République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université Abderrahmane Mira Bejaïa
Faculté de Sciences Exactes
Département de recherche opérationnelle

Mémoire de master en mathématiques appliquées

Specialité : Recherche opérationnelle et aide à la décision

Option : Modélisation mathématique et évaluation des performances des réseaux

Détection des attaques par déni de services (DoS) dans les réseaux VANETs

Réalisé par :
M^{Mlle}. Talantikit Manel

Encadré par :
Pr. Boulfekhar Samra
(Univ. A.Mira Béjaia)

Soutenu le 03 Juillet 2023, devant le jury composé de :

Présidente	M^{me}. **Lekadir Ouiza**	**U. A.Mira Béjaïa**
Examinatrice	M^{me}. **Tassoult Nadia**	**U. A.Mira Béjaïa**
Examinateur	M. **Djabri Rabah**	**U. A.Mira Béjaïa**

Promotion : 2022/2023

Dédicace

Je dédie ce travail
À mes chers parents, pour leur soutien ; leur patience, leurs encouragements durant mon parcours scolaire.

À mes sœurs, pour leur patience, et leurs encouragements.

À mes amis, je souhaite exprimer ma reconnaissance pour leur présence dans ma vie.

À moi-même, en reconnaissance de mon travail acharné, de ma persévérance et de ma détermination à atteindre mes objectifs académiques.

[Manel].

Remerciements

”Besmi Allah” je remercie Dieu de m’avoir donné le courage et la volonté de travailler consciencieusement pour l’élaboration de ce modeste travail.
Mes remerciements s’adressent avant tout au Professeur S.BOULFEKHAR pour avoir accepté de diriger ce travail, pour son aide précieuse, ses remarques constructives, ses conseils, et son sérieux suivi dans la préparation de ce travail.
Je tiens aussi à remercier vivement l’ensemble des membres du jury pour avoir accepté de juger ce travail.
Evidemment, mes remerciements les plus chaleureux vont à mes chers parents pour leurs encouragements, leur patience et leur grand soutien durant toutes ces années d’études.
Enfin, je tiens à remercier tous mes amis pour leur soutien moral tout au long de la réalisation de mon humble projet.

Table des matières

Table des figures

Liste des abréviations

— **Wi-Fi** : *Wireless Fidelity.*
— **MANET** : *Mobile Ad-hoc networks.*
— **VANET** : *Vehicular Ad-hoc Network.*
— **RSU** : *Road Side Units.*
— **V2V** : *Vehicule-to-Vehicule.*
— **V2I** : *Vihicule-to-Infrastructure.*
— **GPS** : *Global Positioning System.*
— **UWB** : *Ultra Wide Band.*
— **RSA** : *Rivest–Shamir–Adleman.*
— **APDA** : *Attacked Packet Detection Algorithm.*
— **RRDA** : *Request Response Detection Algorithm.*
— **EAPDA** : *Enhanced Attacked Packet Detection Algorithm.*
— **QLA** : *Queue Limiting Algorithm.*
— **ACK** : *acknowledgment.*
— **2-SDA** : *Two-stage detection algorithm.*

Introduction générale

Aujourd'hui, les transports, qu'il s'agisse de déplacements individuels ou de marchandises, jouent un rôle essentiel dans l'amélioration de la qualité de vie à travers le monde. La circulation routière représente l'une des activités quotidiennes les plus importantes, ce qui a donné naissance à l'utilisationn des technologies sans fil pour permettre aux véhicules de communiquer, et d'établir des connexions entre eux, formant ainsi un nouveau type de réseaux appelé réseaux véhiculaires ad hocs (Vehicular Ad Hoc Networks, (VANETs)).

Les VANETs sont des systèmes de communication sans fil qui permettent aux véhicules de communiquer entre eux et avec les infrastructures routières. Ces réseaux sont devenus un domaine de recherche en plein essor en raison de leur potentiel pour améliorer la sécurité routière, la gestion du trafic et les services aux conducteurs. Cependant, la sécurité des VANETs est une préoccupation majeure en raison de la nature ouverte et dynamique de ces réseaux, ce qui les rend vulnérables à diverses attaques.

L'une des principales menaces auxquelles sont confrontés les VANETs est l'attaque par déni de services (Denial of Service(DoS)). Les attaques DoS visent à perturber ou à bloquer les services offerts par un réseau en inondant celui-ci de trafic malveillant ou en exploitant des vulnérabilités du système. Dans le contexte des VANETs, une attaque DoS peut entraîner des conséquences graves, telles que la perturbation des communications entre les véhicules, la falsification des informations de trafic et même la mise en danger de la sécurité des conducteurs.

Dans le cadre ce mémoire, nous nous intéressons à la sécurité des réseaux VANETs, plus précisement la détection des attaques DoS dans les VANETs. Notre objectif principal est de développer un algorithme efficace pour détecter et prévenir les attaques DoS, afin de garantir la sécurité et la fiabilité des communications dans les réseaux véhiculaires.

Notre travail est d'une importance cruciale, car elle vise à protéger les utilisateurs des VANETs contre les attaques malveillantes et à assurer le bon fonctionnement des applications et des services liés à la sécurité routière.

Pour cette raison, nous allons nous intéresser d'abord aux différentes définitions liées aux réseaux VANETs, ainsi qu'une présentation des notions de sécurité. Nous étudierons aussi divers travaux connexes à ce sujet, avant de présenter notre proposition qui consiste en un nouvel algorithme de détection d'attaques par déni de services à un niveau précoce. Cette dernière consiste à faire des vérifications à différents niveaux. Dans cet algorithme, dès qu'un véhicule est détecté malveillant, il sera éliminé.

Ce mémoire sera organisé en quatre chapitres agencés de la manière suivante :

— Le chapitre 1 regroupe les notions générales sur les réseaux VANETs, par exemple les principaux composants requis pour assurer la communication, les architecture des com-

munications, les caractéristiques, les technologies d'accès, et défis liés aux VANETs.

— Le chapitre 2 définit les différentes notions de sécurité, ainsi que ses objectifs, ensuite, il présente les différentes attaques dans les VANETs.

— Le chapitre 3 traite le concept d'attaques par déni de service, et les diverses attaques qui utilisent cette attaque, puis, il présente divers travaux qui abordent la détection de cette dernière.

— Le chapitre 4 propose un algorithme de détection des attaques par déni de services que nous avons appelé 2-SDA, et qui a deux niveaux de détection des attaques par déni de services (DoS) qui sont la sécurisation des requêtes et la sécurisation des paquets par des mécanismes tel la fonction de hachage, la signature numérique et le chiffrement RSA, puis nous concrétisons l'algorithme par un exemple illustratif dans lequel nous allons traiter plusieurs cas pour bien comprendre la proposition.

— La conclusion permet de clore ce mémoire par quelques perspectives pour nos travaux futurs.

Chapitre 1

Généralités sur les réseaux VANETs

1.1 Introduction

De nos jours, le transport qu'il soit usager ou de marchandise, joue un rôle important dans l'amélioration de la qualité de vie dans le monde. De ce fait, La circulation routière représente l'une des activités quotidiennes les plus importantes. Le domaine du transport connaît en effet de plus en plus de progrés qui intègrent l'utilisation de mécanismes de sécurité plus avancés ainsi que des carburants raffinés et plus respectueux de l'environnement. Cependant, la circulation routière et la conduite restent encore deux points vulnérables de la sécurité routière qui nécessitent des progrès de façon perpétuelle pour plus de sécurité. A cet effet, une description météorologique précise ainsi que des alertes précoces des dangers qui pourraient survenir, tels que les goulots d'étranglement ou l'annnonce de gros accidents, pourraient être très utiles aux conducteurs. C'est pourquoi un nouveau type de technologie de communication appelé VANETs (Ad-hoc Vehicular Networks) a vu le jour et la recherche dans ce domaine est en plein essor. C'est aussi pour cette raison que nous consacrons dans ce mémoire un chapitre entier dédié à la présentation des notions générales sur les VANETs.

Le chapitre commence par une présentation générale des réseaux ad hoc, puis se concentre sur les réseaux VANETs. OAprès avoit dzfini les VANETs, nous examinerons leurs architectures de communication et caractéristiques, ainsi que les différentes applications et les types de services que ces derniers peuvent offrir. Nous discuterons pour finir, des défis liés aux VANETs.

1.2 Réseaux ad hoc

Les réseaux ad hoc sont appelés aussi réseau MANET (Mobile Ad-Hoc Netwok) ou WANET (Wirless Ad-Hoc Network).

1.2.1 Définition des réseaux Ad hoc

Les réseaux ad hoc sont des réseaux sans fil composés de deux nœuds ou plus, capables de communiquer entre eux sans aucune administration centralisée contrôlée par des points d'accès. Chaque nœud dans le réseau fonctionne à la fois comme routeur et hôte. Ainsi, une absence d'infrastructure fixe, laisse la place à une auto-organisation arbitraire des nœuds. L'appellation " MANET" vient de l'aspect mobilité dans les réseaux Ad hoc.

1.2.2 Caractéristiques des réseaux Ad hoc

Les réseaux Ad hoc sont composés d'entités mobiles communiquant entre elles, et leur fonctionnement est sensiblement différent des autres réseaux [**28**]. Les caractéristiques de ces réseaux sont les suivantes :

- **Topologie dynamique** : reconfiguration dynamique du réseau lors du deplacement.
- **Absence d'infrastructure** : l'absence de tout genre d'administration centralisée.
- **Ressources énergétiques limitées** : les nœuds dans les réseaux Ad hoc sont alimentés typiquement par des batteries dont la capacité et l'énergie sont limitées.
- **Sécurité limitée** : les réseaux Ad hoc sont plus vulnérables par rapport aux autres réseaux à cause de la nature du médium qui rend certaines attaques malicieuses, ainsi que la topologie du réseau, qui peuvent être redoutables.

1.3 Réseaux VANETs

1.3.1 Définition des réseaux VANETs

Les réseaux VANETs (Vehicular Ad Hoc Networks) constituent une nouvelle forme de réseaux ad hoc mobiles où les nœuds mobiles sont des véhicules intelligents équipés de moyens de communication (Capteurs). Comme tout autre réseau Ad hoc, les véhicules peuvent communiquer entre eux ou avec des stations de base placées tout au long des routes. Ils permettent d'établir des communications entre véhicules ou bien avec une infrastructure située aux bords des 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.

Les nœuds dans un réseau VANET sont équipés de capteurs véhiculaires (OBU ou On Board Unit) pour calcul et transmition des messages, de GPS(Global Positioning System) pour la détection de la position, d'un EDR(Event Data Recorder), des capteurs radar et d'infrastructures fixes (RSU ou Road Side Unit) pour collecer et analyser des données de trafic générées par les véhicules intelligents. Ces unités permettent l'échange de données entre véhicules, notamment pour améliorer la planification routière et la sécurité routière. Les principaux composants requis pour assurer la communication du réseau VANET (voir la figure 1.1) sont les suivants :

1.3.1.1 Unité de bord de route

Les Road Side Unit (RSU) sont des entités situées et installées au bord de la route. Ces entités présentent des points d'accès au réseau et sont déployées tout au long de la route. Chaque

RSU a pour objectif de transmettre des messages aux véhicules qui se trouvent dans sa zone radio. Ces messages contiennent des informations sur les conditions météorologiques, ainsi que sur l'état de la route (vitesse maximale, autorisation de dépassement, etc.) **[21]**.

1.3.1.2 Unité embarquée

L'On Board Unit (OBU) est une unité embarquée dans les véhicules intelligents. Son rôle est de permettre aux véhicules de se localiser, calculer, enregistrer et envoyer des messages sur une interface réseau à l'aide d'un ensemble de programmes. Dans le réseau VANET, le conducteur ou l' utilisateur peut voir les pseudonymes des véhicules à proximité dans son OBU à l' aide des messages beacon. Ainsi, l'utilisateur peut choisir le véhicule avec lequel il veut communiquer. L'OBU peut posséder un TPD (Tamper Proof Device) qui est un dispositif inviolable dans chaque véhicule responsable du stockage des informations secrètes telles que les clés privées, de la signature des messages sortants. Pour réduire le risque de compromission par des attaquants, le dispositif devrait avoir sa propre batterie, qui peut être rechargée depuis le véhicule, et une horloge qui peut être sécurisée par resynchronisation lors du passage par une station de base fiable en bord de route. L'accès à ce dispositif devrait être restreint aux personnes autorisées. Par exemple, les clés cryptographiques peuvent être renouvelées lors de la vérification technique périodique du véhicule **[21]**[**26**].

1.3.1.3 Autorité centrale

L'Autorité Centrale (CA) est un serveur de stockage et de transaction qui a la confiance de toutes les entités du réseau. Elle fournit des services et des applications à tous les utilisateurs, ainsi que les certificats, les clés ou pseudonymes de communication des véhicules **[21]**.

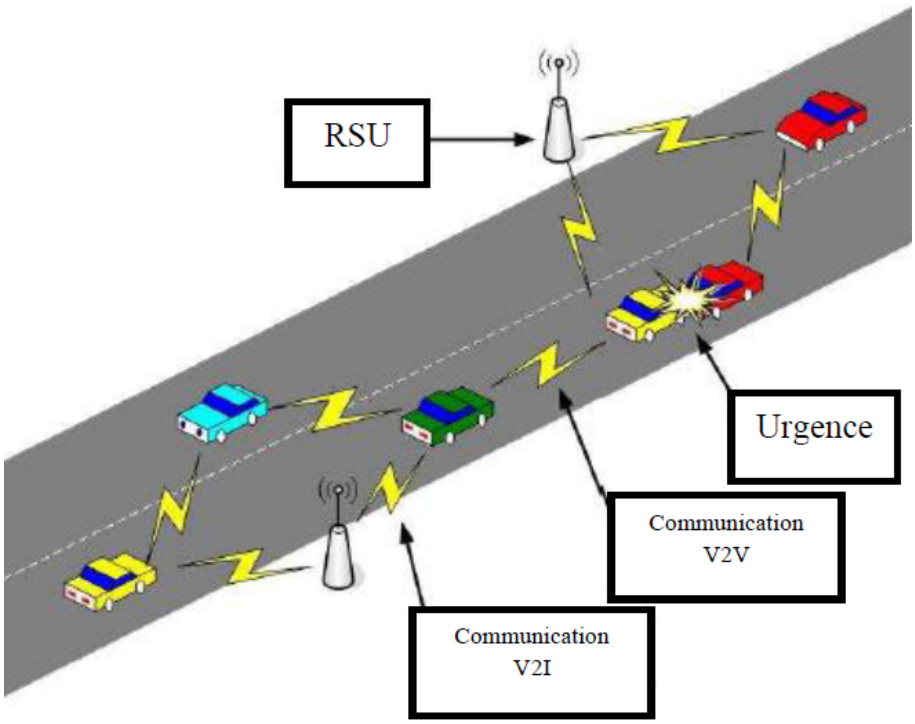

FIGURE 1.1 – Architecture d'un VANET

1.3.2 Architecture des communications dans les VANETs

Dans les VANETs, on distigue deux modes de communications, les communications Véhicule-à-Véhicule (V2V) et les communications Véhicule-à-Infrastructure (V2I). Les véhicules peuvent utiliser un de ces deux modes ou bien les combiner s'ils ne peuvent pas communiquer directement avec les infrastructures. Dans la partie suivante, Nous introduisons la raison d'être et l'utilité de chaque mode.

1.3.2.1 Communication véhicule à véhicule

La communication véhicule à véhicule (V2V) est intéressante pour la diffusion d'alertes (collision, ralentissement, freinage, etc.) ou pour la conduite coopérative. En effet, dans le cas d'applications de sécurité routière, les réseaux à infrastructures montrent leur limite en termes de délais (voir la figure 1.2).

