Liste figures

Introduction générale

Les développeurs et les chercheurs cherchent comment exploiter la technologie sans-fil pour permettre aux véhicules d'établir des liens entre eux, avec ou sans infrastructures installées aux bords des routes. Les nouveaux réseaux sont constitués par VANET (Véhicule AD-Hoc NETwork).Une des applications prometteuses de ces réseaux consiste à permettre aux véhicules équipés de captures spécifiques de détecter l'environnement proche et d'avertir les conducteurs des véhicules aux alentours suffisamment tôt en cas de risques d'accident.

L'apparition des réseaux a rendu l'échange d'information possible ainsi la communication entre les voitures répandant. Vanet est une forme de MANET (Mobile Ad-hoc hoc Network) pour fournir des communications au sein d'un groupe de véhicules à portée les uns des autres et entre les véhicules et les équipements fixes à portée, usuellement appelés équipements de la route.

Dans les réseaux véhiculaires (Vanet), les véhicules sont équipés de dispositifs de communication sans fil, appelés unités embarquées (OBU), pour permettre les différents types de communications. Véhicule à véhicule (V2V) et véhicule à infrastructure (V2I). Au cours de ces communications, les véhicules diffusent une gamme d'informations très sensibles, tels que la position, la vitesse et la direction, et Identifiant.

Ainsi, un adversaire malveillant peut retracer un véhicule et le suivre. Ceci rend la protection de la vie privée des véhicules. Pour résoudre ce problème, les changements réguliers des pseudonymes de communication sont importants pour éviter tout suivi illégal des véhicules et pour assurer l'anonymat dans les réseaux Vanet.
On a choisir la solution « privacy SLOW »qui permet de changer les pseudonyms des véhicules selon [33].

Ce rapport est organisé en trois chapitres :
Chapitre 1 : Présentation des réseaux VANET

Chapitre 2 : La sécurité dans les réseaux VANET

Chapitre 3 : Simulations

Et nous terminerons par une conclusion générale et quelques perspectives.

Présentation des réseaux VANET

1-Introduction

Les réseaux VANET (Réseaux ad hoc de véhicules en anglais Vehicular Ad hoc NETworks) est une nouvelle technologie émergente des réseaux Ad-hoc mobiles (MANET) et ils sont des réseaux constitués de véhicules et d'infrastructures appelés communément nœuds ; ils ne sont qu'une application des réseaux MANET.

Ils constituent le noyau d'un Système de Transport Intelligent(STI) ayant comme objectif principal l'amélioration de la sécurité routière en tirant le profit de l'émergence de la technologie de communication et la baisse du coût des dispositifs sans-fil. En effet, grâce à des capteurs installés au sein de véhicules, ou bien situés au bord des routes et des centres de contrôle, les communications véhiculaires permettront aux conducteurs d'être avertis suffisamment tôt de dangers éventuels.

Ce chapitre fait une présentation générale des réseaux véhiculaires.

2- Qu'est-ce qu'un réseau Ad-hoc ?

Un réseau Ad-hoc se distingue des autres formes de réseaux, et notamment des autres réseaux sans fil, par sa capacité à exister et à s'organiser de manière autonome sans infrastructure fixe.

Le terme "Ad-hoc" nous vient du latin et signifie « allant vers ce vers quoi il doit aller ». Il est également souvent traduit par former dans un but précis. Cela souligne l'autonomie de ce système.

Là où les autres types de réseaux ont besoin de stations de base pour relayer les paquets qui transitent dessus, un réseau Ad-hoc n'est constitué que d'un nombre variable d'entités mobiles qui communiquent entre elles de façon directe.

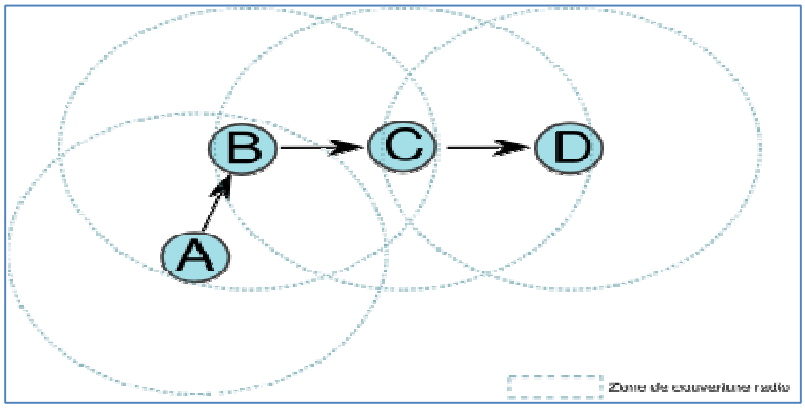

Figure 1 : Transmission de données avec routage ad-hoc

L'échange d'informations est permis par la connaissance mutuelle de l'ensemble de ces nœuds voisins qui peuvent jouer différents rôles (routeur, station de base mobile, etc.) pour faire transiter les données de nœud à nœud sur tout le réseau. Le chemin emprunté pour

transmettre un message d'un nœud source à un nœud destination est déterminé par un protocole de routage [1].

3- Les Systèmes de Transport Intelligents(STI)

Les systèmes de transport intelligents sont des applications ou services avancés associant les technologies de la communication, de l'information et de positionnement, à l'ingénieriedes transports.

Constatant un développement fragmenté de ces services au sein de l'Union, le Parlement européen et le conseil ont adapté le 7/08/2010 la directive 2010/40/UE sur les systèmes de transport intelligents, qui établir un cadre visant à soutenir le déploiement et l'utilisation coordonnés des STI à l'échelle européenne, avec comme priorités les domaines suivant :

- Utilisation optimale des données relatives à la route, à la circulation et aux déplacements
- Continuité des services STI de gestion de la circulation et du fret.
- Application de STI à la sécurité et à la sûreté routière.
- Lien entre le véhicule et les infrastructures de transport.

Cette directive mandate également la Commission pour adopter les spécifications nécessaires au déploiement coordonné des STI dans le cadre de six actions prioritaires [2].

Les principaux objectifs des STI sont :

- L'amélioration de l'efficacité des transports
- L'amélioration des systèmes de contrôle et de sécurité des véhicules.
- La gestion des urgences.
- La maîtrise de la mobilité.
- Le développement des services, dont l'information des voyageurs et le paiement électronique.
- La maitrise de l'énergie et la diminution de la pollution [3].

4. Les grands projets sur les véhicules communicants:

Les véhicules de demain seront connectés et communicants avec leur environnement (véhicules et infrastructures routières) favorisant ainsi le développement de nouvelles applications ITS. Plusieurs projets ont été la nièces dernières années et chacun a ses propres objectifs :

CarTALK 2000 (2001-2004) : Le but principal de ce projet est de travailler sur la conduite coopérative et les réseaux autonomes. Les travaux de CarTalk 2000 se sont basés, principalement, sur les couches basses et l'acheminement des messages dans les VANET[3].

IVHW : L'objectif du projet IVHW (Inter-VéhiculeHazard Warning) a fait l'objet d'une démonstration en conditions réelles de circulation lors du congrès E-Safety qui s'est tenu à Lyon en septembre 2002 et il en est de même dans d'autres pays comme les Etats-Unis ou le Japon.IVHW est de développer un concept commun de système d'alerte inter-véhicules, de mesurer son impact potentiel et d'identifier les conditions de mise en œuvre sur le marché. Le projet est conduit par un consortium franco-allemand dans le cadre du programme DEUFRAKO[3].

SeVeCom [3] : Le projet européen SeVeCom (Secure Vehicular Communication) traite la sécurité des communications dans les réseaux VANET. Sa problématique est de définir une architecture des VANET incluant la sécurité et l'anonymat de la communication véhicule à véhicule et véhicule à infrastructure.

FleetNet (FleetNet - Internet on the Road): l'objectif principal de ce projet fut de développer une Plate-forme complète pour les réseaux VANET. Il a traité également les problématiques de routage et d'accès au canal et il a également proposé de nouveaux services et d'applications, tels que l'accès à Internet qui est l'application principale de ce projet. Ce projet est élaboré par l'Allemagne pendant les années 2000-2003 dans le cadre d'un consortium de six industries et de trois université **[3].**

5- Les réseaux VANET

Les VANET sont des réseaux ad hoc mobiles dont les nœuds sont des véhicules. Bien que ce terme semble générique, tous les travaux réalisés sur ce type de réseaux assimilent "véhicule" à véhicule routier [4].

Les réseaux VANETs (Vehicular Ad hoc NET Works) constituent une nouvelle forme de réseaux ad hoc mobiles (MANET). Ils permettent d'établir des communications entre véhicules ou bien avec une infrastructure située aux bords de routes. Par rapport à un réseau ad hoc classique, les réseaux VANET sont caractérisés par une forte mobilité des nœuds rendant la topologie du réseau fortement dynamique [5].

5.1 Les caractéristiques des réseaux VANET

- **Une topologie dynamique :** Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent, la topologie du réseau peut changer à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels [11].La vitesse et le choix du chemin rendent la topologie du VANET fortement dynamique.
- **Une bande passante limitée :** Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste [11].

- **Des contraintes d'énergie :** Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système [11]. Les nœuds du réseau VANET sont censés avoir une grande capacité de traitement et de stockage de données. Donc, ces nœuds disposent suffisamment d'énergie qui peut alimenter les différents équipements électroniques.
- **Une sécurité physique limitée** : Les réseaux mobiles Ad-hoc (particulièrement VANET) sont plus touchés parle paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.
- **L'absence d'infrastructure** : Les réseaux ad-hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [11].

5.2 Les composant et architecture de réseaux VANETs :

Dans les réseaux VANETs, on trouve principalement, les entités fixes qui constituent l'infrastructure (RSU : Road Side Unit et TA :TrustedAuthority) et les entités mobiles (les véhicules). Pour pouvoir échanger les différentes informations et données liées à la sécurité et au confort des usagers de la route, ces différentes entités doivent établir des communications entre elles. La figure 2 illustre l'architecture d'un réseau VANET ainsi que les modes de communications entre ces entités.

5.2.1 OBU (On-Board Unit)

Ce sont des unités embarquées dans les véhicules communicants, elles regroupent un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres). Leurs rôles sont d'assurer la localisation, la réception, le calcul, le stockage et l'envoi des données sur le réseau. Ce sont des émetteurs-récepteurs qui assurent la connexion du véhicule au réseau.

5.2.2 TA (TrustedAuthority)

L'autorité de confiance « CA » (en anglais TA : **TrustedAuthority**)est une source d'authenticité de l'information. Elle assure la gestion et l'enregistrement de toutes les entités sur le réseau (OBU et RSU). La TA est sensée connaitre toutes les vraies identités des véhicules et au besoin les divulguer pour les forces de l'ordre. Aussi, la TA dans certains travaux se charge de la délivrance et l'attribution des certificats et des pseudonymes de communications [10].

5.2.3RSU (Road Side Unit)

Ces entités sont les subordonnés des TA. Elles sont installées au bord des routes. Elles peuvent être principalement des feux de signalisation, des lampadaires ou autres. Leur

principale responsabilité est de soutenir la TA dans la gestion du trafic et des véhicules. Elles représentent des points d'accès au réseau et aux différentes informations sur la circulation.

5.3 Les modes de communication dans VANET

On distingue deux types de communications véhicule à véhicule (V2V) et véhicule à infrastructure. La combinaison de ces deux types de communications permet d'obtenir une communication hybride très intéressante (voir la figure 2).

5.3.1 Communication véhicule-à-véhicule (V2V)

Ce type de communication fonctionne à l'aide des dispositifs installés dans les véhicules appelés OBU (On-Board Unit), suivant une architecture décentralisée. Il est semblable au type de communications entre les nœuds mobiles des réseaux MANETs. La communication entre deux véhicules se fait directement, en mode Ad-hoc inter-véhiculaire. Ils n'ont pas besoin de faire appel aux infrastructures pour pouvoir communiquer entre eux. À condition que chaque véhicule soit à la portée de l'autre (zone radio). Sinon, ils font appel à d'autres véhicules, qui vont jouer le rôle d'un pont (intermédiaire) pour eux. Ce type de transmission est appelée communication à multi sauts.

5.3.2 Communication véhicules à infrastructure

La communication véhicule à infrastructure (V2I) est aussi appelée « une communication en mode infrastructure ». Ce mode de communication est assuré grâce aux différentes entités du réseau VANETs. En effet, les OBUs des véhicules, les RSUs placés aux bords des routes et même les TA contribuent tous entre eux pour assurer les communications dans le réseau véhiculaire. Ce mode de communication assure une connectivité relativement forte par rapport à la communication en mode V2V (véhicule à véhicule). Comme il assure une meilleure utilisation des ressources du réseau, elle permet aux véhicules de bénéficier de plus de fonctionnalités et services comme l'accès à l'Internet et les informations météo urologiques [7].

