Faculté des Sciences Exactes
Département d'Informatique

Filière : Informatique
Option : Réseaux et sécurité

Mémoire de fin de cycle
En vue de l'obtention du diplôme de Master recherche informatique

Thème

La sécurité et la confidentialité dans les VANETs

Soutenu le : 13 septembre 2023

Réalisé par :

ADNANEN Rima
ABDERRAHMANI Kenza

Devant les membres de jury :

DJEBARI Nabil	M.C.B	Encadrant	univ. de Béjaia
HAMMAMOUCHE Assia	M.C.B	Encadrante	univ. de Béjaia
MOKTEFI Mohand	M.C.B	Président	univ. de bejaia
SADI Mustapha	M.C.A	Examinateur	univ. de bejaia

Année Universitaire : 2022/2023

Remerciements

Tout d'abord, nous remercions Dieu pour nous avoir guidés tout au long de ce processus. Votre grâce et votre sagesse nous ont permis de persévérer et de réaliser notre objectif académique.

Nous sommes également profondément reconnaissants envers nos encadrants M. DJEBARI Nabil et Mm HAMMAMOUCHE Assia, dont la sagesse, les conseils et l'expertise ont été des atouts inestimables tout au long de notre projet. Votre mentorat nous a permis d'acquérir de nouvelles compétences et de développer notre compréhension du sujet.

Un grand merci aux membres du jury qui ont évalué notre travail avec soin et objectivité. Vos commentaires et vos suggestions ont contribué à améliorer notre mémoire.

Nous tenons également à remercier nos familles pour leur soutien indéfectible, leur amour inconditionnel et leur compréhension pendant cette période exigeante. Vous avez été notre source de force et de motivation.

Ce mémoire est le fruit de l'effort collectif de nombreuses personnes, et nous sommes honorés d'avoir été accompagnés par vous tous tout au long de ce voyage académique.

Rima ADNANEN, Kenza ABDERRAHMANI

Dédicace

À mes parents exceptionnels, qui m'ont inlassablement encouragé au cours des moments les plus difficiles de ce parcours académique.

À mes frères et sœurs, mes complices inestimables à chaque étape de ma vie, dont le soutien a été infaillible.

À ma tendre grand-mère, source intarissable de sagesse et d'amour, qui a éclairé mon chemin de sa lumière bienveillante.

À mon fiancé, dont la patience infinie et l'amour sans limite ont été mon refuge et mon inspiration.

À toute ma famille et mes amies, dont le soutien inconditionnel a été une force motrice précieuse tout au long de cette aventure.

Votre soutien inconditionnel m'a inspiré.

Avec tout mon amour et une reconnaissance éternelle,

Rima

Dédicace

À mes chers parents, qui m'ont toujours soutenue avec amour, patience et encouragement tout au long de ce voyage académique. Votre soutien inébranlable a été ma source d'inspiration et de motivation.

À mes frères et ma sœur, mes compagnons de vie, pour avoir partagé avec moi les hauts et les bas de cette aventure. Votre présence et vos précieux conseils ont été un réconfort constant.

À mon amie, qui a partagé avec moi les joies, les peines et les défis de cette période de ma vie. Votre amitié précieuse m'a apporté réconfort, rires et une bouffée d'air frais lorsque j'en avais le plus besoin.

À chacun de vous, je dédie ce mémoire. Vos encouragements, vos sourires et votre amour ont été la force qui m'a poussée à persévérer. Ce travail est autant le vôtre que le mien, et je suis reconnaissante de vous avoir à mes côtés.

Merci du fond du cœur pour tout votre soutien et votre amour.

Avec gratitude,

Kenza

Table des matières

Liste des tableaux

Table des figures

Liste des algorithmes

Liste des abréviations

ABAC *Contrôle d'accès basé sur les attributs*

DAC *Contrôle d'accès discrétionnaire*

DDoS *Distributed Denial of Service attack*

DSRC *Dedicated Short Range Communications*

GPS *Global Positioning System*

IBAC *Contrôle d'accès basé sur l'identité*

IEEE *Institute of Electrical and Electronics Engineers*

IP *Internet Protocol*

MAC *Media Access Control*

MAC *Contrôle d'accès obligatoire*

MITM *Man-in-the-Middle*

OBU *On-Board Unit*

OMS *Organisation Mondiale de la Santé*

RBAC *Contrôle d'accès basé sur les rôles*

RSU *Road Side Unit*

RuBAC *Contrôle d'accès basé sur les règles*

SQ *Sous-requête*

SV *Service Vanet*

TA *Trust Autority*

TPD *Tamper-Proof Devices*

VANET *Vehicular AD hoc Network*

VCS *Services de Communication VANET*

VCU *Vehicle Control Unit*

V2D *Vehicle to Device*

V2I *Vehicle to Infrastructure*

V2P *Vehicle to Pedestrian*

V2V *Vehicle to Vehicle*

V2X *Vehicle to Everything*

WLAN *Wireless Local Area Network*

Introduction générale

Les routes, malheureusement, sont le théâtre de tragédies quotidiennes. Selon l'OMS chaque année, plus de 1,35 million de personnes perdent la vie dans des accidents de la route, tandis que des dizaines de millions d'autres sont blessées. Ces chiffres, bien qu'effrayants, ne capturent qu'une partie du problème, car les accidents de la route ne se limitent pas seulement aux pertes humaines et aux blessures. Ils engendrent également d'énormes coûts sociaux et économiques, affectant les familles, les communautés et les pays entiers.

Face à ce défi majeur, ce mémoire se penche sur une solution novatrice qui vise à améliorer la sécurité routière et à protéger la vie privée des conducteurs. Nous sommes convaincus que les réseaux de communication véhiculaire (VANET) peuvent jouer un rôle clé dans la réalisation de cet objectif essentiel. Dans ce contexte, nous nous concentrons sur le développement d'une solution basée sur le contrôle d'accès pour garantir la sécurité des communications dans les VANET, tout en préservant la vie privée des conducteurs.

Dans un monde de plus en plus connecté, les réseaux de communication véhiculaire (VANET) ont émergé comme une technologie cruciale pour améliorer la sécurité routière, la gestion du trafic et la mobilité urbaine. Les VANETs offrent un potentiel considérable pour prévenir les accidents, réduire les embouteillages et minimiser l'impact environnemental des transports. Cependant, ce progrès technologique s'accompagne d'un dilemme complexe : comment concilier la nécessité d'une communication fiable et sécurisée entre les véhicules connectés dans les VANET, tout en garantissant la protection de la vie privée des conducteurs et en résistant aux menaces potentielles ?
Notre mémoire s'efforcera de répondre à ces questions et d'apporter des solutions innovantes pour relever ces défis. En fin de compte, notre objectif est de contribuer à la création d'un environnement routier plus sûr et plus sécurisé, où la connectivité des véhicules s'accompagne d'une confiance inébranlable en la sécurité et la confidentialité des données échangées.

Dans le cadre de ce projet, plusieurs objectifs ont été fixés afin d'offrir une solution pour renforcer la sécurité et la confidentialité dans les réseaux de communication véhiculaire (VANET).

- Améliorer le sécurité routière et la gestion du trafic ;
- Développer des mécanismes de sécurité robustes ;
- Préserver la vie privée des conducteurs ;
- Résistance aux attaques cybernétiques ;
- Garantir une conduite plus sécurisée et responsable ;

Notre solution consiste en une amélioration significative d'un modèle de contrôle d'accès basé sur les attributs, intégré dans une architecture étendue pour les VANET. Cette approche novatrice vise à renforcer la sécurité des communications et la protection de la vie privée des conducteurs au sein de ces réseaux en constante évolution.

Au cœur de notre solution réside la mise en place d'un système de contrôle d'accès qui utilise les attributs des véhicules et des utilisateurs pour déterminer les autorisations d'accès aux données et aux fonctionnalités du réseau. Nous étendons cette approche en intégrant des mécanismes de gestion des déconnexion, en cas de perte de connexion ou de perturbation du réseau, permettant ainsi une adaptation en temps réel aux besoins de sécurité spécifiques de chaque situation.

Chapitre 1

Généralités sur les VANETs

1.1 Introduction

Les Véhicules Ad Hoc Networks, abrégés VANETs, représentent une innovation majeure dans le domaine des communications sans fil appliquées aux véhicules. Ces réseaux permettent aux véhicules de communiquer entre eux et avec les infrastructures routières, offrant ainsi un potentiel considérable pour améliorer la sécurité routière, la gestion du trafic et le confort des conducteurs. Ce chapitre introductif jettera les bases en explorant les principaux concepts des VANETs, leur architecture, leurs composants clés, ainsi que les défis et les opportunités qu'ils présentent en matière de sécurité et d'applications diverses. En outre, nous aborderons les types de communication, les menaces potentielles et les contre-mesures essentielles pour un déploiement sécurisé des VANETs.

1.2 Architecture et composants

1.2.1 Architecture

L'architecture VANET peut être divisée en trois catégories qui sont :

1. **Architecture cellulaire/WLAN**

   L'infrastructure de réseau se compose d'une passerelle cellulaire ou d'un point d'accès.

2. **Ad hoc**

   Lorsqu'aucune infrastructure n'est disponible, les nœuds doivent communiquer entre eux sans dépendre d'une infrastructure.

3. **Hybrides**

   Parfois, divers points d'accès, tels que des passerelles cellulaires, seront disponibles pour la communication. Dans ce cas, les nœuds peuvent communiquer avec ces infrastructures ou ils peuvent également communiquer directement entre eux.

Voici la figure qui illustre l'architecture générale du VANET.

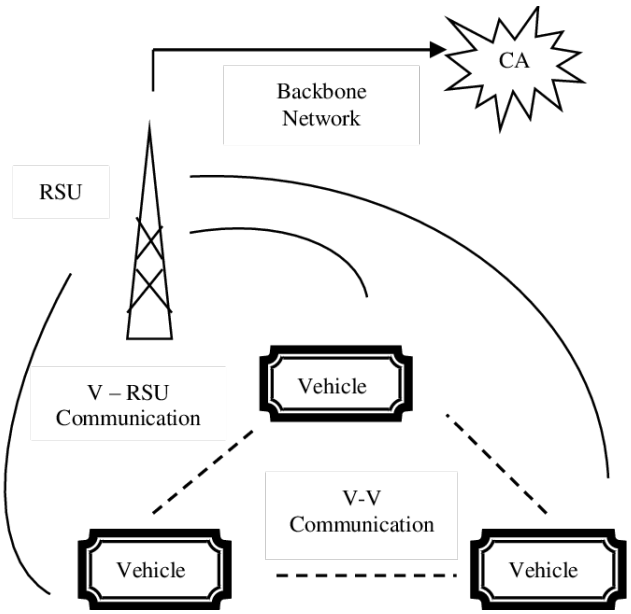


Figure 1.1 – L'architecture générale du VANET
[2]

1.2.2 Composants

Un environnement VANET est principalement composé de trois composants : une autorité de confiance TA, une unité de bord de route RSU et une unité embarquée OBU.