1.3.2.2 Communication véhicule à infrastructure ou infrastructure à véhicule

L'architecture (V2I) est composée de RSU, auxquels les véhicules accèdent pour les applications de sécurité, de gestion et de confort. Les RSU sont administrés par un ou plusieurs organismes publics ou bien par des opérateurs autoroutiers. Un véhicule qui informe le service de voirie au sujet d'un obstacle est un exemple de communication V2I (voir la figure 1.2).

1.3.2.3 Communication hybride

La combinaison des deux communications véhicule à véhicule (V2V) avec la communication de véhicule à infrastructure (V2I), permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures (stations de bases) étant limitées, l'utilisation des véhicules comme relais permet d'étendre cette distance (voir la figure 1.2).

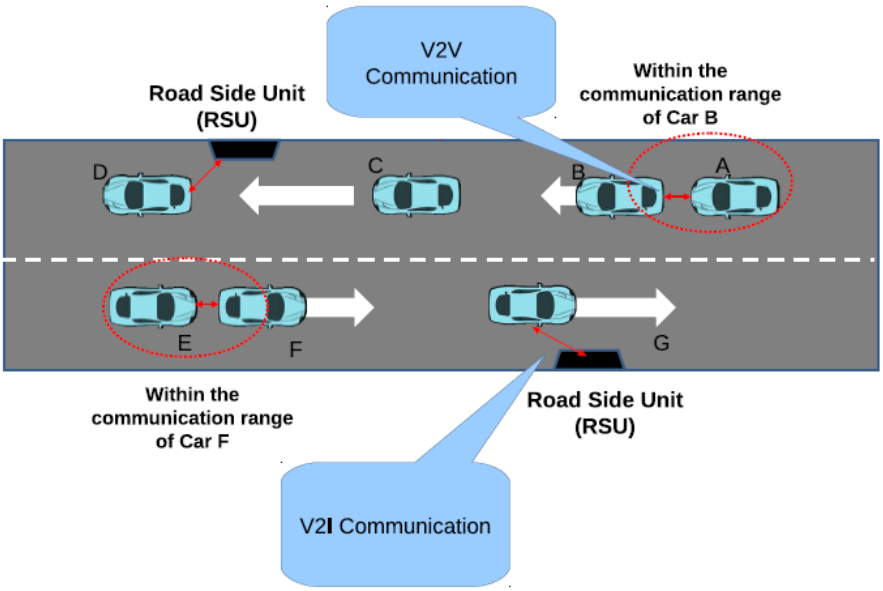

FIGURE 1.2 – Communication dans un VANET

1.3.3 Caractéristiques des VANETs

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des réseaux ad hoc. Dans cette partie, nous présentons quelques propriétés des VANETs **[14]**.

1.3.3.1 Capacité d'énergie et stockage

Contrairement aux réseaux MANETs où la contrainte d'énergie représente un défi pour les chercheurs, les nœuds du VANET n'ont pas de limitation d'énergie ou de stockage. On considère qu'ils ont suffisamment d'énergie et de puissance de calcul **[14]**.

1.3.3.2 Modèle de mobilité

la mobilité des véhicules dans un réseau VANET est contrôlée par plusieurs facteurs comme les infrastructures routières (route, autoroute, panneaux de signalisation, limitation de vitesse). D'autre part, la mobilité dans le VANET est également directement liée au comportement du conducteur et à sa réponse aux obstacles ou aux situations différentes et complexes rencontrées (temps d'embouteillage, accidents, ...) **[14]**.

1.3.3.3 Partitionnement du réseau

Selon le type de route et l'heure de la journée, la densité du réseau varie considérablement. Sur les routes à faible volume de trafic et à faible densité, des groupes de nœuds isolés apparaîtront, entraînant une segmentation du réseau, des taux de ruptures de communication élevés, de longs retards de routage et même des pertes de paquets **[14]**.

1.3.3.4 Sécurité et anonymat

L'importance de l'échange d'informations via les communications des véhicules rend essentiel la sécurisation du fonctionnement de ces réseaux, condition préalable au déploiement des VANET **[14]**.

1.3.3.5 Topologie et connectivité

Comme les réseaux ad hoc mobiles, les réseaux VANETs sont caractérisés par une connectivité sporadique. La forte mobilité des nœuds est liée à la vitesse de déplacement des voitures qui peuvent atteindre jusqu'à 33,33 m/s (120 km/h), à cette vitesse deux voitures allant en sens inverse avec une couverture radio de 250 m aurait une communication directe de seulement 7,5 secondes. Ce qui a pour conséquence un changement de topologie très fréquents.

1.3.4 Applications dans les VANETs

Il existe plusieurs classifications des applications liées VANETs. Dans cette section nous allons nous intéresser à la classification selon l'utilité, et donc nous distingons trois grandes catégories :

1.3.4.1 Applications de gestion routière

Les applications de gestion du trafic se concentrent sur l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Ils apportent une assistance technique aux conducteurs pour adapter leurs itinéraires aux conditions de circulation. Ces applications visent à équilibrer le mouvement des véhicules sur les routes afin d'utiliser efficacement la capacité des routes et des intersections, entraînant une réduction des pertes humaines, une augmentation des temps de trajet, de la consommation d'énergie, etc

1.3.4.2 Applications de sécurité routière

Ce sont des applications liées à la sécurité telles que l'évitement des collisions et la conduite coopérative (par exemple, pour fusionner les voies). Une caractéristique commune de cette catégorie est qu'elle se rapporte à des situations potentiellement mortelles où la présence de services prévient les incidents potentiellement mortels. Par conséquent, ce type de sécurité est obligatoire car le fonctionnement normal de ces applications doit être garanti même en présence d'un attaquant.

1.3.4.3 Applications de confort

Ce sont des applications qui fournissent des informations sur le trafic et améliorent le confort de conduite. Il s'agit d'applications non liées à la sécurité, impliquant généralement une communication V2I ou I2V. Ces services accèdent aux canaux du système de communication, à l'exception des canaux de contrôle. Ils accèdent au canal dans un mode de faible priorité par rapport à l'application sécurisée.Les applications de confort incluent :

- **Optimisation du trafic** : Informations et conseils sur le trafic, guidage d'itinéraire amélioré,etc.
- **Recherche de services routiers** : Trouver les stations-service, les restaurants, etc les plus proches. Cela inclut aussi la communication des véhicules avec l'infrastructure routière et les bases de données associée
- **Services de paiement** : Péage électronique, gestion des parkings,etc.
- **Info-divertissement** : Accès Internet, téléchargements multimédias, messagerie instantanée, etc.

1.3.5 Technologies d'accès dans les VANETs

Pour assurer et faciliter la communication réseau entre différents produits de différents fabricants, il existe actuellement un grand nombre de règles et de méthodes. Ce sont des normes et des standards qui permettent de simplifier le développement et de garantir que les produits fournis par différents fabricants peuvent fonctionner ensemble.

1.3.5.1 IEEE 802.11p

Le standard IEEE 802.11p est un standard de communication sans fil spécialement conçu pour les applications de communication entre les véhicules (V2V) et les infrastructures de transport intelligentes (V2I). Ce standard 802.11p est basé sur la technologie Wi-Fi et utilise une bande de fréquence de 5,9 GHz. Il offre des débits de données élevés (jusqu'à 27 Mbps)

et une faible latence pour des communications en temps réel telles que la transmission d'informations sur les conditions routières, les alertes de sécurité et les informations de navigation. Il s'agit d'un élément clé des systèmes de transport intelligents (ITS) et permet des applications telles que la prévention des accidents, la gestion du trafic et la réduction des émissions de gaz à effet de serre **[14]**.

1.3.5.2 Dedicated Short Range Communication

Dedicated Short Range Communication (DSRC) est une technologie de communication sans fil spécialement conçue pour les communications de courte portée entre les véhicules (V2V) et les infrastructures de transport intelligentes (V2I).

En français, on peut traduire DSRC par "communication dédiée de courte portée". Cette technologie est basée sur le standard IEEE 802.11p et utilise une bande de fréquence de 5,9 GHz pour offrir des communications à haut débit et faible latence. Elle permet aux véhicules et aux infrastructures de communiquer en temps réel des informations sur les conditions de la route, les alertes de sécurité et les informations de navigation, contribuant ainsi à améliorer la sécurité routière et la gestion du trafic **[14]**.

1.3.5.3 Bluetooth

La technologie Bluetooth (IEEE 802.15.1) a été développée à l'origine par la compagnie des téléphones mobiles Ericsson en 1994, permettant une communication radio à courte portée. Cette technologie a été conçue comme une alternative sans fil pour la communication série RS-232 pour des appareils comme les téléphones mobiles, les PDA (Personal Digital Assistant), les ordinateurs portables, e. Elle permet d'obtenir un taux de transfert allant jusqu'à 3 Mbps et une couverture jusqu'à 100 mètres.

1.3.5.4 Ultra Wide Band

UWB peut être considérée comme une évolution du bluetooth connue sous la norme IEEE 802.15.3. UWB est une technologie radio qui peut être utilisée dans de très faibles niveaux de puissance à courte portée (10 m) et en communications à bande passante élevée ($>$ 500 MHz) en utilisant une grande partie du spectre radioélectrique. Cette technologie offre des transmissions avec des débits allant jusqu'à 480 Mbps. L'une des caractéristiques les plus importantes de l'UWB est la faible consommation d'énergie.

1.3.6 Défis liés aux VANETs

Les réseaux de véhicules ad hoc (VANETs) présentent plusieurs problèmes qui peuvent affecter leur utilité et leur efficacité. Voici quelques-uns des défis les plus courants associés aux VANETs :

1.3.6.1 Défis de mobilité

Les réseaux VANETs présentent plusieurs problèmes liés à la mobilité, notamment :

- L'hétérogénéité de la mobilité des véhicules peut entraîner des variations de la connectivité du réseau, ce qui rend la gestion des connexions et des communications plus complexe.

- Les mouvements rapides des véhicules peuvent rendre plus difficile la mise en place de mesures de sécurité efficaces.
- La mobilité peut affecter la qualité et la fiabilité des informations échangées.

1.3.6.2 Défis liés au routage

Le routage dans les réseaux VANETs est un défi important en raison de la nature dynamique et hautement mobile de ces réseaux. Voici quelques-uns des défis les plus courants liés au routage dans les VANETs :

- Les routeurs sont mobiles ;
- Les changements de liaison surviennent assez souvent (perte de paquets) ;
- Les événements de mise à jour sont souvent envoyés, d'où un grand nombre de controles ;

1.3.6.3 Défis d'accès au canal

Voici quelques défis d'accès au canal dans les VANETs :

- Difficulté de gestion des collisions.
- Densité élevée de véhicules. Les véhicules doivent partager le canal avec d'autres véhicules et les communications peuvent être perturbées.
- Difficulté de la prise en charge de la qualité de service (QoS).

1.3.6.4 Défis de sécurité

Les réseaux VANETs posent plusieurs défis de sécurité. Voici quelques-uns des défis les plus courants associés à la sécurité des VANETs :

- Attaques de falsification de données.
- Attaques de déni de service (DoS).
- Problèmes de confidentialité.
- Problèmes de gestion des clés, etc.

1.4 Conclusion

Pour conclure le chapitre sur les réseaux VANETs, il est important de souligner l'importance de ces réseaux dans le domaine de la communication sans fil. Les VANETs offrent des avantages tels que l'amélioration de la sécurité routière, la réduction de la congestion du trafic, la gestion des véhicules et l'amélioration de l'efficacité du transport.
Ainsi, malgré les avantages qu'offrent les réseaux VANETs, il est important de continuer à travailler sur des technologies de sécurité avancées pour garantir la sécurité et la confidentialité des données. En somme, la sécurité est un problème crucial dans les réseaux VANETs et il est important de prendre des mesures pour garantir que ces réseaux sont sûrs et fiables pour tous les utilisateurs. La sécurité fera l'objet du deuxième chapitre qui est intitulé "**Sécurité des réseaux VANETs**.

Chapitre 2

Sécurité dans les VANETs

2.1 Introduction

Compte tenu de l'importance des informations échangées entre les véhicules et de l'ouverture de l'environnement VANET, il est important de s'assurer de la non existence des attaquants qui peuvent émettre des messages d'alerte avec un contenu falsifié ou qui bloquerait la livraison de messages légitimes afin de provoquer des accidents. Nous consacrons pour celà ce chapitre sur la sécurité des réseaux VANETs, dans lequel nous définirons quelques notions de base sur la sécurité, puis nous mettrons en avant quelques attaques liées aux VANETs ainsi que des mécanismes de sécurité relatifs à ces dernières

.

2.2 Notions de bases sur la sécurité

La sécurité est un concept très large qui englobe de nombreux aspects et domaines, tels que la sécurité physique, la sécurité informatique, la sécurité financière, la sécurité des personnes, etc. Dans le cadre de ce mémoire, nous nous intéressons évidemment à la sécurité informatique, et plus précisément la sécurité dans les réseaux VANETs.

2.2.1 Définition de la sécurité

La sécurité informatique consiste à identifier les risques et à trouver un équilibre entre les solutions techniques et organisationnelles qui assurent que les ressources du système informatique (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

2.2.2 Objectifs de la sécurité

Il est primordial de bien cerner les conditions requises que doit respecter un système pour son bon fonctionnement avant d'adresser les questions relatives à la sécurité de ce dernier. Lorsqu'une condition requise n'est pas respectée, une faille de sécurité est préssentie. Nous présentons dans ce qui suit quelques critères qu'un réseau VANET doit respectés.

2.2.2.1 Authentification

Il s'agit d'un critère requis par tout système. Pour les VANETs, il très important de connaitre plusieurs informations sur le nœud émetteur telles que son identifiant, son adresse, ses propriétés, sa position géographique, etc. Il est donc important d'authentifier l'émetteur du message ainsi que 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 contribuer à la prévention des attaques de Sybil [1] en spécifiant un identifiant unique pour chaque véhicule. Grâce à cette technique , un véhicule ne pourra pas se proclamer d'avoir plusieurs identifiants et de faire croire qu'il s'agit de plusieurs véhicules et ainsi laisser pénétrer une attaque sur le réseau [**8**].

2.2.2.2 Intégrité

L'intégrité a pour but de garantir que le message n'est pas altéré entre son émission et et sa réception. Le récepteur du message vérifie le message reçu afin de s'assurer 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. 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 [**8**].

1. L'attaque Sybil est une attaque dans laquelle un attaquant produit de fausses identités.(On détaille la définition dans la séction suivante)

2.2.2.3 Confidentialité

Le cryptage des messages permet d'empêcher à des véhicules n'ayant pas les autorisations nécessaires de lire les messages qui ne leur sont pas destinés. C'est en d'autres termes un moyen de respecter la confidentialité des échanges [**8**].

2.2.2.4 Non répudiation

La répudiation n'autorise pas une entité de nier d'avoir participé à une communication. Elle protège le système contre le déni d'un nœud qui prétend à tort n'avoir pas participé à une communication. La non-répudiation permet donc au récepteur de prouver qu'il a bien reçu le message d'un tiers. Ainsi, pour chaque message reçu, l'émetteur peut être clairement identifié [**8**].

2.2.2.5 Disponibilité

La disponibilité des canaux de communication est un point essentiel dans les réseaux véhiculaires, et de façon encore plus pertinente dans le cas d'applications portant sur la sûreté. En effet, les applications critiques de la sécurité routière ont besoin que le canal soit toujours disponible pour garantir l'envoi imminent de messages de sûreté [**14**].

2.2.2.6 Contrôle d'accès

L'accès au réseau pour un usager est conditionné par un droit d'accès ainsi que des priviléges qui lui sont accordés selon les cas. Certaines communications comme celle de la police ou d'autres autorités ne doivent pas être écoutées par les autres usagers. L'accès à certains services fourni s par les infrastructures est réservé à une catégorie d'usagers. Il est donc indispensable de mettre en place un système qui permet de définir tous ces politiques d'accès pour garantir un contrôle d'accès personnalisé dans le réseau [**8**].