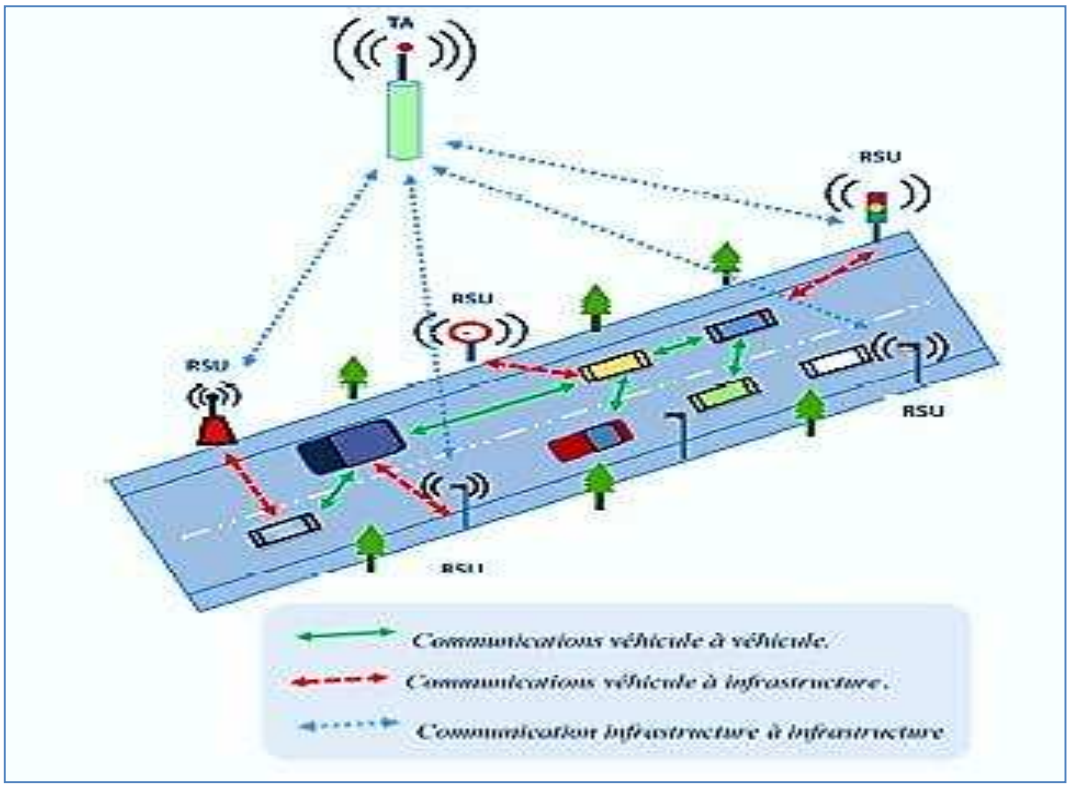

Figure 2 : Modèle de réseau VANETs et ses modes de communication [8].

6 les types de message dans réseaux VANET

Les messages transmis dans le réseau VANET sont classifié selon leurs utilités et leurs contenus en deux grands types de message :

6.1 Message lié à la sécurité

Le but est d'offrir une meilleure protection à travers la route. Ainsi on trouve deux types de messages de sécurités :

- **Le message beacon**

Ce type de message joue un rôle primordial dans la plupart des protocoles de routage et de sécurité. Ce type de message contient souvent des informations relatives à l'identité et à l'état actuel du véhicule (Position, vitesse, direction et autres), il est diffusé périodiquement et est utilisé principalement pour permettre l'identification du voisinage [8].

- **Le message d'alerte (d'urgence)**

Ce type de message est envoyé pour prévenir les autres véhicules de différentes urgences et des catastrophes sur la route (accident, congestion de la circulation, information météorologique, passage d'un véhicule de secoure et autres), afin qu'ils aient plus de temps pour agir. Ce type de message aide à améliorer la circulation et la sécurité routière [8].

6.2Message à valeur ajoutée

Il contient des données multimédias ou n'importe quelle donnée ou information, qui peut améliorer le confort des usagers de la route. Il peut contenir aussi n'importe qu'elle autre information ou donnée sur des services tel que l'endroit des restaurants ou des hôtels[8].

7. Les applications des réseaux VANET

Les principales applications des réseaux VANET peuvent être placées selon le service offert en trois grandes catégories, chaque catégorie peut avoir diverses classes, et sur chaque classe plusieurs applications peuvent être distinguées.

7.1. Catégorie liées aux STI et à la gestion de trafic routier

Les applications liées aux *STI* comprennent les messages rappelant les limitations de vitesse ou les distances de sécurité aussi les systèmes d'aide à la conduite et les véhicules coopératifs: aide aux dépassements de véhicules, prévention des sorties de voies en ligne ou en virage, etc.… [26].

Les applications liées à la gestion de trafic routier consistent à fournir aux conducteurs des informations leur permettant d'adapter leur parcours à la situation du trafic routier, comme exemple : l'ordonnancement des feux de signalisations et la surveillance du trafic [32]. La catégorie de la gestion du trafic est liée à la classe de l'efficacité du trafic coopérative. Depuis que les congestions dépassent la capacité de demande de la circulation, une approche efficace basée sur la gestion du trafic est nécessaire pour réduire la congestion. L'efficacité de trafic coopérative se compose de deux applications : les applications liées à la gestion de la vitesse coopérative et des applications liées à la navigation coopérative [27].

7.2. Catégorie de la sécurité routière et prévention

La sécurité routière est prise en première priorité suite au nombre élevé d'accidents. Pour remédier à la sécurité des déplacements et faire face aux accidents routiers, les communications inter-véhicules offrent la possibilité de prévenir les conducteurs sur l'existence d'un accident, des travaux sur la route et même 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 [27].

Les applications liées à la sécurité ont suscité une attention considérable car elles sont directement liées à minimiser le nombre d'accidents de la route. Cette catégorie est associée aux applications de la classe « sécurité routière active » qui vise à fournir des services de sensibilisation et d'alerte au conducteur à travers trois types d'applications : la sensibilisation coopérative (CA), l'assistance à la conduite coopérative (CDA), et les applications d'alertes de risque de collision (RHCW). En fait, la classe de la sécurité routière active fournit des fonctions de sensibilisation qui fournissent des informations au conducteur pendant la

conduite normale, avertissent le conducteur des conditions de danger de la route et les accidents probables et aident activement le conducteur à éviter des accidents imminents. En d'autres termes, les applications liées à la sécurité sont responsables de: sensibilisation, mise en garde et d'assistance [27].

1. **les applications de sensibilisation coopérative**

Consistent à sensibiliser les conducteurs des autres véhicules et fournir des informations sur l'environnement alentours du véhicule. Plusieurs applications sont offertes dans cette catégorie. Parmi ces applications, nous mentionnons : l'indication d'un véhicule d'urgence, indication de l'approche d'une moto et signalisation d'un véhicule lent. Pour ces derniers exemples d'applications, le véhicule diffuse des messages d'alertes à l'approche des véhicules dans son entourage. Les informations diffusées aident les conducteurs routiers à s'adapter aux conditions de la route [27].

2. **les applications d'assistance et d'aide à la conduite coopérative**

Ces applications fournissent des services d'assistance au conducteur. Beaucoup de services appartiennent à cette catégorie, entre autres:

- **Systèmes de conduite coopérative** *:* cette application exploite l'échange de données de capteurs ou d'autres informations d'état entre les voitures. Ces systèmes de conduite aident les conducteurs pour maintenir un temps et une distance des écurité entre les véhicules pour s'assurer que le freinage d'urgence ne causera pas de collisions entre les voitures. Le système de calcul des progrès adapte le progrès d'un véhicule en tenant compte des nouvelles conditions environnementales, la dynamique du véhicule, et des considérations de sécurité [29].
- **Assistance au changement de voie :** Cette application assiste le conducteur dans le choix de l'instant optimal pour changer de voie et influe sur le comportement des conducteurs en vue d'améliorer les performances de conduite [29].

3. **Application d'avertissement de collision et risque de la route :** *Ces* applications fournissent des informations au sujet des collisions imminentes dues à l'état dangereux de la route, obstacles et conducteurs erratiques pour que les conducteurs soient vigilants à la collision imminente. Les systèmes de détection d'accident (CD) se fondent sur des radars, des capteurs, ou des caméras afin de détecter une collision imminente. Plusieurs services sont offerts dans cette classe :

   - Avertissement Coopératif de Collision : Un véhicule surveille activement les messages concernant le statut de la cinématique des véhicules de son voisinage pour avertir la collision potentielle[29].

   - Emergence électronique des feux de stop : un freinage dur d'un véhicule provoque un message d'avertissement qui sera diffusé aux conducteurs mis en danger au sujet de la situation critique avec une latence minimum [30].

7.3 Catégorie liées au confort du conducteur et des passagers

Le genre de ses applications permet d'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. Nous citons comme exemple d'application la gestion des espaces libres dans un parking, l'application permet de rassembler des informations sur la disponibilité de l'espace libre de stationnement dans les parkings et de renvoyer au conducteur la place libre la plus proche [31].
L'objectif général de cette catégorie est d'améliorer le confort des passagers. Elle est liée à deux classes, d'une part la classe des services locaux de coopération et d'autre part la classe des services d'internet globale.

La classe des services locaux publics coopérative : fournit des services d'application basés sur géo-localisation (LBS) :

- ✓ Les points de services de notification d'intérêt comprennent les véhicules, station de l'approvisionnement en énergie, installation d'entretien des véhicules, la gestion des transports en commun, zone de repos, parking, hôtel / restaurant, lieu du tourisme, locale lieu de rencontre de l'événement, centre médical, poste de police et postes de péage.
- ✓ Annonces de service : les entreprises transmettent des données de marketing à des clients potentiels qui passent [27].

8 La motivation/problématique

Bien que la recherche dans le domaine des réseaux VANETsoit récente, elle est vaste et diversifiée. En effet, des travaux de recherche conséquents sont actuellement en train d'être effectués par des chercheurs dans le but de normaliser un ou plusieurs protocoles MAC qui peuvent être utilisés pour la communication dans les réseaux VANETs. Aujourd'hui, il semble que c'est le standard IEEE 802.11p qui sera adopté pour ce type de communication. En outre, de nombreux autres travaux (par exemple, et portant sur des protocoles de diffusion spécifiques au V2V ont été proposés pour garantir la qualité de service (QoS) pour les applications de diffusion des messages de sécurité, soutenir la capacité de prioriser et de gérer plusieurs types de messages, etc. Cependant, le support de la QoS demeure un défi dans les réseaux VANETs.

Les protocoles de diffusion (broadcastprotocols) joueront un rôle très important par rapport aux messages unicast (point à point) dans les réseaux VANET, car ils sont conçus pour communiquer des messages de sécurité importants pour tous les nœuds. Ces protocoles de diffusion ne sont pas fiables et ils souffrent de plusieurs problèmes, à savoir :

1. Tempête de diffusion (broadcaststorm).
2. Nœud caché (hiddennode) : Deux nœuds peuvent entendre l'activité d'un troisième nœud mais ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles qui les empêche de communiquer entre eux.

3. Échec de la transmission.

Dans des réseaux très denses causés par le fait que tous les nœuds partagent le même canal, il y a un besoin pressant de développer de nouveaux protocoles de diffusion dans les réseaux VANET. De plus, de nouvelles approches pour la sécurité de la communication doivent être conçues pour adapter les besoins spécifiques du réseau et garantir des services fiables et dignes de confiance. Ces problèmes doivent être résolus pour fournir une diffusion fiable et rapide [9].

9 Conclusion

Toutes les applications de STI exigent des concepteurs la prise en compte de l'importance des informations échangées entre les véhicules. Ainsi, il n'y a aucune garantie que les membres des réseaux VANET ne créent pas des messages arbitrairement falsifiés ou ne changent pas le contenu d'un message lié à la sécurité afin de causer un accident par exemple. La notion de sécurité de communication dans les réseaux véhiculaires est traitée dans le chapitre suivant.