1. **Autorité de Confiance**

   l'autorité de confiance joue un rôle central dans la garantie de la sécurité et de la confidentialité des communications au sein des VANETs. Elle assure l'authentification des véhicules, la gestion des clés, la prévention des attaques et la mise en place de politiques de sécurité efficaces pour protéger les utilisateurs et les données dans ces réseaux critiques. Elle peut aussi dans certaines circonstances révéler l'identité de l'expéditeur d'un message.

2. **Unitée Embarquée**

   Une unité embarquée (OBU) est un dispositif matériel monté sur le véhicule. L'objectif principal d'une OBU est de communiquer avec d'autres UBO et RSU. Il a typiquement un émetteur-récepteur composé d'une antenne de radiofréquence attachée à un processeur, tout comme un routeur. Il a également la mémoire de lecture / écriture pour stocker et récupérer des informations, et une interface utilisateur. L'unité de contrôle des véhicules (VCU) coordonne avec l'OBU la collecte et la diffusion de statistiques sur les véhicules. Un OBU peut également avoir d'autres interfaces, comme USB et Bluetooth, pour se connecter à d'autres appareils sur le véhicule, comme les ordinateurs portables, les smartphones..etc, Voir figure 1.2.
   Bien qu'un OBU puisse être rendu très sophistiqué en ajoutant un certain nombre de caractéristiques, les exigences de base et les responsabilités d'un OBU sont les suivantes :
   - Une antenne de radiofréquence pour accéder au canal sans fil afin de communiquer avec d'autres OBU et RSU.
   - Transmission de données pour le compte d'autres OBU, ce qui comprend le routage, le contrôle de la congestion du réseau, la sécurité des données et la mobilité IP.
   - Une interface utilisateur pour échanger des informations avec l'utilisateur final, ou une connexion avec un dispositif doté d'une interface utilisateur.
   - Mécanisme de génération de messages de sécurité à partager avec d'autres OBU et RSU.

FIGURE 1.2 – L'unité embarquée
[2]

3. **Unitée de Bord de Route**

Les RSU sont généralement des dispositifs fixes qui sont fixés le long des routes ou dans des endroits dédiés tels que les places de stationnement ou les intersections routières. Semblable à un OBU, un RSU dispose également d'un émetteur-récepteur, d'une antenne, d'un processeur et de capteurs. Les RSU ont des interfaces filaires et sans fil. L'interface sans fil est utilisée pour communiquer avec les OBU montés sur les véhicules, et l'interface filaire est utilisée pour se connecter avec d'autres RSU et Internet. Chaque RSU utilise une radio DSRC basée sur la technologie radio IEEE 802.11p pour accéder au canal sans fil. OBU interagit avec l'unité de contrôle du véhicule VCU pour l'échange d'informations. RSU a une interface supplémentaire pour se connecter aux autres RSU et Internet, Voir figure 1.3.
En résumé, les principales fonctionnalités d'une RSU sont les suivantes :

- Une antenne à haute fréquence, haute puissance et longue portée pour accéder à un support sans fil.
- Transmission de paquets de données aux OBU de sa gamme et aux autres RSU.
- Agrégation des informations de sécurité provenant des OBU par le biais de demandes de sécurité et d'alarmes concernant les OBU entrantes.
- Travailler comme passerelle pour fournir une connectivité Internet aux OBU.
- Capacité de stockage pour stocker les informations provenant de l'OBU du véhicule et de la TA.

FIGURE 1.3 – L'unité de board de la route
[19]

Les RSU prennent en charge les protocoles IEEE 802.11p et les quatre protocoles IEEE 1609. En plus des protocoles d'accès aux canaux sans fil, les RSU prennent également en charge l'accès aux canaux filaires, comme un câble coaxial ou un câble à fibre optique, avec des protocoles Ethernet.

1.3 Types de communication dans VANET

Il existe trois types de communication dans les VANET : véhicule à véhicule V2V, véhicule-infrastructure V2I et Hybride [14] comme illustré dans la figure 1.4.

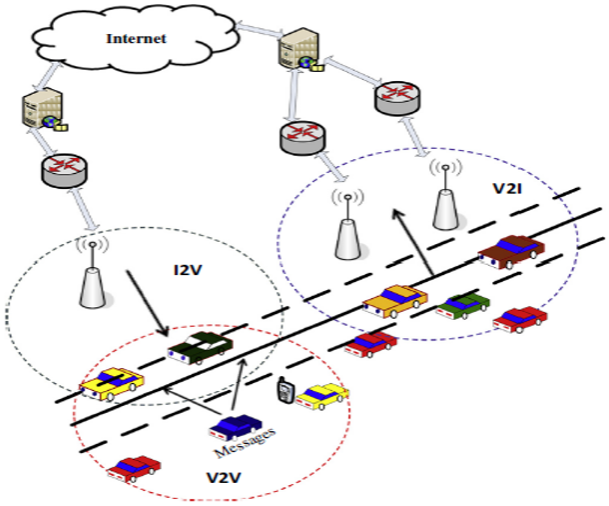


FIGURE 1.4 – Les types de communication dans VANET
[14]

1.3.1 Communications V2V

Dans ce mode, aucune infrastructure n'est utilisée, aucune installation n'est nécessaire sur les routes, chaque véhicule est équipé pour communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds (véhicules) voisins qui les séparent comme des relais, Voir figure 1.5.

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

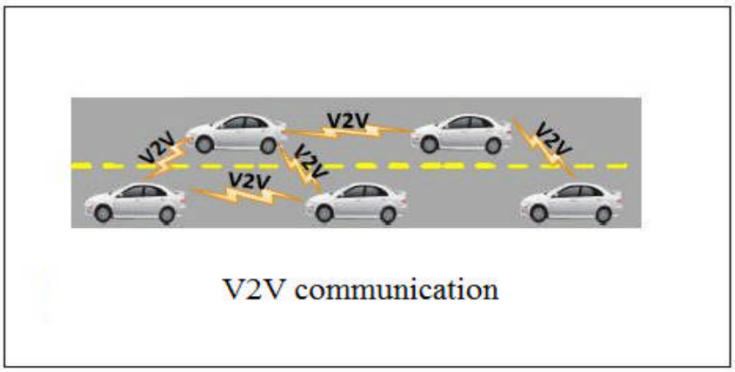


FIGURE 1.5 – Communication véhicule à véhicule
[14]

1.3.2 Communications V2I

Celle-ci est une architecture centralisée basée sur des stations de bases (Infrastructure) dans leurs communications, les véhicules garantissent des communications avec l'infrastructure en utilisant des points d'infrastructure. Ces points d'accès sont également connus sous le nom RSU (Road Side Unit), situés dans certaines sections critiques de la route, tels que les feux de circulation, les zones d'intersections, ou les panneaux de Stop, afin d'améliorer l'expérience de conduite et la rendre plus sûre. Cette architecture peut être utilisée dans les scénarios comme accès à Internet, état de la circulation, contrôle de vitesse...etc, Voir figure 1.6.

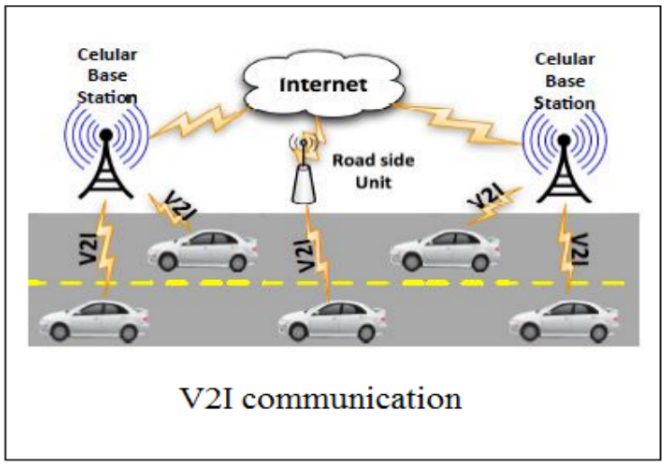


FIGURE 1.6 – Comunication véhicule à infrastructure
[14]

1.3.3 Communication véhicule-à-tout V2X

La communication V2X englobe tous les types de communication dans les VANET, y compris V2V, V2I, mais aussi V2P (véhicule à piéton) et V2N (véhicule à réseau)[7]. Voir figure 1.7.

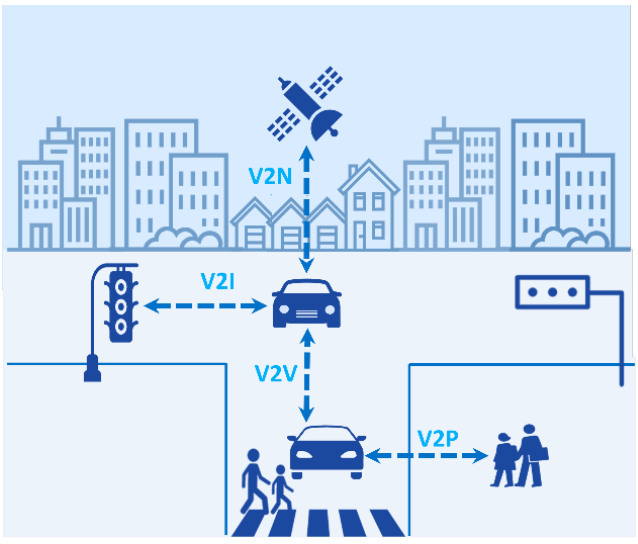


FIGURE 1.7 – Comunication véhicule à tout
[7]

1.3.4 Communications Hybrides

La combinaison de ces deux types de communications permet d'obtenir une communication hybride très intéressante (voir FIGURE 1.8). En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette portée. Dans un but économique et afin d'éviter la multiplication des stations de base, l'utilisation des sauts par véhicules intermédiaires prend toute son importance. Les entités formant un réseau sans fil véhiculaire vont générer et s'échanger des messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer ou recevoir un message de contrôle, d'alerte ou autre, Voir figure 1.8.

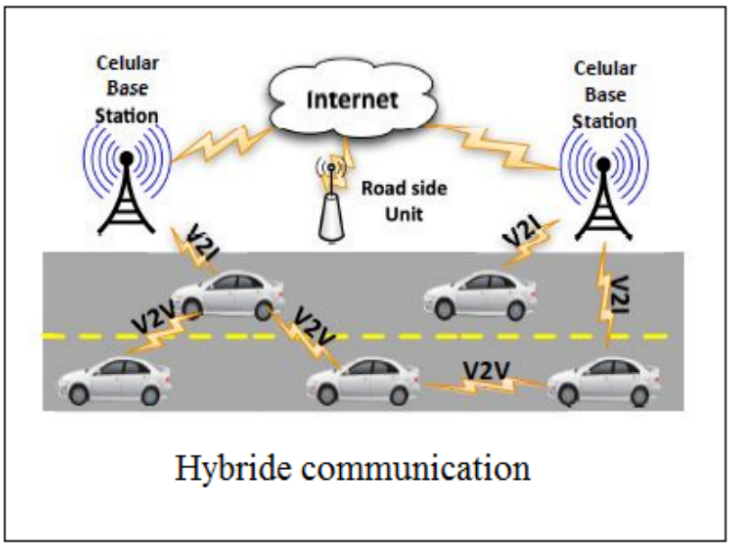


FIGURE 1.8 – Communication hybride
[14]

1.4 Caractéristiques du réseau VANET

Les réseaux véhiculaires (VANET) présentent des caractéristiques spécifiques telles que [1] :

1.4.1 Mobilité

Chaque nœud de VANET se déplace généralement à grande vitesse. Par conséquent, la grande mobilité des nœuds réduit le temps de communication entre les nœuds du réseau.

