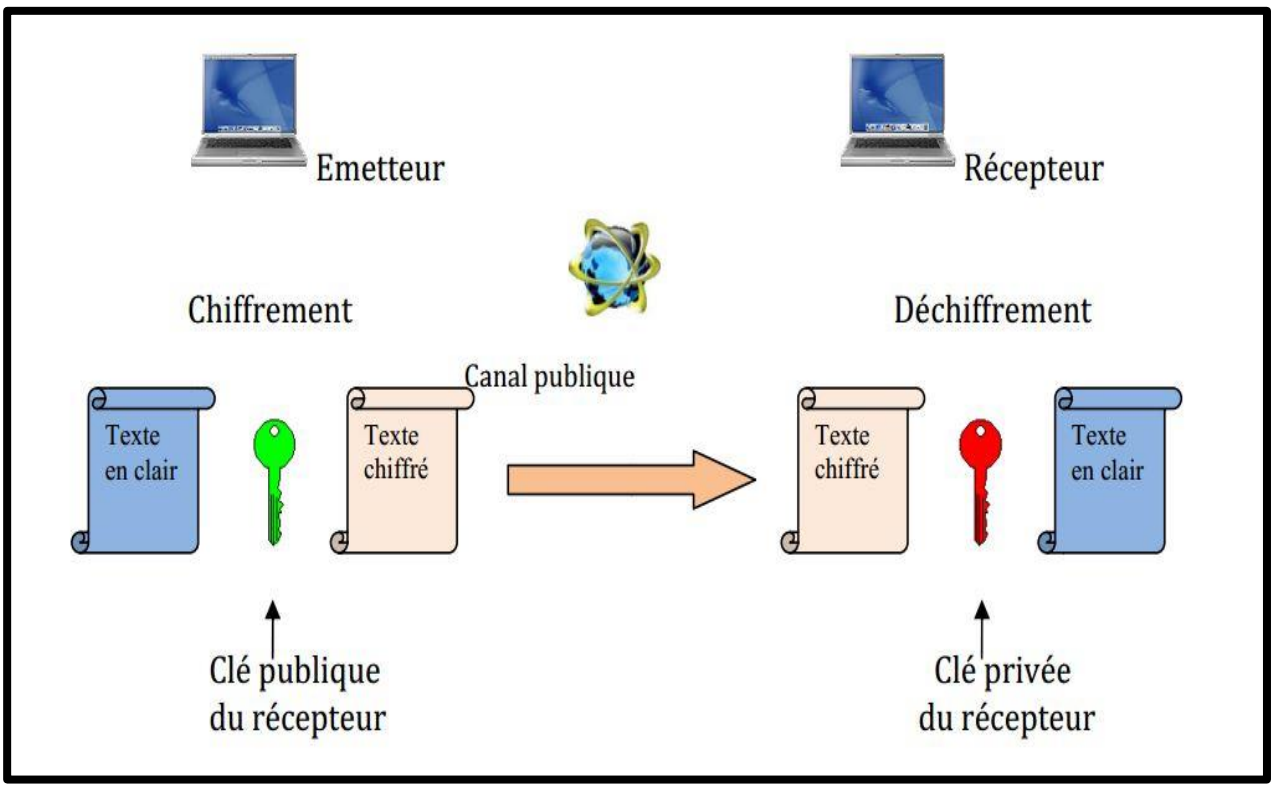

Figure II.6.le principe de chiffrement asymétrique. [2]

➢ **PKI Auto-organisée**

Capkun and Hubeau ont proposé une infrastructure à clé public auto-organisée inspirée du PGP pour authentifier les nœuds d'un réseau mobile ou les certificats numériques sont créés, signés, émis et enregistrés par les nœuds eux-mêmes. Dans cette PKI chaque nœud établi des certificats pour les nœuds en qui il a confiance, et si deux nœuds veulent communiquer sans connaissance préalable l'un à l'autre, ils s'échangent leur liste de certificat afin de créer un certificat entre eux. [6]

Par exemple si un nœud A veut communiquer avec un nœud C, et que le nœud A fait confiance en un troisième nœud B comme le nœud C, alors A peut établir une chaine de confiance à travers B. [6]

➢ **La signature numérique** [2]

La signature numérique est définie comme des « données ajoutées à un message », ou transformation cryptographique d'un message, permettant à un destinataire de :

1. Authentifier l'auteur d'un document électronique.

2. Garantir son intégrité.

3. Protéger contre la contrefaçon (seul l'expéditeur doit être capable de générer la signature), assuré alors la non-répudiation.

La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage, et de la cryptographie asymétrique.

- **Étapes de signature d'un message :**

La signature numérique comprend deux étapes :

A. Évaluation du condensé de message : l'émetteur commence par générer un condensé, qui est une représentation réduite et unique du message complet, à l'aide d'une fonction de hachage.
B. Signature du condensé : l'émetteur chiffre ce condensé avec un algorithme asymétrique à l'aide de sa clé privée. Il obtient une signature électronique qu'il appose au message original avant d'émettre l'ensemble, message et signature, sur le réseau.

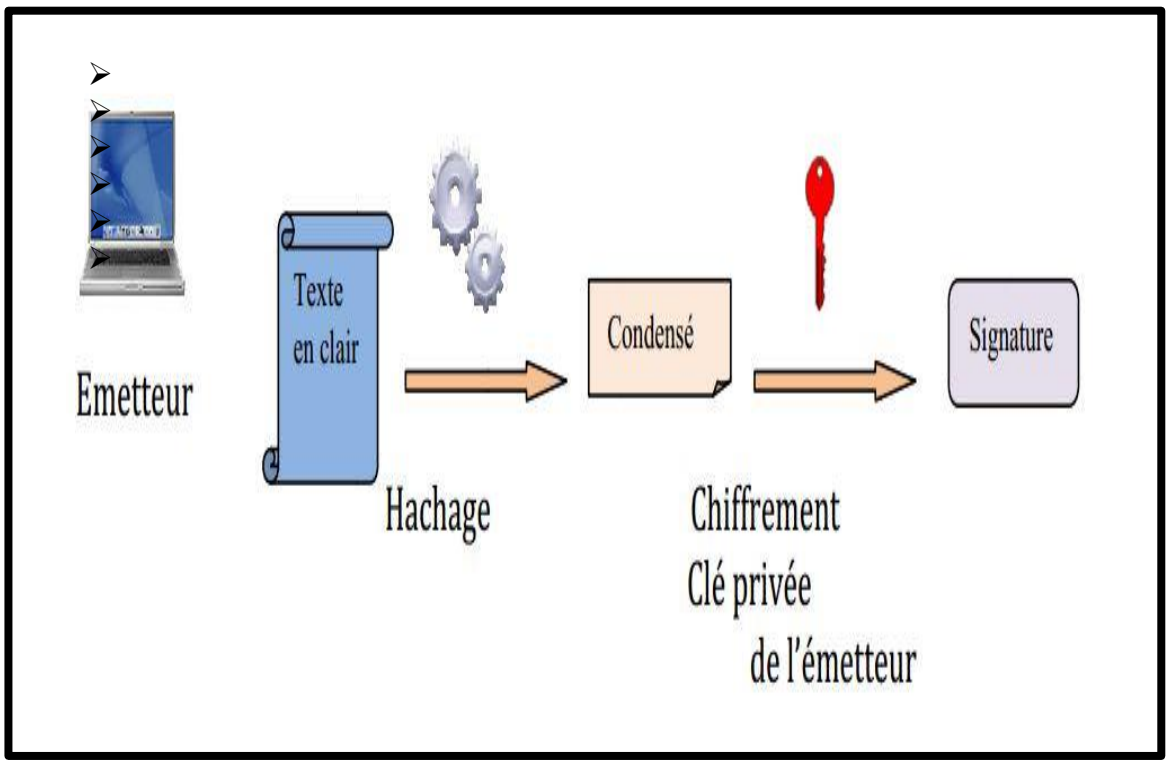

Figure II.7.le principe de signature. [2]

- **Certificats électroniques** [2]

Un certificat est un élément d'information qui prouve l'identité du propriétaire d'une clé publique. Les certificats sont signés et transmis de façon sécuritaire par un tiers de confiance appelé autorité de certification (Certificate Authority, ou CA). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cettedate en cas de compromission de la clé (ou du propriétaire).

La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat :

- ✓ Version
- ✓ Numéro de série de l'autorité de certification
- ✓ Algorithme de signature du certificat
- ✓ Le nom de l'autorité de certification
- ✓ Le nom du propriétaire du certificat
- ✓ La date de validité du certificat
- ✓ Le propriétaire du certificat
- ✓ La clé publique du propriétaire

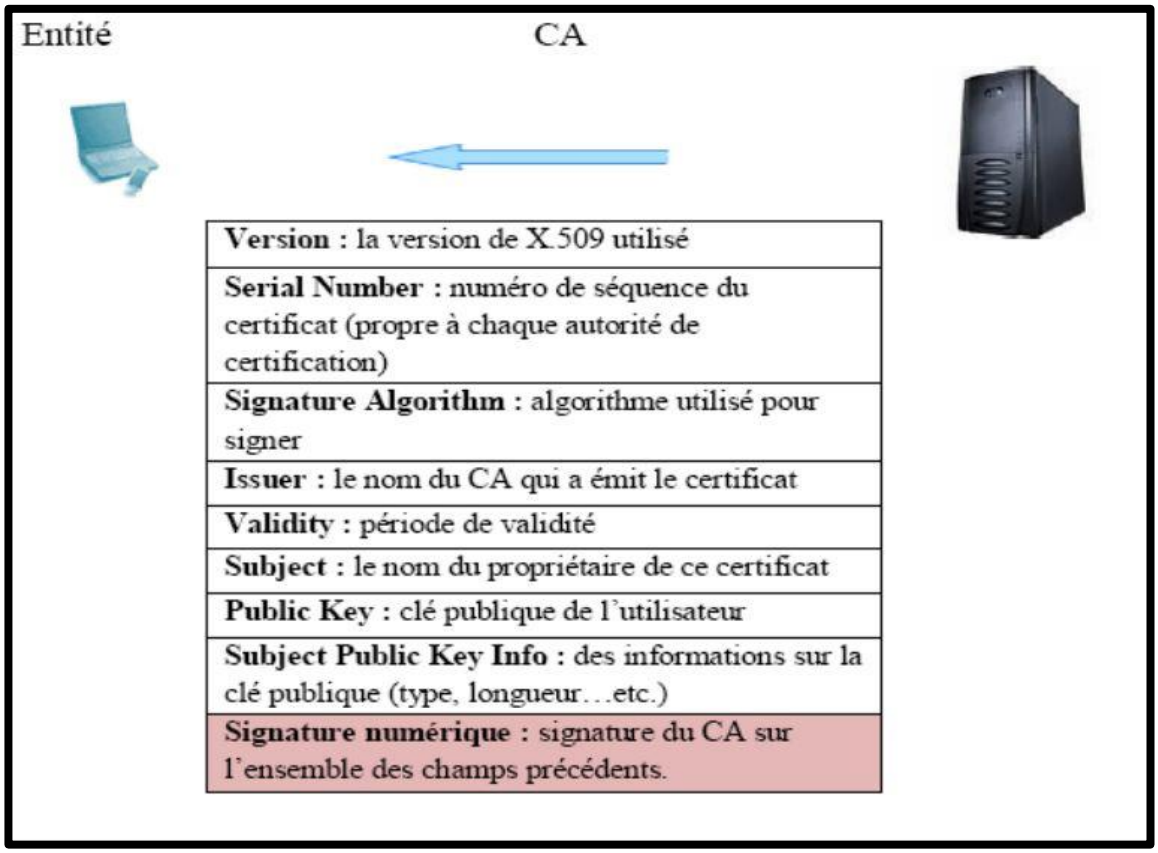

Figure II.8. Contenu d'un certificat. [2]