1. Introduction

Les communications véhiculaires constitueront dans le futur le plus grand réseau Ad-hoc viable. De plus, la vie de milliers d'êtres humains sera dépendante des informations échangées entre les véhicules eux-mêmes et avec les infrastructures. A cause de l'importance des informations échangées et du nombre énorme d'utilisateurs, l'environnement des réseaux véhiculaires sera plus vulnérable. En effet, les messages liés à la sécurité peuvent être falsifiés ou éliminés par des entités malveillantes afin de causer des accidents et mettre en péril la vie des personnes. Donc, avant le déploiement de ces réseaux, des mécanismes de sécurité appropriés doivent être mis en œuvre afin d'éviter ces mauvais scénarios et d'identifier les entités responsables de ces activités malveillantes.

Dans ce chapitre, nous allons présenter la notion de sécurité des réseaux, les caractéristiques de la sécurité des VANETs, les différents types d'attaques et les mécanismes de base de la sécurité pour ce type de réseau**.**

2. La sécurité d'un réseau ?

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionne de façon optimale et que les utilisateurs des machines possèdent uniquement les droits qui leur ont été octroyés.

Il peut s'agir :

- d'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- d'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système.
- de sécuriser les données en prévoyant les pannes.
- de garantir la non-interruption d'un service.

3. La sécurité dans les réseaux mobiles Ad hoc

3.1 Les objectifs de la sécurité

La sécurisation des communications dans les réseaux sans-fil comme dans les réseaux filaires nécessite la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent [13]:

- **L'authentification**: cet objectif de sécurité permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels ils communiquent.
- **La non-répudiation**: cet objectif de sécurité permet de s'assurer qu'aucun émetteur ne peut nier d'être à l'origine d'un message. Cet objectif est indispensable dans les transactions électroniques et dans toutes les communications sensibles.
- **La confidentialité**: cet objectif de sécurité garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau. Ces données peuvent concerner la couche applicative ou les couches inférieures.
- **L'intégrité**: cet objectif de sécurité permet de s'assurer que les données échangées ne sont pas soumises à une altération volontaire ou accidentelle. Donc, il permet aux destinataires

de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants.

- **La disponibilité:** cet objectif de sécurité vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate.

3.2 Infrastructure à clés publiques PKI (*Public Key Infrastructure*)

Une infrastructure à clés publiques est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériels), de procédures humaines (vérifications, validation) et de logiciels (système et application) qui permettent de gérer le cycle de vie des certificats numériques [21].
Une infrastructure à clés publiques fournis un ensemble de services pour le compte de ses utilisateurs comprenant leur enregistrement, la génération et le renouvellement de certificats et la publication de la liste de révocation de certificats LRC1. Ce dernier service est vital pour la sécurité d'un réseau ad hoc, dans lequel les clés peuvent être compromises à n'importe quel moment ; donc les membres du réseau doivent pouvoir accéder à cette information à tout moment et avec un coût raisonnable en termes de bande passante et de traitement.

4. 3.3 Caractéristiques de la sécurité des réseaux VANET

Pour mieux concevoir et mettre en place des protocoles et des dispositifs de sécurité dans les réseaux VANETs, il est judicieux de commencer par l'analyse de la nature des communications dans ces réseaux et leurs caractéristiques à savoir [22] :

- **Un support de transmission partagé :**

La communication sans fil et l'utilisation des on des radio permettent aux entités attaquantes d'intercepter facilement les signaux et avoir accès aux différents messages échangés entre les entités, mais aussi elle leur permet d'agir en injectant des données erronées ou des informations falsifiées dans le réseau [22].

- **Les communications multi-sauts :**

Dans les réseaux VANETs, il faut avoir des communications sans fil sur une très grande portée, afin d'atteindre certaines entités du réseau. Pour cette raison, il est nécessaire d'utiliser des communications à multi-sauts. Mais cela n'est pas sans conséquence. Car certaines entités malveillantes exploitent cette caractéristique pour mettre en péril le réseau, soit en altérant les communications, soit en refusant la retransmission des messages [22].

- **La diffusion d'information de localisation :**

Les entités mobiles (véhicules dans les réseaux véhiculaires) envoient périodiquement des messages qui indiquent leur localisation. Cette information est très importante, mais relativement très sensible, étant donné qu'elle peut être utilisée par une entité malveillante pour poursuivre facilement les entités qui l'intéressent (vole d'identités). [22]

- **Les opérations autonomes :**

Dans les réseaux VANETs, les entités sont autonomes par l'envoi des messages et la transmission des différentes informations et alertes. Ce qui donne la possibilité aux entités malveillantes d'envoyer à leurs tours, des informations erronées ou falsifiées, pour nuire considérablement aux autres entités du réseau ou causer le dysfonctionnement du système [22].

5. Routage dans les VANETs

Tous les services supportés, unicast ou multicast, se basent sur des communications multi-saut pour l'acheminement des données.

Les transferts de information et donnée fichier et les jeux. Les communications multicast sont utilisées dans les applications de sécurité et de gestion de trafic telles que l'avertissement de collision et le platooning. Pour réaliser les échanges, les protocoles de routage utilisent des informations locales, sur le voisinage immédiat, ou globales, concernant tout le réseau, an de déterminer les nouds relais qui participent à l'acheminement des données communications unicast sont généralement utilisées dans les applications de confort telles que le [32].

6. Classification des protocoles de routage dans le réseau VANET

Vanet a comme caractéristique principale une forte mobilité qui entraîne une topologie très dynamique. Cette caractéristique fait que les protocoles de routage traditionnels des MANETS sont pour la plupart in adaptée aux VANETS. En effet, dans les VANETS, la vitesse peut être beaucoup plus élevée que les MANETS dans certains environnements de communication comme les autoroutes. Dans [35] [36] Différentes solutions pour le routage dans les réseaux VANET ont été proposées, nous distinguons deux classes de protocoles de routage: les protocoles basés sur la Unicast (topologie) qui sont divisés en protocoles proactifs, réactifs et hybrides et les protocoles basés sur la localisation (géographique) qui utilisent la position physique des nœuds mobiles pour configurer le routage.

5.1 Les protocoles de routage basés sur la topologie

- **Les protocoles réactifs**

Des algorithmes classiques ont étés adaptées comme routage par facteur de distance.les routes sont faites seulement sur demande et uniquement en cours d'utilisation sont maintenus.et là, un délai supplémentaire est très nécessaire au dé début de chaque session pour faire une recherche du chemin .lorsqu'un nœud veut envoyer des paquets ,une étape de découverte de route est initiée par la diffusion d'un message de recherche d'une route .ce message qui a été réçu par un nœud qui ne dispose pas d'informations à propos de la destination diffuse a son tour le message. Mécanisme est appelé mécanisme d'inondation [35].

a. **Le protocole AODV:** Le protocole de routage AODV (Ad hoc On-demand Distance Vector) [37] est un protocole décrit dans la [47]. AODV invoque des paquets de contrôle HELLO qui permettent de vérifier la connectivité des routes. AODV repose sur deux mécanismes : découverte de route et maintenance de route. La découverte de route permet

de trouver une route pour atteindre une destination et la maintenance de route permet de détecter et signaler les coupures de routes provoquées éventuellement par la mobilité des nœuds. Ce protocole crée les routes au besoin et utilise le principe de numéro de séquence afin d'utiliser les routes les plus nouvelles, dites encore les plus fraîches. En plus, il utilise le nombre de sauts comme métrique pour choisir entre plusieurs routes disponibles. Trois types de paquets sont utilisés par AODV : les paquets de requête de route RREQ (Route Request Message), les paquets de réponse de route RREP (Route Reply Message) et les paquets d'erreur de route RERR (Route Error Message).

b. **Le protocole DSR:** DSR (Dynamic Source Routing) [37] est un protocole qui est normalisé dans la [46] Ce protocole crée les routes à la demande comme le protocole AODV. DSR est composé de deux mécanismes : la découverte de route et la maintenance de route. Le premier permet de chercher les routes nécessaires à la demande, tandis que le second permet de s'assurer de la maintenance des routes tout au long de leur utilisation.

   Le protocole DSR utilise la technique "routage à la source" dans laquelle la source inclut dans l'entête du paquet la route complète par laquelle un paquet doit passer pour atteindre sa destination. Les nœuds intermédiaires entre la source et la destination n'ont pas besoin de maintenir à jour les informations sur la route traversée puisque la route complète est insérée dans l'entête du paquet.

- **Les protocoles proactifs**

a. **Le protocole OLSR:** OLSR (Optimized Link State Routing) est un protocole de routage proactif développé dans le cadre du projet Hypercom de l'Institut National de la Recherche en Informatique et Automatique (INRIA) de France et proposé en tant que RFC (Request For Comment) expérimentale à l'IETF (Internet Engineering Task Force). Il est considéré comme une optimisation du protocole à état des liens filaires pour les réseaux mobiles Ad Hoc.

Donc le principe est que chaque nœud construit un sous ensemble appelé MPR (MPR : Multi-Point Relaying), parmi ses voisins, qui permet d'atteindre tous ses voisins à deux sauts, les nœuds de cet ensemble servent à acheminer et retransmettre les messages qu'ils reçoivent. Les voisins d'un nœud qui ne sont pas MPRs, lisent et traitent les paquets mais ne les retransmettent pas.

b. **Le protocole DSDV:** DSDV (Destination-Sequenced Distance-Vector) est un protocole de routage de type vecteur de distance.

Dans le protocole DSDV, une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination afin de mettre à jour l'entrée associée à cette destination dans la table de distance. De ce fait, la réaction de DSDV aux changements de la topologie est considérée lente. D'autre part, ce protocole cause une charge de contrôle importante dans le réseau à cause des paquets de mise à jour envoyés périodiquement ou à la suite des événements.

Chaque nœud maintient une table de routage contenant des informations sur les destinations accessibles dans le réseau. Ces informations comprennent les nœuds suivant utilisé pour atteindre la destination, le nombre de sauts qui sépare le nœud de la destination et le numéro de séquence estampillé par la destinataire. Ce numéro de séquence permet de distinguer les nouvelles routes des anciennes. Chaque nœud envoie périodiquement à ses voisins la totalité de sa table de routage. D'autres paquets de mise à jour sont aussi envoyés à la suite d'un changement dans la topologie du réseau.

Ces paquets n'incluent que les entrées de la table affectées par le changement et ont pour objectif de propager les informations de routage aussi rapidement que possible. Quand un nœud reçoit un paquet de mise à jour, il le compare avec les informations existantes dans sa table de routage. Toute entrée dans la table est mise à jour si l'information reçue est plus récente (ayant un numéro de séquence plus grand), ou si elles ont le même numéro de séquence mais avec une distance plus courte. [37]

c. **Le protocole GSR (Global State Routing):** GSR diffère des protocoles à état de liens dans le fait que les nœuds ne diffusent pas leurs états de liens à tout le réseau, mais ils se limitent à l'envoyer aux voisins uniquement. Ainsi, GSR réduit le trafic des paquets de contrôle. Le problème de GSR est la taille de ses paquets de mise à jour (table de topologie) qui peuvent devenir considérable si le réseau contient un grand nombre de nœuds. En plus, il a une lenteur dans la détection des changements de la topologie. GSR est un protocole proactif à état de liens où chaque nœud connaît la topologie globale du réseau ce qui lui permet de calculer les routes pour atteindre chaque destination [37].

- **Protocoles hybrids**

a. **Le protocole ZRP (Zone Routing Protocol) :** est un protocole hybride qui combine les deux approches proactives et réactive. Le protocole ZRP divise le réseau en différentes zones. Pour chaque nœud, il définit une zone de routage exprimée en nombre de sauts maximal σ. Ainsi, la zone de routage d'un nœud inclut tous les nœuds qui sont à une distance au maximum de σ sauts. Les nœuds qui sont exactement à σ sauts sont appelés nœuds périphériques [37] [38].

   ZRP utilise soit le protocole de contrôle d'accès au support (MAC) pour connaître les voisins immédiats ou le protocole NDP (NeighbourDiscovery Protocol) pour la transmission et la gestion des échanges de messages HELLO. Par la suite, chaque nœud invoque le protocole IARP pour découvrir les routes vers tous les autres nœuds qui se trouvent dans sa zone de routage. Cependant, le protocole IERP est utilisé à la demande pour chercher les routes entre un nœud et une destination qui se trouvent à l'extérieur de sa zone de routage. Un troisième protocole BRP (Bordercast Resolution Protocol) est inclus avec IERP pour guider la propagation des requêtes de recherche de route dans le réseau. BRP utilise les données de la topologie fournies par le protocole IARP afin de construire sa liste des nœuds de périphérie et la façon de les atteindre [39].