1.4.2 Aucune contrainte d'énergie

Les VANET ne souffrent pas de problèmes d'alimentation comme dans les MANET, car les OBU peuvent obtenir une alimentation continue grâce à la batterie longue durée.

1.4.3 Applications diverses

Les VANETs prennent en charge une variété d'applications allant de la sécurité routière et des alertes de trafic aux services de divertissement et de communication pour les occupants du véhicule.

1.4.4 Autonomie des nœuds

Les véhicules dans les réseaux véhiculaires ad hoc (VANET) fonctionnent comme des nœuds autonomes du réseau, leur permettant ainsi d'établir et de gérer des connexions sans avoir besoin d'une infrastructure centrale fixe.

1.5 Défis du réseau VANET

Les défis des VANET sont liés à la diffusion fréquente de balises émises par chaque véhicule équipé d'OBU, contenant des informations essentielles telles que l'emplacement, la vitesse, le cap et les événements de circulation. Ces balises sont diffusées plus de trois fois par seconde sur une courte portée de quelques mètres. En raison de cette diffusion dans un environnement de libre accès, chaque nœud situé à l'intérieur de cette portée reçoit ces balises, qu'il soit légal ou illégal. Pour assurer le bon fonctionnement du VANET, des défis importants doivent être relevés[6].

1.5.1 Contrainte de temps

Une exigence importante des VANET concerne la capacité à transmettre des messages dans un délai acceptable. Quelques applications, telles que celles relatives à la sécurité, nécessitent des délais. Cependant, il peut être difficile de vérifier l'authenticité des messages, ce qui augmenterait par conséquent la livraison temps et respecter le délai de livraison du message. Il est très important de respecter des délais critiques dans des cas spécifiques avec certaines applications.

1.5.2 Routage

Les protocoles de routage sont utilisés en communication ad hoc, ils permettent de déterminer la suite de nœuds que les paquets doivent traverser pour un échange d'information entre entités distantes. Les problèmes auxquels doivent répondre les protocoles de routage sont la connectivité intermittente qui rend les routes déjà établies obsolètes et le partitionnement du réseau qui empêche la propagation des paquets.

1.5.3 Sécurité

Les exigences en sécurité doivent être prises en compte aussi bien dans la conception architecturale du réseau que dans la conception des protocoles de communication. Elles diffèrent en fonction des applications et comprennent principalement la confidentialité, l'authentification, la cohérence et l'intégrité des données et la disponibilité. La satisfaction de ces exigences dans des systèmes aussi dynamiques et mobiles que les réseaux véhiculaires est difficile mais particulièrement importante étant donné que des vies humaines sont concernées.

1.5.4 Volatilité

La durée de connectivité entre deux nœuds dans les réseaux véhiculaires ad hoc (VANET) peut être variable, et ces connexions peuvent être interrompues après un seul événement. En raison de la

mobilité élevée des véhicules, les connexions entre les véhicules peuvent être perdues après seulement quelques sauts sans fil et pendant une durée limitée. De plus, étant donné que les véhicules connectés peuvent se déplacer dans des directions opposées, il peut être difficile, voire impossible, d'obtenir un contexte de longue durée dans les VANETs.

1.6 Applications des réseaux VANET

Dans le réseau véhiculaire sans fil, on trouve plusieurs types d'applications ou services qu'on peut classer en 3 catégories [4] :

1.6.1 Applications liées au confort

Comme certains voyages peuvent parfois être longs, dû au trajet ou aux congestions sur la route, les réseaux VANETs contribuent également à l'amélioration du confort en permettant d'assurer le confort des véhicules et leurs occupants durant leurs voyages ; ces services comprennent, entre autres l'accès à Internet, la messagerie, le chat inter – véhicule, etc. L'utilisation de ce genre d'applications permet aux passagers de s'échanger des musiques, vidéos ou d'accéder à des jeux. Aussi, on pourra procéder à la vérification à distance des permis de conduire, des plaques d'immatriculation par les autorités compétentes, le paiement électronique au niveau des points de péage afin de faire gagner du temps aux utilisateurs.

1.6.2 Applications d'optimisation et d'amélioration du trafic routier

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

1.6.3 Applications de prévention et de sécurité du trafic routier

Comme les applications de préventions et de sécurité du trafic routier ont un impact direct sur la sécurité des personnes et des biens, les conducteurs peuvent être avertis des accidents ou autres situations dangereuses (alerte pour les travaux routiers, informations météorologiques) en recevant des messages d'alerte diffusés entre les différentes entités afin d'être plus vigilant et de réduire leur vitesse. Comme ces applications contribuent à la diminution du nombre d'accidents sur les routes, elles aident à préserver la vie humaine. Un service de ces applications qui est un service SOS en cas d'accident est déjà implémenté dans certaines voitures actuelles. Il consiste à envoyer un message afin de prévenir le secours le plus proche.

1.7 Exigences de sécurité

La sécurité joue un rôle crucial dans les réseaux véhiculaires ad hoc (VANET), afin d'assurer un déploiement sécurisé du réseau VANET, certaines exigences doivent être satisfaites[1].

1.7.1 Confidentialité

Garantie que les informations échangées entre les véhicules restent confidentielles et ne sont pas accessibles par des parties non autorisées,et garantit ainsi que les données n'ont pas été consultées jusqu'à leur réception par le destinataire désigné.

1.7.2 Intégrité

L'intégrité des données garantit que le contenu des données est préservé de toute modification pendant le transit.

1.7.3 Autentification

L'authentification joue un rôle crucial pour protéger les réseaux véhiculaires ad hoc (VANET) contre les attaques malveillantes. En vérifiant l'identité des véhicules et des utilisateurs, elle assure que seuls les véhicules autorisés peuvent accéder au réseau et échanger des informations.

1.7.4 Disponibilité

La disponibilité est une exigence cruciale dans les réseaux véhiculaires ad hoc (VANET). Elle garantit que le réseau reste opérationnel et fonctionnel en permanence, permettant ainsi aux utilisateurs et aux véhicules participants d'accéder aux informations et aux services à tout moment.

1.7.5 Non-répudiation

La non-répudiation est le service qui garantit que les parties émettrice et réceptrice des données ne peuvent pas refuser leur transmission et leur réception en cas de litige.

1.7.6 Contrôle d'accès

Le contrôle d'accès gère les autorisations d'accès, bloque les utilisateurs non autorisés et définit les niveaux d'accès. Cela assure la sécurité des réseaux en limitant l'entrée aux entités autorisées, notamment dans les applications de sécurité routière.

1.8 Normes et standards

1.8.1 La norme DSRC (Dedicated Short Range Communications)

La norme DSRC (Dedicated Short-Range Communications) est une norme de communication sans fil spécialement conçue pour les réseaux véhiculaires ad hoc (VANET) et les applications de

transport intelligent. Elle a été développée pour permettre aux véhicules de communiquer entre eux et avec les infrastructures routières afin d'améliorer la sécurité routière, l'efficacité du trafic et la connectivité des véhicules. Le spectre DSRC de 75 MHz comme le montre la figure 1.7 est divisé en sept canaux de 10 MHz, allant du canal 172 (Ch 172) au canal 184 (Ch 184). Le Ch 178 est entièrement utilisé comme canal de contrôle qui prend en charge toutes les diffusions d'applications de sécurité de niveau de puissance. Les canaux 172 et 184 sont réservés exclusivement à l'envoi de messages de sécurité, tandis que les autres canaux de service (Ch 174, Ch 176, Ch 180 et Ch 182) sont utilisés pour transmettre à la fois des messages de sécurité et de non-sécurité[2].

1.8.2 La norme WAVE (Wireless Access in Vehicular Environments)

La norme WAVE englobe un ensemble de normes et de protocoles d'accès sans fil destinés aux environnements véhiculaires. Cette architecture comprend des standards, des services et des interfaces spécialement conçus pour assurer la sécurité des divers types de communications dans le réseau VANET. L'IEEE (Institute of Electrical and Electronics Engineers) a également défini le standard WAVE sous la désignation IEEE 1609[2].

1.8.3 IEEE 1609.1

Elle fournit un gestionnaire de ressources qui facilite la communication entre les applications et les véhicules en gérant efficacement l'allocation et l'utilisation des ressources réseau. Elle définit également le format de message et le mode de stockage des données.

1.8.4 IEEE 1609.2

Elle définit les services de sécurité des applications, les conditions d'échange, la gestion et les formats des messages dans les réseaux VANET. Elle répond aux exigences de sécurité du système de réseau VANET en assurant la confidentialité, l'intégrité et l'authenticité des communications.

1.8.5 IEEE 1609.3

Elle se concentre sur les couches de services de transport et de réseaux, incluant l'adressage et le routage dans les réseaux VANET. Elle définit également le WSM (Wave Short Message) ainsi que le protocole d'échange WSMP (Wave Short Message Protocol), ce qui facilite la transmission rapide et fiable d'informations.

1.8.6 IEEE 1609.4

Elle définit les opérations multi-canaux en utilisant le mécanisme EDCA (Enhanced Distributed Channel Access) de la sous-couche MAC (Medium Access Control). Ce mécanisme s'appuie sur le principe du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) utilisé dans les réseaux informatiques pour gérer l'accès au canal.

1.8.7 IEEE 802.11p

Plus couramment connue sous le nom de Wi-Fi. Cette norme a été spécifiquement conçue pour répondre aux besoins des réseaux véhiculaires ad hoc (VANET). Le standard IEEE 802.11p définit des caractéristiques spécifiques pour ce domaine, en utilisant une bande passante de 5,9 GHz pour permettre l'échange de données avec un débit variant de 6 à 27 Mb/s et une portée allant jusqu'à 1000 mètres[2].

1.9 Types de messages

Trois types de messages s'échangent entre les différentes entités du réseau véhiculaire sans fil [4].

1.9.1 Messages beacon

Aussi appelé message de contrôle ou d'identification, ils sont envoyés à intervalles réguliers, par convention. Un véhicule envoie un message beacon tous les 100ms. Ils contiennent des informations personnelles sur les véhicules telles que : sa vitesse, sa position GPS, sa direction, etc. Grâce à ce type de message, les véhicules se font connaître à leur entourage .