3.2.2. Gestion de clé Symétrique

Le but d'échange de clés symétriques est d'établir une clé secrète commune entre les parties communicantes sans avoir aucune information préalable l'une sur l'autre. Parmi les protocoles d'échanges de clés on peut citer celui inventé par Diffie et Hellman. [6]

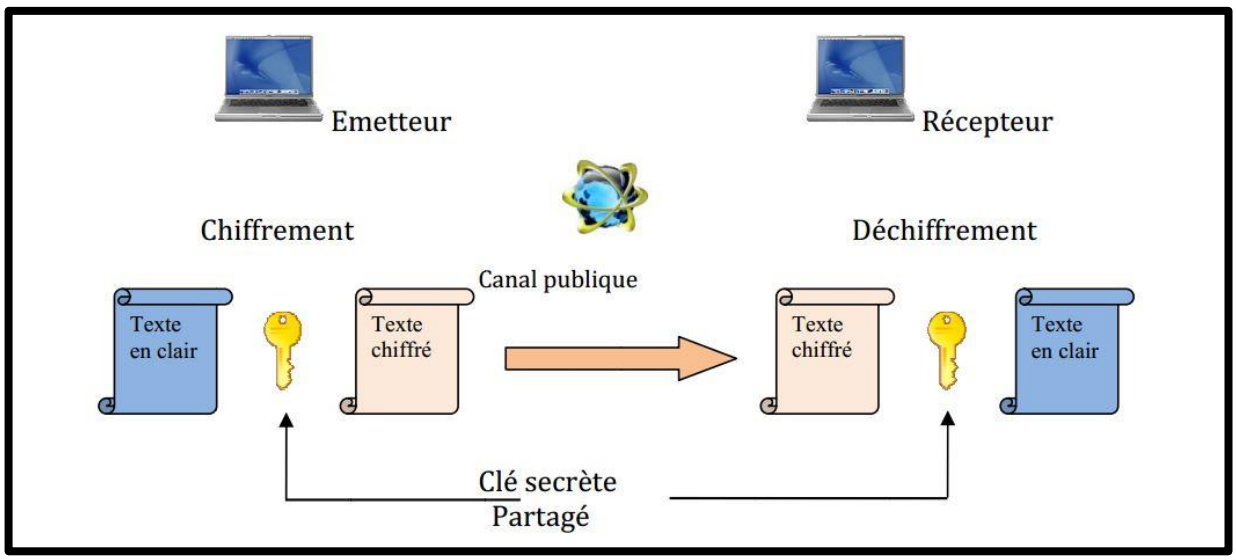

Figure II.9. Le principe de chiffrement symétrique. [2]

➢ **L'échange de clés Diffie-Hellman** [6]

L'échange de clés Diffie-Hellman , du nom de ses auteurs Whitfield Diffie et Martin Hellman, est une méthode par laquelle deux nœuds notés M1 et M2 peuvent se mettre d'accord sur une clé qu'ils peuvent utiliser pour chiffrer une conversation.

Le protocole d'échange de clés de Diffie-Hellman, repose sur une fonction de la forme $k = g^x \bmod p$, avec P premier et g < P.

Une telle fonction est très facile à calculer, mais la connaissance de K ne permet pas d'en déduire facilement X. Cette fonction est publique, ainsi que les valeurs de g et P.

Voici comment se passe l'échange Diffie-Hellman. Les calculs indiqués sont faits dans le groupe cyclique fini qui possède g comme générateur.

1. Le nœud M1 tire au hasard un entier a tel que 1 < a < P − 1 et le garde secret
2. Le nœud M1 envoie à M2 $A = g^a \ mod \ p$.
3. Le nœud M2 choisit un nombre b tel que 1 < b < P − 1 et le garde secret.
4. Le nœud M2 envoie à M1 $B = g^b \ mod \ p$.
5. Le nœud M1 a reçu B et calcul $B^a \ mod \ p$ (c'est-à-dire en passant par, $(g^b)^a = mod \ p$, mais il ne connaît pas B) : $S = B^a mod \ p$.
6. Le nœud M2 a reçu A et calcul $A^b mod \ p$. (c'est-à-dire en passant par, $(g^a)^b = mod \ p$. mais il ne connaît pas A) : $S = A^b mod \ p$.

M1 et M2 obtiennent à la fin de leurs calculs respectifs le même nombre qui n'a jamais été exposé à la vue des indiscrets : c'est la clé S. La figure présente le processus d'échange de clé Diffie Hellman.

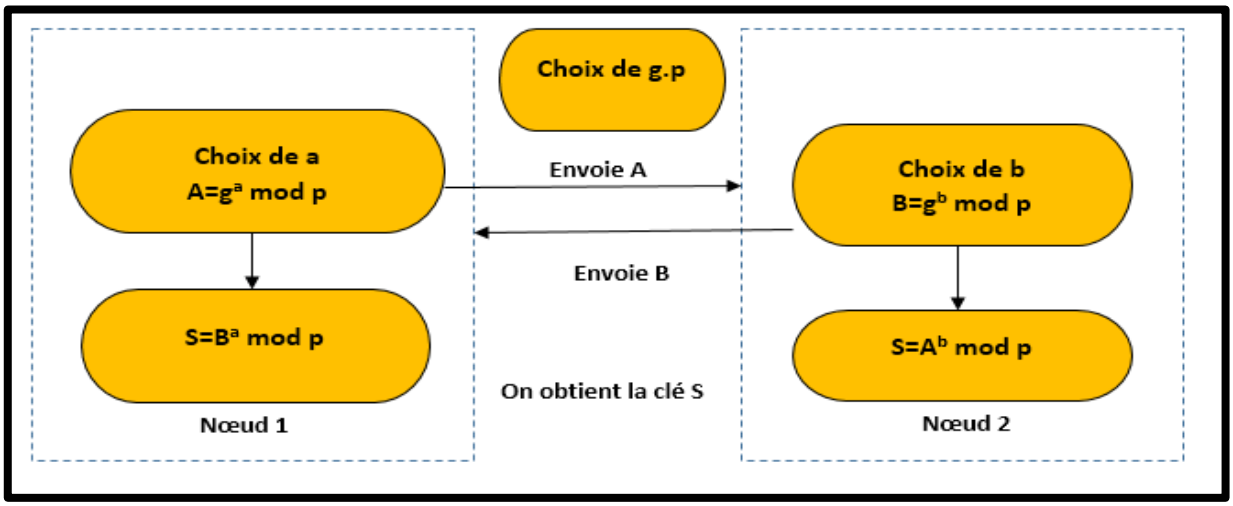

Figure II.10. Echange de clé Diffie Hellman. [6]

D'après cette étude, on peut constater que la solution symétrique semble être la plus adaptée pour les **VANETs** pour sa facilité de déploiement et sa rapidité de calcul.

3.3. Les systèmes détection d'intrusion

Pour surveiller les nœuds des **VANETs**. [6]

3.3.1. Définition d'IDS

Un **IDS** (Internet Detection Scanner), est un outil qui a pour vocation la surveillance d'un ou plusieurs réseaux de machines. Il permet de détecter des attaques ou des événements suspects, pouvant poser problèmes, de tenter de les supprimer en suggérant des actions correctives, de déclencher des actions sur événements (alertes, courrier, RESET de connexion...). Typiquement, une architecture de détection d'intrusion pourra être composée d'une console qui supervise un ou plusieurs agents placés sur différents segments du réseau, ainsi que des agents installés sur les machines sensibles de ces segments. Le terme **IDS** recouvre des équipements destinés à la surveillance du trafic d'un réseau ou de l'activité de machines. Pour une plus grande efficacité il est possible de coupler les deux. [37]

- **Notion de base**

Alerte : est un message formaté et émis par un analyseur lorsqu'il y a des activités intrusives contre une source de données. [38]

Analyseur : c'est un outil matériel ou logiciel qui met en œuvre l'approche choisie pour la détection (comportementale ou par scénarios), il génère des alertes lorsqu'il détecte une intrusion. [38]

Capteur : un logiciel générant des événements en filtrant et en formatant les données brutes provenant d'une source de données. [38]

3.3.2. Pourquoi utiliser un IDS ?

- ✓ La surveillance du trafic d'un (plusieurs) réseau(x) de machines en vue de la surveillance « Temps Réel » du trafic, par opposition à la consultation des traces (« logs ») qui se fait forcement en différé, sans parler des difficultés de repérer des failles.
- ✓ Ce que qu'on peut attendre d'un **IDS** : l'émission d'alertes qui permettront la détection de la préparation d'une attaque, (scans massifs à la recherche de failles sur un ensemble de machines…), une attaque en cours (trafic sur des ports correspondants à des failles), et à posteriori, la détection d'une machine compromise avant qu'elle ne puisse servir de base d'attaques vers d'autres systèmes.
- ✓ En outre, il permet d'éditer des rapports permettant d'avoir une vision globale du degré de sécurité d'un réseau ou d'un ensemble de machines, et cela de différents niveaux. [37]

3.3.3. Les architectures d'IDS

Les systèmes de détection d'intrusions sont classés en trois types : individuels, coopératifs et hiérarchiques. [4]

- **IDS individuels**

La première solution adoptée pour les réseaux ad hoc est celle des **IDS** individuels. Elle se base sur le fait que chaque nœud n'a confiance qu'en lui-même. Le processus de détection d'intrusions se déroule localement sans aucun échange d'informations entre les nœuds du réseau. [4]

Les **IDS** individuels sont caractérisés par une indépendance entre les différents nœuds dans le processus de détection. En effet, chaque nœud ne s'occupe que de sa propre protection. [4]

- **IDS coopératifs**

Contrairement aux **IDS** individuels, dans les **IDS** coopératifs les nœuds coopèrent pour détecter d'éventuelles attaques. Cette coopération est réalisée par l'échange des informations ou encore des alertes. [4]

Le problème majeur pour ces **IDS** est qu'ils dégradent les performances du réseau. Ceci est dû principalement au trafic échangé entre les différents agents. [4]

- **IDS hiérarchiques**

Pour remédier aux limites des **IDS** coopératifs et ainsi améliorer les performances du réseau, une autre approche a été proposée pour la détection d'intrusion. [4]

Cette approche dite **IDS** hiérarchiques consiste à diviser le réseau en un ensemble de groupes (cellules) ayant chacun un seul chef de groupe. [4]

Les systèmes de détection d'intrusions hiérarchiques essayent alors de réduire la coopération entre les nœuds et ceci par la division du réseau en groupes. Dans ce cas, la coopération est effectuée entre le chef de groupe élu et chacun des membres du même groupe. [4]

Une alerte sera reportée au chef de groupe si un nœud membre du même groupe n'arrive pas à détecter seul une attaque ou qu'il manque d'autres informations ou encore que la certitude de détection est inférieure à un certain seuil. [4]

Le chef de groupe dans ce type **d'IDS** joue le rôle d'un administrateur de son groupe et permet de surveiller ce qui se passe au sein de sa cellule. [4]

D'autre part, l'agent de détection est distribué dans tous les nœuds du réseau alors que la réponse aux alertes se fasse d'une manière hiérarchique. [4]

3.3.4. Les types d'IDS

- **HIDS (Host-based IDS)** [38]

Un HIDS (Host Intrusion Detection System) est un agent logiciel installé sur la machine à protéger afin d'analyser en temps réel les flux de trafic de cette machine ainsi que les fichiers journaux. Contrairement à un NIDS, un HIDS ne protège donc que le système local.

Un HIDS est capable de détecter les changements dans les fichiers et dans le système d'exploitation de la machine hôte.

➢ **Les avantages** [39]

- ✓ La capacité de contrôler les activités locales des utilisateurs avec précision.
- ✓ Capable de déterminer si une tentative d'attaque est couronnée de succès.
- ✓ La capacité de fonctionnement dans des environnements cryptés.