Routage proactif		Routage réactif	
Avantages	**inconvénients**	**Avantages**	**inconvénients**
La topologie du réseau est connue de tous les mobiles. Les routes sont disponibles immédiatement.	Il faut diffuser régulièrement des informations sur les changements de topologie du réseau.	Les mobiles ne conservent pratiquement aucune information sur la topologie globale du réseau : seules les informations sur les routes actives sont stockées.	
Les protocoles proactifs disposent en permanence d'une route pour chaque destination dans le réseau.	Un volume de signalisations important.	Les protocoles réactifs génèrent à priori un volume plus faible de signalisations.	Les protocoles réactifs engendrent un délai lors de la construction (ou de la reconstruction) des routes et produisent plus difficilement des routes optimales.

Tableau 1 : Comparaison entre protocoles proactifs et protocoles réactifs. [**40**]

7. Les protocoles de routage basés sur la géographique

a. **Le protocole A-STAR:** (Anchor-based Street and Traffic Aware Routing) est un protocole utilise particulièrement les informations sur les itinéraires d'autobus de ville pour identifier une route d'ancre (anchor route) avec une connectivité élevée pour l'acheminement des paquets. Il basé sur la localisation (position) pour un environnement de communication véhiculaire métropolitain. A-STAR adopte une approche de routage basée sur l'ancrage (anchor based) qui tient compte des caractéristiques des rues. Un point est associé à chaque rue en fonction de sa capacité (grande ou petite rue qui est desservie par un nombre de bus différent). Les informations de routes fournies par les bus donnent une idée sur la charge du réseau véhiculaire dans chaque rue [40] [41].

b. **Le protocole UMB(Urban Multi hop Broadcast Protocol):** C' est un protocole basé sur l'algorithme de diffusion multi saut pour les réseaux inter véhiculaires avec support d'infrastructure, dans le but de réduire les collisions et d'utiliser efficacement la bande passante.UMB est décomposé en deux phases : la première diffusion aux intersections pour disséminer les paquets dans toutes les directions, pour cela UMB utilise des répéteurs installés dans les intersections pour l'envoi des paquets vers tous les segments. On suppose que chaque véhicule est équipé par un récepteur GPS (Global Position System) et une carte routière électronique. Le principal avantage du protocole UMB est la fiabilité de diffusion multi-saut dans les canaux urbains

La deuxième appelée diffusion directionnelle, où le véhicule source sélectionne un nœud dans la direction de diffusion pour faire un relayage de données sans aucune information sur la topologie. [42].

c. **Le protocole GyTAR** (improved Greedy Traffic-Aware Routing protocol): est un protocole de routage géographique basé sur la localisation (position) et adapté aux réseaux véhiculaires capable de trouver des chemins robustes dans un environnement urbain. L'objectif de ce protocole est de router les données de proche en proche en considérant les différents facteurs spécifiques à ce genre d'environnements/réseaux.

   GyTAR c'est protocole suppose que chaque véhicule connaît sa position courante et ceci grâce au GPS. De plus un nœud source est sensé connaître la position du destinataire pour pouvoir prendre des décisions de routage, cette information est donnée par un service de localisation tel que GLS (Grid Location Service) et peut déterminer la position des intersections voisines à travers des cartes numériques [40].

d. **Le protocole VADD**(*Vehicle-Assisted Data Delivery*) est un protocole de routage qui prend en considération le contexte des réseaux de véhicules et exploite le mouvement prévisible des véhicules pour décider de retransmettre ou non le message.

VADD utilise particulièrement les informations sur le trafic routier au niveau d'une route pour estimer le délai mis par un paquet pour parcourir un tel segment. Par conséquent, les paquets seront achemines le long d'un chemin ayant le plus faible délai de bout en bout [41] .

e. **Le protocole MORA**

Le protocole de routage MORA (*MOvement-based Routing Algorithm*) propose dans [43] [44] exploite la position et la direction de mouvement de véhicules pour adapter les décisions de retransmission au contexte des véhicules et faire face ainsi a la forte mobilité des nœuds et au changement assez fréquent de la topologie

f. **Le protocole GPSR**

Le protocole de routage GPSR (Greedy Perimeter Stateless Routing) est donc un protocole de routage basé sur la position, qui contient deux parties. La première correspond à une méthode de choix du prochain noud transmetteur qui aura le rôle de retransmettre les paquets, et cela tout en se basant sur les informations de position des voisins (nouds candidats) et de la destination des paquets. Cette méthode consiste à choisir le candidat qui est à une distance la plus proche à vol d'oiseau de la destination. La deuxième partie de GPSR est en fait une méthode pour contourner les obstacles et les zones géographiques vides, qui ne présentent aucun candidat transmetteur dans le voisinage [45].

8. Menaces

Le manque de contrôle de sécurité des réseaux ad-hoc augmente le risque d'attaques qui peuvent être orchestrées par des nœuds externes ou internes en tenant compte du positionnement du nœud malhonnête par rapport au réseau [12].

- Les attaquants externes sont des nœuds qui ne font pas partie du réseau.
- Les attaquants internes sont des nœuds faisant légitimement partie du réseau.

Quelque soit sa position (interne ou externe), le nœud malhonnête utilise plusieurs techniques pour perturber le bon fonctionnement du réseau. La combinaison de ces techniques peut aboutir à une attaque plus élaborée. Ces techniques sont présentées ci-après:

- Rejeu de messages: l'attaquant enregistre une séquence de trafic qu'il réinjecte ensuite dans le réseau.
- Modification de messages: l'attaquant modifie un ou plusieurs champs du message avant de le retransmettre.
- Suppression de messages: l'attaquant supprime des messages.
- Fabrication de messages: l'attaquant fabrique un message et l'injecte dans le réseau.

Les attaques que l'on peut observer sur les réseaux VANET sont : des attaques de blocage de la circulation, attaque de mensonge sur les informations transmises, les attaques de déni de service, les attaques de mascarade, attaque de vol d'identité, attaque d'illusion, attaque sur les équipements de communication …etc. [17].

9. Sécurité de l'application d'alerte de danger local

L'application d'alerte de danger local base ses alertes sur les informations collectées par les capteurs locaux a chaque véhicule. Un véhicule pourra ainsi alerter d'un danger (obstacle, accident, etc.). La sécurité d'un tel système est primordiale, car une information erronée ou falsifiée peut entrainer une de gradation de la sécurité routière. Dans un système hautement dynamique, a forte densité de véhicules, comme les réseaux véhiculaires, les mécanismes de sécurité conventionnels comme la signature numérique et l'équipement robuste ne sont pas suffisants. En effet, ces mécanismes visent a assurer qu'un attaquant ne puisse manipuler le réseau ou une partie du véhicule. Ces protections n'étant pas infaillibles, il existe toujours une possibilité de manipulation. Comme les alertes sont générées a partir de la lecture des capteurs locaux, un attaquant peut détourner le processus de détection en altérant l'environnement physique du capteur. Ainsi, une fausse alerte peut être générée et diffusée. Les protections cryptographiques ne vérifient pas la sémantique de l'information. Une manipulation d'un capteur peut donc entrainer une alerte parfaitement signée et certifiée. C'est pourquoi une approche de vérification de plausibilité de l'information est proposée.
Le mécanisme de vérification de plausibilité peut intervenir a deux niveaux :
- durant le processus de détection (en vérifiant la plausibilité de l'information lue par le capteur)
- durant le processus de décision (en évaluant la plausibilité de l'information reçue)

Si l'attaquant contrôle l'ensemble du véhicule, alors le processus de détection est inutile. Cette solution semble toute fois plus intéressante pour détecter les défaillances matérielles. En effet, supposons qu'un véhicule équipe de trois capteurs de température extérieure reçoit les valeurs +30°C, +29°C, 0°C. Le véhicule détectera, par le biais d'un mécanisme de vote majoritaire, que le capteur n°3 est défaillant et ne l'utilisera plus jusqu' a la prochaine révision du véhicule. Le processus de détection est aussi intéressant pour déceler la manipulation partielle du véhicule. Si l'OBU détecte l'envoi d'un message indiquant une vitesse nulle et que les capteurs des roues et de vitesse annoncent une vitesse différente d'au moins 2 km/h (chaque équipement admet une incertitude relative qui lui est propre), alors le véhicule aura une suspicion de manipulation malveillante et décidera d'envoyer ou non le message concerne. Comme notre contexte considère le pire cas ou l'attaquant a le contrôle total du véhicule, nous nous intéressons au deuxième niveau qu'est le processus de décision. Cette solution permet d'évaluer la plausibilité de l'information en recoupant l'information avec de multiples sources (voisinage, réputation, capteurs, etc.). Par exemple, sur une route a deux voies a double sens, un véhicule reçoit une alerte indiquant une route barrée. Si le véhicule capte dans son voisinage un autre véhicule arrivant dans le sens oppose et qu'il ne détecte pas de freinage devant lui, alors il mettra en doute l'alerte. Notre but est donc de protéger le processus de décision contre les attaques, notamment l'injection de fausses informations qui peut avoir de graves conséquences.[24]

10. . Modèles d'attaquant

Afin de mieux cerner les attaques possibles sur un réseau véhiculaire, il est nécessaire de définir les modèles d'attaquant possibles. Ainsi, nous pourrons déterminer les mécanismes pouvant répondra la sécurisation des réseaux véhiculaires.

- **Actif ou Passif**: Un attaquant passif ne peut qu'écouter clandestinement le canal de transmission. Cette attaque peut être conduite par un voisinage curieux, mais aussi pour une entreprise qui cherche à créer des profils de conducteurs. Un attaquant actif peut générer, modifier, rejeter ou rejouer des messages afin de disséminer de fausses informations. Le but d'un attaquant actif est de s'octroyer des privilèges afin d'améliorer son environnement de conduite. Ainsi, il peut usurper l'identité d'un véhicule de secours pour faciliter son déplacement [18].
- **Interne ou Externe:** Un attaquant interne est un membre authentifie du réseau qui peut communiquer avec les autres membres du réseau. Comme il fait partie du réseau, il possède déjà quelques avantages comme les clés publiques utilisées par les autres véhicules. Un attaquant interne peut causer plus de dommages au réseau que l'attaquant externe qui a un accès limite au système [18].
- **Malicieux ou Rationnel**: Un attaquant malicieux cherche à prouver une capacité ou une réussite personnelle. Pour cela, il cherche à détecter des zones de vulnérabilité et à les exploiter pour perturber le système, ou blesser des membres du réseau. Des attaquants qui causent délibérément des accidents de la route sont considérés comme malicieux. Par conséquent, l'attaquant malicieux est prêt à tout pour arriver à ses fins quels que soient les couts et les conséquences. Par opposition, l'attaquant rationnel vise l'accomplissement

d'une tache spécifique sur le réseau en défaveur (ou en faveur) d'une personne identifiée. Les attaques rationnelles sont plus prévisibles que les attaques malicieuses [18].

- **Mal intentionné ou Involontaire :** Un attaquant est dit « mal intentionné » s'il vise délibérément à remettre en cause le bon fonctionnement du réseau. Ce type d'attaquant est à distinguer d'un attaquant involontaire qui peut par exemple lancer (sans le vouloir) une attaque à partir d'un capteur défectueux [18].
- **Indépendant ou Collaboratif**: Les attaquants peuvent agir indépendamment les uns des autres ou bien collaborer. Lorsqu'ils collaborent, les attaquants s'échangent des messages et coopèrent afin de rendre l'attaque plus efficace. Par exemple, des véhicules attaquants en collaboration annoncent un embouteillage fictif pour convaincre les véhicules honnêtes. Ces derniers vont alors changer de chemin, libérant ainsi la voie pour les attaquants [18].
- **Local ou Étendu :** Un attaquant peut avoir une portée d'action limitée, même s'il contrôle plusieurs entités (OBU ou RSU). On dit qu'il est local parce que la portée limitée des OBU et des RSU, rend l'attaque limitée. Un attaquant étendu contrôle plusieurs entités qui sont éparpillées sur le réseau, ce qui lui confère une portée étendue [18].