2.3 Attaques dans les réseaux VANETs

La sécurité est un élément essentiel des VANETs, car les communications entre les véhicules peuvent être sensibles et potentiellement critiques pour la sécurité des passagers et des autres usagers de la route.
Compte tenu de la diversité d'applications et services qui opéreront sur les réseaux véhiculaire (comme vu dans le chapitre 1), il est facile d'imaginer le nombre d'attaques auxquelles ils risquent d'être exposées. Comme il est difficile de prévoir toutes les attaques possibles pouvant survenir dans un réseau VANETs, nous nous contenterons de présenter quelques unes [**14**].

2.3.1 Usurpation d'identité

L'usurpation d'identité, également connue sous le nom de attaque mascarade est une technique d'attaque dans laquelle un attaquant se fait passer pour une entité légitime en utilisant des informations d'identification frauduleuses. Dans le contexte des VANETs, l'usurpation d'identité peut se produire lorsque des nœuds malveillants se font passer pour des nœuds légitimes pour accéder à des informations confidentielles ou pour perturber le fonctionnement normal du réseau. Les attaques d'usurpation d'identité ont un impact sur les services d'authentification et

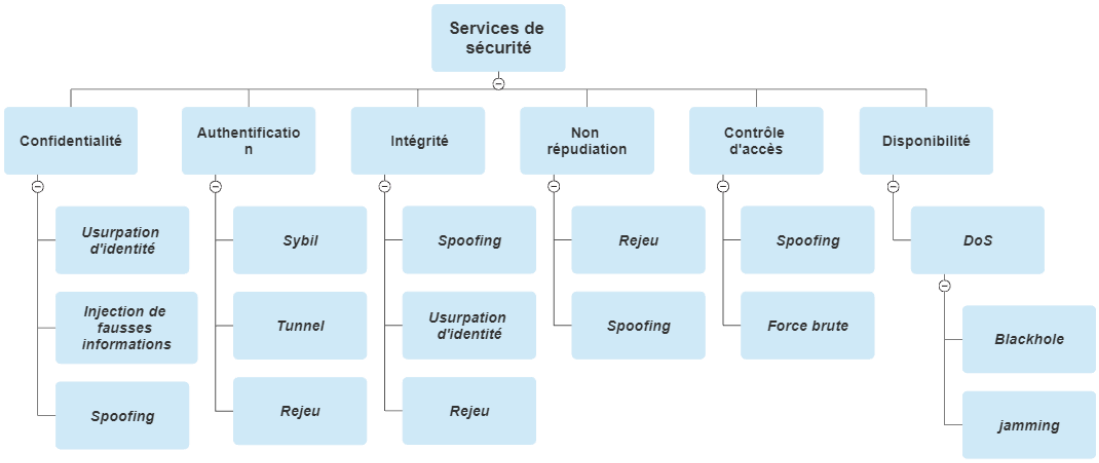

FIGURE 2.1 – Classification des attaques dans les réseaux VANETs

de confidentialité. En usurpant l'identité d'un nœud légitime du réseau, les attaquants peuvent accéder à des informations confidentielles et perturber les communications dans le réseau.

2.3.2 Injection de fausses informations

Les attaques par injection de fausses informations, également connues sous le nom d'attaques de falsification de données, sont des techniques d'attaque dans lesquelles un attaquant insère de fausses informations dans un système ou un réseau de communication afin de tromper les utilisateurs ou de perturber le fonctionnement normal du système. Dans le contexte des VANETs, les attaques par injection de fausses informations peuvent inclure l'envoi de fausses données de localisation pour tromper les nœuds du réseau sur la position d'un véhicule, l'envoi de fausses données de trafic pour perturber la circulation, ou l'envoi de fausses informations sur les conditions météorologiques pour tromper les conducteurs.

Ces attaques par injection de fausses informations affectent principalement le service de confidentialité, car les attaquants peuvent injecter de fausses informations dans le réseau pour tromper les utilisateurs légitimes et leur faire prendre de mauvaises décisions.

2.3.3 Attaque Sybil

Il s'agit d'une attaque très dangereuse dans laquelle un nœud peut produire de nombreuses fausses identités pour perturber le mode normal de fonctionnement des VANETs en diffusant plusieurs messages utilisant des ID falsifiées. L'attaquant peut manipuler le comportement d'autres véhicules et envoyer dans le réseau MANET des messages transmis à partir de différents véhicules. Par conséquent, les utilisateurs ont l'impression qu'il y a une congestion (une fausse congestion) sur la route et sont obligés de changer à tort leur itinéraire afin de libérer la voie [**24**].

2.3.4 Attaque Tunnel

Il s'agit d'une attaque où un attaquant exploite la perte momentanée d'informations de positionnement lorsqu'un véhicule entre dans un tunnel et avant qu'il ne reçoive les informations de positionnement authentiques, l'attaquant injecte de fausses données dans l'unité embarquée [**24**].

2.3.5 Attaque par rejeu

L'attaque par rejeu est une technique d'attaque dans laquelle un attaquant intercepte et enregistre des données de communication légitimes, puis les rejoue ultérieurement pour tromper le destinataire. Dans le contexte des VANETs, une attaque par rejeu peut se produire lorsque des données de communication, telles que des messages de sécurité émis par des véhicules légitimes, sont capturées par un attaquant et sont ensuite réémises dans le réseau pour provoquer des perturbations ou des dysfonctionnements. Les attaques par rejeu ont un impact sur les services d'intégrité et de non-répudiation. Les attaquants peuvent capturer et rejouer les données de communication pour tromper les nœuds légitimes du réseau.

2.3.6 Attaque Spoofing

Dans les VANETs, l'attaque de spoofing est une attaque dans laquelle un attaquant falsifie ou usurpe l'identité d'un nœud légitime du réseau. Cela peut permettre à l'attaquant d'envoyer de fausses informations aux autres nœuds du réseau, de les tromper ou de perturber leur communication. L'attaque de spoofing peut également permettre à l'attaquant de masquer sa propre identité et d'agir de manière anonyme sur le réseau [**11**].

2.3.7 Force brute

C'est une méthode de tentative-erreur qu'un attaquant utilise pour obtenir des informations telles qu'un mot de passe utilisateur ou un numéro d'identification personnel, ou pour casser des données cryptées, ou tester la sécurité du réseau [**11**].

2.3.8 Déni de service

L'attaque par déni de service (DoS - Denial of Service) dans les VANETs consiste en une tentative malveillante pour empêcher ou perturber la communication entre les véhicules et les infrastructures de transport intelligente, en surchargeant le réseau de trafic ou en le faisant planter. Dans le contexte des VANETs, une attaque DoS peut avoir des conséquences graves sur la sécurité routière, car elle peut empêcher les véhicules de recevoir des informations importantes, comme les alertes de sécurité, les informations de trafic, ou les messages de signalisation routière. L'attaque affecte principalement le service de disponibilité, car il vise à empêcher les utilisateurs légitimes d'accéder au réseau. Cette dernière sera l'objet de ce travail qui sera détaillé dans les prochains chapitres [**22**].

Remarque 2.3.1. *Les attaques Blackhole et Jamming décrites par la figure 2.1 seront présentées dans le troisième chapitre (* ***Détection des attaques DoS****).*

2.4 Mécanismes de Sécurité

Les mécanismes de sécurité sont des techniques et des procédures utilisées pour protéger les systèmes informatiques, les réseaux et les données contre les menaces potentielles. Voici quelques-uns des mécanismes de sécurité couramment utilisés dans les VANETs :

2.4.1 Cryptographie

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible. C'est ce qu'on appelle le chiffrement, qui à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Il existe deux types de chiffrement à savoir le chiffrement symétrique et le chiffrement asymétrique.

2.4.1.1 Chiffrement symétrique

Dans le chiffrement symétrique, appelé aussi chiffrement à clé secrète, la même clé est utilisée pour le chiffrement et le déchiffrement. Deux interlocuteurs désirant communiquer des données confidentielles doivent partager une clé secrète k. Cette même clé est utilisée par l'émetteur pour chiffrer le message et par le récepteur pour déchiffrer le message reçu. Lorsque l'utilisateur A envoie le message m chiffré avec la clé k, soit le message (mk) vers l'utilisateur B, ce dernier est capable de le déchiffrer en utilisant la même clé k et récupérer m. Le chiffrement à clé symétrique a l'avantage d'être rapide en termes de calculs **[31]**.

2.4.1.2 Chiffrement asymétrique

Dans le chiffrement asymétrique, appelé aussi chiffrement à clé publique, chaque interlocuteur détient un couple de clés : une clé visible clé publique et une clé secrète appelée clé privée. Si un texte est chiffré avec la clé publique de l'utilisateur A, il ne sera déchiffré que par la clé privée de A. Et s'il est chiffré avec la clé privée de A, il ne sera déchiffré qu'avec la clé publique de A **[31]**.

2.4.2 Fonction de hachage

C'est une fonction mathématique qui transforme une entrée de données (comme un fichier, un message ou un mot de passe) en une empreinte numérique unique de taille fixe, appelée "hash". Cette empreinte est un résumé cryptographique des données d'origine, qui peut être utilisé pour vérifier l'intégrité et l'authenticité des données sans avoir besoin d'accéder à l'ensemble des données d'origine **[31]**.

2.4.3 Signature numérique

C'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à la clé privée du signataire **[31]**.

2.4.4 Code d'authentification des messages

Message Authentification Code (MAC) est un code accompagnant des données qui assure les mêmes fonctionnalités que la signature numérique, mais son implémentation se base sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage **[31]**.

2.4.5 Certificat numérique

C'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'autorité de certification (AC) [**31**].

2.4.6 Autorité

Les autorités sont des entités de confiance, qui sont responsables de l'établissement des clés, la gestion des identités et les qualités des nœuds dans un réseau.

2.5 Conclusion

En conclusion, la sécurité des VANETs est cruciale pour protéger les utilisateurs de la route et assurer la fiabilité du réseau. Les attaques liées aux VANETs peuvent être classées en différentes catégories, chacune ayant des conséquences spécifiques sur la sécurité du réseau. Parmi les attaques vues dans ce chapitre, nous nous focalisons dans la suite de notre travail de master sur l'attaque par déni de services qui affecte particulièrement la disponibilité. Les attaques DoS feront l'objet des deux prochains chapitres.

Chapitre 3

Attaques DoS dans les réseaux VANETs

3.1 Introduction

En raison de la mobilité et du mouvement des véhicules, les réseaux VANETs font l'objet d'attaques et de menaces sérieuses. Parmi elles, nous retenons les attaques DoS qui provoquent l'indisponibilité du réseau. Dans ce chapitre, on reviendrons sur le concept d'attaques par déni de service, suivi d'un aperçu des diverses attaques qui utilisent cette méthode. De plus, nous présenterons divers travaux qui abordent la détection de cette attaque.

3.2 Rappels sur DoS dans les VANETs

Une attaque par déni de service dans un réseau informatique vise à interrompre le fonctionnement normal d'un réseau VANETs. Il existe de nombreuses méthodes pour faire face à ces attaques. Les attaquants peuvent utiliser des techniques telles que la diffusion de faux

messages, la falsification de données ou la manipulation de la topologie du réseau pour causer des interruptions de service ou affecter la sécurité du système.

3.3 Les attaques par déni de services

Les attaques basées sur le déni de service (DoS) dans les VANETs peuvent se montrer sous différentes formes. La figure 3.1 expose une classification des attaques DoS dans les deux modes suivants :
Mode application :
Dans ce type d'attaque, l'attaquant diffuse des messages erronés aux autres nœuds du réseau dans le but de les détourner vers un autre chemin (eg :l'attaque Sybil).

Mode réseau :
Dans ce type d'attaque, l'attaquant bloque la bande passante, ce qui entraine un bloquage du réseau aussi.

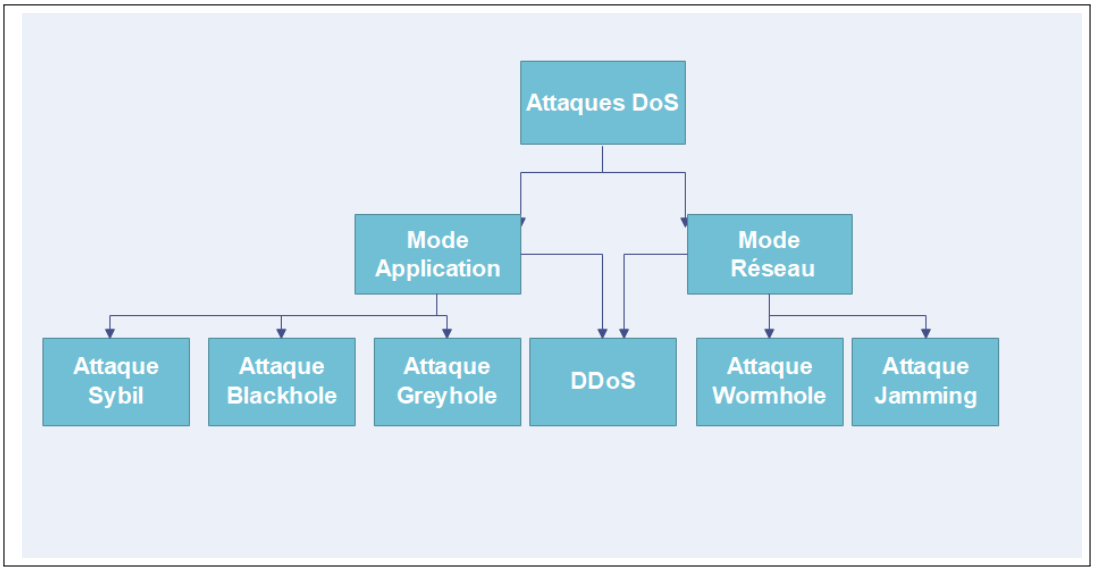

FIGURE 3.1 – Classification des attaques DoS

3.3.1 Attaque Blackhole

Il s'agit de la principale attaque visant la disponibilité dans les réseaux ad hoc, qui existe également dans les réseaux VANETs. Cette attaque est généralement provoquée par un utilisateur enregistré du réseau VANETs. Le nœud suspect reçoit les paquets du réseau mais refuse de contribuer au fonctionnement du réseau. Cela peut perturber la table de routage et empêcher la transmission d'un message important aux destinataires en raison de la présence d'un nœud malveillant qui prétend contribuer à la communication **[19]**.

3.3.2 Attaque Greyhole

Cette attaque se produit lorsque des véhiciules non fiables séléctionnent certains des paquets de données à transmettre et abandonnent les autres paquets sans sans être repérés **[15]**.

3.3.3 Attaque par déni de service distribué

L'attaque DDoS (déni de service distribué ou "distributed denial of service" en anglais) est une attaque encore plus grave que l'attaque DoS parce que le mécanisme de cette dernière est distribué. Dans ce cas, les attaquants lancent des attaques à partir de différents endroits. Ils peuvent utiliser différents créneaux horaires pour lancer leurs attaques. La nature de l'attaque et les créneaux horaires peuvent varier d'un attaquant à l'autre **[12]**.

3.3.4 Attaque Wormhole

Dans cette attaque, un attaquant enregistre un paquet, ou des bits individuels d'un paquet, à un endroit du réseau, tunnelise le paquet (éventuellement de manière sélective) vers un autre endroit, puis le rejoue à cet endroit **[30]**.
De même, dans les réseaux VANETs, un attaquant qui contrôle au moins deux entités éloignées l'une de l'autre et un lien de communication à grande vitesse entre elles peut acheminer par tunnel des paquets diffusés d'un endroit vers un autre, diffusant ainsi des messages erronés (mais correctement signés) dans la zone de destination **[17]**.

3.3.5 Attaque Jamming

Dans cette attaque, l'attaquant perturbe le canal de communication dans les réseaux VANETs en utilisant un signal de forte puissance avec une fréquence équivalente. Il s'agit de l'attaque la plus dangereuse pour les applications de sécurité, car elle ne suit pas l'alerte de sécurité valide. Pour toute attaque de brouillage réussie, le brouilleur peut, en effectuant une action, bloquer le signal utile dans le même temps que l'occurrence d'un événement **[18]**

3.4 Travaux connexes

Dans cette section, nous résumons une sélection d'ouvrages scientifiques traitant du thème de la détection des attaques DOS dans les réseaux VANETs.