1.9.2 Messages d'alerte

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

1.9.3 Autres messages

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

1.10 Profils d'Attaquants

Les différents profils d'attaquants présents dans les VANETs sont [6] :

1.10.1 Outsider vs insider

Les outsiders sont les noeuds qui n'appartient pas au VANET et qu'ils ne sont pas authentifiés, ils peuvent espionner le réseau afin de racueillir des informations sur les usagers de la route et les utilises pour une attaque future. Les insiders sont des noeuds authentifiés, ils ont accés a toutes les connaissances dans le réseau et ils peuvent compromettre tout type d'attaques.

1.10.2 Malveillant vs rationnel

L'entité malveillante est motivée par le plaisir de le faire, elle n'a pas une cible spécifique et elle ne cherche pas un résultat précis, tandis que l'entité rationnelle a une cible précise comme l'usurpation d'identité, l'espionnage ou retarder ou supprimer les messages.

1.10.3 Actif vs passif

Le noeud actif c'est celui qui peut envoyer des messages pour nuire d'autres noeuds, tandis que le noeud passif est celui qui écoute les communications entre les noeuds, il n'a aucune autorisation et il ne cause pas des dommages directes, le noeud passif est un outsider.

1.11 Attaquants

Un attaquant est une entité qui compromet la sécurité et viole la vie privée d'une autre entité. Certains attaquants le fait que pour le plaisir tandis que d'autres leurs intentions est de provoquer des dommages graves. Quelque catégories d'attaquants sont abordé dans cette section, qui sont [12] :

1.11.1 Conducteur égoïste

Un conducteur qui exploite le système pour maximiser les profits.

1.11.2 Snooper

Cette personne essaie de recueillir des informations sur le véhicule cible à partir de ses émissions afin qu'il puisse être identifié et facilement suivi.

1.11.3 Espion industriel

Est une personne qui appartient au fabricant d'automobiles et qui pourrait trafiquer le système GPS, les capteurs du véhicule ou d'autres dispositifs sensibles. Un dispositif (TPD) est recommandé d'être utilisé pour empêcher ce type d'attaquant.

1.12 Menaces de sécurité

Les VANETs souffrent de différents types de menaces et d'attaques, et les dommages causés par ces attaques peuvent dysfonctionner les applications du réseau. Cette section présente les attaques

les plus courantes dans les VANEt, qui sont classifiées en 2 classes qui sont [12] :

1.12.1 Attaques par déni de service

Attaques par déni de service

C'est l'une des attaques courantes dans les VANETs, elle se produit lorsque le véhicule malveillant envoie plusieurs messages qui bloquent tous les moyens de communication possibles. L'attaque peut être effectuée par plusieurs attaquants simultanément d'une manière distribuée qui est appelée déni de service distribué (DDoS).

Attaque de spamming

Elle consiste à envoyer de manière excessive et non sollicitée des messages aux véhicules participants ou aux infrastructures routières. Ces messages non désirés peuvent surcharger les canaux de communication, perturber les échanges d'informations légitimes entre les véhicules, et entraîner une dégradation des performances du réseau.

Attaque de trou noir

Est une forme d'attaque malveillante où un nœud compromis ou malveillant annonce faussement qu'il possède la route la plus courte ou la meilleure connectivité vers une destination spécifique. En conséquence, les autres nœuds du réseau peuvent rediriger leur trafic vers ce nœud malveillant, entraînant ainsi la perte de données ou la déconnexion des nœuds du réseau.

Attaque de brouillage

Est une forme d'attaque malveillante où un attaquant émet intentionnellement des signaux radioélectriques perturbateurs sur la même fréquence utilisée par le réseau VANET. Ces interférences peuvent entraîner des connexions instables, des déconnexions ou une dégradation générale des performances du réseau. L'objectif de cette attaque est de perturber les communications sans fil entre les véhicules et les infrastructures, rendant ainsi les transmissions inefficaces ou impossibles.

Attaque par rejeu

Est une forme d'attaque où un attaquant enregistre et répète les messages échangés entre les nœuds du réseau. L'objectif de cette attaque est de perturber le bon fonctionnement du réseau en répétant les messages déjà transmis, ce qui peut entraîner une surcharge du réseau et une dégradation des performances.

Attaque Sybil

Un attaquant utilise une entité défectueuse pour créer plusieurs fausses identités et agit ensuite comme quelques véhicules pour prendre le contrôle d'une partie du système, ce qui permit à l'attaquant de produire une illusion à d'autres véhicules.

1.12.2 Attaque d'intrusion

Écoute clandestine

Cette attaque se produit lorsque l'attaquant se trouve dans un véhicule immobile ou en mouvement, ou dans une fausse RSU. Le but est d'obtenir un accès non autorisé à des données confidentielles.

Attaque de l'homme du milieu (MITM)

Est une forme d'attaque où un attaquant intercepte et modifie les communications entre deux nœuds sans que les parties concernées en aient conscience. L'attaquant se place entre les véhicules participants ou entre un véhicule et une infrastructure routière, agissant comme un relais dans les communications. De cette manière, il peut non seulement accéder aux données échangées mais également les manipuler, altérant ainsi les informations transmises ou en injectant des données malveillantes

Usurpation d'identité

Un attaquant se fait passer pour un autre véhicule en utilisant une fausse identité dans un but malveillant, il peut prétendre être un RSU pour envoyer de fausses publicités aux véhicules dans sa gamme de couverture.

1.13 Contre-mesures

Dans le tableau 1.1 nous résumons les attaques de sécurité mentionné précédemment dans les VANET. Pour chaque attaque, nous décrivons les services de sécurité violés et décrivons également les contre-mesures possibles associées [1].

Attaque	**Service de sécurité violé**	**Contre-mesure**
Attaque par déni de service	Disponibilité	Utiliser un schéma de pré-authentification.
Attaque de spamming	Disponibilité	cadre intégré de lutte contre les logiciels malveillants.
Attaque de trou noir	Disponibilité	Utiliser un protocole AODV (Ad hoc On-Demand Distance Vector) avec détection, prévention et réaction aux attaques.
Écoute clandestine	Confidentialité	Utiliser des techniques de chiffrement
Attaque de l'homme du milieu	Confidentialité	Utiliser des méthodes d'authentification solides Utiliser des fonctions de hachage.
Attaque de brouillage	Disponibilité	Utiliser une technique de contre-mesure basée sur un seuil de brouillage.
Attaque par rejeu	Authentification et Intégrité	Utiliser une heure globalement synchronisée pour tous les nœuds.
Usurpation d'identité	Authentification et Intégrité	Ne pas enregistrer les mots de passe sur les ordinateurs. Changer les mots de passe régulièrement.
Attaque Sybil	Authentification	Utiliser une approche de série de timestamps.

Table 1.1 – Contre-mesures associées aux attaques pour assurer la sécurité. [1]

1.14 Conclusion

En conclusion, VANET doit être parfaitement sécurisé pour qu'il soit largement adopté par la société, et pour avoir ce but la recherche et l'industrie se concentre pour arriver à une communication inter véhicule sécurisée et un niveau de sécurité plus élevé.

Chapitre 2

Revues de la littérature

2.1 Introduction

Le chapitre 2 de ce mémoire se penche sur l'examen approfondi des solutions et des approches qui ont été préalablement proposées pour garantir la sécurité et la confidentialité au sein des Réseaux Ad hoc Véhiculaires (VANETs). Avec l'évolution rapide des technologies de communication et la croissance constante des véhicules connectés, la sécurité des échanges d'informations et la préservation de la confidentialité sont devenues des préoccupations majeures. Ce chapitre vise à présenter une synthèse des travaux antérieurs dans ce domaine, en mettant en lumière les diverses stratégies et méthodes développées pour relever ces défis complexes. À travers une série de résumés des propositions clés et des approches étudiées, ce chapitre offre un aperçu des avancées significatives réalisées jusqu'à présent, tout en jetant les bases nécessaires pour la conceptualisation et la mise en œuvre de solutions novatrices dans le domaine des VANETs.

2.2 État de l'art et approches explorées

Dans cette section dédiée à l'état de, nous allons mettre en lumière différentes propositions visant à améliorer la sécurité et l'efficacité des communications au sein des réseaux VANET, Ci-dessous (figure 2.1) le diagramme illustratif qui résume quelques travaux sur lesquel nous avons parlés dans ce chapitre.

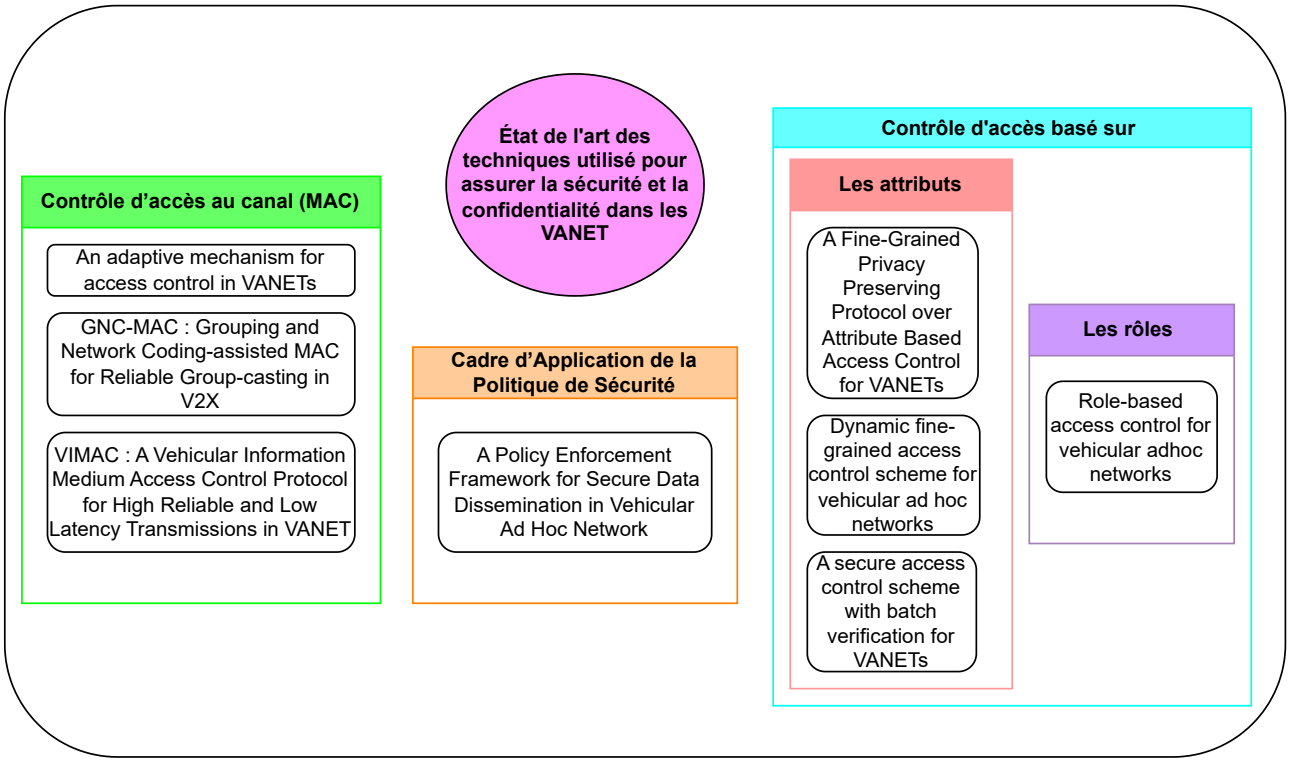


FIGURE 2.1 – Techniques utilisées pour assurer la sécurité et la confidentialité dans les VANET