On peut reclasser les attaques de la manière suivante :

- **Attaque du trou noir** : Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est en suite de ne rien transférer, créant ainsi une sorte de puits ou « trou noir » dans le réseau.
- **Attaque du trou de ver** : Cette variante du trou noir consiste à réinjecter les paquets absorbés en un autre point (souvent distant) du réseau. Pour des distances plus longues que la couverture normale d'une transmission sans fil d'un hop, un attaquant peut s'arranger pour faire arriver ses paquets plus rapidement que par une route multi-hop. Il suffit pour lui d'utiliser un réseau externe câblé ou un transfert sans fil directionnel à forte puissance.
- **Attaque de l'identité multiple** : Cette attaque porte le nom anglais de « Sybil attaque ». Un nœud se fait passer pour plusieurs nœuds potentiellement distants, créant des incohérences dans les tables de routage des nœuds voisins.
- **Attaque par chantage :** Elle est connue sous le nom anglais de « Blackmailattack »[18]. Un nœud malicieux fait annoncer qu'un autre nœud légitime est malicieux pour éliminer ce dernier du réseau. Si le nœud malicieux arrive à attaquer un nombre important des nœuds, il pourra perturber le fonctionnement du réseau.
- **Attaque de l'inondation de HELLO** : De nombreux protocoles de routage utilisent des paquets « HELLO » pour découvrir les nœuds voisins et ainsi établir une topologie du réseau. La plus simple attaque pour un intrus consiste à envoyer un flot de tels messages pour inonder le réseau et empêcher d'autres messages d'être échangés. De plus, s'il parvient à émettre à une portée suffisante, des nœuds distants vont ajouter l'intrus comme nœud voisin dans leurs routes et fausser ainsi complètement le routage de l'information dans le réseau.
- **Brouillage radio :** Il consiste à perturber le canal radio en envoyant des informations inutiles sur la bande de fréquences utilisées. Ce brouillage peut être temporaire,

intermittent ou permanent. De même, son champ d'action doit être pris en compte ; son effet est-il limité à quelques nœuds ou est-il suffisamment puissant pour bloquer le réseau tout entier ?

- **Privation de mise en veille** : Elle a pour but de consommer toutes les ressources de la victime en l'obligeant à effectuer des calculs ou à recevoir ou transmettre des données inutilement.

L'attaque délibérée ou non d'un VANET repose sur un but précis. Nous dressons une liste des attaques évidentes ou faisables et qui constituent un risque non négligeable en cas de réalisation. En raison de l'impossibilité d'envisager, toutes les attaques possibles dans les réseaux véhiculaires, nous nous limitons aux exemples les plus significatifs dans contexte suivant :

✓ **Attaque sur la vie privée :** Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou des informations personnelles d'un utilisateur du réseau. Cela peut également se traduire par tracer l'activité et les déplacements de cet utilisateur. Pour identifier et tracer une victime, l'attaquant peut utiliser toute chaine de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaine de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat, etc. Au-delà des chaines de caractères, l'empreinte radio de la victime peut également t'être utilisée: on parle alors d'attaque de la couche physique [19].

D'après les modèles d'attaque, l'attaquant peut être Interne ou Externe, Mal intentionné, Passif et Indépendant.

✓ **Attaque sur la cohérence de l'information:** Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. L'intention de l'attaquant est d'altérer la perception qu'ont ses victimes des conditions de circulation (position, vitesse, direction). Ce faisant, l'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. Comme montre la figure-3, l'attaquant (M) diffuse des informations de trafic erronées amenant les victimes A et B a changer de voie. Dans cette attaque, l'attaque est Interne ou Externe, Intentionnelle, Active et Indépendante.[19]

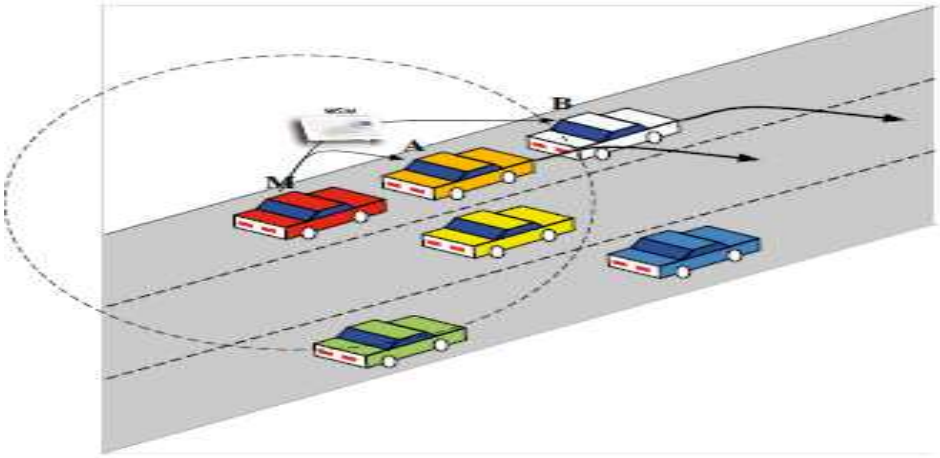

Figure 3 : Attaque sur l'incohérence de l'information

- ✓ **Usurpation d'identité ou de rôle :** Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Figure-4 illustre le cas où l'attaquant M usurpe l'identité du véhicule A pour récupérer des données du véhicule B. L'attaquant peut être Interne ou Externe, Malicieux ou Rationnel, Mal intentionné, Actif et Indépendant [19].

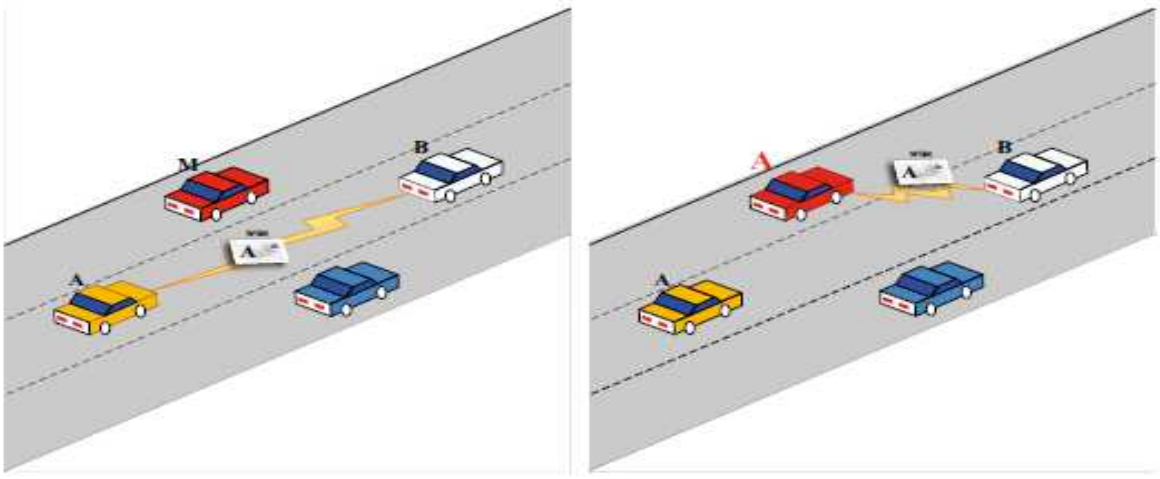

Figure 4. Usurpation d'identité ou de rôle

- ✓ **Déni de service :** Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau. Ce type d'attaque peut être généré en brouillant le canal radio, en surchargeant ou en épuisant les ressources du réseau par des requêtes abondantes, en exploitant la vulnérabilité des protocoles, ou en ayant une attitude non coopérative (refus de relayer des paquets par exemple). La Figure-5 illustre que l'attaquant M empêche l'échange de messages critiques entre le véhicule accidente B et le véhicule A.L'attaquant peut être Interne ou Externe, Mal intentionné, Actif et Indépendant.

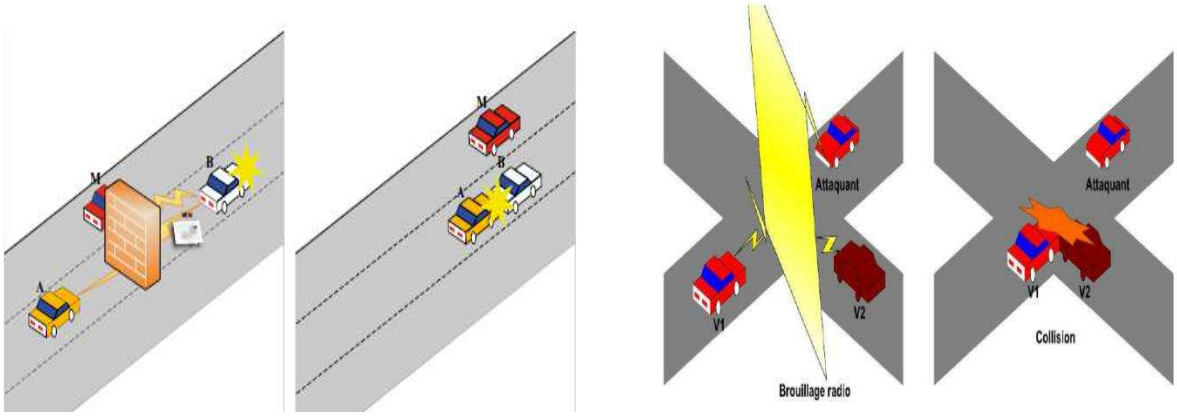

Figure 5 : Attaque Déni de service **[21]**

- ✓ **Écoute clandestine du réseau:** pour cette attaque, l'entité malveillante collecte les données transmises dans le réseau afin d'en extraire une information dont elle pourrait tirer profit. Un exemple d'attaque est un attaquant qui espionne une transaction commerciale, typiquement un paiement électronique à un péage, en vue d'en extraire les informations bancaires. L'attaquant peut être Interne ou Externe, Mal intentionné, Passif et Indépendant [19].

- ✓ **Véhicule caché :** C'est un exemple de falsification des informations de positionnement, et une variante du ≪ Sybil attaque≫. Dans le protocole de distribution des messages d'alerte, si un véhicule diffusant l'alerte détecte un voisin mieux positionné que lui pour diffuser, alors il arrête d'émettre. Ce protocole permet de réduire la congestion du canal radio. La Figure-6 illustre cette attaque. L'attaquant M fait donc croire qu'il est en meilleure position (M') afin d'être le seul à émettre l'alerte. Mais il ne va pas diffuser l'information d'alerte, rendant le véhicule en danger B (cache) des autres véhicules (A)[19].

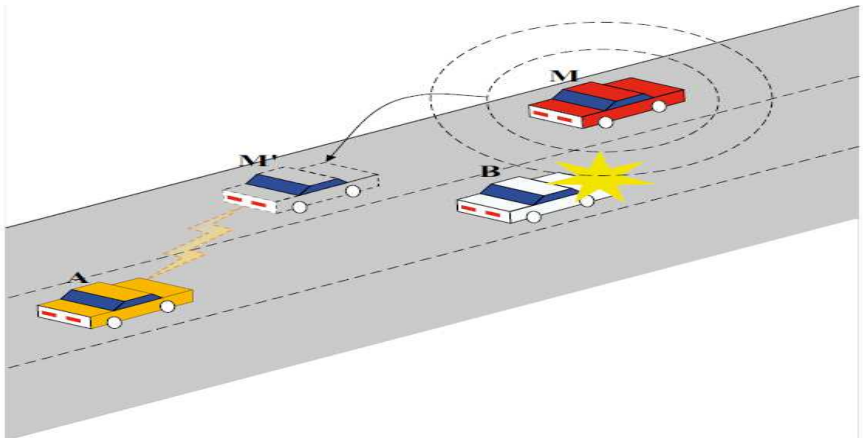

Figure6 : Attaque du véhicule cache

- ✓ **Tunnel :** Comme le signal GPS connait des pertes (dans un tunnel ou dans certaines zonesperturbatrices), un attaquant peut exploiter cette perte de positionnement temporaire. En effet, il peut envoyer de fausses données de la sortie du ≪ tunnel ≫ avant que le véhicule victime ne reçoive une mise à jour de position authentique [19].

- ✓ **Wormhole :** Un attaquant qui contrôle plusieurs entités s éloignées, peut établir un tunnel entre ces entités et peut ainsi injecter des données d'un endroit à l'autre. Il diffuse ainsi des informations erronées (mais signées) à divers endroits. C'est un example d'attaque étendue [19].

- ✓ **L'injection des messages erronés**: dans cette attaque, l'entité malveillante crée des messages contenant des informations erronées afin de causer un accident ou de rediriger le trafic routier de manière permettant la libération de la route utilisée (voir Figure 7).