➢ **Les inconvénients** [39]

- ✓ La vulnérabilité aux attaques du type déni de service puisque l'**IDS** peut résider dans l'hôte cible par les attaques.
- ✓ La difficulté de déploiement et de gestion, surtout lorsque le nombre d'hôtes qui ont besoin de protection est large.

- **NIDS (Network-based Intrusion Detection System)** [38]

Un NIDS (Network Intrusion Detection System) est un **IDS** orienté réseau. Il permet de d'analyser le trafic qui circule au niveau IP (couche réseau) pour détecter d'éventuelles intrusions. Il est composé de sondes (capteurs) qui capturent le trafic acheminées sur le réseau et d'un moteur pour analyser ce trafic.

➢ **Les avantages** [39]

- ✓ L'**IDS** basé réseau est capable de contrôler un grand nombre d'hôte avec un petit coût de déploiement.
- ✓ L'IDS basé réseau est capable d'identifier les attaques de /à multiples hôtes.
- ✓ L'**IDS** basé réseau assure une grande sécurité contre les attaques parce qu'il est invisible aux attaquants.

➢ **Les inconvénients** [39]

- ✓ L'**IDS** basé réseau ne peut pas fonctionner dans des environnements cryptés.
- ✓ Ce type d'**IDS** ne permet pas d'assurer si une tentative d'attaque est couronnée de succès.

- **IDS hydride**

Une version d'**IDS** hybride est possible et désormais supportée par différentes offres commerciales. Même si la distinction entre HIDS et NIDS est encore courante, certains HIDS possèdent maintenant les fonctionnalités de base des NIDS. [40]

3.3.5. Les Classification d'un système de détection d'intrusions

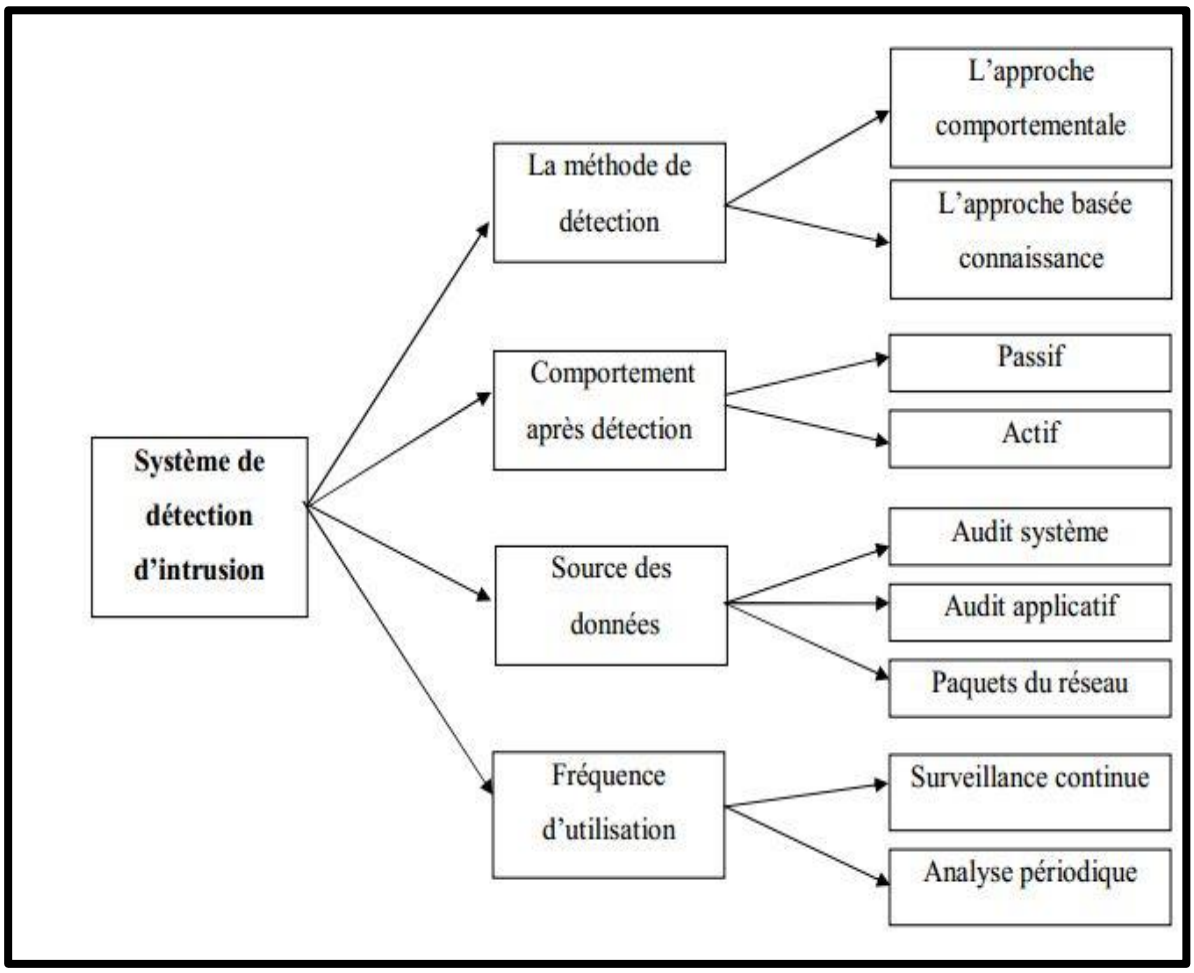

Figure II.11. Les Classification d'IDS. [39]

3.3.5.1. Les approches d'IDS

- **L'approche basée connaissance (La détection d'abus (misuse detection)**

Dans la détection d'abus (aussi appelée détection de mauvaise utilisation), l'**IDS** analyse l'information recueillie et la compare avec une base de données de signatures (motifs définis, caractéristiques explicites) d'attaques connues (i.e., qui ont déjà été documentées), et toute activité correspondante est considérée comme une attaque (avec différents niveaux de sévérité). Un système de détection d'abus est, par exemple, STAT (State Transition Analysis Toolkit). [41]

➢ **Les avantages**

- ✓ est très efficace pour la détection d'attaque avec un taux très bas des alarmes de type positif faux.
- ✓ Les alarmes générées sont significatives. [39]

➢ **Les inconvénients**

- ✓ permet seulement la détection des attaques qui sont connues au préalable. Donc, la base de connaissances doit être constamment mise à jour avec les signatures de nouvelles attaques . [39]

- **L'approche comportementale (La détection d'anomalie (anomaly detection)**

La détection d'anomalie de comportement est une technique assez ancienne (elle est utilisée également pour détecter des comportements suspects en téléphonie, comme le phreaking).

L'idée principale est de modéliser durant une période d'apprentissage le comportement "normal" d'un système/programme/utilisateur en définissant une ligne de conduite (dite baseline ou profil : Par exemple, profil de connexion : fréquence de login (combien de fois par jour/semaine l'utilisateur se connecte-t-il ?), lieu de login (statistiques sur la connexion distante/locale), etc.

Un profil est donné par une métrique et un modèle statistique. Une métrique est une variable aléatoire X modélisant le comportement quantitatif sur une période de temps.

Un modèle est utilisé pour détecter si les nouvelles valeurs de X concordent avec les valeurs de X déjà observées (et supposées légitimes)), et de considérer ensuite (en phase de détection) comme suspect tout comportement inhabituel (les déviations significatives par rapport au modèle de comportement "normal"). [40]

➢ **Les avantages**

- ✓ n'exige pas des connaissances préalables sur les attaques.
- ✓ Elle permet la détection de la mauvaise utilisation des privilèges.
- ✓ Elle permet de produire des informations qui peuvent être employées pour définir des signatures pour la détection d'abus . [39]

➢ **Les inconvénients**

- ✓ Les approches comportementales produisent un taux élevé des alarmes de type positif faux en raison des comportements imprévisibles d'utilisateurs et des réseaux.

- ✓ Ces approches nécessitent des phases d'apprentissage pour caractériser les profils de comportement normaux.
- ✓ Les alarmes générées par cette approche ne sont pas significatives. [39]

➢ **Les techniques utilisées dans l'approche comportementale** [39]

Pour pouvoir formaliser le comportement normal d'un système, des approches diverses ont été utilisées :

➢ **L'approche de data mining**

Le but de cette approche est l'exploitation des techniques de data mining pour extraire des anomalies à partir des grandes quantités de données du trafic réseau. Parmi les travaux existants, on peut citer ADAM « Audit Data Analysis and Mining » qui est un système de détection d'intrusions qui exploite des techniques de data mining pour construire des profils du trafic réseau normaux.

ADAM utilise les règles d'association pour construire des profils du trafic de réseau normaux qui seront employées par la suite pour détecter les comportements incorrects de trafic de réseau. Pour détecter des anomalies, ADAM extrait les règles d'association à partir des données du trafic réseau et qui seront comparées aux profils du réseau. Si n'importe quelle règle d'association produite à partir des données de trafic de réseau rassemblées n'est pas incluse dans les profils, alors cette règle est considérée comme une indication d'un comportement incorrect.

➢ **L'approche statistique**

L'approche statistique est utilisée pour la génération d'un modèle de comportement normal d'un système. Elle consiste à générer le profil de comportement normal à partir d'un ensemble de variables aléatoires, échantillonnées à des intervalles réguliers dans le temps, ces variables peuvent être par exemple :

- ✓ Le temps CPU utilisé.
- ✓ Le nombre de connexions établi durant une période de temps.
- ✓ Les fichiers les plus fréquemment utilisés.
- ✓ Les entrées/sorties effectuées.
- ✓ … Etc.

Dans cette approche, Denning a proposé un ensemble de modèles statistiques, leur but est de définir à partir de n observations x1, x2,…xn sur une variable donnée x, si la valeur xn+1 de l'observation n+1 est anormale. Parmi ces modèles, on peut citer les modèles suivants :

A. **Le modèle opérationnel :** ce modèle est très simple, une anomalie est détectée par la comparaison de la valeur d'une nouvelle observation avec un seuil fixe qui est défini d'une manière intuitive en se basant sur les données historiques.

B. **Le modèle de déviation standard et moyen :** Ce modèle définit un seuil d'anomalie par l'estimation d'un intervalle de confiance. L'intervalle de confiance est la moyenne et l'écart type des n observations qui peuvent être considérées normales. Si la valeur d'une nouvelle observation est en dehors de cet intervalle alors elle est considérée anormale.
C. **Le modèle de covariances :** Il est similaire au modèle précédent mais il se base sur la corrélation de plusieurs variables pour tirer des conclusions.

Ces approches ont été adoptées dans le développement de plusieurs systèmes de détection d'intrusions, on peut citer par exemple :

- MIDAS « Multics Intrusion Detection and Alerting System ».
- NIDES « Next Generation Real time Intrusion Detection Expert System ».

➢ **L'approche de réseaux de neurones**

Les réseaux de neurones sont utilisés dans la détection d'anomalies afin d'exploiter leurs capacités d'apprentissage. L'idée de base est d'utiliser les mécanismes d'apprentissage des réseaux de neurones pour apprendre les profils de comportements normaux des utilisateurs ou d'un système.

Plusieurs travaux ont été élaborés qui ont essayé d'abord d'apprendre à un réseau de neurones le comportement normal d'un système pour qu'il puisse par la suite de décider si un ensemble d'action est normal ou suspect. Parmi ces travaux, nous citons le travail de Debar qui a proposé l'utilisation des réseaux de neurones pour construire un modèle du comportement des utilisateurs du système informatique. Le travail proposé s'intéresse à l'aspect dynamique du comportement et à sa présentation sous des séries d'actions temporelles.