2.2.1 Solutions basé sur les protocoles de contrôle d'accès au canal de communication (MAC)

Souza et al.[15], ont proposé un mécanisme d'auto-adaptation du temps de backoff dans les réseaux véhiculaires (VANETs) qui a été développé avec le soutien de l'intelligence floue pour mieux contrôler les VANET et adapter le contrôle d'accès au support de transmission (MAC). L'architecture proposée comprend deux modules principaux : un capteur d'informations contextuelles et un analyseur d'informations. L'analyseur reçoit la densité provenant du module Capteur, et le temps de recul basé sur la plage de fenêtre de contention définie par le protocole 802.11p. En utilisant la valeur reçue, l'analyseur vérifiera si cette valeur est conforme à la situation actuelle de la circulation des véhicules, ils ont utilisé un système flou pour décrire les valeurs. Ainsi, un réseau très dense devrait augmenter son temps de recul afin de réduire la quantité de collisions de paquets. Un réseau peu dense devrait réduire le temps de recul afin de ne pas sous-utiliser les ressources du réseau. L'objectif principal était d'améliorer les performances de diffusion des données dans les VANET en ajustant dynamiquement le temps de backoff des véhicules. Ils ont utilisé le simulateur NCTUns 6.0 pour les expérimentations et ont évalué les métriques de réception de paquets par seconde, de pertes et de

taux de succès. Les résultats ont montré que leur approche adaptative surpassait l'approche standard (802.11p) en termes de réception de paquets et de partage du support sans fil. Cependant, l'article présente certaines limitations, telles que la taille limitée de la simulation, la méthode d'obtention de la densité basée sur le simulateur, l'absence de comparaison avec d'autres approches d'adaptation du temps de backoff, et l'évaluation limitée des performances. Des validations expérimentales dans des environnements réels et une évaluation plus complète des performances seraient nécessaires pour confirmer l'efficacité de cette solution dans des conditions réelles de VANET. Voir figure 2.2.

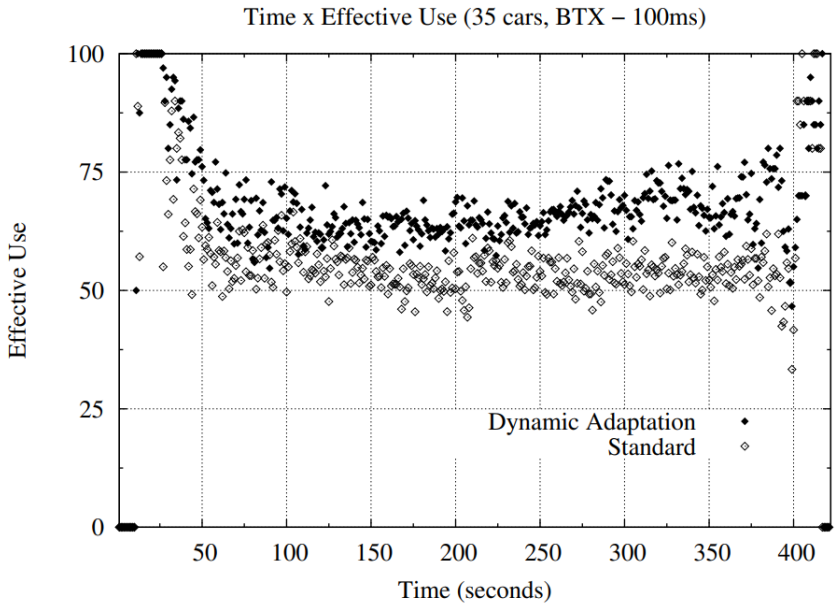


FIGURE 2.2 – Pourcentage de réussite pour les scénarios à faible densité [15]

Sun et al.[16], ont présenté un protocole MAC (Medium Access Control) basé sur TDMA (Time Division Multiple Access) pour les réseaux de véhicules (VANETs - Vehicular Ad-Hoc Networks) appellé VIMAC (Vehicular Information-based MAC). Le protocole vise à améliorer la fiabilité de la communication dans un scénario où des véhicules se déplacent sur une route à deux directions avec plusieurs voies dans chaque direction. Le protocole se compose de deux processus principaux : la prédiction et l'allocation. La prédiction vise à anticiper les collisions potentielles entre véhicules en utilisant des informations sur la position, la vitesse et la direction des véhicules. Il introduit également des éléments tels que la coopération entre les véhicules, les messages de notification d'événements d'urgence et la gestion des collisions d'accès. Des simulations sont effectuées pour comparer les performances de ce protocole avec d'autres protocoles TDMA basés sur les VANETs, montrant que le protocole proposé réduit efficacement les collisions et améliore la fiabilité de la communication.

Yue et al.[11], ont proposé un protocole conçu pour améliorer la fiabilité des communications en groupe dans les réseaux véhiculaires (VANET) appelé GNC-MAC (Generalized Network Coding-based Medium Access Control). Le GNC-MAC adopte une approche basée sur le groupement dynamique des véhicules dont Les membres d'un groupe partagent des ressources pour transmettre leurs balises aux autres membres du groupe. Il intègre un mécanisme de rétroaction basé sur le préambule qui permet aux véhicules de signaler un NACK (Negative Acknowledgement) en cas de

non-réception correcte d'une balise. Cela déclenche la retransmission de la balise, améliorant ainsi la récupération des balises perdues. Les auteurs ont effectuer une simulation où ils ont comparé le protocole proposé au protocole C-V2X (Cellular Vehicle-to-Everything). Les résultats montrent que le GNC-MAC offre des gains significatifs en termes de fiabilité de communication. Ces gains sont particulièrement notables dans des scénarios densément peuplés, où la portée de diffusion et le nombre de véhicules jouent un rôle crucial.

2.2.2 Solutions basé sur le contrôle d'accès

a) **Solutions basé sur le contrôle d'accès basé sur les attributs**

Lewis et al.[13], ont proposé un protocole de contrôle d'accès basé sur les attributs pour les réseaux véhiculaires ad hoc (VANET) afin de garantir la confidentialité des informations personnelles tout en permettant l'accès à plusieurs services sans nécessiter de nouveaux credentials. Le protocole utilise un schéma de partage de secret linéaire pour permettre un contrôle d'accès fin-grain en attribuant des clés de déchiffrement basées sur un arbre d'accès associé à des attributs. Les véhicules envoient une demande d'accréditation chiffrée au serveur, qui renvoie une autorisation chiffrée, permettant aux véhicules de générer leurs clés de déchiffrement en fonction de leur arbre d'accès. Le protocole assure l'authentification, l'autorisation et la préservation de la confidentialité de l'identité des véhicules. Les performances du protocole ont été évaluées en termes de sécurité et de coût de calcul, montrant une amélioration du taux de réception par rapport à une approche existante. Cependant il existe des limitations à prendre en compte, notamment en termes de complexité du calcul, de dépendance à une autorité de confiance centrale, et de portée de communication limitée. Voir figure 2.3.

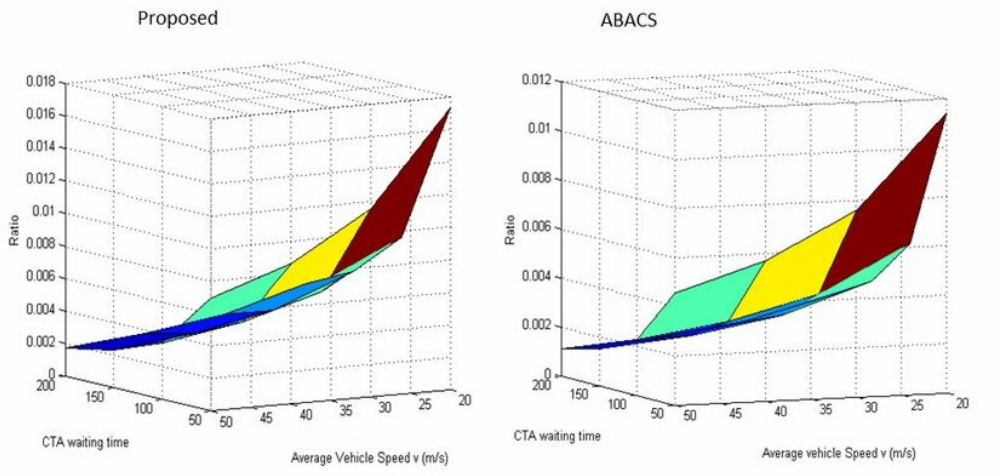


FIGURE 2.3 – Comparaison du rapport de réception entre ce protocole et ABACS pour d = 4 [13]

Djebari et al.[5], ont présenté un modèle de contrôle d'accès novateur conçu pour l'environnement des services Web, en particulier dans le contexte de l'Internet des Objets (IoT). Le modèle se base sur le modèle de contrôle d'accès basé sur les attributs (ABAC) et introduit une approche complète pour gérer les autorisations d'accès. Le processus de contrôle d'accès est divisé en trois

étapes principales : Décomposition de la demande : Cette étape permet de répartir les tâches et d'améliorer la sécurité en divisant les informations de la demande en attributs de l'utilisateur, sous-requêtes (dans le cas des services Web composites) et un plan d'exécution de la demande. Vérification des autorisations : Chaque service Web simple impliqué dans la demande vérifie les autorisations d'accès à ses opérations en se basant sur les attributs de l'utilisateur et les attributs des objets connectés de l'utilisateur. Chaque service est responsable de la vérification des sous-requêtes qui lui sont associées. Résolution des conflits : En cas de conflits d'autorisation (par exemple, des services fournissent des réponses contradictoires), le gestionnaire de sécurité utilise le plan d'exécution initial de la demande pour créer un schéma d'autorisation composite en remplaçant les sous-requêtes par leurs autorisations respectives. La résolution des conflits se fait à l'aide d'opérateurs logiques (tels que "ET" et "OU") appliqués aux autorisations.

Wang et al.[18], ont proposé un algorithme concret basé sur la politique de chiffrement du texte (CP-ABE). L'algorithme proposé DFGACS comprend quatre parties qui sont : configuration, enregistrement, chiffrement, déchiffrement. Cet algorithme permet de gérer l'accès aux informations de service diffusées dans les VANETs de manière granulaire et dynamique. Il utilise des attributs pour définir les autorisations de déchiffrement des véhicules et prend en charge la révocation dynamique des autorisations. L'objectif de cette étude est la conception d'un schéma de contrôle d'accès sécurisé et à granularité fine pour les VANET, qui implique moins de calcul et qui soit plus flexibile. Les auteurs ont examiné l'analyse des délais de calcul et de la surcharge de communication de DFGACS par rapport à d'autres schémas similaires tels que ABACS et le schéma de Lewis. Les résultats ont montré que DFGACS présente des délais de calcul inférieurs et une surcharge de communication optimisée, ce qui le rend plus adapté aux VANETs à haute vitesse. Les résultats de la simulation montrent que ABACS et le schéma de Lewis créent plus de délai de traitement que le schéma proposé. Voir figure 2.4.