3.4.1 Détection des attaques Jamming à l'aide de la distribution d'erreurs

Dans l'article **[6]**, Hamieh et al. se concentrent sur la question des attaques jamming dans les réseaux ad hoc sans fil. Ils proposent comme solution à ce problème une technique qui consiste à surveiller la distribution des erreurs pour détecter de telles attaques. Leur approche consiste à détecter des brouillages en utilisant la mesure de corrélation entre les temps d'erreur et de réception correcte. Ensuite grâce à des simulations, les auteurs évaluent l'efficacité de leur méthode et la comparent à d'autres méthodes existantes. Sur la base de leurs études, les auteurs concluent que leur approche est un outil fiable pour détecter les attaques jamming et peut être un atout précieux pour sécuriser les réseaux ad hoc sans fil. Cependant la méthode proposée ne peut être appliquée dans toutes les attaques par déni de service.

3.4.2 Contrôle d'accès basé sur la localisation

Dans l'article **[9]**, les auteurs s'intéressent à un certain nombre de mécanismes de sécurité de la localisation spécialement conçus pour les réseaux VANETs et pricipalement contre l'attaque sybil qui est une attaque par déni de service. Parmi les méthodes présentées, les auteurs s'intéressent au contrôle d'accès. En règle générale, le contrôle d'accès est autorisé par une entité unique qui sert d'authentificateur. La validation doit être réussie pour accorder l'accès, qui peut inclure des autorisations de lecture, d'écriture, de suppression, de modificat ion ou autres. Dans le domaine des réseaux VANET, les données de localisation peuvent améliorer l'efficacité du contrôle d'accès. Plus précisément, l'accès aux données est limité aux utilisateurs d'une région désignée, ceux en dehors de ladite région ne pouvant y accéder. Afin de déterminer cette région, les auteurs utilisent les coordonnées GPS. La figure 3.2 a été utilisée comme exemple pour montrer la région de contrôle d'accès spécifiée par le véhicule "a" décrite par deux coordonnées GPS $P_0(x_0; y_0)$ et $P_1(x_1; y_1)$, qui est le carré rouge. Le véhicule émetteur "a" envoie un message aux véhicules de cette région. Les véhicules situés en dehors de cette région, par exemple "b", ne peuvent pas lire ce message. Seul le véhicule "c" peut lire ce message. Lorsqu'un véhicule situé à $P_2(x_2; y_2)$ reçoit un message de contrôle d'accès, il vérifie :

$$\begin{cases} x_0 \geq x_2 \geq x_1 \\ y_0 \geq y_2 \geq y_1 \end{cases}$$

Si la position du véhicule P_2 est la bonne, les droits d'accès lui sont accordés, sinon l'accès lui est refusé.

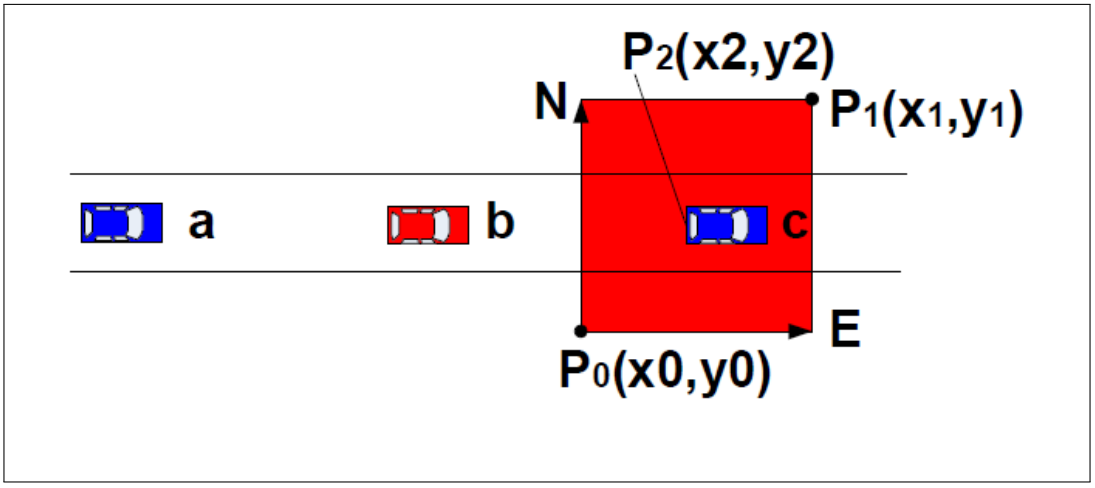

FIGURE 3.2 – Illustration d'une région de contrôle d'accès

3.4.3 Modèle de sécurité contre l'attaque DoS dans les VANETs

Dans l'article **[10]**, Halabi et al. ont proposé un modèle réactif contre l'attaque DoS dans lequel ils ont doté les OBU des véhicules d'un processeur qui permet à ces derniers de réagir à l'intrusion. Le modèle constitue quatre (4) solutions illustrées par la figure 3.3.

Malheureusement le modèle en question ne fonctionne qu'après l'exécution des attaques DoS au lieu de les détecter à l'avance.

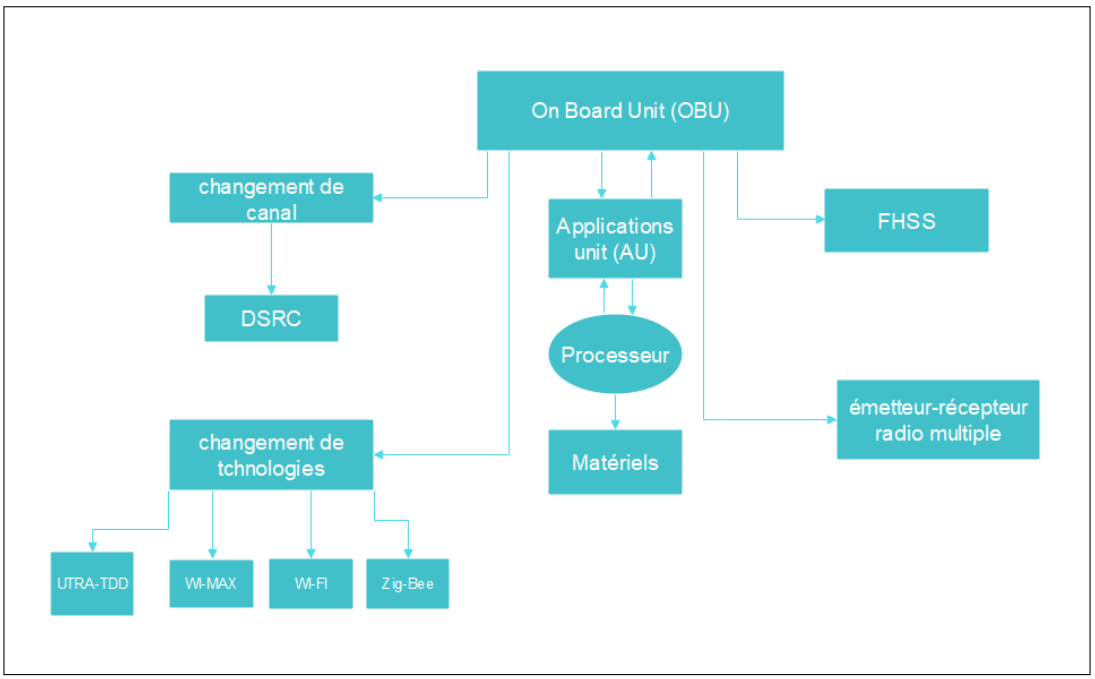

FIGURE 3.3 – Modèle de soltions proposées pour l'attaque DoS

3.4.4 Algorithme IP-Chock

Dans l'article **[13]**, les auteurs ont proposé une approche appelée "IP CHOCK" qui utilise un filtre de Bloom avec une fonction de hachage pour prévenir les attaques par déni de service (DoS) dans les réseaux VANET. Cette approche permet d'identifier les véhicules malveillants sans échange d'informations secrètes. Pour détecter les attaques DoS à un stade précoce, deux détecteurs sont utilisés : le détecteur de demande et le détecteur de réponse. Le détecteur de demande est déployé à la périphérie du routeur d'hôtes, tandis que le détecteur de réponse est déployé par le détecteur de choc protégé pour détecter les attaques.

Les attaques DoS peuvent être détectées en se basant sur un tableau de surveillance constamment mis à jour. Ce tableau est une structure de données efficace en termes de stockage, car il nécessite un tableau de longueur fixe pour enregistrer les informations pertinentes sur les véhicules.
Ainsi, l'approche "IP CHOCK" propose une méthode de détection des attaques DoS dans les réseaux VANETs en utilisant un filtre de Bloom et une fonction de hachage. Cette approche permet de repérer les véhicules malveillants sans avoir besoin d'échanger des informations secrètes. Les détecteurs de demande et de réponse sont déployés pour surveiller les attaques, en se basant sur un tableau de surveillance mis à jour régulièrement.

3.4.5 Algorithme de détection des paquets attaqués

Dans l'article **[25]**, les auteurs ont présenté un mécanisme appelé APDA qui est un algorithme permettant de détecter l'emplacement des véhicules dans le réseau. L'idée est que chaque RSU soit équipée de l'algorithme APDA et que tous les véhicules puissent communiquer entre eux ainsi qu'avec les RSU en utilisant uniquement cet algorithme. Cet algorithme permet de détecter la position des véhicules dans le réseau. Une fois la position détectée, elle est stockée dans une RSU en vue d'une utilisation ultérieure.
Chaque véhicule est équipé d'une unité embarquée (OBU) et d'un dispositif de protection

contre les intrusions, qui stockent tous deux des informations détaillées sur le véhicule, telles que sa vitesse et sa position. La fréquence (f), la vitesse (v) et l'utilisation de l'OBU du véhicule sont utilisées pour identifier sa position. L'algorithme commence par calculer la fréquence (f) en utilisant la formule suivante $\alpha * |v - v_{max}/2|$ avec : α le coefficient déterminé par les caractéristiques de la route et v_{max} la vitesse maximale. La figure 3.4 représente l'organigramme de l'algorithme de détection des paquets attaqués (APDA) où R est la requete, *high* et *low* sont des seuils limites de la vitesse (v) et la fréquence(f). L'inconvénient de cet algorithme est qu'il ne précise pas l'issue des véhicules malveillants une fois les paquets attaqués détectés.

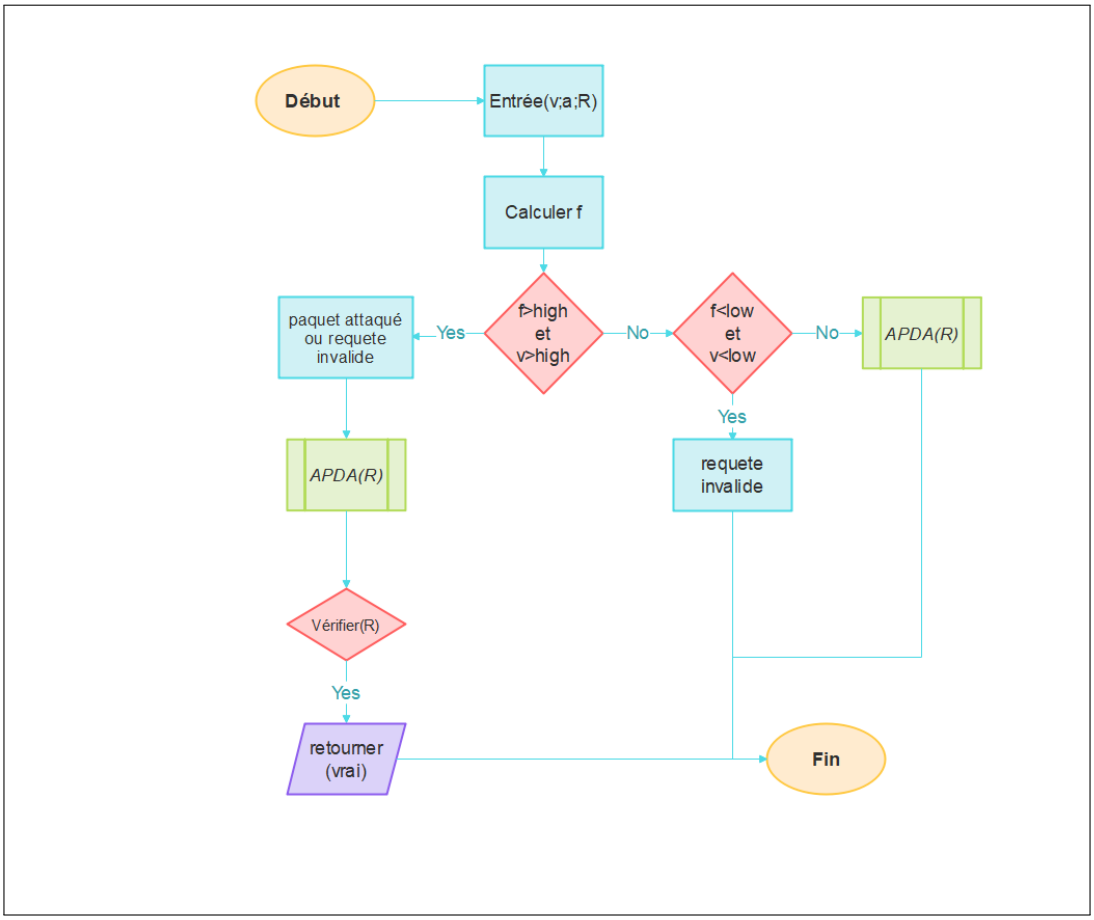

FIGURE 3.4 – Organigramme de l'algorithme APDA

3.4.6 Algorithme de limitation d'une file d'attente contre les attaques DoS

Dans l'article [**4**], les auteurs ont proposé l'algorithme QLA(Queue Limiting Algorithm) pour la protection des véhicules. Le concept de protection des véhicules implique un mécanisme dans lequel chaque véhicule est équipé d'une barre supérieure désignée pour recevoir un nombre fini de messages de sécurité.Par conséquent, le nombre de messages de sécurité reçus sera limité. Afin d'éviter que le nœud ne soit la cible d'attaques par déni de service, des mesures de sécurité doivent être mises en œuvre. Pour déterminer la limite supérieure de réception des messages de sécurité, chaque véhicule envoie périodiquement un paquet de salutation dans le réseau et attend une réponse. Lorsque la réponse est reçue, l'unité de bord (OBU) compte le nombre de réponses. L'efficacité de cette approche est évaluée en fonction de critères tels que les coûts de routage, la réception des messages et le taux de livraison des paquets. Grâce à cette approche, le VANET est en mesure de prévenir les attaques de déni de service (DoS) et de maintenir une communication normale même pendant une attaque. Mais dans le cas de limitation de nombre de messages reçus, il est possible d'empêcher des véhicules honnêtes d'émettre des messages.

3.4.7 Algorithme de détection des réponses aux demandes

Dans l'article [**29**], les auteurs ont proposé un algorithme de détection des réponses aux requêtes pour détecter les attaques DoS dans les réseaux VANETs et qui consiste à appliquer d'abord l'algorithme APDA (cité plus haut dans ce chapitre) ensuite l'application du second algorithme qui est le RRPDA utilisé dans la vérification des nouvelles demandes qui souhaitent rejoindre le réseau. Cet algorithme réduit l'inondation en limitant son compteur et en n'autorisant pas les véhicules falsifiés par l'attaquant. La figure 3.5 représente l'organigramme de l'algorithme (RRDA), avec $nbrSEffect$ est le nombre de sauts effectuer et $nbrSAtt$ nombre de sauts attendus per le RSU.