4.3.5.2. Le comportement après la détection d'intrusions [39]

Le comportement d'un **IDS** après la détection d'une intrusion est l'ensemble des actions prises par le système lorsqu'il détecte une attaque. Ces réponses peuvent être actives ou bien passives.

➢ **Réponse active**

La réponse active implique des actions automatisées prises par un **IDS** quand le système détecte une intrusion. Par exemple interrompre le progrès d'une attaque pour bloquer ensuite l'accès suivant de l'attaquant.

➢ **Réponse passive**

Dans ce cas, quand une attaque est détectée, le système de détection d'intrusions ne prend aucune action. Il génère seulement une alarme pour notifier

l'administrateur de système qui va prendre des mesures en se basant sur les rapports générés par le système de détection d'intrusions.

3.3.5.3. La nature des données analysées [39]

Les systèmes de détection d'intrusions sont classés en fonction de l'origine des données qui seront exploitées pour détecter des actions intrusives. La source de données utilisée est une caractéristique essentielle pour classer les systèmes de détection d'intrusions. On distingue trois catégories de sources d'informations :

- **Les audits systèmes**

Les audits systèmes sont produits par le système d'exploitation d'un hôte. Ces données permettent à un **IDS** de contrôler les activités d'un utilisateur sur un hôte. Elles peuvent être également de plusieurs types, par exemple :

- **Historique des commandes systèmes :** tous les systèmes d'exploitation possèdent des commandes pour obtenir des informations instantanées sur les processus actifs courants dans un ordinateur. Grâce à ces commandes, l'**IDS** peut avoir des informations précises sur les événements systèmes.
- **Accounting :** l'accounting fournit des informations sur l'usage des ressources partagées par les utilisateurs. Ces ressources sont par exemple : le temps processeur, la mémoire, l'espace disque, les applications lancées, etc.

- **Systèmes d'audit de sécurité**

Les systèmes d'exploitation sont dotés par ce service pour définir des événements, les associer à des utilisateurs et assurer leurs collectes dans un fichier d'audit. L'**IDS** possède potentiellement des informations sur toutes les actions effectuées par un utilisateur.

L'avantage de ces données systèmes réside dans leur fiabilité et leur granularité fine, qui permettent un diagnostic précis des actions effectuées sur un hôte par un attaquant.

Cependant, le volume d'événements généré par les audits systèmes est très volumineux ce qui implique un impact très important sur les performances de la machine surveillée. Les **IDS** qui se basent sur cette catégorie des sources de données sont appelés :Les **IDS** basés hôte « Host Based Intrusion Detection System ».

- **Les sources d'informations réseau**

Ce sont des données du trafic réseau. Cette source d'informations est prometteuse car elle permet de collecter et analyser les paquets de données circulant sur le réseau.

Les **IDS** qui exploitent ces sources de données sont appelés : Les **IDS** basés réseau « Network Based Intrusion Detection System ».

- **Les audits applicatifs**

La troisième catégorie de source de données est constituée des audits applicatifs. Les données à analyser sont produites directement par une application, par exemple des fichiers logs générés par les serveurs ftp et les serveurs Web.

L'avantage de cette catégorie est que les données produites sont très synthétiques, elles sont sémantiquement riches et leur volume est modéré.

3.3.5.4. La fréquence d'utilisation [39]

La fréquence d'utilisation d'un système de détection d'intrusions peut exister selon deux formes :

- **Surveillance périodique**

Ce type de système de détection d'intrusions analyse périodiquement les différentes sources de données à la recherche d'une éventuelle intrusion ou une anomalie passée.

- **Surveillance en temps réel**

Les systèmes de détection d'intrusions en temps réel fonctionnent sur le traitement et l'analyse continue des informations produites par les différentes sources de données. La détection d'intrusions en temps réel permet de limiter les dégâts produits par une attaque car elle permet de prendre des mesures qui réduisent le progrès de l'attaque détectée.

Conclusion

Les objectifs que doit respecter pour assurer la sécurité des réseaux **VANETs,** sont les suivants : l'authentification, l'intégrité, La non-répudiation, la confidentialité et la disponibilité.

Les types des attaques dans un réseau **VANET** sont : externes ou interne, actif ou passif, malveillant vs ou rationnel.

Les déférentes attaques sur les réseaux **VANETs** sont : attaque sur la vie privée, attaque sur la cohérence de l'information, usurpation d'identité ou de rôle, Déni de, écoute de communication, véhicule caché et wormhole.

Il y a trois mécanismes pour sécuriser le routage dans les réseaux Ad hoc : Les mécanismes de gestion des clés, Les mécanismes de routage sécurisé et Les systèmes détection d'intrusion pour surveiller les nœuds des **VANETs**.

Les types d'**IDS** sont : NIDS installé sur la machine pour analyser le trafic dans elles, HIDS pour analyser e trafic réseau et hybride.

L'architecture d'**IDS** soit : individuelle, coopérative ou hiérarchique

Il y a deux approches d'**IDS** : la détection la détection d'abus et détection d'anomalie ; la détection d'anomalie utiliser plusieurs techniques parmi elles le datamining, le réseau de neurone.

Dans le chapitre suivant en va voir quelque méthodes de détection d'intrusion dans un réseau **VANET** utiliser pour éviter quelques attaques et en va faire une comparaison entres elles.

CHAPITRE III :

ETAT DE L'ART ET L'IDS DANS LES RESEAUX VANETS

Introduction

La sécurité des réseaux **VANNET** est très un importent pour détecter les nœuds maillantes.

Pour assurer la sécurité de réseaux **VANETs** en à utiliser les **IDS**, il y a plusieurs **IDS** contre les attaques existent.

Dans notre chapitre en va faire une étude comparative de quelque méthode **IDS** existantes et conclu les points faibles et des points forts de chaque méthode étudiée.

En fin de chapitre en propose une solution pour minimiser les points faibles de méthode choisir.

Parti 1: Etat de l'art et l'IDS dans les réseaux VANETs

1. L'IDS dans les VANETs

1.1. IDS basé véhicule

Dans les réseaux **VANETs**, plusieurs méthodes ont été proposées pour positionner les **IDS**. Parmi celles-ci, l'**IDS** basé véhicule, ou chaque véhicule du réseau **VANET** serait équipé d'un de ces systèmes pour détecter les' attaques dont il pourrait être la cible. Néanmoins ces systèmes, pour être performant requièrent des processeurs performants, ce qui pourrait ralentir certaines applications à bord du véhicule. [7]

1.2. IDS basé infrastructure

Les **IDS** basés sur l'infrastructure sont quant à eux installés sur le RSU. Chacun des véhicules du réseau devient un nœud et retransmet toutes ses données reçues au RSU pour les faire analyser. Le RSU analyse toutes les données en vue d'une attaque. La décentralisation de l'**IDS** à l'avantage de ne pas ralentir les applications présentes sur les véhicules. De plus, le RSU peut facilement accueillir une grande capacité de calcul. Néanmoins, le trafic réseau généré sera plus important entre les véhicules et le RSU. [7]

2. Les techniques d'IDS utilisé dans les VANETs

2.1. Watchdog and Pathrater

Marti, Giuli, and Baker ont présenté une solution pour détecter les nœuds malicieux qui suppriment les paquets (de façon sélective ou aléatoire) passant par ce nœud de transit. Cette solution nommée Watchdog consiste en effet, à surveiller le comportement de tous les nœuds d'une part, et choisir la route la plus sécuritaire grâce au module nommé Pathrater d'une autre part. [6]

c observateur comptabilise un échec de retransmission et les considère comme des nœuds malveillants. Pour ce faire, le watchdog (c'est en fait le nœud qui vient d'émettre) garde un buffer des paquets qu'il a envoyés puis écoute le trafic émis du nœud intermédiaire à qui il a confié le routage du paquet. Si le paquet est retransmis, alors il le supprime de son buffer. Sinon au bout d'un laps de temps défini si le paquet est toujours dans le buffer, il considère le nœud comme « se comportant mal» et comptabilise l'échec de retransmission. A partir du moment où le compteur pour un nœud dépasse un seuil fixé, l'information est reportée au Pathrater(l'évaluateur de chemins). Le Pathrater est ensuite utilisé pour sélectionner les chemins les plus fiables entre une source et une destination, en évitant les nœuds qui ont été détectés comme non coopératifs. [2]

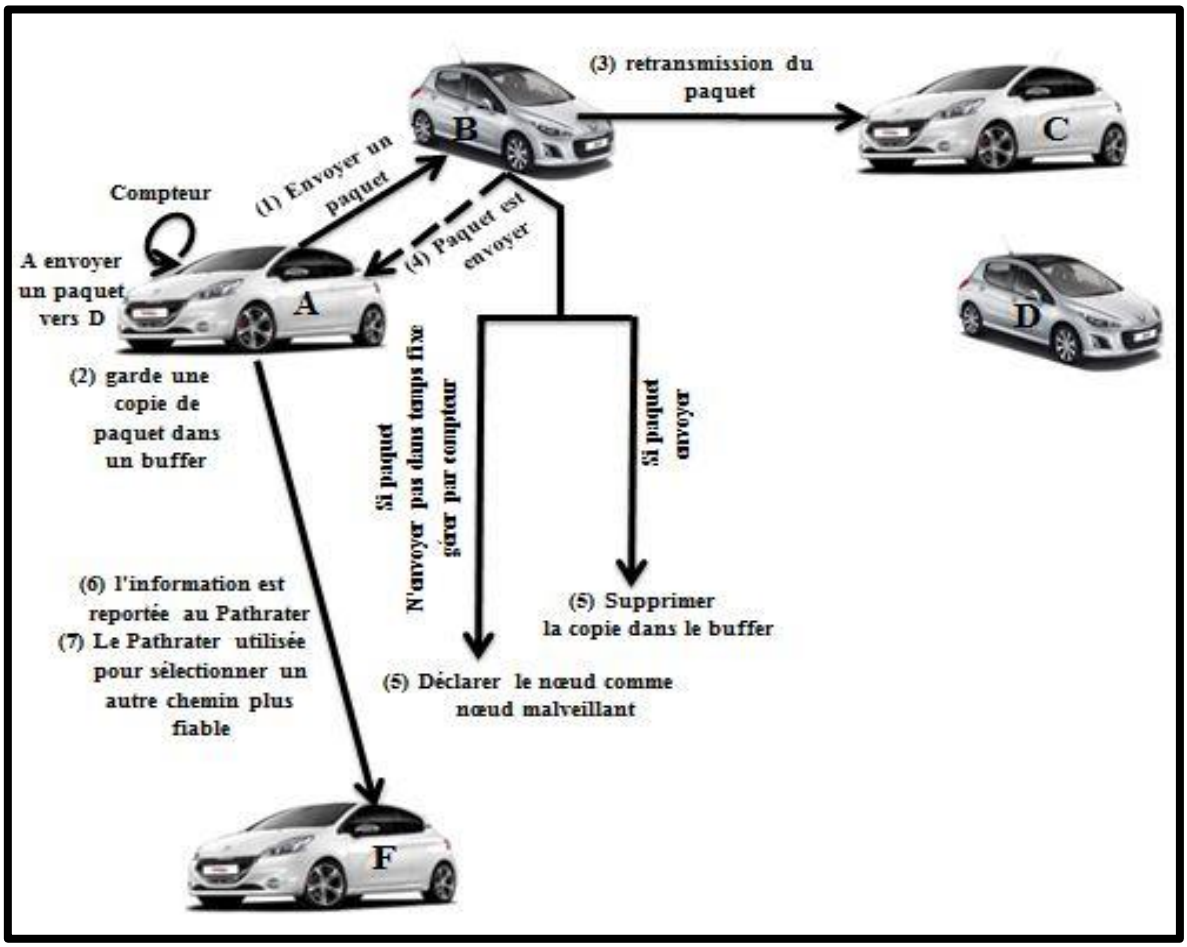

Figure III.1. Le principe de wotchdog and pathrater.