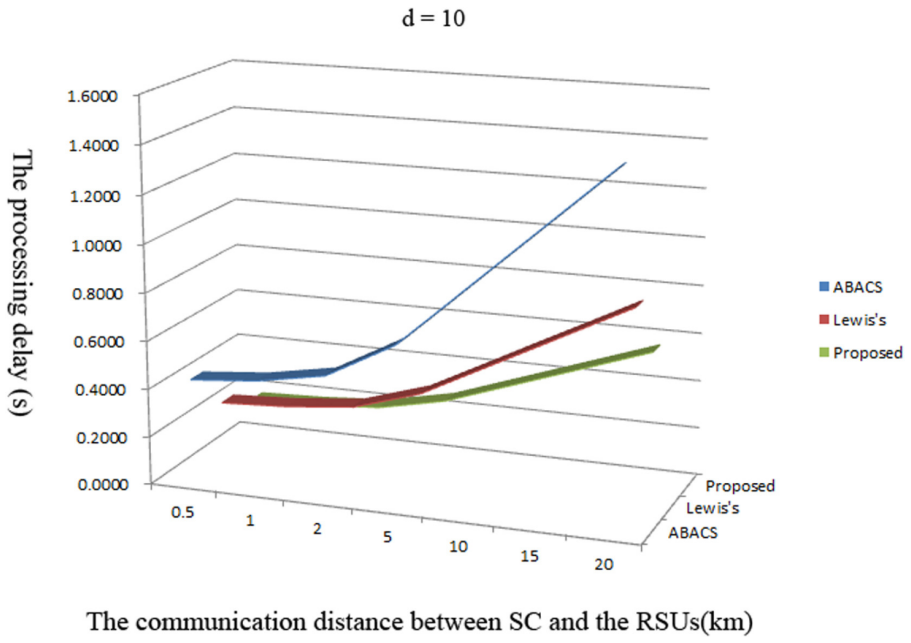


FIGURE 2.4 – Délai de traitement VS. distance de communication [18]

Wang et al.[17], ont proposé un schéma sécurisé de contrôle d'accès qui prend en charge la vérification par lots pour les VANET appelé SACSBV (Secure Access Control Scheme with Batch Verification).La solution proposé vise a assurer une authentification rapide et éfficace lorsque un nombre important d'OBU demandent d'authentifier au pris d'une RSU, dans cette proposition deux méthodes de verification de l'identité d'une OBU est presenté, la première c'est lorsque une dizaine d'OBU qui demandent d'authentifier, la verification se fait en individuel. Si le nombre de demandes dans une courte durée est grand, la verification se fait par lots. Par conséquent, l'utilisation de la vérification par lot peut grandement améliorer l'efficacité. Après l'authentification d'identité, la RSU fournit des services d'application de sécurité aux OBU autorisés selon les besoins. Cette solution est basé sur le schéma DFGACS [18]. Voir figure 2.5.

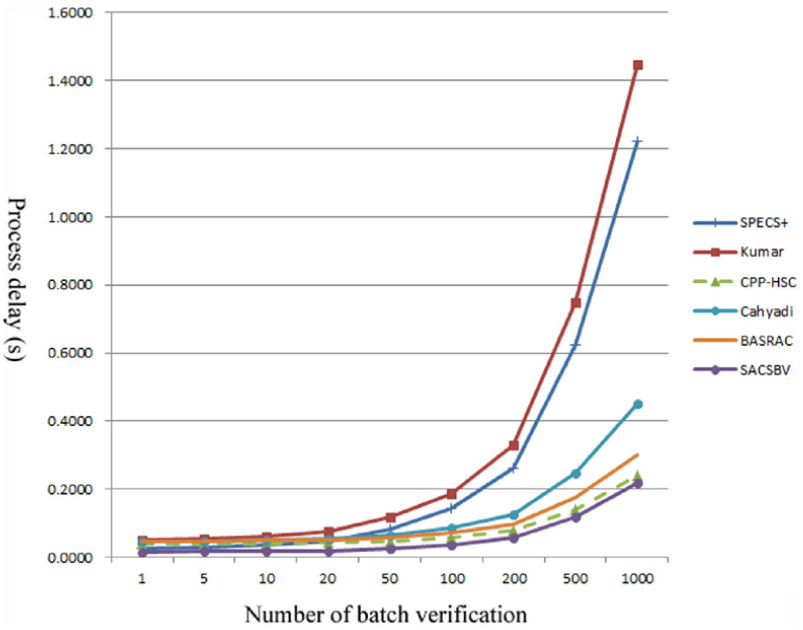


FIGURE 2.5 – Délai de traitement par rapport au nombre de vérifications par lots [17]

b) **Solution basé sur le contrôle d'accès basé sur les rôles**

kalinin et al.[9], ont développé une approche novatrice de contrôle d'accès basée sur les rôles (RBAC), spécifiquement taillée pour les VANET, visant à assurer un contrôle d'accès efficace tout en préserver la confidentialité des données sensibles. Au cœur de ce modèle RBAC se trouvent les éléments clés tels que les utilisateurs, les rôles, les sessions, les autorisations et les services, avec l'introduction d'une hiérarchie d'objets et de rôles pour refléter la complexité des interactions spécifiques aux VANET. Ce modèle permet également une réaffectation dynamique des rôles, prenant en compte des attributs variables tels que la localisation géographique et l'heure, tout en incorporant des principes de sécurité tels que la hiérarchie des rôles et la séparation des tâches pour guider sa conception. Néanmoins, il est souligné que la complexité pourrait augmenter avec la prise en compte de nombreux types d'objets et de transactions, exigeant une gestion attentive des autorisations et potentiellement un nombre élevé de rôles.

2.2.3 Solution basé sur un cadre d'application de la politique

Xia et al.[20], ont proposé un cadre d'application de la politique pour la diffusion sécurisée des données dans les réseaux ad hoc de véhicules (VANET). L'objectif principal de leur système est de permettre une diffusion sécurisée des données tout en assurant un contrôle d'accès précis et granulaire pour les véhicules participants. Les chercheurs ont utilisé le chiffrement basé sur les attributs de texte chiffré (CP-ABE) pour garantir la confidentialité des données diffusées. Ainsi, seuls les véhicules autorisés et qui satisfont aux conditions définies peuvent déchiffrer les données diffusées. Le cadre prend en compte les politiques conçues par les unités embarquées (OBU) et les stations de route (RSU). En cas de conflit, il combine les stratégies des OBU et des RSU pour garantir une diffusion des données cohérente et sans ambiguïté. Cependant, des erreurs de perception des unités de bord et des stations de route peuvent limiter l'efficacité, et la complexité des politiques peut également affecter les performances. Malgré cela, le cadre d'application de la politique se révèle prometteur pour améliorer la sécurité et la précision de la diffusion des données dans les VANET.

2.3 Tableau comparatif

Traveaux	**Catégorie**	**Critères**			
		Sécurité	**Performance**	**Adaptabilité**	**Année**
Souza et al.[15]	Basé sur les protocoles de contrôle d'accès au canal de communication (MAC)	Un meilleur contrôle d'accès au support de transmission.	L'utilisation de l'approche proactive. Qualité de transmission et de réception élevé. Résistant aux collisions. Débit élevé.	Moyenne	2011
Lewis et al. [13]	Basé sur le contrôle d'accès basé sur les attributs	Contrôle d'accès à granularité fine. Confidentialité garanti. Authentification garanti.	Délai de calcul faible. Amélioration du taux de réception par rapport à une approche existante.	Élevé	2015

Djebari et al.[5]	Basé sur le contrôle d'accès basé sur les attributs.	Contrôle d'accès à granularité fine.	L'utilisation de l'approche proactive.	Élevé	2017
kalinin et al.[9]	Basé sur le contrôle d'accès basé sur les rôles.	Confidentialité garantie Prendre en compte les défis de mobilité, de topologie changeante et de flux de données évolutifs.	Offre une réaffectation dynamique des rôles.	Élevé	2018
Sun et al.[16]	Basé sur les protocoles de contrôle d'accès au canal de communication (MAC)	Un meilleur contrôle d'accès au support de transmission.	Les réduction de collision plus élevé	Élevé	2019
Yue et al.[11]	Basé sur les protocoles de contrôle d'accès au canal de communication (MAC)	Feedback et détection d'erreurs. Fiabilité de la diffusion des messages. Gestion de groupes restreints. Prévention de collisions.	Taux de perte des balises faible. Taux de récupération des balises élevé. Assure la Scalabilité dans les scénarios denses	Élevé	2020
Wang et al.[18]	Basé sur le contrôle d'accès basé sur les attributs	Confidentialité garanti. Révocation dynamique. Contrôle d'accès à granularité fine .	Délai de calcul faible. Surcharge de communication faible.	Élevé	2021
Xia et al.[20]	Basé sur un cadre d'application de la politique	Confidentialité et sûreté renforcé	Diffusion cohérente et efficace des données	Élevé	2021

Wang et al.[17]	Basé sur le controle d'accès basé sur les attributs	Confidentialité garanti. Authentification garanti. Révocation dynamique. Contrôle d'accès à granularité fine.	Surcharge de communication faible.	Élevé	2023

TABLE 2.1: Comparaison entre les différentes solutions.

Parmi les travaux examinés dans ce chapitre, certains d'entre eux partagent des thématiques similaires. Les travaux [13][18][17][5] ont tous abordé des schémas de contrôle d'accès basés sur les attributs. Ces schémas visent à fournir une sécurité renforcée et un contrôle d'accès à granularité fine pour les VANETs. Ils ont tous adopté des approches différentes pour gérer les autorisations de déchiffrement et l'accès aux informations de service diffusées. Néanmoins, malgré les avancées significatives de ces travaux, il convient de noter les limites potentielles de la complexité de calcul. La nécessité de gérer des attributs multiples et de garantir la révocation dynamique peut entraîner des défis en matière de performances et de gestion des autorisations. Dans le cas de [15], bien que le mécanisme d'auto-adaptation du temps de backoff ait montré des améliorations en termes de réception de paquets et de partage du support sans fil, des limitations subsistent. Ces limitations incluent la taille limitée de la simulation, la méthode d'obtention de la densité basée sur le simulateur et l'absence de comparaison approfondie avec d'autres approches. D'autre part, dans [20] les auteurs ont introduit un cadre d'application de la politique pour la diffusion sécurisée. Et dans [9] les auteurs ont développé un modèle de contrôle d'accès basé sur les rôles, visant à garantir un accès efficace tout en préservant la confidentialité des données. Dans [11] les auteurs ont proposé un protocole innovant, le GNC-MAC, pour renforcer la fiabilité des communications de groupe dans les réseaux véhiculaires (VANET). Face aux perturbations fréquentes dans les scénarios denses, malgré ses bonne performance il présente certaines limitations, notamment en termes de portée de diffusion et de délai de latence.Le protocole présenté dans [16] vise à améliorer la fiabilité des communications en prévenant les collisions, à la fois dans le cas de merge collisions (collisions dues à la mobilité des véhicules) et d'access collisions (collisions dues à la concurrence pour l'accès au canal), mais il présente aussi des limitations dans les Scénarios de Mobilité Élevée, il peut y avoir des situations où la rapidité de la mobilité ou la densité de véhicules rendent plus difficile la prédiction et la prévention de toutes les collisions. Des scénarios de forte mobilité peuvent présenter des défis pour la détection et l'anticipation efficace de collisions. Une évaluation rigoureuse des performances et une adaptation aux défis spécifiques des VANETs sont essentielles pour garantir l'efficacité et la fiabilité de ces solutions dans des conditions réelles.