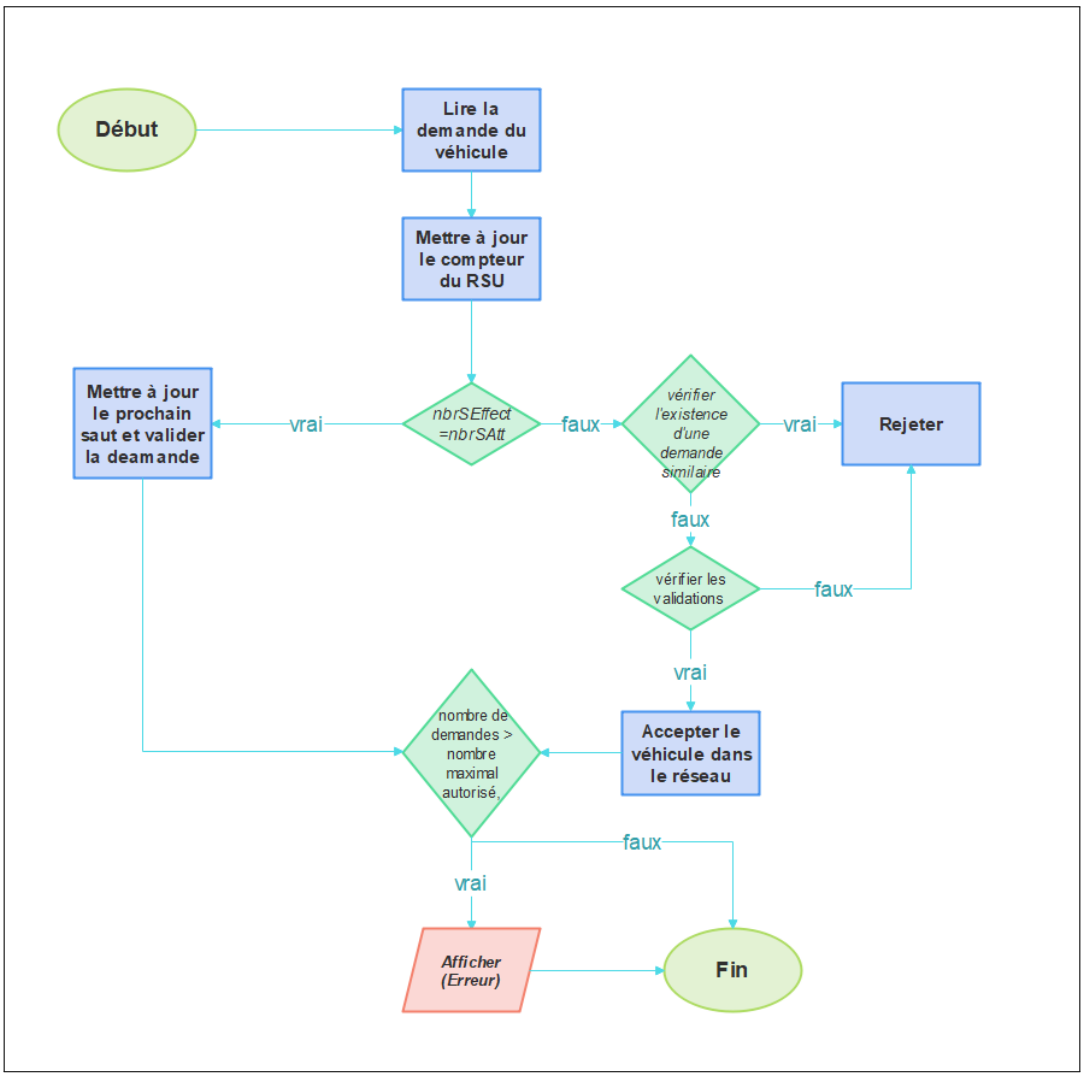

FIGURE 3.5 – Organigramme de l'algorithme RRDA

3.4.8 Algorithme amélioré de détection des paquets attaqués

Dans l'article **[5]**, les auteurs ont proposé une solution pour lutter contre les attaques par déni de service DOS détectées à l'aide de fenêtres temporelles (timeslot) qui sont calculées par la formule suivante :

$$TS = \sum_{i=0}^{n} (timestamp\ received_i - timestamp\ sent_i)/nombre\ de\ noeuds$$

qui se base sur le temps de communication moyen des nœuds. Par conséquent, l'algorithme amélioré de détection des paquets attaqués (EAPDA) réagit et vérifie avec moins de latence et un débit plus élevé. L'EAPDA, comme l'APDA et le RRDA, utilise les RSU pour vérifier les rêquetes et enregistrer dans sa base de données les informations relatives au véhicule, Comme cet algorithme utilise des accusés de réception des demandes et des créneaux horaires (TS), il détecte donc l'attaque DOS pendant le processus de vérification.

La figure 3.6 représente l'organigramme de l'algorithme amélioré de détection des paquets attaqués (EAPDA), avec ACK = acknowledgement packet et TS = timeslot.

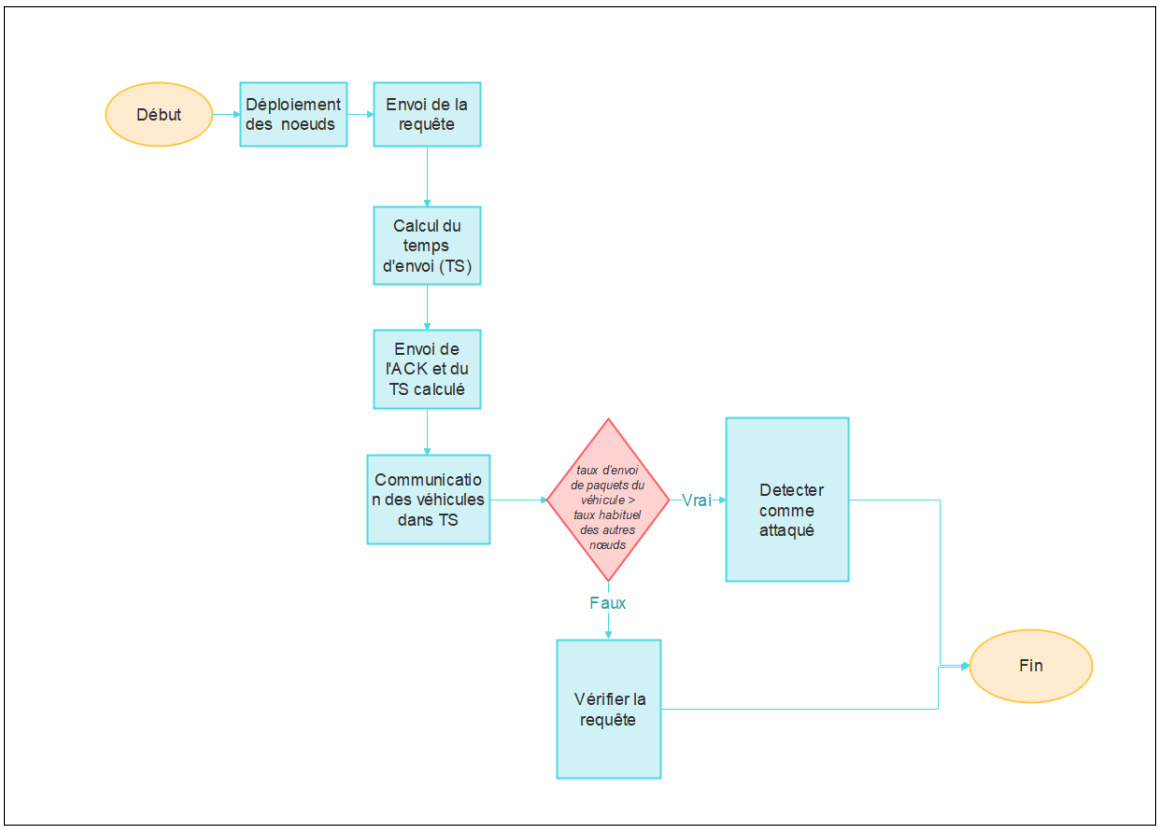

FIGURE 3.6 – Organigramme de l'algorithme EAPDA

3.4.9 Isolation des comportements erronés à l'aide de l'ACO

Dans l'article **[16]**, Kishan et al. proposent l'algorithme Ant Colony Optimization (ACO), technique efficace, optimisée et sécurisée qui protège le processus de routage en isolant les attaquants malveillants en route vers leurs cibles. Les algorithmes de routage basés sur ACO créent des chemins avec des valeurs de fiabilité et de phéromone pour détecter les nœuds malveillants. Les nœuds avec des scores de confiance et de phéromone faibles sont identifiés comme malveillants et toutes les routes passant par ce nœud sont abandonnées. Le traitement via ce nœud est abandonné.
Ainsi, l'approche d'isolation comportements erronés à l'aide des colonies de foumis utilise la confiance et la valeur de la phéromone pour éliminer les véhicules malveillants sur le chemin. Cette approche permet de sélectionner le chemin optimal qui n'a pas de véhicules malveillants. L'inconvénient de cette approche est dû au surcoût causé par les opérations de mise à jour de la confiance et de mise à jour de la phéromone.

3.4.10 Algorithme de détection de nœuds malveillants multiples

Dans l'article **[27]**, Sushil Kumar et al. proposent un algorithme d'identification de plusieurs nœuds malveillants. Cet algorithme vise à identifier les paquets malveillants et les nœuds malveillants dans un réseau en fonction de la fréquence (freq), de la vitesse (vel) et du nombre de nœuds multiples (N), ainsi que des plages de valeurs seuil pour freq et vel (low, high). Son mécanisme ressemble au mécanisme de l'algorithme APDA mais la différence est que dans ce cas l'algorithme fonctionne sur plusieurs nœuds malveillants à la fois. Il procéde par comparaison de la fréquence et de la vitesse par rapport aux taux prédéfinis "high" et "low", si elles sont dans l'intervalle [low, high] cela indique que les paquets sont authentiques et sont diffusés dans

le réseau, sinon si la fréquence (freq) et la vitesse (vel) sont élevées pour plusieurs nœuds, cela indique que le paquet provient d'un nœud malveillant. A cette étape, le véhicule malveillant est suivi et sa trajectoire est enregistrée et tous les paquets provenant du véhicule malveillant sont supprimés. Dans le cas contraire, si la fréquence et la vitesse sont basses, cela indique que le paquet est non pertinent.

3.5 Comparaison des traveaux connexes

Dans le tableau suivant, nous allons comparer les diffrents articles traités dans la section précédente.

	Année	Principe	Type de DoS	Mode d'attaque	Paramètres utilisés	Élimination (paquets/nœuds)	Utilisation de RSU	Utilisation de la requête	Sécurisation de la requête	Performances évaluées
Hameieh et al.	2009	Mesurer la corrélation entre les temps d'erreur et de réception correcte	Jamming	Réseau	Coefficient de corrélation	Paquets	Non	Non	Non	Débit en cas d'attaque ; coefficient de corrélation en fonction du nombre de stations mobiles ; coefficient de corrélation en fonction de la taille des paquets
Yan et al.	2009	Limitation de l'accès aux données aux utilisateurs d'une région désignée par les coordonnées GPS	Sybil	Application	Position (GPS)	-	Non	Non	Non	-
Halabi et al.	2010	-	DoS	Réseau et application	-	-	Non	Non	Non	-
Ip-Chock	2013	Utilisation de bloom-filter pour stocker l'adresse IP afin de filtrer les véhicules malveillants	DoS	Réseau et application	Fonction de hachage	-	Non	Non	Non	Probabilité de détection des erreurs
APDA	2013	APDA détecte la position du véhicule et des paquets envoyés afin de détecter les attaques	DoS	Réseau et application	Vitesse et fréquence	Paquets	Oui	Oui	Non	-

QLA	2014	Utilisation d'une barre supérieure pour recevoir un nombre limité de messages de sécurité	DoS	Réseau et application	Nombre de paquets	Nœuds	Non	Non	Non	Réception des messages ; taux de livraison des paquets
RRDA	2014	Applique APDA ensuite et réduit l'inondation à RRDA	DoS	Réseau et application	Vitesse et fréquence	Paquets	Oui	Oui	Non	-
EAPDA	2015	Afin de détecter d'éventuels nœuds malveillants, RSU utilise une méthode de comparaison de la quantité de paquets transmis reçus de chaque nœud et d'analyse de tout modèle anormal	DoS	Réseau et application	Fréquence, vitesse et nombre de nœuds multiples	Paquets	Oui	Oui	Non	Délai ; taux de faux positifs ; débit
Kishan et al.	2015	Utilisation de la confiance et de la valeur de la phéromone pour éliminer les véhicules malveillants sur le chemin	DoS	Réseau et application	Colonie de fourmis	Nœuds	Non	Non	Non	Délai moyen de bout en bout ; taux de livraison de paquets ; frais généraux de routage normalisés

Sushil et al.	2019	Détecte l'attaque DoS grâce à la vitesse, fréquence, et le nombre de noeuds, puis élimine les paquets et les noeuds	DoS	Réseau et application	vitesse fréquence nombres de noeuds	Paquets et nœuds	Oui	Oui	Non	Perte de paquets ; durée de vie du réseau ; débit du réseau ; taux de distribution des paquets ; nombre de nœuds morts et vivants

Les articles de la section précédente présentent différentes techniques de détection d'attaques DoS. Parmi les dix articles, quatre proposent des algorithmes de détection de paquets : APDA (2013), RRDA (2014), EAPDA (2015) et l'identification de multiples nœuds malveillants (2019). Malgré leurs différences, ces quatre algorithmes reposent tous sur la RSU pour détecter les messages nuisibles.

Dans l'article de Hamieh et al., l'étude se concentre sur l'attaque Jamming, une forme de déni de service. Cependant, le modèle proposé ne s'applique pas à toutes les attaques DoS. Yan et al., quant à eux, ont adopté une méthode différente en utilisant les coordonnées GPS pour sécuriser les données contre les attaques. À l'inverse, Halabi et al. ont choisi un modèle réactif pour contrer les attaques par déni de service. Verma et al. ont utilisé des fonctions de hachage pour identifier les véhicules malveillants, alors que les algorithmes de détection de paquets visent à identifier les paquets malveillants. L'algorithme EAPDA, en plus des paquets, vérifie également les requêtes et les véhicules.

En examinant le tableau, on constate que la plupart des articles traitent de l'attaque DoS de manière générale, à l'exception de deux : Hamieh et al. se concentrent sur l'attaque Jamming, et Yan et al. sur l'attaque Sybil. On remarque également que seuls, quatre travaux ont utilisé les RSU et les requêtes : APDA, RRDA, EAPDA et le travail de Sushil Kumar et al, sauf qu'ils ne s'intéressent pas à la sécurisation des requêtes qui est une étape cruciale dans la sécurisation des VANETs.

Sushil Kumar et al. ont utilisé les mêmes paramètres que les algorithmes APDA et RRDA, à savoir la vitesse et la fréquence, mais ont ajouté un autre paramètre : le nombre de nœuds.

Dans l'algorithme Ip-Cock, les auteurs ont combiné les fonctions de hachage avec le filtre de Bloom (inspiré d'une autre étude). Kishan et al. ont choisi les colonies de fourmis pour acheminer les paquets échangés. Dans l'algorithme EAPDA, les auteurs ont utilisé des paramètres différents, à savoir les time slots et le taux d'envoi des paquets.

3.6 Conclusion

En conclusion, dans ce chapitre, nous avons souligné les différents aspects des attaques DoS dans les réseaux VANETs, et qui ont fait l'objet de nombreuses recherches. Nous avons mis en lumière les attaques et les dégâts qu'elles peuvent causer aux réseaux VANETs sous différents angles. De plus, nous avons présenté divers travaux connexes visant à détecter et contrer les attaques DoS dans les VANETs, offrant une diversité de solutions potentielles pour améliorer la sécurité dans ces derniers. Cependant, il convient de noter que la plupart des travaux proposés se concentrent sur un seul niveau de vérification, qu'il s'agisse des nœuds, des paquets ou des requêtes.