Exemple :

Si le nœud S veut transmettre un paquet vers le nœud D via les nœuds intermédiaires A, B et C, le paquet est transmis au nœud A qui le retransmet à son tour au nœud B mais garde une copie du paquet.

La prochaine étape du processus est de surveiller si B va retransmettre ce paquet vers le nœud C en écoutant et en comparant tous les paquets émis par le nœud B. Si le nœud B ne retransmet pas le paquet au bout d'un certain temps, un compteur est incrémenté. Si le compteur atteint une valeur maximale préétablie (nombre de fois que le nœud B ne transmet pas un paquet), le nœud A peut conclure que le nœud B est malicieux. Sa décision est rapportée au nœud S. [6]

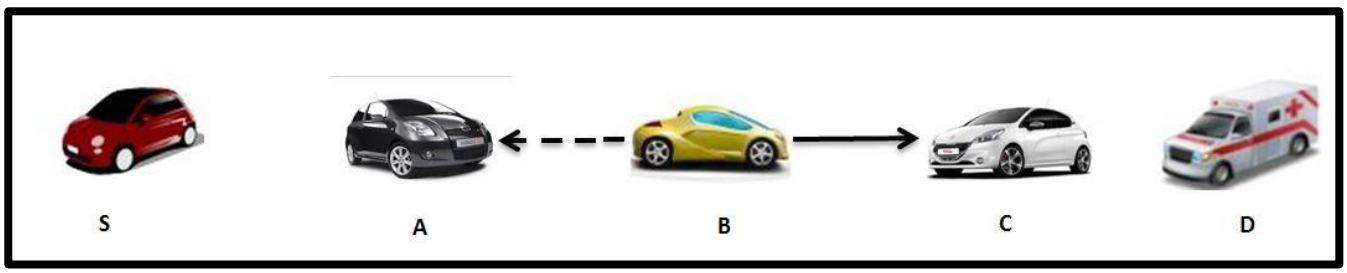

Figure III.2. Exemple de wotchdog.

2.2. CONFIDANT : un système basé sur la réputation

2.2.1. L'égoïsme

Les comportements égoïstes ne sont pas vraiment des attaques, mais des comportements des nœuds qui refusent de coopérer avec les autres pour assurer le bon fonctionnement du routage ad hoc, afin d'économiser la bande passante et les ressources de calcul.[6]

2.2.2. CONFIDANT (Cooperation of Nodes-Fairness in Dynamic Ad hoc NeTworks)

2.2.2.1. Architecture de CONFIDANT

Le protocole CONFIDANT est composé de quatre éléments complémentaires [4] :

- **Moniteur (Monitor) :**

le rôle de ce module est de collecter les informations locales sur le comportement des nœuds dans le réseau, ensuite, classer un nœud comme honnête ou malveillant. L'information obtenue est basée donc sur une observation directe par le nœud i sur le nœud j. Cette information est appelée information en première main (first-hand information) ou information locale f_{ij} . Elle est utilisée comme paramètre d'entrée pour le module gestionnaire de réputation. [4]

- **gestionnaire de réputation (Reputation system)**

le gestionnaire de réputation a pour rôle de gérer une table constituée de deux colonnes : une réservée aux identificateurs des nœuds et l'autre à leur valeur de réputation correspondante. Cette valeur de réputation ne change que si les deux conditions suivantes sont vérifiées : (i) Il y a suffisamment de preuves concernant le comportement malicieux du nœud; (ii) Le nombre d'occurrences du comportement malicieux dépasse un certain seuil. La mise à jour de la valeur de réputation est faite selon une fonction qui attribue des poids selon la provenance de la détection. En effet, une plus grande pondération est affectée à sa propre observation, une autre plus petite à des expériences du voisinage et une pondération faible à des observations rapportées. Cette différence d'attribution de pondération est basée sur le principe que le nœud fait plus confiance à ses propres expériences qu'aux autres. Si la valeur de réputation d'un nœud est inférieure à un certain seuil, le gestionnaire du chemin sera invoqué pour prendre les mesures nécessaires. [4]

- **gestionnaire de confiance (Trust Manager) :**

le rôle de gestionnaire de confiance est de décider si on fait confiance à l'information globale reçue et de gérer la confiance attribuée aux autres nœuds. Ainsi, l'objectif de ce module est de minimiser le risque de fausses informations. [4]

Des messages d'ALARME sont envoyés par le gestionnaire de confiance afin d'avertir les autres nœuds de la présence des nœuds malicieux. Ces messages d'ALARME sont générés par le nœud lui-même après vérification, observation ou réception d'un rapport sur un comportement malicieux d'un nœud. [4]

Le module gestionnaire de confiance a trois composants qui sont :

1. une table d'ALARME qui contient des informations sur les messages d'ALARME reçus
2. une table de confiance pour gérer les niveaux de confiance des nœuds afin de déterminer la sureté du message d'ALARME reçu
3. une liste d'amis contenant la liste de tous les nœuds susceptibles d'envoyer des messages d'ALARME. [4]

Le gestionnaire de confiance a un rôle important dans la prise de décision pour :

- ✓ fournir et accepter des informations de routage
- ✓ accepter la participation d'un nœud dans une route
- ✓ prendre une partie d'une route envoyée par d'autres nœuds. [4]

➢ **un gestionnaire de chemins (Path Manager) :**

Après la classification d'un nœud malveillant j par un nœud honnête i, il l'isole afin de l'empêcher de participer aux services du réseau. Cette isolation permet de réduire l'effet du comportement malveillant, de motiver les nœuds à coopérer et d'améliorer les services du réseau. [4]

2.2.2.2. Le principe du protocole CONFIDANT

Le principe du protocole CONFIDANT est de traiter à la fois les nœuds malicieux et égoïstes à travers la supervision et l'analyse de deux processus du routage à savoir le transfert des données et la découverte des voisins. [4]

Une fois qu'un comportement malicieux est détecté, le nœud malicieux est exclu de tous les services offerts par le réseau (retransmission des paquets par exemple) et l'isole grâce à un système de réputation en alertant les autres nœuds par la diffusion d'un message d'alarme. [6]

Le mécanisme proposé utilise le module Monitoring pour détecter toute activité malicieuse. [6]

Si un cas suspect est détecté, le module Monitor en voie une notification au module Reputation System qui, à son tour, fait une mise à jour de sa table de réputation en fonction des rapports d'activité reçus. Si la valeur de réputation dépasse un seuil critique, une alarme est envoyée aux autres nœuds via le module Trust Manager ainsi qu'au Path Manager qui supprime toutes les routes contenant le nœud malicieux. [6]

Puisque ce protocole permet l'envoi d'alarmes, le réseau peut être sujet à des attaques envoyant de fausses accusations. Ainsi, un déni de service peut être facilement réalisé. [4]

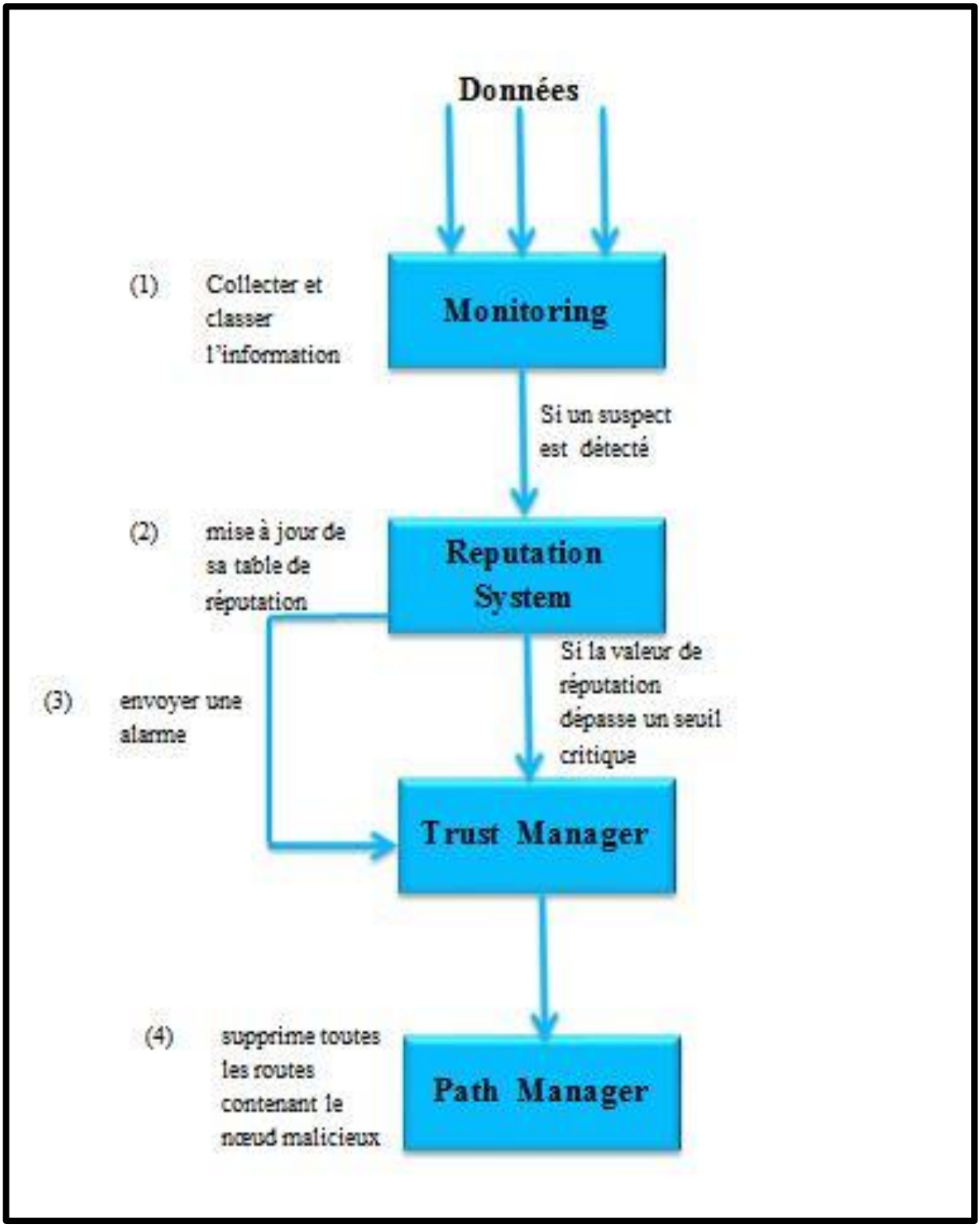

Figure III.3. Le principe de CONFIDANT.

2.3. Zhang et Lee IDS

Zhang et Lee ont proposé un **IDS** distribué coopératif où chaque nœud appelé agent **IDS**, est responsable de la collection des données et la détection des activités malicieuses. Chaque agent **IDS** peut initier une réponse (punition) indépendamment des autres nœuds. Toutefois, les agents **IDS** voisins pourraient coopérer entre eux pour une détection d'intrusion globale. [4]

Un agent **IDS** est structuré en six modules [4] :

- **le module local data collection** : qui est responsable de la collecte les données en temps réel.
- **le module local detection engine** : décide à partir des données collectées si le système est attaqué ou non. Le module peut initier une réponse si une attaque est détectée.
- La réponse est exécutée par **le module local response** (alerte à l'utilisateur local) ou **le module global response** (alerte globale) en fonction du type d'attaque.

- **Le module cooperative detection engine** : est exécuté quand une anomalie est détectée et sollicite la coopération des autres nœuds via un autre module de communication sécurisée appelé **secure communication**.