2.4 Conclusion

le chapitre 2 a présenté une analyse approfondie des solutions existantes et des approches adoptées pour répondre aux enjeux de sécurité et de confidentialité au sein des Réseaux Ad hoc Véhiculaires (VANETs). Cette revue de la littérature a permis de mettre en évidence la diversité des stratégies déployées, allant des mécanismes d'adaptation du temps de backoff aux schémas avancés de contrôle d'accès basés sur les attributs. Néanmoins, il ressort que malgré les avancées notables, des défis demeurent à relever, tels que la complexité des politiques de contrôle d'accès et la nécessité d'une adaptation dynamique aux environnements changeants. Cette synthèse servira de base pour la conceptualisation et l'élaboration de nouvelles solutions innovantes dans le domaine des VANETs, en vue de garantir une sécurité et une confidentialité accrues dans les échanges d'informations au sein de ces réseaux.

Chapitre 3

Application d'un contrôle d'acces dans VANET

3.1 Introduction

L'évolution constante des technologies de communication et des véhicules autonomes a ouvert la voie à une révolution dans le domaine de la mobilité. Les Réseaux de Véhicules Ad Hoc (VANETs) sont au cœur de cette transformation, offrant un potentiel immense pour améliorer la sécurité routière, l'efficacité du trafic et la connectivité des véhicules. Cependant, avec cette avancée technologique viennent également des défis significatifs en matière de sécurité et de confidentialité. Ce chapitre se concentre sur l'application pratique d'un modèle de contrôle d'accès basé sur les attributs (ABAC) spécifiquement adapté aux VANETs, explorant les défis uniques de ce domaine et mettant en lumière les avantages considérables qu'une telle approche peut offrir en termes de sécurité, de confidentialité et d'efficacité dans ces réseaux en constante évolution.

3.2 Contrôle d'accès

Le contrôle d'accès en informatique est un mécanisme qui permet de gérer l'accès aux ressources d'un système informatique, telles que les fichiers, les bases de données, les applications ou les réseaux. Il vise à contrôler qui peut accéder à quelles ressources et quelles actions ils sont autorisés à effectuer. Les modèles de contrôle d'acces reposent habituellement sur les trois entités qui sont le sujet, l'objet et l'action [3].

- **Sujet** Un sujet est une entité active, correspondant à un processus qui s'exécute pour le compte d'un utilisateur. Il peut être une application, une adresse IP, un utilisateur...etc.
- **Objet** Un objet est une entité considéré comme passive qui contient ou reçoit des informations, comme un fichier.
- **Action** l'action est une opération qui permet au sujet de manipuler l'objet. comme une lecture d'un fichier, une requête dans une base de données.

3.3 Modèles de contrôle d'accès

a) **Contrôle d'accès basé sur l'identité (IBAC)** IBAC est parmi les premiers modèles de contrôle d'accès, il est basé sur l'identité du sujet et l'identificateur de l'objet. Son objectif est de contrôler l'accès direct des sujets aux objets. Ce modèle repose sur une matrice composée d'un ensemble fini de sujets, d'objets et d'actions. Les permission sont affectées directement aux comptes utilisateurs [8].

b) **Contrôle d'accès discrétionnaire (DAC)** Selon les modèles de politiques discrétionnaires, chaque sujet peut détenir un droit de possession sur un objet. Le propriétaire de l'objet peut alors accorder d'autres droits sur l'objet. Cependant, cela entraîne une perte de confidentialité des informations [21].
Exemple :
Un droit d'accès peut être transmis sans que son propriétaire soit informé :
   - A donne un droit en lecture à B sur un de ses fichiers.
   - B copie ce fichier.
   - B étant propriétaire de la copie transmet son droit de lecture à C.

c) **Contrôle d'accès obligatoire (MAC)** Dans ce modèle, l'accès aux ressources est déterminé par des règles strictes et prédéfinies, qui sont imposées par un système de sécurité centralisé, les sujets ne peuvent pas altéré l'accès aux objets. Et donc le problème de perte de confidentialité est réglé. parmi les modèles existants : Bell-La Padula (1973), Biba (1977). [21]
Bell-La Padula : Pour éviter la divulgation de l'information, deux caractéristiques doivent être maintenues :
   - No-read-up : Un sujet ne doit pas lire des informations appartenant à un niveau supérieur car il peut connaître des informations qui ne lui sont pas autorisées.
   - No-write-down : Un sujet ne doit pas écrire dans des informations de niveau inférieur car il peut révéler des secrets.

   La politique de Bell-La Padula vise à assurer la confidentialité.

d) **Contrôle d'accès basé sur les règles (RuBAC)** RuBAC est un modèle de contrôle d'accès basé sur les règles qui utilise des règles préétablies pour contrôler l'accès aux ressources. Il s'applique a plusieurs systèmes qui améliorent le contrôle d'accès aux informations par un ensemble de normes établies par l'organisation.

e) **Contrôle d'accès basé sur les rôles (RBAC)** Le modèle de controle d'accès rbac est un modèle basé sur les rôles ce qui fait que les permissions sont affecté a des roles contrairement au modele IBAC qui donne les permissions aux utilisateurs, par exemple lors de l'enregistrement d'un nouvel utilisateur, il suffit de lui attribuer les rôles nécessaire pour la réalisation de sa mission.[21]
Exemple :
Si un docteur est à la fois chirurgien et directeur de l'hôpital, en tant que chirurgien, il aura le droit d'accès aux dossiers médicaux, alors qu'en tant que directeur, il pourra accéder aux informations administratives.

f) **Contrôle d'accès basé sur les attributs (ABAC)** Le contrôle d'accès basé sur l'attribut est le modèle de contrôle d'accès le plus granulaire et permet de réduire le nombre d'affectations de rôles. ABAC est un modèle d'authentification et d'autorisation relevant de la gestion des identités qui permet aux utilisateurs d'accéder en utilisant les attributs plutôt que les rôles. Les décisions concernant l'accès sont prises dans le cadre du contrôle ABAC en fonction des caractéristiques du sujet ou de l'utilisateur effectuant la demande d'accès, de la ressource demandée, de ce que l'utilisateur fera avec la ressource et de l'environnement (géolocalisation, réseau, etc.) ou du contexte de la demande [8].

3.4 Contrôle d'accès dans les VANETs

Les trois entités essentielles d'un contrôle d'accès dans les VANETs représentent[10] :

3.4.1 Sujet

Le sujet fait référence à l'entité qui demande un accès ou une autorisation pour effectuer une action spécifique dans le VANET. Dans ce contexte, le sujet peut être un véhicule, un utilisateur du véhicule (conducteur ou passager), un dispositif embarqué tel qu'un capteur ou un système de navigation, ou même une entité externe souhaitant interagir avec le VANET.

3.4.2 Objet

L'objet est l'entité ou la ressource à laquelle le sujet souhaite accéder ou effectuer une action. Dans le cadre des VANETs, l'objet peut être un autre véhicule, une infrastructure de communication ou de transport, des informations de localisation, des données de capteurs, des services applicatifs, etc.

3.4.3 Action

L'action représente l'opération ou l'activité spécifique que le sujet souhaite effectuer sur l'objet dans le VANET. Cela peut inclure l'échange d'informations, l'accès aux ressources, l'envoi ou la réception de messages, l'utilisation de services, etc. Les actions peuvent varier en fonction des besoins spécifiques des applications ou des services déployés dans le VANET.

3.5 ABAC dans les VANET

Le modèle de Contrôle d'Accès Basé sur les Attributs (ABAC) dans le contexte des Véhicules Connectés et Ad-Hoc (VANET) fonctionne en prenant en compte les attributs spécifiques des véhicules, des ressources et de l'environnement pour autoriser l'accès de manière granulaire et contextuelle. Voici comment ce modèle opère dans un environnement VANET :

a) **Attributs des Véhicules :** Chaque véhicule au sein du VANET est associé à des attributs qui définissent ses caractéristiques, telles que la vitesse, la localisation géographique, l'identité du

conducteur et le type de véhicule.

b) **Attributs des Ressources :** Les ressources disponibles dans VANET, comme les informations sur les conditions routières ou les alertes de sécurité, possèdent également des attributs spécifiques. Par exemple, une ressource peut être marquée comme sensible à la vitesse.

c) **Attributs Environnementaux :** Le modèle ABAC prend en compte les attributs de l'environnement, tels que les conditions météorologiques, la densité du trafic et la présence d'autres véhicules à proximité.

d) **Politiques d'Accès :** Des politiques d'accès sont définies en fonction de combinaisons d'attributs des véhicules, des ressources et de l'environnement.

e) **Demandes d'Accès :** Lorsqu'un véhicule souhaite accéder à une ressource, il envoie une demande d'accès incluant ses propres attributs ainsi que ceux de la ressource demandée.

f) **Évaluation des Politiques :** Un contrôleur d'accès évalue les demandes d'accès en fonction des politiques définies. Il vérifie si les attributs du véhicule et de la ressource satisfont les conditions énoncées dans les politiques.

g) **Décision d'Accès :** En se basant sur l'évaluation des politiques, le contrôleur d'accès prend une décision quant à l'autorisation d'accès. Si les attributs satisfont les conditions des politiques, l'accès est accordé. Sinon, l'accès est refusé.

3.6 Solution proposée

Après avoir identifié les défis liés à la sécurité et à la confidentialité au sein des réseaux VANETs, nous proposons une solution innovante reposant sur une architecture étendue. Cette architecture, conçue pour répondre aux exigences spécifiques des VANETs, vise à intégrer harmonieusement les véhicules connectés dans ces environnements dynamiques, tout en renforçant les capacités de communication et de service. Notre approche s'inspire d'une architecture existante, "Composite Web Access Control Model Applied to the Internet of Things"[5], tout en étant soigneusement élargie pour prendre en compte les attributs des véhicules connectés. Cette extension ouvre de nouvelles perspectives passionnantes en matière de sécurité, d'autorisation et de gestion des accès. Dans cette section, nous allons explorer les différentes couches de cette architecture, en mettant en lumière leur rôle crucial dans la gestion des opérations au sein des VANETs.