Suite à notre étude de l'état de l'art et de la synthèse que nous en avons faite, nous nous engageons sur une réflexion pour proposition que nous présenterons dans le chapitre suivant.

Chapitre 4

Algorithme 2-SDA de détection de l'attaque DoS dans les VANETS

4.1 Introduction

Les attaques DoS constituent une menace majeure pour la sécurité des réseaux, mettant en péril la disponibilité des services en submergeant les infrastructures cibles avec un trafic malveillant. Dans ce contexte, nous présentons dans ce chapitre un nouvel algorithme DoS avec une sécurité à deux niveaux visant à contrer efficacement ces attaques et renforcer la résilience du réseau.

Notre algorithme repose sur une double ligne de défense, combinant la détection des attaques au niveau des requêtes ainsi que des paquets. Cet algorithme vise à fournir une protection robuste en identifiant et en bloquant les nœuds malveillants dès les premières étapes de l'attaque. Pour illustrer concrètement l'efficacité de notre algorithme, nous fournissons un exemple d'application dans un scénario réel. Cet exemple détaille les étapes de détection et de filtration des attaques DoS, mettant en évidence les mécanismes utilisés à chaque niveau de sécurité. Il démontre ainsi l'application pratique de notre algorithme dans des situations concrètes.

4.2 Modèle du réseau

Dans ce chapitre, nous proposons un nouvel algorithme de détection des attaques DoS dans un réseau VANET. C'est loin d'être une solution aboutie mais il nous semble qu'elle a le mérite d'être tout de même présentée dans ce mémoire et nous espérons pouvoir l'investiguer davantage par la suite. La figure 4.1 présente une modélisation de notre algorithme qui a pour but de détecter des attaques par déni de services (DoS) dans les réseaux VANETs.
Cet algorithme comprend des RSU utilisées pour faciliter la communication entre les véhicules afin d'éviter que les nœuds ne soient occupés par le processus de vérification au détriment de tâches utiles. Les RSU sont capables de communiquer entre elles ainsi qu'avec les véhicules. Cependant, les véhicules ne peuvent pas communiquer directement entre eux sans l'autorisation préalable d'une RSU.
Chaque véhicule est équipé d'une unité embarquée (OBU) et d'un dispositif inviolable (TAMPER PROOF). Ces dispositifs stockent des informations détaillées sur les véhicules, telles que la vitesse, la position, etc.

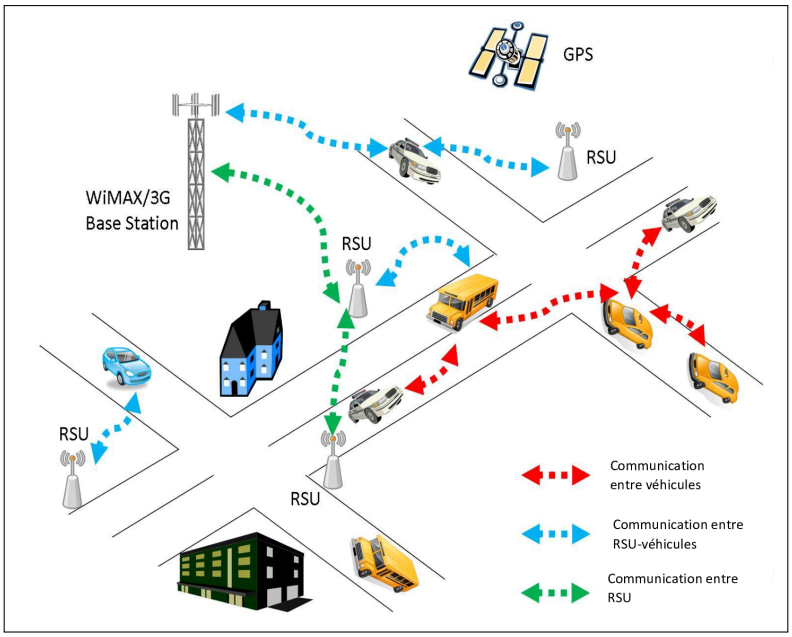

FIGURE 4.1 – Modèle du réseau

4.3 Algorithmme proposé

Dans cette section, nous présentons l'algorithme de détection des attaques de déni de service (DoS) qui utilise les RSU comme moyen de communication. Dans ce système, les RSU jouent un rôle central en gérant l'ensemble des communications. Ceci signifie qu'aucun véhicule ne peut contacter son voisin sans passer par une RSU.
Chaque véhicule voulant émettre un message aux autres doit envoyer une requête aux RSUs dans laquelle il va demander une autorisation d'émission de message à un ou plusieurs véhicules du réseau en précisant le type du message. Une fois la requête reçue, la RSU vérifie si elle n'a pas été interceptée par un autre véhicule. Aprés avoir vérifié la requête, la RSU envoie un accusé de réception (ACK) au véhicule demandeur et diffuse (Broadcast) un temps ($TimeSlot = TS$), temps pendant lequel la communication doit se faire par tous les véhicules. En d'autres termes TS est le délai de communication.
La deuxième partie de cet algorithme consiste à vérifier les messages ou paquets envoyés par les

véicules durant ce temps "TS" que la RSU a fourni. Chaque véhicule a la capacité de vérifier si son voisin lui a transmis le paquet dans le délai imparti(TS). Ensuite, il passe à la vérification de la vitesse (v) et de la fréquence (f) en utilisant la RSU qui supervise tous les nœuds du réseau.

4.3.1 Déscription générale de l'algorithme

Dans cette section, nous présentons un algorithme de détection des attaques de déni de service (DoS) qui s'appelle "Two-stage Detection Algorithm" (2-SDA). L'algorithme 2-SDA repose sur une combinaison de techniques de chiffrement, de la signature numérique pour garantir la confidentialité, l'authentification, et l'intégrité des données échangées.
2-SDA utilise les RSU comme moyen de communication. Dans 2-SDA, les RSU jouent un rôle central en gérant l'ensemble des communications. Ceci signifie qu'aucun véhicule ne peut contacter son voisin sans passer par une RSU.

Chaque véhicule voulant émettre un message aux autres véhicules doit envoyer une requête aux RSU dans lequel il va demander une autorisation d'émission d'un message à un ou plusieurs véhicules du réseau en précisant le type de message (message de sécurité ou d'alerte, message d'information générale). Une fois la requête reçue, la RSU vérifie si elle n'a pas été interceptée par un autre véhicule, Après avoir vérifié la requête, la RSU diffuse un accusé de réception (ACK), pour que le véhicule puisse communiquer avec les autres véhicules. Dans le cas où la RSU reçoit deux requêtes en même temps, elle donne la priorité au message de type sécurité ou d'alerte avant de passer au message d'information générale.

La deuxième partie de l'algorithme 2-SDA consiste à vérifier la validité des messages envoyés ou paquets. Pour cela nous considérons qu'une fois qu'un véhicule reçoit le droit d'émettre il doit le faire impérativement dans le TS qui lui est accordé. Si un des véhicules participant à la transmission du paquet ne transmet pas le paquet dans le TS indiqué, il est considéré comme malveillant. Sinon, la RSU procède à la vérification de deux autres paramètres qui sont la vitesse (v) et la fréquence (f) dans le but de détecter les paquets attaqués. Les paramètres v et f doivent être dans les intervalles respectifs $[V_{min}; V_{max}]$ et $[F_{min}; F_{max}]$. Si ce n'est pas le cas la RSU élimine le nœud et le paquet transmis.

4.3.2 Sécurisation des requêtes

Dans cette étude, nous considérons la possibilité qu'un attaquant puisse intercepter une requête et générer une nouvelle requête d'importance supérieure. Nous considérons également que si un véhicule dépasse un certain nombre de requêtes envoyées dans un court laps de temps, il est classé comme malveillant. Nous notons NBR_L et NBR_{RE} le nombre limite de requêtes à envoyer et le nombre de requêtes envoyé par le véhicule demandeur dans un laps de temps, NBR_L et NBR_{RE} sont déterminés par rapport aux caractéristiques de la route c'est à dire que le nombre de requête change en fonction du type de route (agglomération, zone rurale, autoroute, etc) dans lequel le réseau est établi.

Afin de sécuriser la requête nous utilisons deux mécanismes de sécurité à savoir RSA et la fonction de hachage que nous présentons dans ce qui suit. Mais avant cela nous vérifions le nombre de requêtes envoyées par le véhicule pour ne pas occuper la RSU inutilement.

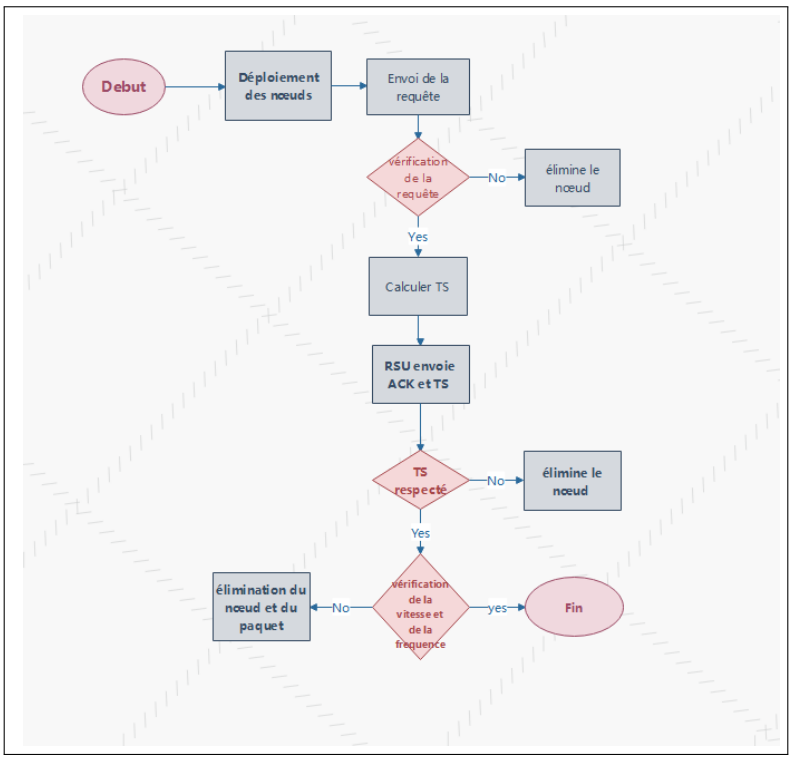

FIGURE 4.2 – Organigramme de l'algorithme 2-SDA

4.3.2.1 Principe du RSA

Le système RSA est un système de cryptographie asymétrique à clé publique très fiable , assez récent (1977) développé par Rivest, Shamir et Adelman. Il utilise 2 clés créées par une personne. Une clé est publique pour le chiffrement, tandis que l'autre est privée pour le déchiffrement. Une personne rend la clé publique accessible qui sera utilisée par l'éméteur pour chiffrer le message qu'il envoie. La clé privée est utilisée par le destinataire pour déchiffrer le message qui lui est envoyé. Le destinataire peut utiliser la clé privée pour signer les documents qu'il envoie à l'éméteur qui à son tour peut utiliser la clé publique pour vérifier la signature. L'algorithme 1 montre les étapes du RSA.

Algorithm 1: Algorithme RSA

1 **Étape 1 :** Choisir les nombres premiers p et q;

2 **Étape 2 :** Calculer $n = pq$ (n sera le modulo de chiffrement);

3 **Étape 3 :** Calculer $\phi(n) = (p-1)(q-1)$ (ϕ est la fonction d'Euler);

4 **Étape 4 :** Choisir $e \in \mathbb{N}^*$ tel que $e < \phi(n)$ et $\gcd(e, \phi(n)) = 1$ (e et $\phi(n)$ sont premiers entre eux);

5 **Étape 5 :** Calculer d, l'inverse de e modulo $\phi(n)$ avec $d < \phi(n)$;

6 **Étape 6 :** La paire ordonnée (n, e) est la clé publique;

7 **Étape 7 :** La paire ordonnée (n, d) est la clé privée;

8 **Étape 8 :** Le message m, avec $m < n$, est chiffré comme $c = m^e \mod n$;

9 **Étape 9 :** Le texte chiffré c ($c < n$) est déchiffré comme $m = c^d \mod n$;

4.3.2.2 Principe des fonctions de hachage et des signatures numériques

1. **Fonction de hachage** : c'est une primitive de sécurité qui est utilisée dans plusieurs constructions de la cryptographie moderne (algorithme de chiffrement et protocoles). Ce type de fonction fait partie des fonctions dites à sens unique (i.e, Fonction facile à calculer mais difficile à inverser). Elle associe une information de taille quelconque en entrée à une information de taille réduite qui la représente de manière unique **[2]**.
2. **Signature Numérique** : c'est un mécanisme qui permet d'authentifier un message, autrement dit permet de prouver qu'un message provient bien d'un émetteur donné à l'instar d'une signature sur un document papier.
   Pour générer une signature numérique d'un message, il est possible d'utiliser l'algorithme RSA comme le montre l'algorithme 2 **[2]**.

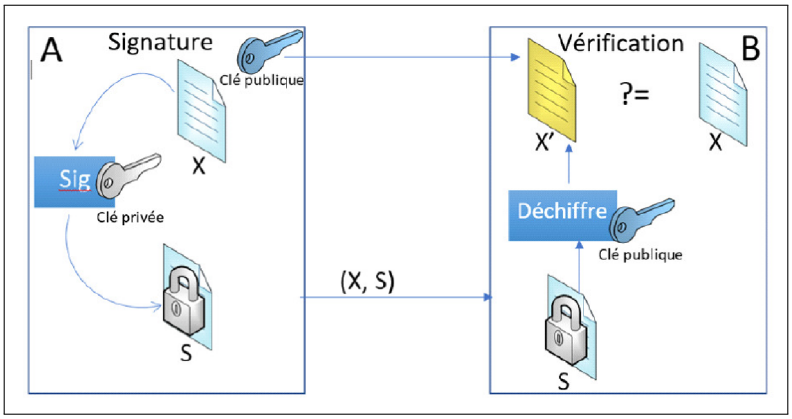

FIGURE 4.3 – Signature numérique

Algorithm 2: Algorithme de signature numérique RSA

Étape 0 : Prérequis : Choisir deux nombres premiers secrets, notés p et q

Étape 1 : Calculer $n = pq$ (n sera le module de chiffrement);

Étape 2 : Calculer $\phi(n) = (p-1)(q-1)$ (ϕ est la fonction indicatrice d'Euler);

Étape 3 : Choisir $e \in \mathbb{N}^*$ tel que $e < \phi(n)$ et $\text{pgcd}(e, \phi(n)) = 1$;

Étape 4 : Calculer d l'inverse de e modulo $\phi(n)$ avec $d < \phi(n)$;

Étape 5 : La paire ordonnée (n, e) est la clé publique;

Étape 6 : Signer le document D en utilisant $S = D^d \pmod{n}$;

Étape 7 : La paire ordonnée (n, d) est la clé privée;

Étape 8 : Vérifier que $S^e = D \pmod{n}$ pour valider la signature;

Étape 9 : Résultats : Obtenir les clés publique et privée à partir des valeurs calculées

4.3.2.3 Etapes de sécurisation de la requête

Pour résumer, voici les différentes étapes nécessaires pour sécuriser la requête.

1. Le véhicule demandeur génère une paire de clés RSA : une clé privée (n, d) et une clé publique (n, e). Il garde la clé privée secrète et partage la clé publique avec RSU.
2. Le véhicule demandeur souhaite envoyer une requête au RSU.