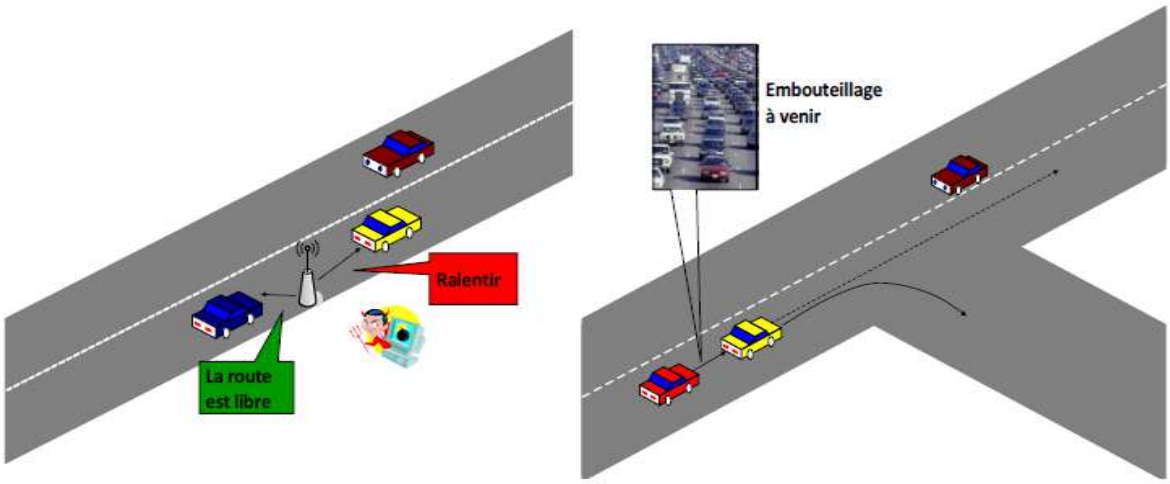

Figure 7 : Attaques par l'envoi de messages falsifiés [20]

- ✓ **La révélation d'identité et de position géographique des autres véhicules:** dans cette attaque, l'entité malveillante collecte des informations sur les transmissions radio effectuées par le véhicule victime afin de surveiller sa trajectoire (Figure 8). L'utilité de cette attaque est diverse et dépend de l'entité collectant ces informations (il peut être par exemple une entreprise de location de voitures qui veut suivre ses propres véhicules de manière illégitime).

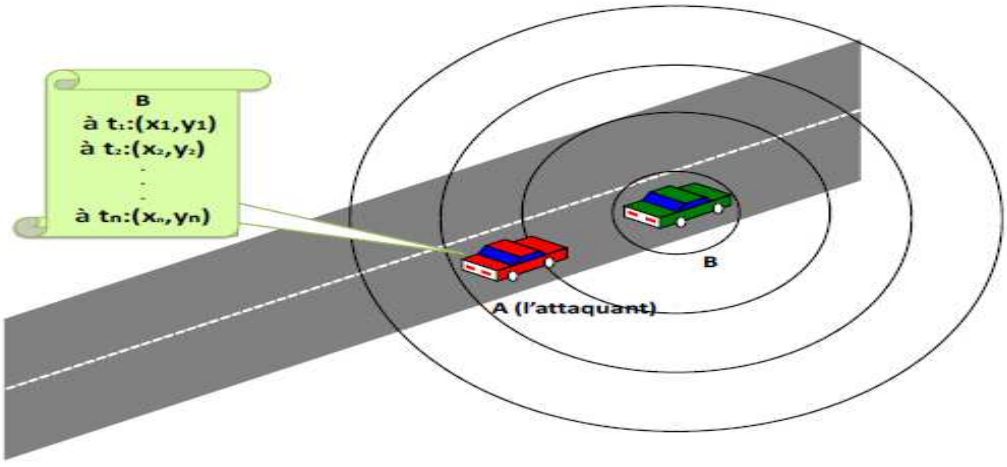

Figure8: Attaquederévélationd'identitéetdepositiongéographiqued'unvéhicule [21]

11. Mécanismes de la sécurité

- **Les certificats**

Parmi les résultats des algorithmes de la cryptographie, on trouve les certificats, qui permettent d'augmenter le degré de la sécurité dans les réseaux VANET. Chaque véhicule possède un seul certificat à long terme, qui contient l'identité et les caractéristiques du véhicule. Il se charge principalement de renouveler les certificats à court terme. Ainsi, le véhicule possède donc plusieurs certificats à court terme, qui contiennent un identifiant virtuel et des pseudonymes de communication. Les certificats doivent permettre la préservation de la vie privée et l'anonymat du véhicule [23].

- **Le hachage**

Le hachage consiste à déterminer une information de taille fixe et réduite appelée «L'empreinte ou le condensé » à partir d'une chaine de données fournit en entrée, de différentes tailles plus longues. Les fonctions de hachage à sens unique sont les plus utilisées. La particularité de cette fonction est qu'il est très facile de calculer et d'extraire une empreinte de n'importe quelle chaine donnée, mais très difficile, voire impossible, de retrouver la chaine initiale à partir de l'empreinte. C'est une fonction irréversible [24].

- **La signature numérique**

La signature numérique est un code (une donnée) numérique, associé à un message afin de permettre aux destinataires de vérifier son authenticité et ainsi prouver son intégrité. Elle est implémentée et obtenue avec des fonctions de hachage en utilisant la clé privée de la source du message (l'expéditeur) appelée aussi signataire du message.

- **La technique MAC**

L'un des mécanismes de base de la sécurité dans les réseaux VANETs est la technique MAC (Message Authentification Code). Elle assure la même fonctionnalité que la signature numérique. C'est un code qui accompagne les données. Il est implémenté en utilisant la clé secrète de la cryptographie avec des fonctions similaires à celle de hachage. Il assure principalement l'authentification des messages dans le réseau [23].

- **Le dispositif TPD**

Le TPD (Tamper-Proof Device) est un dispositif composé de matériels et logiciels qui contiennent plusieurs capteurs, de hautes performances, qui permettent de détruire automatiquement les informations stockées, après chaque manipulation du matériel. Son mécanisme permet de stocker et garder en secret les données liées à la confidentialité du véhicule, comme les certificats et les pseudonymes privés. Ainsi il se charge de la signature de tous les messages envoyés par le véhicule [23].

- **La cryptographie**

La cryptographie est la technologie utilisée pour la protection des données transmises, qui contiennent les messages des différentes communications. La cryptographie utilise principalement des clés et des codes secrets pour crypter (coder) le contenu d'un message à l'aide d'un algorithme de chiffrement, pour le rendre illisible et donc inexploitable par les entités malveillantes. Pour rendre un message crypté lisible, les entités destinataires disposent d'une clé (code) et d'algorithmes de déchiffrement appropriés pour décrypter le message et rendre son contenu lisible et utilisable. Il existe deux types de cryptographies : cryptographie symétrique et asymétrique.

12.. Exigences de performance

Afin d'assurer les communications de sécurité routière dans les VANETs, les exigences applicatives doivent être prises en compte, et les exigences de sécurité satisfaites. Les protocoles de communication sécurisée utilises par les applications de sécurité du trafic routier sont conçus afin de satisfaire ces exigences. En dehors des exigences de sécurité, il est essentiel qu'ils répondent aussi aux exigences de performance, sans quoi ils ne seront pas applicables dans le contexte routier. Dans les VANETs, les conditions environnementales impactent la fiabilité, la latence et l'efficacité du canal radio. Ces conditions sont par exemple la vitesse, la densité du trafic réseau ou la porte de transmission. La densité du trafic réseau dépend de la fréquence d'envoi des messages, de la taille des messages et de la densité du trafic routier. Il est donc important de bien choisir ces paramètres. Par exemple, si un message d'alerte arrive âpres que le conducteur l'a déjà détecte par lui-même (délai d'envoi supérieur a 700 ms), alors le conducteur ne fera plus confiance au système. Dans les protocoles utilises, d'autres paramètres influencent la taille du message et le délai de communication la taille des informations cryptographiques (clé, certificat, signature, hachage, etc.) et le temps nécessaire au processus d'authentification.

Dans notre contexte d'applications sensibles au délai, le cout de la sécurité doit être maitrise. Nous nous intéressons donc a la fréquence d'appel des services de sécurité. La signature numérique, le hachage, la vérification des certificats sont des exemples de services proactifs appelés pour chaque message transmis. Sachant qu'un message (beacon) est émis toutes les 100 millisecondes, nous comprenons l'impact que peut avoir un mécanisme consommateur (en temps et en calcul). A contrario, la gestion des pseudonymes, la distribution des clés, des certificats et des listes de révocation, sont des exemples de services de sécurité proactifs appelés moins fréquemment (de l'ordre de la minute dans le pire des cas).

Le cout de la sécurité est donc la somme des couts des mécanismes proactifs et des mécanismes réactifs. A partir de ce constat, nous nous intéressons aux services de sécurité proactifs, et plus particulièrement a l'authentification. En effet, les services a forte fréquence ont besoin d'être les plus économes en temps possible. La génération et la vérification de signature numérique sont appelées pour chaque message émis dans le VANET. Il est donc primordial de comprendre l'impact de ces mécanismes sur les performances des applications.

De plus, grâce à l'application LDW, un conducteur peut anticiper un freinage d'urgence [25].

13.. Conclusion

Les réseaux VANETs sont vulnérables aux attaques menaçant la vie de leurs usagers et les biens si des mécanismes appropriés n'ont pas été mis en œuvre. Les techniques cryptographiques existant peuvent apporter des solutions aux objectifs de l'authentification, l'intégrité et la non-répudiation, mais la disponibilité est difficile à assurer car les attaques peuvent la viser au niveau des différentes couches de la pile protocolaire. L'objectif de la confidentialité ne peut être assuré qu'au détriment de la sécurité et de la performance du système de communication dans les VANET.

Sommaire

1. Introduction

L'objectif principal de simulateur VANETsim est de soutenir les chercheurs dans le domaine de la sécurité VANET. L'architecture de VANETsim fournit un moyen simple de composer plusieurs concepts de sécurité existants ainsi que mettre en œuvre de nouveaux. Les modules de sécurité et de confidentialité sont exécutés par des nœuds (véhicules) eux-mêmes ou font partie de l'infrastructure sur la carte. Ce simulateur est clairement structuré. Nous avons implémenté sous le simulateur VANETsim un concept de sécurité qui permet aux véhicules le changement de ces pseudonymes.

2. Présentation le simulateur Vanetsim

VANETsim est un simulateur pour des concepts de sécurité et de confidentialité dans VANETs. Ayant comme caractéristiques:

- **Independence de la plateforme :**Le VANETsim est développé en Java 6.Il peut être exécuté sur la plupart des systèmes d'exploitation et plateformes matérielles.
- **Scénario complet et éditeur de carte :** Le puissant éditeur intégré facilite la création et l'altération des cartes ainsi que la créationet la configuration des scénarios et des pistes de simulation.
- **Sécurité :** avec son accent sur la sécurité du VANET-Sim offre aux utilisateurs un moyen rapide et facile de vérifier leurs concepts de sécurité.
- **Extensibilité :** la structure du code source prend en charge l'adaptation facile et l'extension des fonctionnalités.
- **Plans réalistes :**Vanet-sim a une interface pour importer des cartes du « open-street-map projet ». Ainsi, la simulation du trafic sur de véritables réseaux routiers est prise en charge.
- **L'intégration des technologies d'amélioration de la vie privée :** quatre techniques sont implémenté pour améliorer la vie privée dans les réseaux véhiculaires (pro-zone,mix-zone, les périodes de silence sont mis en œuvre).
- **Micro simulation :**Chaque véhicule est simulé individuellement et prend des décisions sur son propre afin que le trafic routier soit simulé aussi réaliste que possible.

3. Création d'une simulation

Le réseau routier est modélisé avec une structure de données de type graphique composée de nœuds tel que les intersections et les routes (voir le modèle utilisé par OpenStreetMap [31]).

VANETsim prend en charge les deux, l'importation de cartes de villes réelles afin d'étudier le comportement réel d'une technique, ainsi que la création de réseaux routiers à partir de zéro afin de provoquer des situations particulières de circulation ou de vérifier les résultats

analytiques. Nous avons choisi de travailler avec des cartes d'OpenStreetMap [31], en raison de la grande quantité de matériel de haute qualité librement disponible.

- **Visualisation :** une interface utilisateur graphique permet une visualisation détaillée de la simulation fonctionne avec beaucoup d'éléments d'information pertinents. Une interface de ligne de commande pour la simulation haute performance est également disponible.
- **Création de Map ou carte :** Pour obtenir suffisamment de carte frais de rue (nom, type, Une manière, vitesse, couleur) ou télécharger une carte avec OpenStreetMap (http://www.openstreetmap.org).