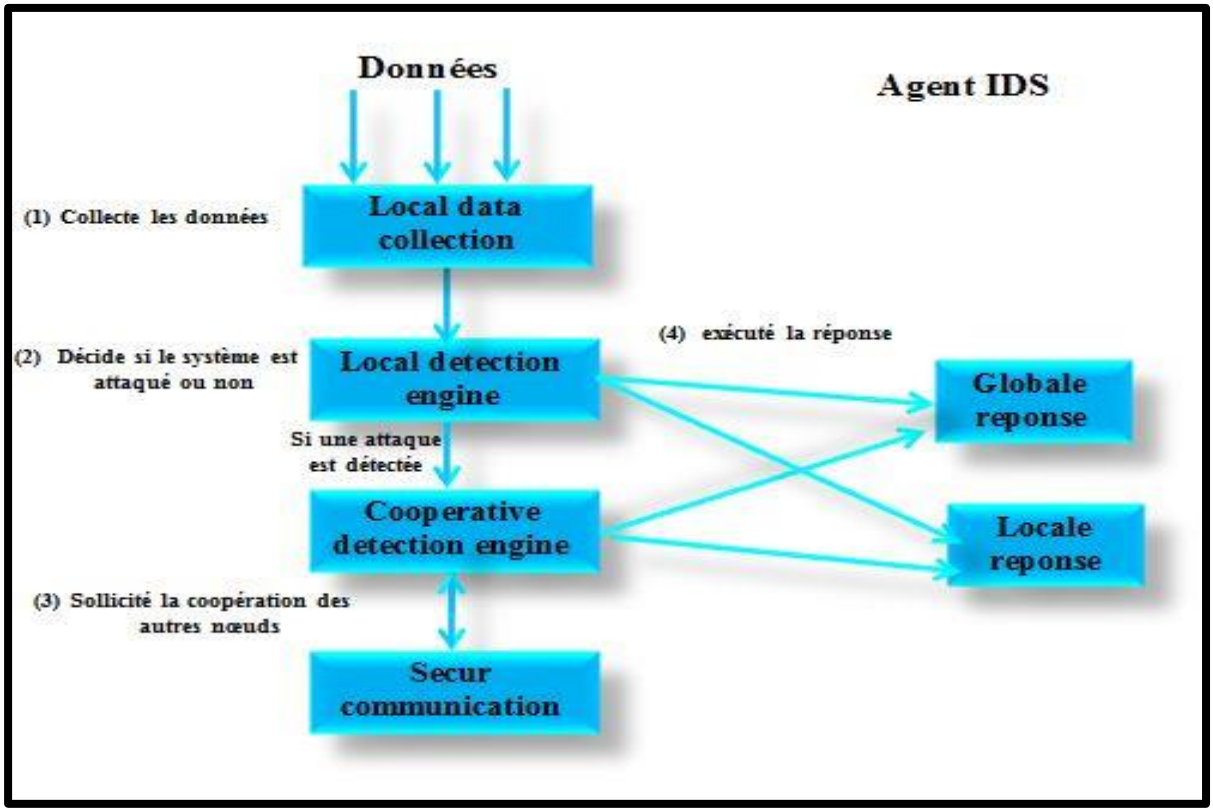

Figure III.4. Le principe de Zhang et Lee IDS.

2.4. Système de détection d'intrusion clustérisé

Les réseaux ad hoc véhiculaires sont caractérisés par une forte mobilité c'est pourquoi une hiérarchie statique n'est pas appropriée pour une telle topologie dynamique de réseau. [6]

2.4.1. La clustiration

La clusterisation, est dans les réseaux informatiques classiques, un concept visant à regrouper des entités (ordinateur), appelée également nœud, entre eux. L'objectif étant la répartition du calcul sur plusieurs processeurs, le partage de données sur des disques durs communs, etc. Dans les réseaux **VANETs**, le concept de regroupement est le même: on rassemble des véhicules (nœuds) entre eux. Néanmoins, les objectifs diffèrent. La topologie dynamique des **VANETs**, permet, après la clusterisation. D'améliorer la qualité des services proposés, mais également la sécurité des véhicules .Il existe dans les **VANETs** deux types de clusterisation, passive, ou active [7]:

2.4.1.1. Clusterisartion active

La clusterisation active est un type de clusterisation dans lequel chaque nouveau véhicule détecté dans le réseau doit immédiatement se clustériser. Les clusters et la tête de cluster sont ainsi reformés régulièrement, dépendamment des nœuds entrants et sortants. [7]

2.4.1.2. Clusterisartion passive

La clusterisation passive quant à elle, est un type de clusterisation dans laquelle les véhicules ne se clustérisent pas immédiatement. Le processus n'est amorcé que lorsqu'un véhicule souhaite diffuser de l'information. Les véhicules présents dans la zone vont alors élire une tête de cluster pour retransmettre les informations dans le réseau. [7]

Un groupe de véhicules doit être capable de s'autoformer comme cluster sur la route. De plus, il doit pouvoir élire une tête de cluster pour permettre une communication avec le RSU. La tête de cluster a un rôle spécifique; c'est une passerelle vers le RSU qui conserve des informations à propos des clusters de sa zone. Les informations sauvegardées sont ensuite envoyées aux RSU s à sa portée. [7]

2.4.2. Mécanisme interne du cluster

La méthode utilise la clusterisation passive. Le cluster est formé automatiquement en fonction de la vitesse des véhicules. Ils proposent une table statique faisant la correspondance entre les groupes de clusters et la vitesse du groupe. Leurs postulats sont les suivants: chaque véhicule connait sa position et sa vitesse grâce au GPS (Global Positioning System). Chaque véhicule dans la même zone avec la même catégorie de vitesse est en mesure de se clustériser. [7]

Vitesse	la vitesse de groupe	le groupe de c1uster
0-30	0	0
30-45	1	1
45-60	2	1
60-75	3	2
75-90	4	2
90-110	5	2
110-120	6	3
120+	7	3

Tableau III.1. Relation entre la vitesse de groupe et le groupe de c1uster. [7]

La méthode utilise des intervalles de vitesse, des groupes de vitesses et des groupes de clusters, comme montrés dans le Tableau 1. Les auteurs mentionnent seulement 3 différents groupes de clusters, on réduit ainsi la surcharge de paquets et les communications entre les groupes. Si deux différents groupes souhaitent communiquer, ils vont utiliser le RSU pour faire suivre leurs paquets de données. [7]

L'approche initiale définit 4 états pour les véhicules: initiale (INIT), Tête de cluster (CH), passerelle (GW) et ordinaire (ORD) [7] :

- **INIT:** Chaque véhicule débute dans cet état et peut devenir CH. Il n'y a qu'un CH par cluster. Les véhicules dans l'état INIT vont passer par l'état ORD et peuvent devenir CH ou GW.
- **CH:** la tête de cluster a pour charge de faire suivre les paquets d'une source vers d'autres véhicules et vers les passerelles. Seulement 2 sources peuvent être trouvées dans l'approche: les GWs et les ORDs. L'élection de la tête de cluster est simple; le premier véhicule déclarant «je suis la tête de cluster » le devient.
- **ORD:** chaque véhicule déjà présent dans le cluster et qui n'est ni CH, ni GW, est dans l'état ORD. C'est l'état basique des nœuds après l'élection de la tête de cluster. Celui-ci peut être éligible au rang de GW temporaire.
- **GW:** par défaut, le RSU est une passerelle statique. Le RSU fait suivre les paquets de données venant d'une GW, d'un CH ou d'un véhicule ORD. Il peut aussi transmettre les paquets de sa zone vers une zone proche en faisant suivre les données par un autre RSU. Dans notre méthode, les seuls paquets retransmis sont les informations de sécurité. Les véhicules peuvent devenir GW lorsque le CH les proclame. Une réélection des GWs peut avoir lieu lorsqu'une GW quitte le cluster.

Seuls le CH et la GW peuvent faire suivre les paquets de données. Les véhicules GW sont sélectionnés par le CH après un certain temps. Un véhicule quitte le cluster lors d'un changement de vitesse de groupe, celle-ci sera mise à jour après quelques secondes. Dans notre approche, le RSU est une passerelle permanente, chaque véhicule sur la route peut envoyer des informations de sécurité via celui-ci. Nous allons donc distinguer 2 types de passerelle, les statiques (RSU) et les dynamiques (véhicules). Les RSUs ne font pas partie des clusters. [7]

2.4.3. Les approches d'IDS clustérisé

Il y a deux approches Dans la première, la détection est faite au sein des véhicules, tandis que dans la deuxième, elle est faite par les RSUs [7] :

2.4.3.1. Approche d'IDS basées véhicules :

Dans cette approche, chaque véhicule est équipé avec un **IDS** personnel. Le système de détection d'intrusions est actif en permanence. Les véhicules peuvent être isolés, seuls ou dans un groupe de c1uster. Chacun des nœuds détecte de manière individuelle les attaques. Lorsqu'une attaque est détectée, l'information de l'attaque est transmise au CH.

Celui-ci gère les informations d'alerte comme le suivant :

- **Méthode mathématique de corroboration d'attaque pour les IDS basées véhicules :**

Pour les **IDS** basés véhicules, il y a une méthode simple pour valider qu'une attaque est réellement en cours. Voici les hypothèses de cette approche :

- Il y a un **IDS** installé sur chaque véhicule.
- Les communications entre les véhicules et entre les véhicules et les RSUS sont sécurisées. Les données sont chiffrées.
- Les RSUS sont fiables.
- Toutes les alertes transmises aux RSUS sont considérées comme vraies.
- Lorsqu'un **IDS** détecte une anomalie, on la considère toujours comme une attaque réelle.

Lorsqu'un membre du c1uster détecte une attaque, il envoie l'information et la signature de l'attaque à la tête de c1uster. La tête de c1uster analyse la signature et envoie ces informations aux autres membres du c1uster pour avoir leurs opinions. Lorsque tous les véhicules ont fourni leurs avis sur la signature, la tête de c1uster les transmet au RSU de sa zone. Celui-ci conserve les informations transmises et renvoie la signature à un autre c1uster de la zone pour avoir leurs opinions. Le RSU calcule ensuite la probabilité de l'attaque $P_{attaque}$ en utilisant la formule :

$$P_{attaque} = \frac{Nb\_détection}{Nb\_véh\_total}$$

Ou:

$P_{attaque}$: Représente la probabilité de corroboration de l'attaque.

Nb_détection : Représente le nombre de véhicules ayant détecté l'attaque.

Nb_véh_total : Est le nombre total de véhicule ayant donné leurs opinions.

Lorsque $P_{attaque} > 0{,}50$, plus de la moitié des véhicules ont validé l'alerte, il s'agit donc d'une attaque.