3. Le véhicule demandeur applique RSA sur la requête pour obtenir un message chiffré : "C" en utilisant sa clé publique (n, e).
4. Le véhicule demandeur applique la fonction de hachage sur la requête pour obtenir le haché de la requête : "H1".
5. Le véhicule demandeur chiffre le haché obtenu avec sa clé privée (n, d) pour créer la signature numérique.
6. Le véhicule demandeur envoie la requête chiffrée et la signature numérique au RSU.
7. RSU reçoit la requête chiffrée et la signature numérique du le véhicule demandeur.
8. RSU vérifie : si $NBR_{RE} > NBR_L$ alors éliminer le nœud sinon passer à l'étape suivante (avec NBR_{RE} : nombre de requête envoyées/temps et NBR_L nombre de requête limite/temps.
9. RSU déchiffre la signature numérique avec la clé publique (n, e) du le véhicule demandeur pour obtenir le haché de la requête signée.
10. RSU applique la fonction de hachage sur la requête reçue pour obtenir le haché du requête "H2".
11. RSU compare le haché de la requête obtenue à l'étape précédente avec le haché de la requête signée (H1 et H2).

Si les hachés correspondent, l'intégrité de la requête est vérifiée et l'authenticité est établie. Cela garantit à la fois l'intégrité (aucune modification de la requête), l'authenticité (la requête provient bien du véhicule demandeur), et la disponibilité de la requête (grâce au chiffrement RSA).

4.3.3 Sécurisation des paquets

Aprés avoir eu l'autorisation d'une RSU, le véhicule émetteur commence la transmission de son message. Mais la transmission du message ne peut se faire directement, elle doit passer par d'autres nœuds (les nœuds voisins) avant d'arriver à sa destination, ce qui fait que le message peut être modifié, ou dévié pour ne pas arriver à destination, par un des voisins participants à la transmission.
Nous suggérons alors de rajouter un paramètre qui permet de determiner si un nœud est malveillant ou non. Ce paramètre est le temps de transmission des messages ou délai de transmission des messages qu'on note "TS". TS est donné par la RSU qui a autorisé la communication, et qui doit être respecté par tous les véhicules qui participent à la transmission du message. TS est calculé comme suit :

$$TS = \sum_{i=1}^{NTN} \frac{(temps\ de\ reception_i - temps\ d'envoi_i)}{\alpha \times NTN}$$

avec NTN : nombre total de nœuds, α est déterminé par le protocole de routage utilisé.

Remarque 4.3.1. *Les protocoles de routage sont établis pour gérer la procédure de détermination des nœuds à traverser par les paquets de données afin d'assurer l'échange d'information entre véhicules distants. Il existe plusieurs protocoles de routage. et donc notre proposition dépend du protocole utilisé, du nombre de nœuds participant à la transmission du paquet. Pour cela nous choisissons de rajouter un paramètre α tel que $0 < \alpha \leq 1$ qui est déterminé par le protocole de routage utilisé.*

Comme déjà dit, TS est diffusé à tous les véhicules. Par conséquent, tout véhicule qui reçoit le message est en mesure de vérifier si le message a été reçu dans le délai alloué. Si ce n'est pas le

cas le véhicule en question contacte la RSU pour l'informer que le véhicule qui lui a transmis le message n'a pas respecté le délai TS alloué. La RSU élimine le véhicule qui a n'a pas respecter le délai TS du réseau, et le message ou paquet sera retransmis sur un autre chemin.
Dans le cas où le délai TS est respecté, l'algorithme 2-SDA vérifie grâce à la RSU l'appartenance des deux paramètres vitesse (v) et fréquence (f) aux intervalles respectifs $[V_{min}; V_{max}]$ et $[F_{min}; F_{max}]$. (f) est calculée par la formule suivante :

$$f = \frac{\beta \times |v - V_{max}|}{2}$$

avec : β : est déterminé par les caractéristiques de la route, V_{min} (resp V_{max}) : vitesse minimale autorisée (resp vitesse maximale autorisée), F_{min} (resp F_{max}) : fréquence minimale (resp fréquence maximale).

Les étapes suivantes résument le principe de sécurisation des paquets (messages) :

1. RSU diffuse un délai de communication "TS" à tous les véhicules.
2. Début de la communication, le véhicule émetteur envoie le message (paquet) à son voisin.
3. A chaque fois qu'un véhicule reçoit le message (paquet, il vérifie si le délai TS a été respecté. Si oui il transmet le message à son voisin et passe à l'étape 6, sinon, il contacte RSU pour l'informer.
4. RSU supprime le véhicule qui n'a pas respecté le délai de transmission TS.
5. Le message sera retransmis par un autre chemin.
6. Si(($V_{min} \leq v \leq V_{max}$) et ($F_{min} \leq f \leq F_{max}$)) alors le paquet est correct ; sinon émilie le paquet et le nœud.

4.3.4 Elimination des nœuds

Après avoir sécurisé la requête et le paquet, il est possible de déterminer les cas où un nœud sera supprimé. Au niveau de la requête, un nœud sera éliminé s'il envoie un nombre de requêtes supérieur à la limite autorisée (NBR_L). Si un nœud envoie plusieurs requêtes dans un court laps de temps, cela suggère que le nœud vise à occuper RSU avec un travail supplémentaire, ce qui est considéré comme un comportement malveillant. D'autre part, un véhicule est considéré comme malveillant et sera éliminé du réseau s'il ne respecte pas le délai de transmission "TS". Tout retard dans la transmission d'un message est considéré comme une tentative d'attaque, car cela suggère que le véhicule a essayé de modifier le message. Le dernier cas où l'algorithme 2-SDA élimine un nœud est si la vitesse (v), $v \notin [V_{min}; V_{max}]$ et la fréquence (f), $f \notin [F_{min}; F_{max}]$.

4.4 Exemple d'illustration de l'algorithme 2-SDA

Dans cet exemple, nous allons prendre en considération plusieurs cas afin de monter l'efficacité de l'algorithme 2-SDA. Nous avons choisi pour cet exemple un laps de temps d'une heure par rapport au nombre de requêtes, c'est à dire que NBR_L et NBR_{RE} représentent réspectivement le nombre de requêtes limite et le nombre de requêtes envoyées par le véhicule demandeur dans un laps de temps égale à une heure. Nous avons distingué 5 cas qui sont :

4.4.1 Cas 1 : Requête non sécurisée

Un véhicule v_1 envoie une requête à RSU (comme le montre la figure 4.4) pour lui demander l'autorisation d'envoyer un paquet aux autres véhicules un message d'information générale (par exemple : l'état de la route, position GPS, etc).
Un véhicule v_2 intercepte cette requête et envoie une fausse requête (comme le montre la figure 4.4) à RSU pour lui demander l'autorisation d'émettre un message aux autres véhicules pour les informer qu'il y a par exemple un accident ou que la route est bloquée. Vue l'importance de l'information que v_2 a ramené, RSU traite la deuxième requête qui est la requête formulée par v_2, or la requête est fausse donc RSU et les autres véhicules seront occupés par un travail supplémentaire, qui est transmettre une fausse information.

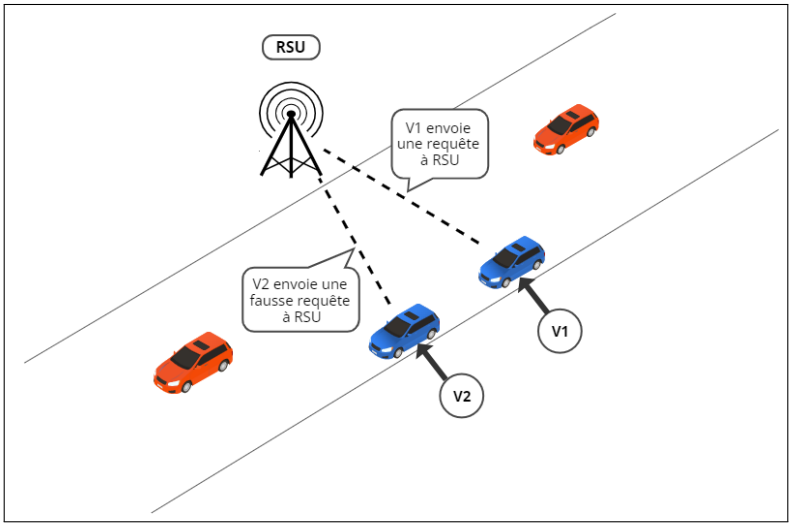

FIGURE 4.4 – Schéma illustratif du cas 1 : requête non sécurisée

4.4.2 Cas 2 : Requête sécurisée

Dans ce cas, on concidère qu'on a appliqué la première partie de l'algorithme qui est la sécurisation de la requête grâce au chiffrement RSA et à la fonction de hachage. Ici, on se retrouve devant deux cas selon le type de route :

Cas 2.1 Route rurale : Dans le cas, d'une zone rurale, le nombre de véhicules dans le réseau est petit ce qui fait que le nombre de requêtes que la RSU reçoit doit être aussi petit, pour l'exemple on pose $NBR_L = 3req/h$.

Un véhicule v_1 envoie toutes les 10 minutes une requête à RSU pour demander l'autorisation d'émettre un message (comme le montre la figure 4.5), au bout de 40 minutes. Par conséquent, quand il envoie la quatrième requête à RSU, RSU l'élimine du réseau car il est considéré comme malveillant puisqu'il a dépassé le nombre limite de requêtes à envoyer (Il a envoyé 4 requêtes en 40 minutes. Ce qui est supérieur à 3 requêtes par heure).
Un véhicule v_2 envoie une requête toutes les demi-heures (comme le montre la figure 4.5). Au bout de deux heures le véhicule ne sera pas éliminé car le nombre de requêtes envoyées en une heure est de 2. Ce qui est inférieur à $3req/h$.

Cas 2.2 : Autoroute : Dans ce type de route, le nombre de véhicules est plus important que dans une zone rurale et donc le NBR_L dans ce cas doit être plus grand pour un laps de temps d'une heure. Posons $NBR_L = 30req/h$.

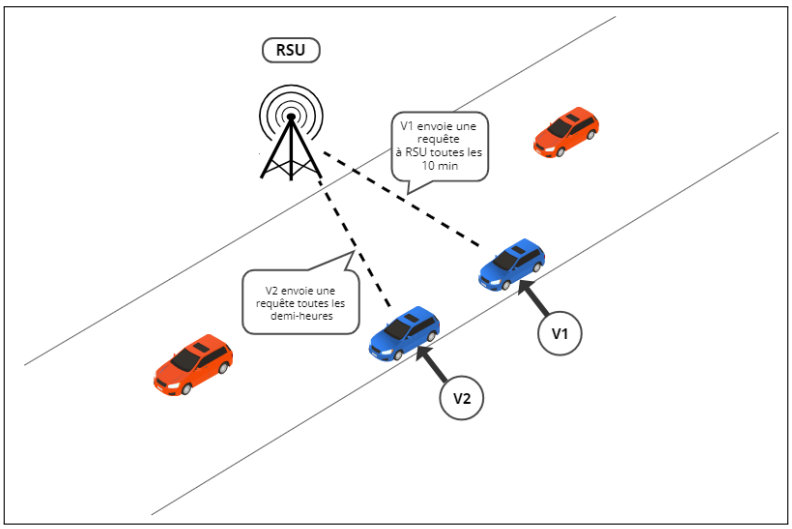

FIGURE 4.5 – Schéma illustratif du cas 2 : requête sécurisée dans une zone rurale

Un véhicule v_1 souhaite envoyer un message à v_2 et v_3 comme le montre la figure 4.6, il envoie une requête à RSU pour demander l'autorisation toutes les 10 minutes. Au bout d'une heure v1 est toujours dans le réseau, il n'a pas été supprimé par RSU. Dans ce cas v_2 sera éliminé du réseau par RSU car il a dépassé le nombre de requête limite.

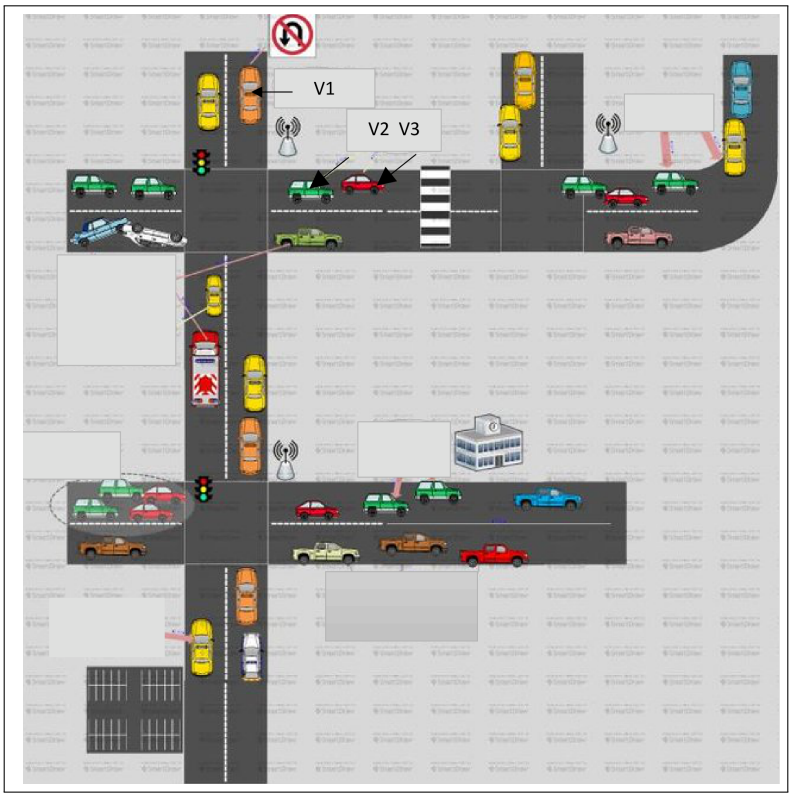

FIGURE 4.6 – Schéma illustratif du cas 2 : requête sécurisée dans une autoroute

4.4.3 Cas 3 : Type de messages

Dans ce cas, nous expliquons la priorité des messages de sécurité par rapport aux autres messages.
v_1 et v_2 deux véhicules qui envoie à RSU une requête comme le montre la figure 4.7, v_1 envoie une requête pour demander l'autorisation d'émettre un message de sécurité aux autres véhicule (urgence) et v_2 envoie une requête pour demander l'autorisation d'émettre un message à v_3 qui n' est pas classé comme message de sécurité qui veut dire qui est moins important qu'une alèrte (par exemple : sa localisation GPS, etc.). Dans ce cas RSU commence par la requête de v_1 car elle est plus urgente ensuite passe à la requête de v_2.

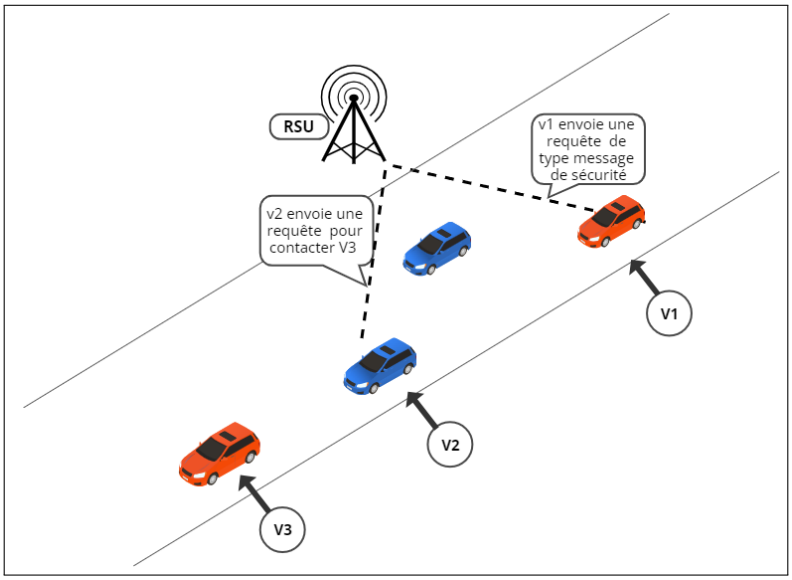

FIGURE 4.7 – Schéma illustratif du cas 3 : message de sécurité et message d'information générale

4.4.4 Cas 4 : Paquet non sécurisé

Le véhicule v_1 souhaite envoyer un message à v_5 (comme le montre la figure 4.8). Il demande l'autorisation à RSU qui après vérification de la requête autorise v_1 d'émettre son message et lui donne un TS à respectrer. v_1 envoie le message via 3 véhicules qui sont v_2, v_3 et v_4, la transmission du paquet entre v_2 et v_3 se passe dans un temps TS_1 tel que $TS_1 > TS$. v_3 contacte RSU pour l'informer que v_2 n'a pas respecté le délai TS(comme le montre la figure 4.9) , et donc RSU procède à l'élimination du véhicule v_2 du réseau et demande à v_1 de retransmettre le message via un autre véhicule (par exemple un véhicule v_6).