Exemple:

```
<Street>
        <Name>Plastine</Name>
                        <StartNode>
                                <x>76320</x>
                                <y>230254</y>
                                <trafficSignal>false</trafficSignal>
                        </StartNode>
                        <EndNode>
                                <x>76979</x>
                                <y>230069</y>
                                <trafficSignal>false</trafficSignal>
                        </EndNode>
                        <Oneway>false</Oneway>
                        <StreetType>service</StreetType>
                        <Lanes>1</Lanes>
                        <Speed>277</Speed>
                        <Color>-1</Color>
                </Street>
```

- **Création d'un scénario**

1 **Véhicule :** Chaque véhicule suit une trajectoire aléatoire de sa création à son arrivée, il dispose d'un ensemble d'attributs qui lui identifie (vitesse, temps départ, temps d'arrivé, nœuds de départ, nœud d'arrivée).

Exemple

```
<Vehicle>
<VehicleLength>600</VehicleLength>
```

<MaxSpeed>3533</MaxSpeed>
<MaxCommDist>10000</MaxCommDist>
<Wifi>true</Wifi>
<emergencyVehicle>false</emergencyVehicle>
<braking_rate>800</braking_rate>
<acceleration_rate>300</acceleration_rate>
<timeDistance>109</timeDistance>
<politeness>12</politeness>
<Color>-16777216</Color>
<isAttacker>false</isAttacker>
<isAttacked>false</isAttacked>
<Destinations>
<WayPoint>
<x>17627</x>
<y>261960</y>
<wait>10</wait>
</WayPoint>
<WayPoint>
<x>406140</x>
<y>109377</y>
<wait>10</wait>
</WayPoint>
</Destinations>
</Vehicle>

2 **Ajouter un attaquant :** sélectionner « attacked » et « attecker ».

3 **Event:** ajouter un évenement“start Blocking” et “stop Blocking”.

4 **Ajouter traffic light** …

4. L'onglet de simulation

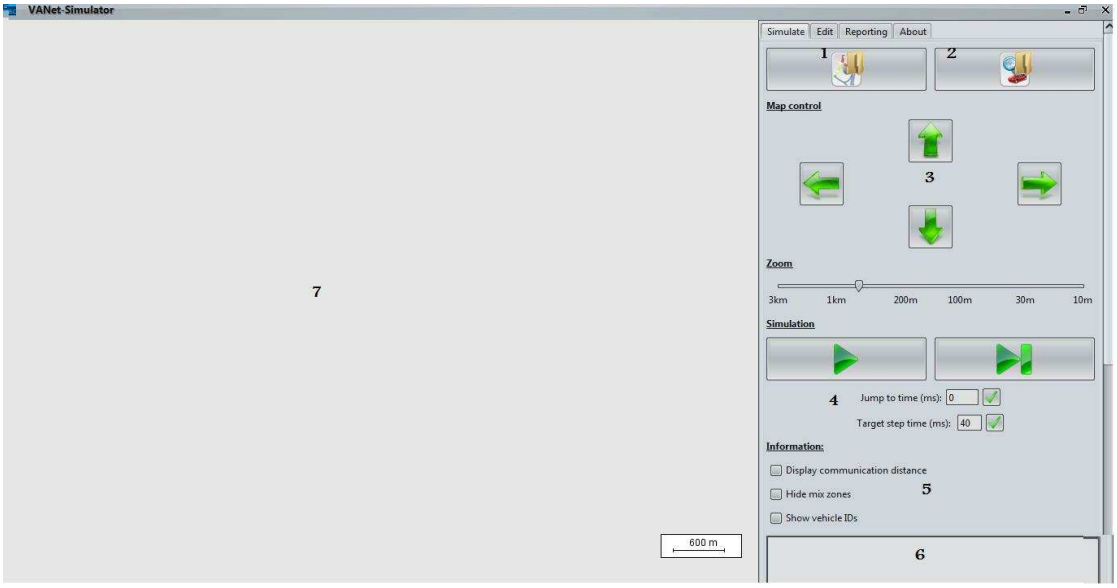

Figure 9 : fenêtre principale

- **1-** Ouvrir une carte VANET-Simulator (transformé à partir d'un planouvert dans le mode d'édition)

- **2-** Utilisez ce bouton pour ouvrir un fichier de scénario qui contient des informations sur les véhicules, mix-zones …

- **3-**Utilisez ces boutons pour naviguer sur la carte

- **4-**Utilisez ces boutons pour démarrer, mettre en pause des simulations ou sauter à un moment précis.

- **5-**Utiliser ces cases pour afficher des informations supplémentaires comme ids de véhicules, mix-zones et le rayon wifi

- **6-**Cette fenêtre fournit des informations supplémentaires des véhicules rues und marqués sur la carte

- **7** Affichage de la simulation

Un simpleClic sur le bouton 1 pour choisir répertoire et sélectionner le fichier .xml (Map.xml) et sur le bouton 2 pour choisir répertoire et sélectionner le fichier .xml (scénario.xml).
La figure 10 donne un aperçu de simulation d'un scénario

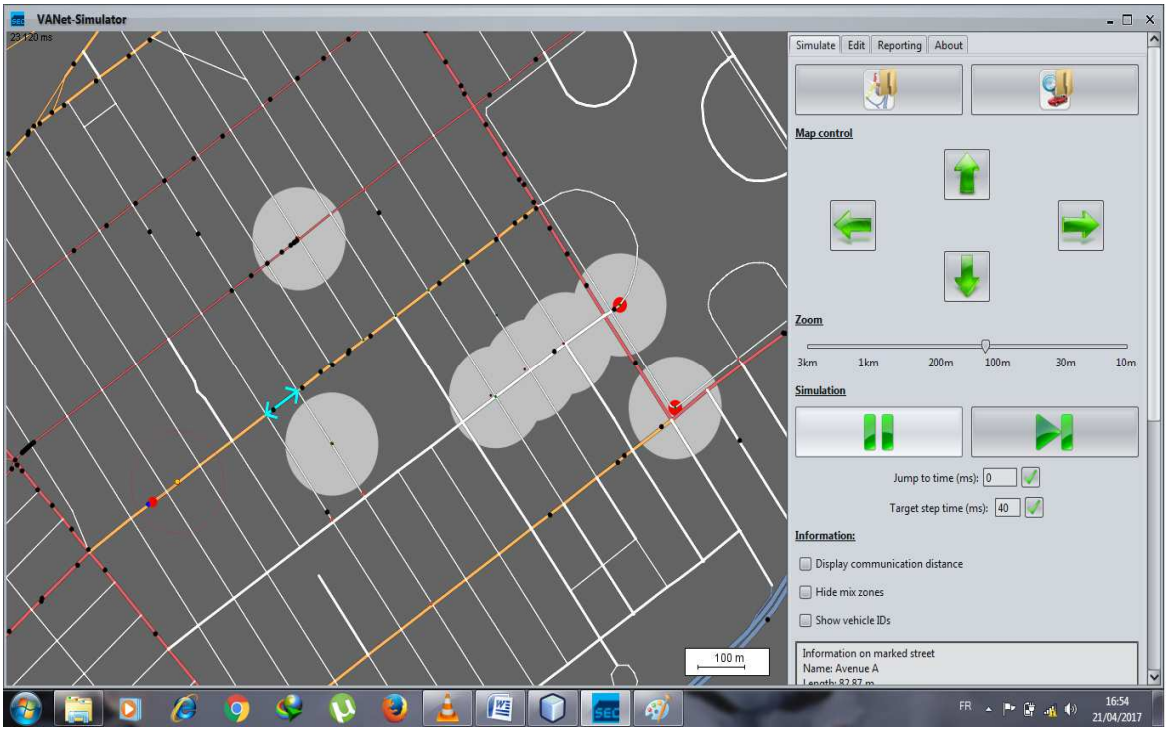

Figure 10 : aperçu de simulation en cours

Une fois qu'un véhicule entre dans une zone de mixage, il s'arrête de diffuser des balises et de passer à un nouveau pseudonyme afin de garantir la non-accessibilité. Du point de vue de l'adversaire, la Zone Mix est une boîte noire. Il ne peut enregistrer que les véhicules entrant et quittant une zone de mélange et lireles pseudonymes respectifs (En gris).
Les cercles rouges indiquent des entrées instables, en raison de l'insuffisance du trafic de couverture de véhicule ou des routes prévisibles, l'adversaire pourrait établir une association entre les pseudonymes utilisés par les véhicules avant d'entrer et après avoir quitté ‘mix-zone’. Cette visualisation permet de déterminer dans quels scénarios de Mix-Zones sont adaptées et quand préfèrent d'autres concepts pour la protection de la vie privée.

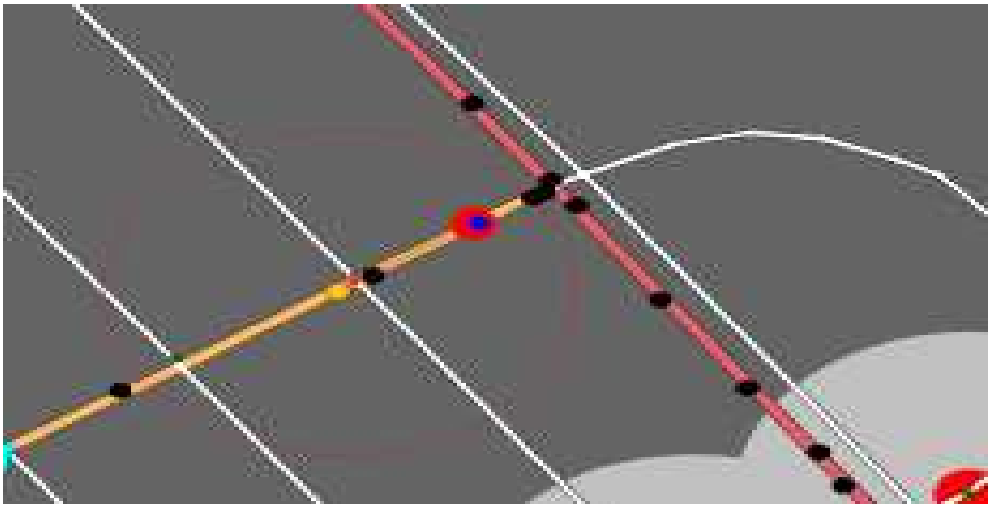

Figure 11 : Ajouter d’une attaque

Le simulateur Vanetsim, nous permet d'ajouter une attaque interne passive (un nœud attaquant et un nœud victime). Dans la figure 11, on voit des nœuds noirs et un nœud bleu (nœud victime) et un nœud jaune (attaquant).
L'objectif de cette attaque est que l'attaquant suive un nœud victime

Le simulateur Vanetsim permet de récupérer toute les informations d'une voiture et une route par exemple (Nom_route, Nom_véhicule, position, vitesse, point_départ…). Aprèsle lancement de simulation, il suffit de cliquer sur un véhicule ou une route pour afficher ces informationsdans la partie droite de la fenêtre (voir la Figure12).

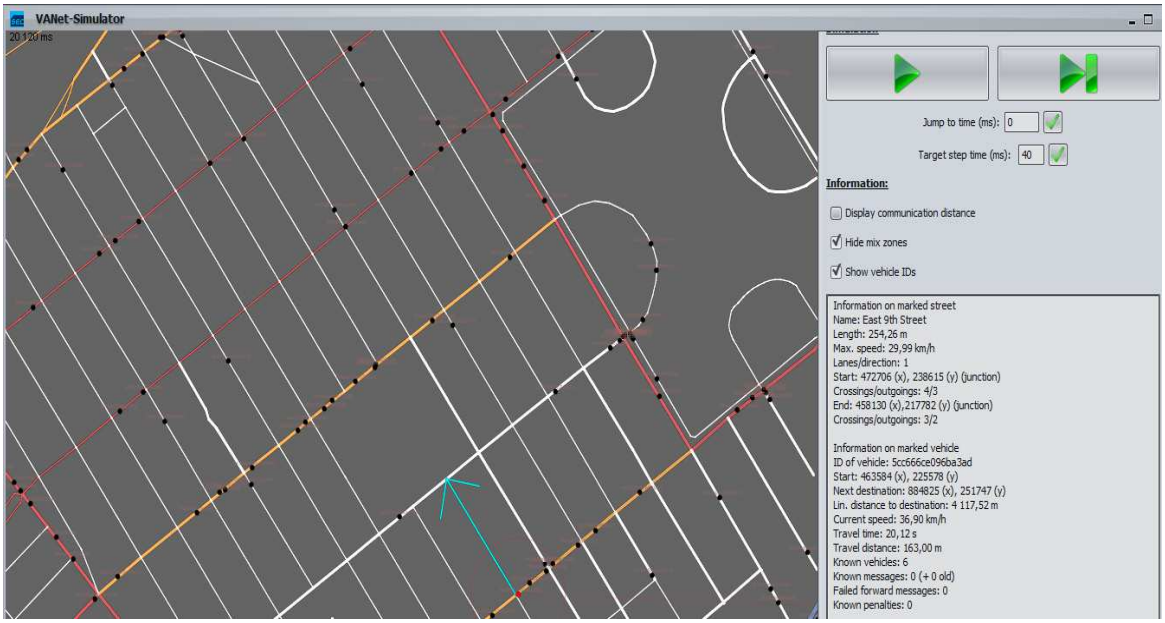

Figure 12 : Affichage des informations d'un véhicule ou une route

Comme les messages spéciaux dans VANET peuvent divulguer des données telles que l'ID, la vitesse, l'accélération et l'emplacement à d'autres véhicules, des problèmes de confidentialité surviennent. Les modules de confidentialité de VANETsim contiennent des implémentations prêtes à l'emploi d'un certain nombre de concepts de confidentialité compatibles avec le véhicule, SilentPeriods [50],ainsi que des concepts de confidentialité basés sur l'infrastructure : Mix Zones [49] et Pro-Mix [48].