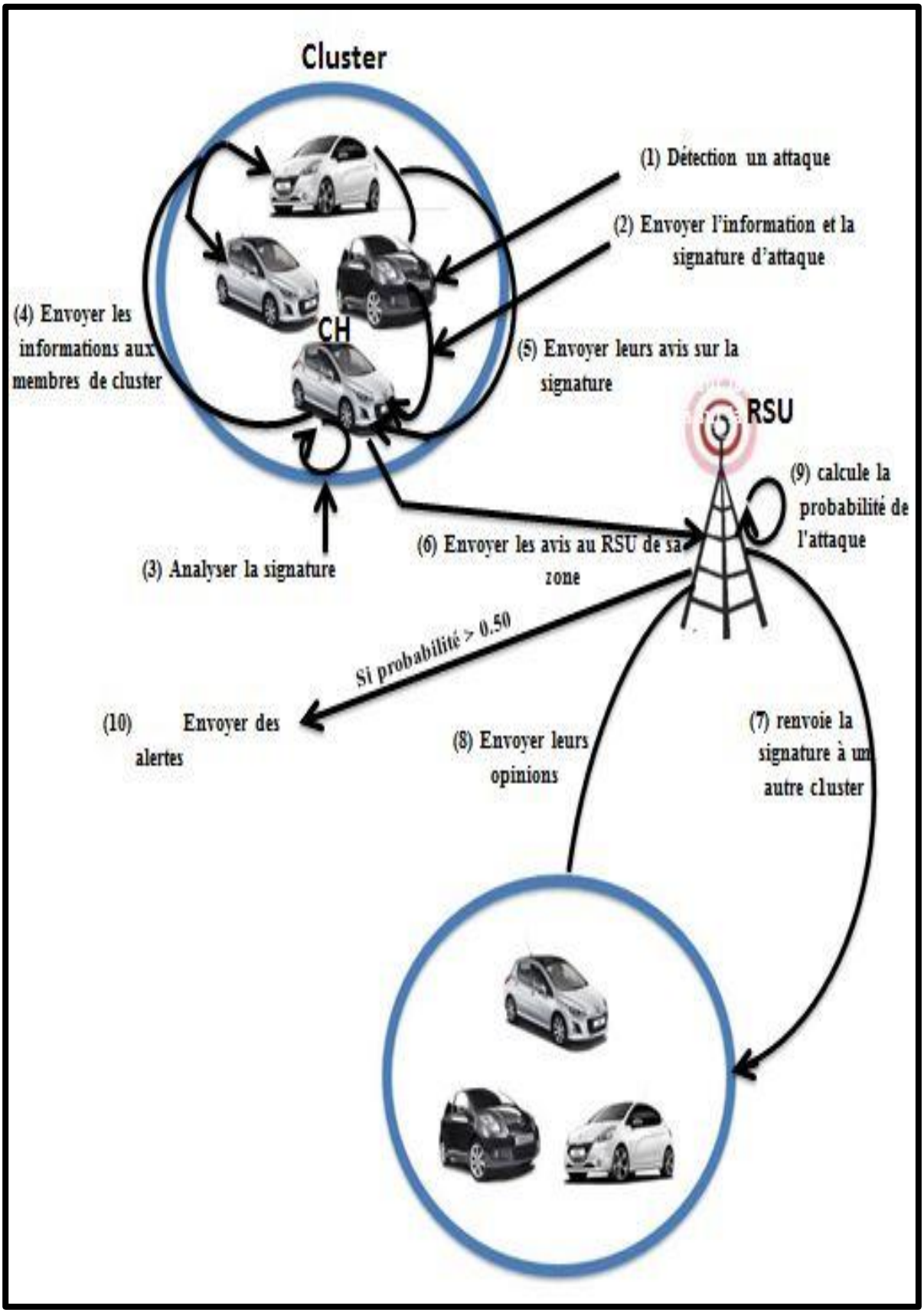

Figure III.6. Le principe de la méthode IDS clustérisé basée véhicule.

2.4.3.2. Approche d'IDS basées RSUs :

L'approche de détection d'intrusions basée sur les RSUs est une alternative à l'approche basée véhicules. Elle préserve une bonne sécurité du système, car les paquets sont analysés par une entité externe: le RSU.

- **Algorithme de l'approche d'IDS basées RSUs**

Le cluster existe et le CH est déjà en place.

Les données échangées au sein du c1uster et vers le RSU sont:

1. Les paquets de données de tous les véhicules sont envoyés au CH.
2. Le CH fait suivre tous les paquets vers le RSU.
3. Le RSU analyse ceux-ci. Lorsqu'une attaque est détectée, le CH est alerté.

- **Méthode mathématique de corroboration d'attaque pour les IDS basées RSUs**

Tous les paquets venant du c1uster sont retransmis au RSU. Lorsque le RSU détecte une attaque, il envoie la signature de l'attaque aux RSUs suivants et précédents. Ceux-ci retournent leurs opinions au RSU initiateur du protocole. Le RSU calcule ensuite le ratio (la probabilité de l'attaque) comme dans l'**IDS** basé véhicule. Lorsque l'attaque est corroborée, une alerte est envoyée aux têtes de c1uster de la zone. [7]

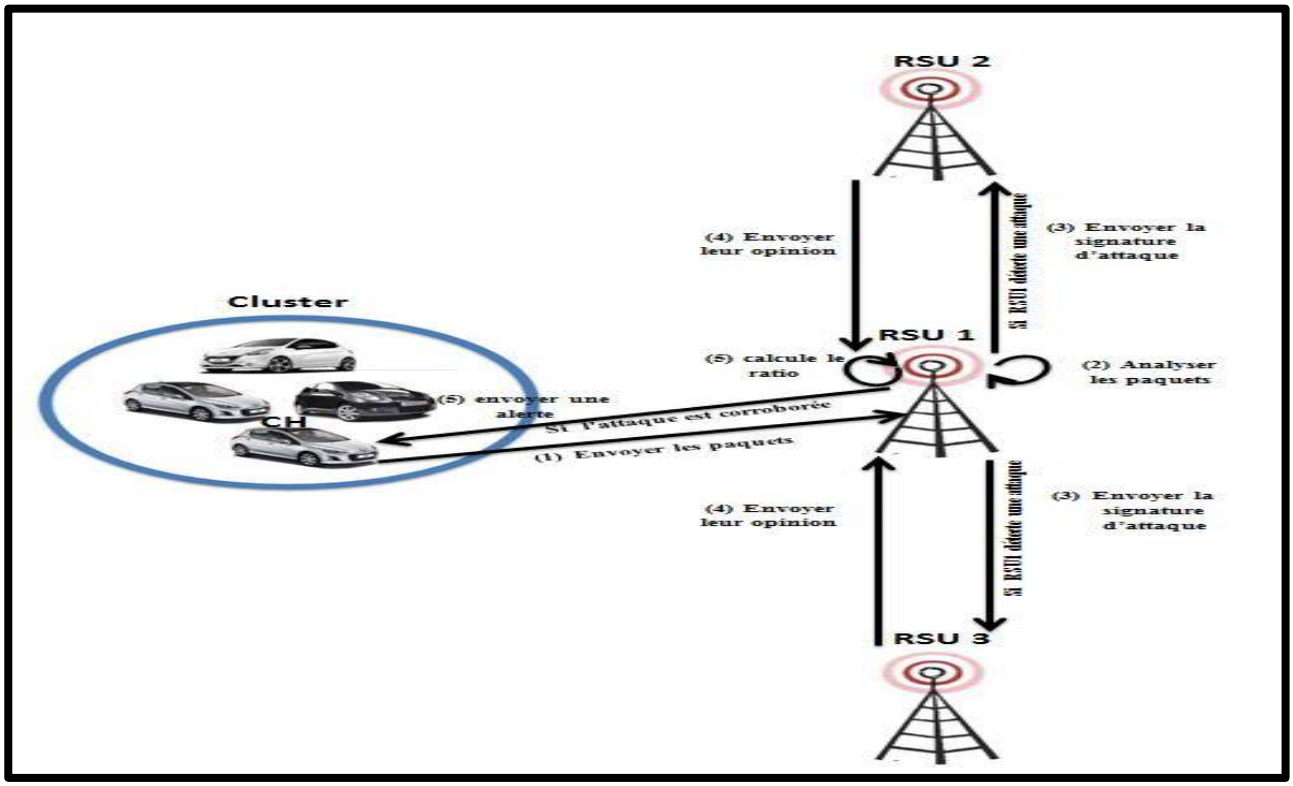

Figure III.7. Le principe de la méthode IDS clustérisé basée RSU.

3. Comparaison des IDS étudié

IDS	Architecture	La méthodologie	Avantages	Inconvénients
Waatchdog and pathrater	Individuel	surveillance de nœuds	Evité les nœuds malicieux.	Les nœuds malicieux n'est pas punis, ils suivre d'utiliser les services réseau
CONFIDANT	Coopérative	Réputation	Détecté les nœuds égoïsmes et les nœuds malicieux. punition de nœud malveillant.	Dans le temps de calcule la valeur de réputation, le déni de service est facilement réalisée.
Zhang et Lee IDS	Coopérative	Détection coopérative	Détection locale indépendamment des autres nœuds	Dans le temps de calcule la valeur de réputation, le déni de service est facilement réalisée Les nœuds malicieux n'est pas punis, ils suivre d'utiliser les services réseau
IDS clustered				
IDS basé véhicule	Clustérisé	signature	Détecter le nœud malveillant punition de nœud malveillant.	Les nœuds égoïsmes ne sont pas détectés. Occupée le système par un nœud malicieux envoyer des Faus alerte. Limite de capacité de calcule et de stockage.
IDS basé RSU	Clustérisé	signature	punition de nœud malveillant. Aucune fausse alerte transmis vers les véhicules après l'analyse par RSU. Exploiter la Grande capacité de calcule et de stockage dans RSU	Les nœuds égoïsmes ne sont pas détectés .

Tableau III.1 : Comparaison des IDS étudié.

Parti 2 : contribution

A partir de notre étude comparative des nombres **IDS** existant : watchdog and pathrater, CONFIDANT, Zhang et Lee **IDS** et **IDS** clustered ; la conséquence de cette travaille est chaque IDS on a des points faibles.

A notre avis l'**IDS** clustered basé RSU est très évidence par a port à les autres **IDS** existantes, car :

- ✓ Tous paquets transmissions est analysé par les RSUs.
- ✓ Aucune fausse alerte transmis vers les véhicules après l'analyse.
- ✓ une grande capacité de calcule dans RSUs.

Malgré tous ces avantages de cet **IDS**, les nœuds égoïsmes et les nœuds malveillants qui supprimes les paquets n'est pas détecter par cet **IDS**.

Nous avons présenté une proposition pour évite l'inconvénient de **IDS** clustred basé RSU; cette proposition est une combinaison entre deux **IDS** : **IDS** clustred basé RSU et watchdog and pathrater.

1. Le principe de méthode proposé

Le principe de notre méthode qui nous proposée est le suivant :

1. installer un **IDS** watcdog and pathrater dans chaque véhicule.
2. si l'**IDS** détecter un nœud malveillant, il ajoute à la tête de paquet la signature de cet nœud.
3. envoyer le paquet vers RSU.
4. **IDS** basé sur RSU analysé le paquet si la tête de paquet contient la signature de nœud malveillant l'**IDS** envoyer des alerte au les véhicules de la zone et isolé les nœuds si non **IDS** basé RSU analysé le paquet si un comportement anormal en va faire :

a. Envoyer la signature d'attaque vers les RSUs de leur zone et demande leurs opinions.
b. Les RSUs renvoyer leurs opinions sur cette signature.
c. RSU calcule la probabilité d'attaque.
d. Si la probabilité d'attaque dépasse la limite, RSU envoyer des alertes à les véhicules de sa zone et isolé le nœud malveillant.