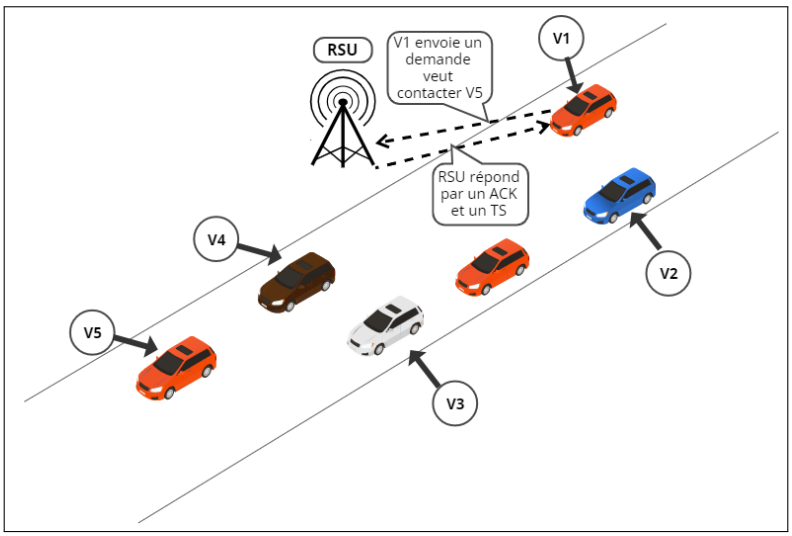

FIGURE 4.8 – Schéma illustratif du cas 4 : paquet non sécurisé

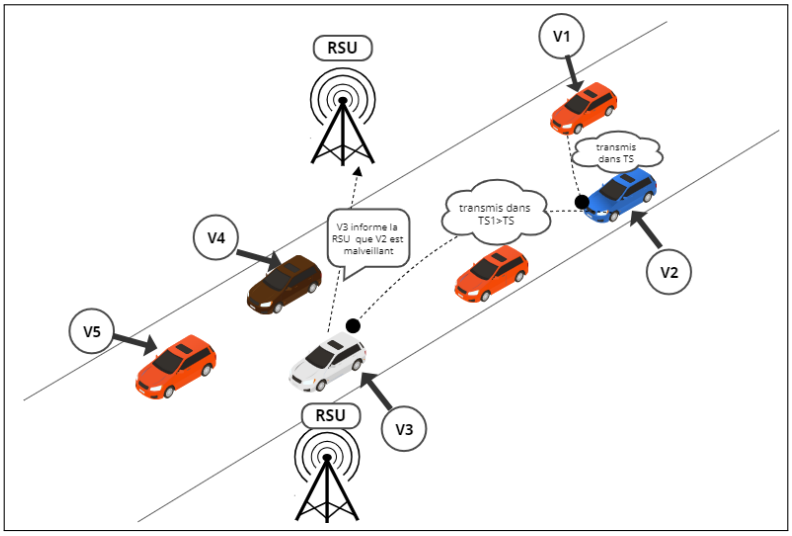

FIGURE 4.9 – Schéma illustratif du cas 4 : détection du véhicule malveillant v_2

4.4.5 Cas 5 : Paquet sécurisé

Un véhicule v_1 souhaite envoyer un message à v_7, RSU vérifie la requête l'autorise et lui donne un TS. Le véhicule transmet son message via v_3, v_4, v_5 et v_6. La transmission se fait dans le délai TS accordé par la RSU et le paquet arrive à destination correctement.

4.5 Conclusion

Dans ce chapitre, nous avons présenté un nouvel algorithme DoS avec une sécurité à deux niveaux pour contrer les attaques par déni de service. Notre algorithme vise à renforcer la résilience du réseau en fournissant une première ligne de défense basée sur la détection des attaques des requêtes, ainsi qu'une seconde ligne de défense basée sur détection des paquets attaqués.

Nous avons décrit le modèle du réseau sur lequel repose notre algorithme, en identifiant les vulnérabilités potentielles face aux attaques DoS. Ensuite, nous avons présenté les mesures prises à chaque niveau de sécurité. Au premier niveau, nous avons détaillé les filtres et les mécanismes de détection précoce utilisés pour identifier et bloquer le trafic malveillant. Au deuxième

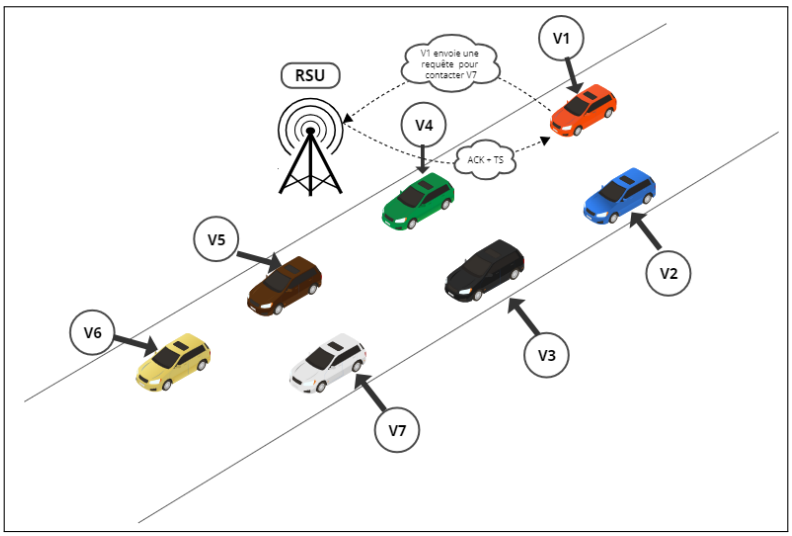

FIGURE 4.10 – Schéma illustratif du cas 5 : paquet sécurisé

niveau, nous avons expliqué les mécanismes de gestion du trafic et de redondance mis en place pour atténuer les attaques et maintenir la disponibilité des services.

Nous avons également fourni un exemple d'illustration pour montrer comment notre algorithme peut être appliqué dans un scénario concret. Cet exemple a mis en évidence les étapes de détection, et de filtration des attaques DoS, en mettant en avant les mécanismes utilisés à chaque niveau de sécurité. Cependant, des recherches supplémentaires et des tests approfondis sont nécessaires pour affiner et valider cet algorithme. Il s'agit d'une base solide à partir de laquelle de futures améliorations peuvent être développées pour assurer une protection plus robuste contre les attaques DoS.

Conclusion générale

En conclusion, le sujet de ce mémoire a porté sur les réseaux VANET (Vehicular Ad-Hoc Networks) et la sécurité dans ces réseaux. Les concepts généraux sur les réseaux VANET, tels que leur définition, leur architecture de communication, leurs caractéristiques, leurs applications et les technologies d'accès utilisées, ont été présentés dans la première partie. Nous avons également mis l'accent sur les difficultés liées à ces réseaux.
La deuxième partie du mémoire a mis l'accent sur la sécurité dans les VANETs. Nous avons défini la sécurité et énoncé ses objectifs, puis nous avons examiné différentes attaques qui peuvent survenir dans les réseaux VANETs, telles que l'usurpation d'identité, l'injection de fausses informations et les attaques par déni de service. Ensuite, nous avons exploré divers mécanismes de sécurité, tels que la cryptographie, les fonctions de hachage, les signatures numériques, les codes d'authentification de message et les certificats numériques.

La troisième partie du mémoire a été spécialement consacrée aux attaques par déni de service (DoS) dans les réseaux VANET. Nous avons examiné plusieurs attaques DoS (l'attaque Blackhole, l'attaque Greyhole, l'attaque par déni de service distribué, l'attaque Wormhole et l'attaque Jamming). De plus, nous avons présenté des travaux connexes à ce domaine, tels que la détection d'attaques Jamming, le contrôle d'accès basé sur la localisation et divers algorithmes de détection et de prévention des attaques DoS.
Enfin, nous avons proposé un algorithme de détection d' attaques DoS dans les VANETs dans la quatrième partie. Nous avons décrit cet algorithme en détail en mettant l'accent sur la sécurisation des requêtes et des paquets ainsi que l'élimination des nœuds malveillants. Pour mieux comprendre comment fonctionne l'algorithme, nous avons également fourni un exemple.
En résumé, ce mémoire nous a aidé à mieux comprendre les réseaux VANETs et leur sécurité. Les recherches effectuées ont permis de souligner les différents types d'attaques potentielles, les systèmes de sécurité employés et les techniques de détection et de prévention des attaques DoS. De nouvelles recherches dans le domaine de la sécurité des réseaux VANETs seront menées dans le but de renforcer la protection des communications et de garantir la fiabilité des échanges d'informations au sein de ces réseaux en constante évolution. Les résultats obtenus ouvrent la voie à de nouvelles recherches dans ce domaine.

Venir à la réalisation de ce mémoire a été une étape cruciale dans notre compréhension des réseaux VANETs et de la sécurité informatique. Notre aspiration est que cette recherche facilite la poursuite de la recherche et du développement dans ce domaine, fournissant une base solide pour les futures progressions de la sécurité des réseaux VANETs.

Ce travail est bien évidemment loin d'être achevé. Nous souhaitons simuler et proposer une modélisation de cet algorithme dans un avenir proche, ainsi q'une étude des performences de ce denier.

Bibliographie

[1] A.BERRABAH, H.Saidi , Université Abou Bakr Belkaid– Tlemcen . Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique Option : Réseaux et Systèmes Distribués (R.S.D). Sous le thème Balancement de charges dans les réseaux Ad Hoc 2013.

[2] A. AKILAL,Cours de sécurité des systèmes d'information, 2022.

[3] A.Koffi , École de technologie supérieure UNIVERSITÉ DU Quebéc. Mémoire à l'obtention de la maîtrise avec mémoire en génie concentration, réseaux de télécommunications sous le thème : optimisation d'un réseau ad hoc de véhicules aériens sans pilote (uav) dans un environnement urbain : positionnement des uav à l'aide de l'apprentissage automatique, 2021.

[4] Aditya Sinha Prof. Santosh K. Mishra, Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack,2014.

[5] Amarpreet Singh Priya Sharma,A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA),2015.

[6] Ali Hamieh, Jalel Ben-Othman, Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution, 2009.

[7] B.Ait-salem, UNIVERSITÉ DE LIMOGES. thèse doctorat : Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques, 2011.

[8] Engoulou Richard, Sécurisation des VANETS par la méthode de réputation des nœuds,2013.

[9] Gongjun Yan, Stephan Olariu, Michele C. Weigle, Providing Location Security in Vehicular Ad-hoc Networks, 2010.

[10] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, Denial of Service (DOS) Attack and Its Possible Solutions in VANET,2010.

[11] HAMSSA HASROUNY,GESTION DE CONFIANCE ET SOLUTIONS DE SECURITE POUR LES RESEAUX VEHICULAIRES, 2018.

[12] Irshad Ahmed Sumra, Halabi Bin Hasbullah and Jamalul-lail Bin AbManan, Attacks on Security Goals (Confidentiality,Integrity, Availability) in VANET : A Survey, 2015.

[13] Karan Verma · Halabi Hasbullah · Ashok Kumar, Titre du livre2, Prevention of DoS Attacks in VANET, 2013.

[14] Kenza MEKLICHE,Les attaques Sybil dans les réseaux véhiculaires, 2012.

[15] Kerrache, C.A. ; Calafate, C.T. ; Cano, J. ; Lagraa, N. ; Manzoni, P. Trust Management for Vehicular Networks : An Adversary-Oriented Overview. IEEE Access 2017.

[16] Kishan PatelRutvij H JhaveriRutvij H Jhaveri, Isolating Packet Dropping Misbehavior in VANET using Ant Colony Optimization, 2015.

[17] Maxime Raya,Data-Centric Trust in Ephemeral Networks,2009.

[18] Minhas, R. ; Tilal, M. Efects of Jamming On IEEE 802.11 P Systems ; Chalmers University of Technology : Gothenburg, Sweden, 2010.

[19] Mohamed NidhalMejri Jalel Ben-Othman MohamedHamdi, Survey on VANET security challenges and possible cryptographic solutions, 2014.

[20] Muhammad Sameer Sheikh Jun Liang and Wensong Wang , A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs),2019.

[21] Naveen RjNikhil SrinivasNikhil SrinivasNandhini VineethNandhini VineethSiva Venkata Chaitanya NannapaneniSiva Venkata Chaitanya Nannapaneni,A Survey on Detection and Prevention of Security Attacks in VANET, 2020.

[22] Ouanes Yessinia, Détection d'attaque DOS dans les réseaux véhiculaires,2020.

[23] Rabah Djabri,Introduction to the theory of cryptography, 2022.

[24] Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen Angela Irwin · Aamir Hassan , Vehicular ad hoc networks (VANETS) : status, results, and challenges,2010.

[25] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan, Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA), 2013.

[26] Surabhi Mahajan Prof. Alka Jindal, Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks, International Journal of Computer Applications (0975 – 8887) Volume 1– No.20, 2010.

[27] Sushil Kumar Kulwinder Singh Mann,Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs, 2019.

[28] T. Abbas Mounir , Thèse doctorat : Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et Ad hoc, 2011.

[29] Usha Devi Gandhi, R.y'S.M Keerthana, Request Response Detection Algorithm for Detecting DoS Attack in VANET, 2014.

[30] Yih-Chun Hu Adrian Perrig David B. Johnson,Packet Leashes : A Defense against Wormhole Attacks in Wireless Networks, 2003.

[31] Houssem, CHEBBAH and Boumediene REZKI and Ahmed KOURICHI,Modélisation et simulation du trou noire dans les réseaux VANETs,2018.

Résumé

La préservation de la vie privée et la garantie de la sécurité sont désormais des préoccupations cruciales au sein du réseau ad hoc véhiculaire (**Vehicle Ad Hoc Network** VANETs), qui est exposé à diverses menaces sécuritaires à l'heure actuelle. Parmi ces attaques, l'attaque par déni de services (Denial of Service (DoS)). Cette attaque peut avoir des conséquences graves, notamment en perturbant les communications entre les véhicules, en falsifiant les informations de trafic et même en mettant en danger la sécurité des conducteurs.

Dans ce travail, nous avons proposé un algorithme de détection des attaques DoS dans les VANETs, appelé 2-SDA (Two-stage detection algorithm), qui consiste à sécuriser les communications sur deux niveaux en utilisant le chiffrement RSA, les fonctions de hachage, et les signatures numériques.

L'objectif de l'algorithme 2-SDA est de garantir une protection robuste en détectant et en bloquant les nœuds malveillants à un niveau précoce de l'attaque.

Mots clés : VANETs, Sécurité, DoS, RSA, Fonction de hachage, signature numérique.

Abstract

Preserving privacy and ensuring security have become vital considerations in the Vehicular Ad Hoc Network (VANETs) due to its exposure to an array of security threats. One of these is the Denial of Service (DoS) attack. This attack can have serious consequences, including disrupting inter-vehicle communications, falsifying traffic information and even endangering driver safety.

In this work, we have proposed an algorithm for detecting DoS attacks in VANETs, called 2-SDA (Two-stage detection algorithm), which involves securing communications on two levels using RSA encryption, hash functions, and digital signatures.

The aim of the 2-SDA algorithm is to guarantee robust protection by detecting and blocking malicious nodes at an early stage of the attack.

Keywords : VANETs, Security, DoS, RSA, Hash function, digital signature.