Dans le cadre de notre travail, nous avons implémenté le concept SLOW proposé par L. Buttyn et al.[], leschéma de changement de pseudonyme pratique pour la confidentialité de la localisation dans les VANET.

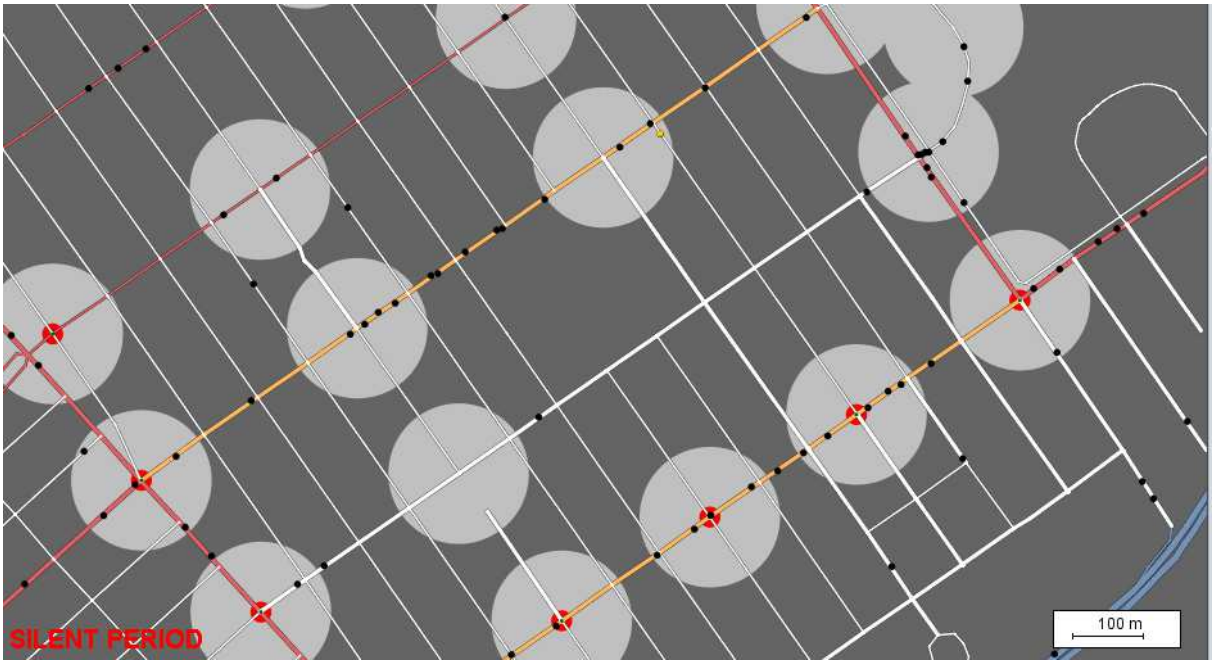

Figure 13: aperçu de simulation Au moment de silence période

Dans les périodes de silence, tous les véhicules arrêtent de manière synchrone l'envoi de messages (pour un intervalle de temps spécifique).

Dans les zones mixtes, le silence radio (ou la communication chiffrée dans le cas de Pro-Mix) est lié à un emplacement spécifique (par exemple, une jonction). Dans SLOW, un véhicule entre dans le silence de la radio lorsque vous conduisez moins d'une vitesse prédéfinie (par exemple, 30 km / h).

5. Implémentation de la solution proposée

Le concept de sécurité « Slow » est un type de sécurité permet d'assurer le changement des ID des voitures dans chaque 3000 ms.
La section suivante présente le code source en java de la méthode SLOW intégré en VANETsim.

```
public class SlowPanelextendsJPanelimplementsActionListener, FocusListener{

/** La constante nécessaire pour la sérialisation.*/
        private static final long serialVersionUID = -8294786435746799533L;

        /** CheckBoxChoisirsiSlow-ModelI are enabled */
        private final JCheckBoxenableSlow_;

        /** JLabeldécrireenableSlow_ checkbox */
        private final JLabelenableSlowLabel_;

        /** Le champ de saisie pour le temps min jusqu'à ce qu'un pseudonyme soit changé */
```

```
	private final JFormattedTextFieldtimeToPseudonymChange_;

	/** JLabeldecriretimeToPseudonymChange_ textfield */
	private final JLabeltimeToPseudonymChangeLabel_;

	/** The input field for the speed limit for the slow modell */
	private final JFormattedTextFieldslowSpeedLimit_;

	/** JLabel to describe slowSpeedLimit_ textfield */
	private final JLabelslowSpeedLimitLabel_;

	/**
	 * Constructor, creating GUI items.
	 */
	publicSlowPanel(){
		setLayout(new GridBagLayout());

		// global layout settings
		GridBagConstraints c = new GridBagConstraints();
		c.fill = GridBagConstraints.BOTH;
		c.anchor = GridBagConstraints.PAGE_START;
		c.weightx = 0.5;
		c.gridx = 0;
		c.gridy = 0;
		c.gridheight = 1;
		c.gridwidth = 2;
		c.gridwidth = 1;
		c.insets = new Insets(5,5,5,5);

		c.gridx = 0;
		timeToPseudonymChangeLabel_ = new JLabel(Messages.getString("" ));
timeToPseudonymChangeLabel_.setText("Time to pseudonym Change");
		++c.gridy;
		add(timeToPseudonymChangeLabel_,c);
		timeToPseudonymChange_ = new
JFormattedTextField(NumberFormat.getIntegerInstance());
		timeToPseudonymChange_.setValue(3000);

		timeToPseudonymChange_.setPreferredSize(new Dimension(60,20));
		c.gridx = 1;
		timeToPseudonymChange_.addFocusListener(this);
		add(timeToPseudonymChange_,c);

		c.gridx = 0;
		slowSpeedLimitLabel_ = new JLabel(Messages.getString("SlowPanel.speedLimit"));


		++c.gridy;
		add(slowSpeedLimitLabel_,c);
slowSpeedLimitLabel_.setText("speedLimit"); //$NON-NLS-1$

		slowSpeedLimit_ = new JFormattedTextField(NumberFormat.getIntegerInstance());
```

```
                slowSpeedLimit_.setValue(30);

                slowSpeedLimit_.setPreferredSize(new Dimension(60,20));
                c.gridx = 1;
                slowSpeedLimit_.addFocusListener(this);
                add(slowSpeedLimit_,c);

                c.gridx = 0;
                enableSlowLabel_ = new JLabel(Messages.getString("SlowPanel.enable"));
enableSlowLabel_.setText("Enabel Slow");
                ++c.gridy;
                add(enableSlowLabel_,c);
                enableSlow_ = new JCheckBox();
                enableSlow_.setSelected(false);
                enableSlow_.setActionCommand("enableSlow"); //$NON-NLS-1$
                c.gridx = 1;
                enableSlow_.addFocusListener(this);
                add(enableSlow_,c);
                enableSlow_.addActionListener(this);


                //to consume the rest of the space
                c.weighty = 1.0;
                ++c.gridy;
                JPanel space = new JPanel();
                space.setOpaque(false);
                add(space, c);
        }

        public void saveAttributes(){

        Vehicle.setTIME_TO_PSEUDONYM_CHANGE(((Number)timeToPseudonymChange_.getVal
ue()).intValue());

        Vehicle.setSLOW_SPEED_LIMIT((int)Math.round(((Number)slowSpeedLimit_.getValue()).intV
alue()  * (100000.0/3600)));
                Vehicle.setSlowOn(enableSlow_.isSelected());
        }

        public void loadAttributes(){

        timeToPseudonymChange_.setValue(Vehicle.getTIME_TO_PSEUDONYM_CHANGE());
                slowSpeedLimit_.setValue((int)Math.round(Vehicle.getSLOW_SPEED_LIMIT() /
(100000.0/3600)));
                enableSlow_.setSelected(Vehicle.isSlowOn());
        }

        }

        public static void writeSlowHeader(){
                PrivacyLogWriter.log("Slow speed limit:" + Vehicle.getSLOW_SPEED_LIMIT() +
":Time to pseudonym change:" + Vehicle.getTIME_TO_PSEUDONYM_CHANGE());
```

```
	}

	@Override
	public void focusGained(FocusEvent arg0) {
		// TODO Auto-generated method stub
		saveAttributes();
	}

	@Override
	public void focusLost(FocusEvent arg0) {
		// TODO Auto-generated method stub
		saveAttributes();
	}

	publicJCheckBoxgetEnableSlow_() {
		returnenableSlow_;
	}

	publicJFormattedTextFieldgetTimeToPseudonymChange_() {
		returntimeToPseudonymChange_;
	}
	publicJFormattedTextFieldgetSlowSpeedLimit_() {
		returnslowSpeedLimit_;
	}

}
```

6. Conclusion

Dans ce chapitre, nous avons présenté le simulateur Vanetsim et leurs caractéristiques, et nous avons présenté aussi l'implémentation de la méthode de sécurité « SLOW ». Ce schéma représente une période de silence à basse vitesse. Les véhicules dont la vitesse est inférieure à la valeur de seuil arrêtent la transmission de messages périodiques et ils commencent à modifier leurs pseudonymes.L'inconvénient d'un tel système est que, dans une zone très dense, il est possible que les véhicules se déplacent à très faible vitesse. Cela entraîne un changement de pseudonyme plus fréquent que prévu. Cela nécessite un grand nombre de pseudonymes, ce qui est pratiquement impossible.

Sommaire

Conclusion générale

Les systèmes de transport intelligent vont améliorer de façon significative le trajet des véhicules par l'accès instantané aux informations sur l'état des routes et aussi, leur permettre d'échanger entre eux des informations visant à rendre plus conviviale leurs trajets. Le fonctionnement de ces systèmes repose sur les réseaux véhiculaires sans fil.

Le réseau VANET est un type de réseau permet la communication entre les véhicules ainsi qu'avec les infrastructures de télécommunication. Il est une sous classe de réseau MANET où il est caractérisé par une forte mobilité des nœuds.

Dans le domaine des réseaux sans fil, le canal caractérisant la propagation de 1'onde électromagnétique dans 1'espace présente une importance distinctive. Ce qui est important, c'est la possibilité pour le récepteur de recevoir sans erreurs l'information que l'émetteur avait l'intention de lui transmettre.

Ces réseaux de véhicules ciblés par de nombreux dangers qui menacent la sécurité des usagers. Par conséquent, l'échange sécurisé des informations est indisponible dont les techniques cryptographiques sont utilisés pour assurer la confidentialité, l'authentification, l'intégrité (mais pas toujours dans certains cas), mais la disponibilité est difficile à assurer.

Responsable de l'envoi de messages entre les différents véhicules est le service du routage. Ces messages sont souvent acheminés avec un protocole de routage multi-sauts, ce qui donne lieu à la possibilité d'avoir plusieurs types d'attaque.

Dans notre projet de fin, nous avons essayé de créer un scénario sur simulateur Vanetsim et appliquer la solution SLOW pour empêcher l'attaque mais ce type de sécurité a l'inconvénient d'un tel système est que, dans une zone très dense, il est possible que les véhicules se déplacent à très faible vitesse. Cela entraîne un changement de pseudonyme plus fréquent que prévu. Cela nécessite un grand nombre de pseudonymes, ce qui est pratiquement impossible.