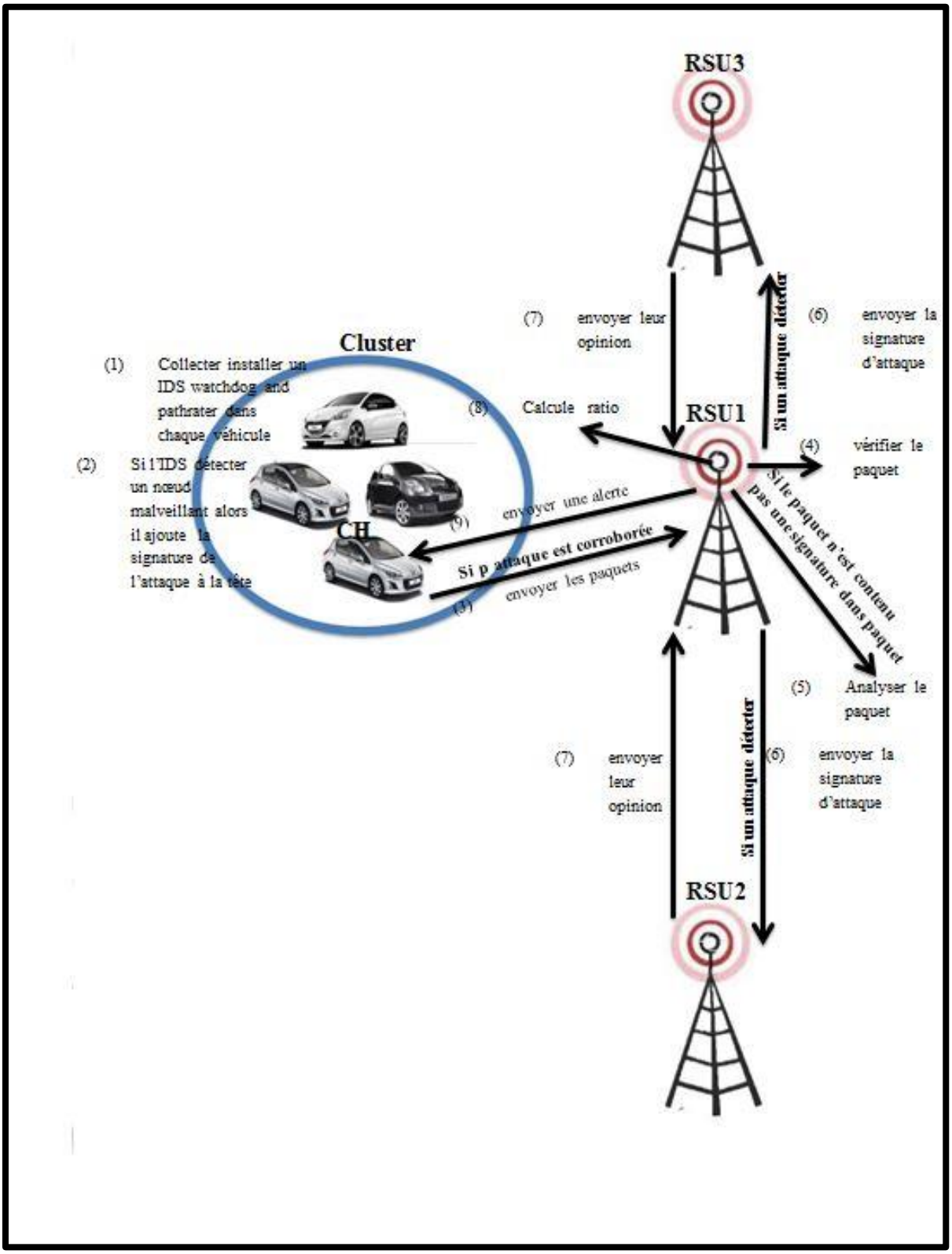

Figure III.8. Le principe de méthode proposé.

Conclusion

Il y a plusieurs méthodes des **IDS** existants parmi elles watchdog and pathrater, CONFIDAND, zang et lee et **IDS** clustred.

Chaque IDS utilisé dans les réseaux **VANETs** y a des points faibles et points forts

Dans notre chapitre, en proposer une solution de les points faibles d'**IDS** clustred basé RSU, en va faire une combinaison entre d'**IDS** clustred basé RSU et watchdog and pathrater.

L'inconvénient de notre proposition est la limite de capacité de stockage et de traitement dans les véhicules.

Le domaine de sécurité dans les réseaux **VANETs** est très important parce que il ya des problèmes jusqu'à manent n'est une solution

Conclusion générale

Les réseaux **VANETs** est une particularité des réseaux MANET où les nœuds mobiles sont des véhicules (intelligents).Parmi les objectifs de ce réseaux: Prévention sur les accidents Anticipation du trafic Préventions d'un véhicules prioritaire Possibilité de jouer, Avoir une prévention sur l'itinéraire, ….etc. leurs nœuds rendant la topologie du réseau fortement dynamique.

Les propriétés des réseaux véhiculaires offrent des challenges importants, ce qui rend les V**ANET** s'ouvrent à plusieurs domaines de recherche : la sécurité, Localisation des véhicules…etc. Dans notre mémoire, nous avoir le domaine de sécurité et comment sécurisé les nœuds des réseaux contre les attaques à partir d'utiliser l'**IDS**.

Parmi les attaques qui attaqué les réseaux **VANETs** sont : Usurpation d'identité ou de rôle (Spoofing), Véhicule caché, Wormhole…ect.

Un **IDS** (Internet Detection Scanner), est un outil qui a pour vocation la surveillance d'un ou plusieurs réseaux de machines. Il y a deux approches des **IDS** : L'approche basée connaissance (La détection d'abus (misuse detection), L'approche comportementale (La détection d'anomalie (anomaly detection).

Dans les réseaux V**ANETs** il y a plusieurs **IDS** utiliser pour détecter les nœuds malveillants qui attaquant le réseau. dans notre mémoire, nous faire une étude comparative être quelque **IDS** utiliser dans **VANET** :watchdog and pathrater, CONFIDANT…etc.

Dans notre mémoire, nous combinai entre deux **IDS** :watchdog and pathrater et **IDS** clustred basé RSU pour éliminer les point faibles de le dernier.

Référence bibliographie

[1] http://members.unine.ch/muriel.aubert/images/uninice.pdf

[2] KHADIDJA AYAD, «Sécurité du routage dans les réseaux ad hoc Mobile », Ecole nationale Supérieure en Informatique (ESI) Oued-Smar Alger , 14 Novembre 2012.

[3] M. MERAIHI Yassine , ROUTAGE DANS LES RESEAUX VEHICULAIRES (VANE T), Boumerdès 2011.

[4] Mlle LAIDOUI Fatma, « Approche basée sur la confiance pour l'établissement des routes dans les réseaux ad hoc mobiles », **E**cole nationale **S**upérieured'**I**nformatique (ESI)Oued-Smar/Alger, 19 décembre 2013.

[5] M. Khaled, B.Saïd ,M .Yacine ,D. Younes, «les réseaux MANET» , Université des Sciences et de la Technologie - HOUARI BOUMEDIENE.

[6] Mohammed ERRITALI, « Contribution à la sécurisation des réseaux ad hoc véhiculaires », UNIVERSITÉ MOHAMMED V –AGDAL FACULTÉ DES SCIENCES Rabat, 10 Octobre 2013.

[7] ROMAIN COUSSEMENT, « MÉCANISME D'AIDE À LA DÉCISION POUR LES IDS DANS LES RÉSEAUX VANETS», L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES, JANVIER 2014.

[8] A.Abdelaziz, **H. Meryam ,** B.Youcef , B.Nadjet, « Les Réseaux Véhiculaires VANET», UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE, 2014/2015.

[9] Noureddine CHAIB , « La sécurité des communications dans les réseaux VANET» , UNIVERSITE ELHADJ LAKHDER – BATNA .

[10] Fethi.Filali, « Les reseaux VANET»Vehicular Ad hoc NETWORK.

[11] Q. Xu and D. Jiang, "Design and analysis of highway safety communication protocol in 5.9 GHz dedicated short range communication spectrum," Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual, vol. 4, pp. 2451-2455, Apr. 2003.

[12] J. Santa, A. F. Gómez-Skarmeta, and M. SJnchez-Artigas, "Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks," Computer Communications, vol. 31, no. 12, pp. 2850-2861, Jul. 2008.

[13] M. JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections," UNIVERSITE D'EVRY VAL D'ESSONNE thèse de doctorat, 2008.

[14] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, Tenerife, 2009, pp. 106-115.

[15] Wikipédia, Wireless LAN, http://en.wikipedia.org/wiki/Wireless_LAN, date de dernière modification, 4 janvier 2014.

[16] Wikipédia, Wi-Fi, http://fr.wikipedia.org/wiki/Wi-Fi, date de dernière modification, janvier 2014.

[17] A. Bachir , A. Benslimane, « A multicast prot ocol in ad hoc networks inter - vehicle g eocast » , Vehicular Technology Conference, 2003. The 57th IEEE Semiannual, Volume: 4, On page(s): 2456 - 2460.

[18] Gokhan Korkmaz, Eylem Ekici, and FusunOzguner « An Efficient Ful ly Ad - Hoc Multi-Hop Broadcast Protocol for Inter -Vehicular communication Systems ». Department of Electrical and Computer Engineering, The Ohio State University, 2006.

[19] G◌ khan Korkmaz. « GPS Based wireless communication protocols for Vehicular Ad Hoc Networks Dissertation »Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University, B.S., M.S. The Ohio State Universi ty, 2006.

[20] R. Meraihi, Mohamed Senouci, Moez Djebri « Réseau mobile Ad Hoc et réseaux de capteur s sans fil » chapitre de livre Edition Hermes ,2006.

[21] Maxim Raya and Jean -Pierre Hubaux: « Securing vehicular ad hoc netw orks »Journal of Computer Security 15 (2007) 39 –68 39 IOS Press.

[22] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[23] F. Kargl, Z. Ma , and E. Schoch, "Security engineering for vanets," in 4th Wksp. Embedded Sec. in Cars, 2006.

[24] S. Biswas, Mis, x030C, ic, x, and J., "Proxy signature-based RSU message broadcasting in VANETs," in Communications (QBSC), 2010 25th Biennial Symposium on, 2010, pp. 5-9.

[25] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: design and architecture," Communications Magazine, IEEE, vol. 46, pp. 100-109, 2008.

[26] A. Stampoulis and C. Z., "Survey of security in vehicular networks," in Project CPSC, 2007.

[27] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," presented at the Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, Philadelphia, PA, USA, 2004.

[28] V. S. Yadav, S. Misra, and M. Afaque, "Security of self-organizing networks," ed, 2010.

[29] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference, pp. 1-12, 2007.

[30] Q. Yi and N. Moayeri, "Design of secure and application-oriented VANETs," in Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, 2008, pp. 2794-2799.

[31] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, 2006, p. 8 pp.

[32] idjiwa.free.fr/wordpress/wp-content/routage v2.pdf , 2011.

[33] Jonathan PETIT, ‘’Surcoût de l’authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires’’, Thèse de doctorat, université Toulouse, 2011.

[34] Ma, Shuo, Ouri Wolfson, and Jie Lin. "A survey on trust management for intelligent transportation system." Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science. ACM, 2011.

[35] Larafa Claire Sondès. ‘’Services AAA dans les réseaux ad hoc mobiles’’. Thèse de doctorat. Télécom SudParis,France,2011.

[36] Jonathan Petit, « Surcoût de l’authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires», l’Université Toulouse III - Paul Sabatier, 13 Juillet 2011.

[37] Thierry Simoni, « Logiciels de détection d’intrusions», *Thierry.Simoni@univ-lyon1.fr.*

[38] Hatem Bouzayani, « Modèle quantitatif pour la détection d’intrusion. Une architecture collaborative IDS-HONEYPOT», Université du Québec en Outaouais, Juin 2012.

[39] Mme LABED Ines, « Proposition d’un système immunitaire artificiel pour la détection d’intrusions», *UNIVERSITE MENTOURI DE CONSTANTINE FACULTE DES SCIENCES DE L’INGENIEUR,* 2005-2006.

[40] Nathalie Dagorn, « D_etection et pr_evention d'intrusion : pr_esentation et Limites Nathalie Dagorn »,https://hal.inria.fr/inria-00084202,6 Jul 2006.

[41] K. Ilgun, R.A. Kemmerer, P.A. Porras, “State transition analysis: a rule-based intrusion detection approach”, IEEE Transactions on Software Engineering, Vol. 21, N° 3, March 1995, pp.181-199.

[42] www.car-2-car.org

[43] Mohamed Bouarir. Protocole de routage intelligent pour les réseaux ad hoc de véhicules.UNIVERSITE DU QUEBEC EN ABITIBI-TEMISCAMINGUE (UQAT) Le laboratoire de recherche TELEBEC EN COMMUNICATIONS SOUTERRAINES (LRTCS).

[44]La sécurité sans fils.