3.6.1 Architecture du Modèle

L'architecture du modèle reste fondamentalement la même, mais elle est étendue pour inclure les véhicules connectés dans les VANETs. L'architecture est illustré dans la figure 3.1. Elle fournit une

infrastructure essentielle pour gérer un ensemble d'opérations cruciales dans ce contexte spécifique. Cette architecture est spécialement conçue pour intégrer les véhicules connectés dans les réseaux de véhicules ad hoc (VANETs), élargissant ainsi les possibilités de communication et de services tout en maintenant les fonctionnalités de base. Les couches de l'architecture sont les suivantes :

1. **Couche de Demande**

   Cette couche gère la réception des demandes émises par les véhicules connectés. Les demandes sont décomposées en trois parties : les sous- requêtes, les attributs des utilisateurs, et maintenant, les attributs des véhicules. Chaque sous-requête est traitée par un service VANET, et les attributs des utilisateurs et des véhicules sont utilisés pour décider de l'autorisation et de la capacité à exécuter la demande.

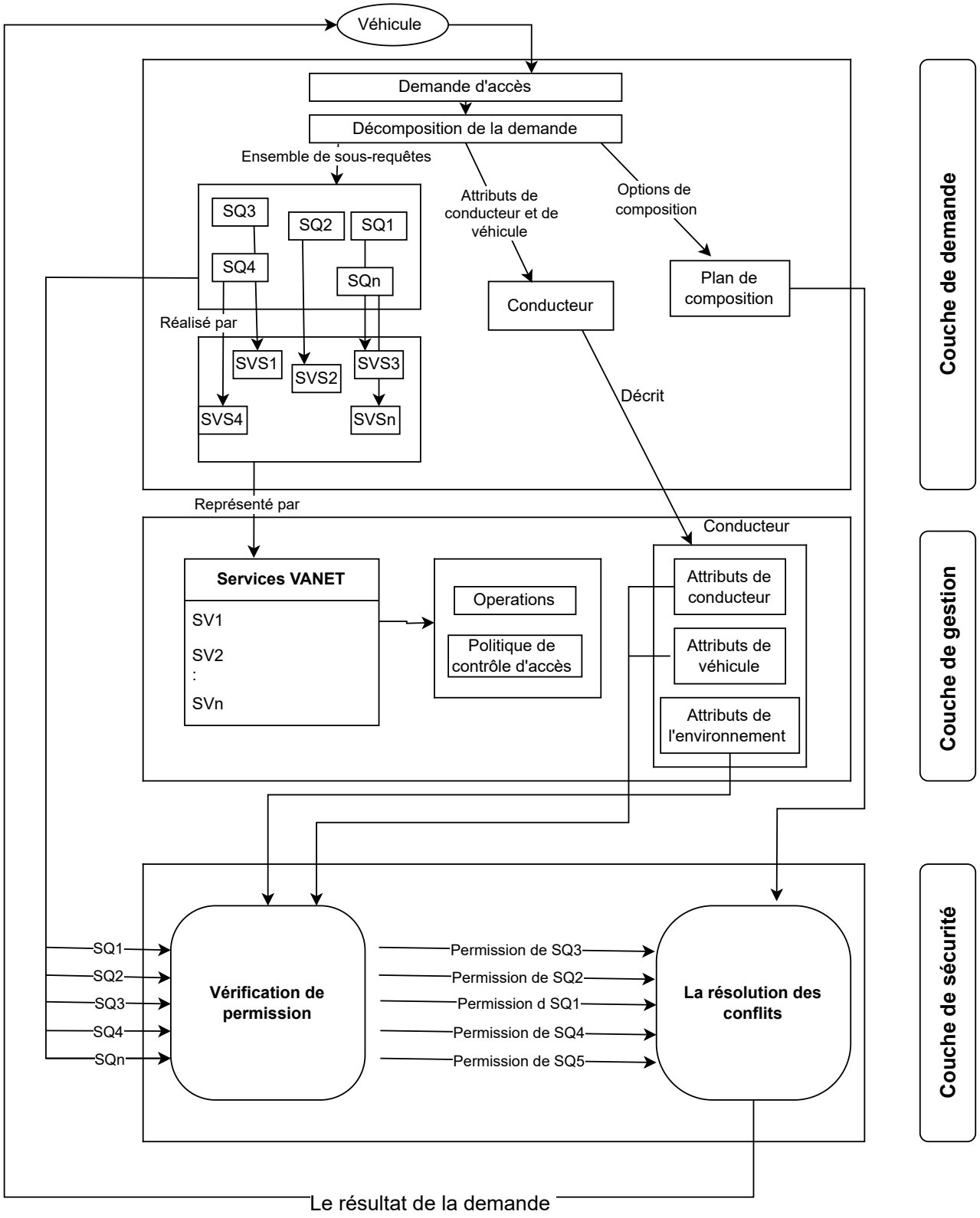
2. **Couche de Gestion**

   Cette couche est responsable de la gestion des informations relatives aux utilisateurs, aux services VANET, aux politiques de contrôle d'accès et désormais aux attributs des véhicules. Les véhicules sont représentés sous forme de profils qui incluent leurs caractéristiques statiques, dynamiques et éventuellement des attributs liés à leurs capacités matérielles et logicielles. Étant donné que les véhicules peuvent fréquemment se déconnecter en raison de changements de position, la couche de gestion effectue des vérifications sur la disponibilité des services de communication des véhicules (VCS) avant d'envoyer une sous-demande, ainsi que pendant l'attente d'une réponse. Si un VCS se déconnecte, la couche de gestion gère cette situation en mettant la sous-demande en attente jusqu'à ce que le VCS redevienne disponible, ou en recherchant un autre VCS disponible pour répondre à la demande.

3. **Niveau de Sécurité**

   Ce niveau contient les modules de vérification des permissions et de résolution des conflits.

FIGURE 3.1 – Architecture du modèle de contrôle d'accès proposé



3.6.2 Composants de Base

Avant de plonger plus en profondeur dans le fonctionnement de notre architecture de sécurité pour les Réseaux de Véhicules Ad Hoc (VANETs), il est essentiel de comprendre les composants fondamentaux qui la composent. Notre modèle repose sur plusieurs éléments clés, chacun jouant

un rôle vital dans la gestion des autorisations et de la confidentialité au sein de ces environnements dynamiques. Nous définirons ci-dessous les principaux éléments du modèle proposé.

1. **Demande d'Accès**

   Une demande d'accès est une requête initiée par un véhicule connecté. Elle englobe les attributs du véhicule les attributs de l'utilisateur et de la ressource, qui spécifient l'opération désirée pour un service VANET donné. Cette demande est adressée soit à un service VANET individuel, soit à une composition de services VANET.

   Cette demande peut être représentée sous la forme de requête, où : Les attributs du véhicule décrivant ses caractéristiques dynamiques matérielles et logicielles, les attributs de l'utilisateur fournissent des informations d'identification et de permissions, et les attributs de la ressource, représentant l'opération spécifique à effectuer (comme la demande de localisation, de trafic, etc.) et l'action associée (lecture, écriture, etc.) Chaque sous-requête est destinée à un service VANET individuel ou à une opération atomique. Les attributs d'options de composition guident la séquence d'exécution des opérations au sein de la demande, garantissant ainsi une utilisation optimale des ressources VANET.

2. **Véhicule**

   Dans notre modèle étendu, le véhicule occupe une place centrale. Il est décrit par une gamme d'attributs qui se divisent en trois catégories distinctes : les attributs statiques qui représentent des informations constantes liées au véhicule. Ils englobent des détails tels que le type de véhicule, son année de fabrication, sa plaque d'immatriculation, etc, les attributs dynamiques telles que la position actuelle du véhicule, sa vitesse, le carburant restant, etc. et les attributs de Capacités du Véhicule : Ces attributs englobent les caractéristiques matérielles et logicielles du véhicule, ils comprennent des éléments tels que la disponibilité des systèmes de géolocalisation, la présence de capteurs, ou d'autres dispositifs pertinents.

3. **Objet**

   Les objets sont les ressources essentielles à sécuriser. Ces ressources peuvent prendre deux formes principales : les services VANET simples, qui englobent diverses opérations avec des règles d'accès spécifiques (autorisation, refus, autorisation conditionnelle), et les compositions de services VANET plus complexes. Ces compositions suivent des plans d'exécution spécifiques, tels que le parallélisme ou la séquentialité. Dans tous les cas, les autorisations d'accès sont déterminées en se basant sur les attributs de l'utilisateur, du véhicule et de la ressource VANET concernée. Cette approche garantit une protection dynamique et adaptative, cruciale dans l'environnement en constante évolution des VANETs.

4. **Attributs Environnementaux**

   Ces attributs incluent les informations de contexte pertinentes, telles que l'heure, la localisation, et désormais, des données spécifiques aux VANETs, comme la densité du trafic ou la disponibilité des services de communication entre véhicules.

5. **Attributs de Capacités du Véhicule**

   Les attributs de capacités du véhicule détaillent les caractéristiques matérielles et logicielles du véhicule connecté, notamment la présence et la fonctionnalité des éléments tels que les systèmes de géolocalisation, les capteurs et d'autres dispositifs pertinents dans l'environnement dynamique des VANETs. Ces attributs sont cruciaux pour déterminer l'autorisation

d'accès, en s'assurant que le véhicule dispose des ressources nécessaires pour traiter efficacement les demandes du réseau VANET. En prenant en compte ces caractéristiques, le modèle de contrôle d'accès s'adapte de manière proactive à la diversité des véhicules connectés et de leurs capacités, ce qui renforce la sécurité et les performances globales du réseau.

6. **Autorisation**

   Les autorisations revêtent une importance cruciale pour déterminer quelles actions sont autorisées concernant les ressources spécifiques, mais elles intègrent désormais les attributs du véhicule en plus des attributs de l'utilisateur.

   Une autorisation typique, notée Pr, prend la forme de :

   $$((OA1 \wedge OA2 \wedge .. \wedge OAn \wedge VA1 \wedge VA2 \wedge .. \wedge VAm), AcA)$$

   où OA1..OAn représentent les attributs de l'objet définissant les propriétés de la ressource, VA1..VAm sont les attributs du véhicule reflétant les caractéristiques matérielles et logicielles du véhicule connecté, et AcA est l'action spécifique autorisée.

   Dans ce modèle étendu, une autorisation est accordée à un ou plusieurs utilisateurs si ces derniers satisfont aux conditions de l'autorisation. Chaque autorisation est associée à des conditions qui doivent être vérifiées comme étant vraies pour qu'un utilisateur puisse effectuer l'action autorisée.

   Exemple :

   $$P_r = (\text{Opération}(\text{InfoTraffic}) \wedge \text{Ressource}(\text{Carte}) = \text{ToutePosition}) \, , \text{Lecture} \tag{3.1}$$

   Cette autorisation est conditionnée, telle que :

   $$\begin{aligned} \text{Cond} = ((&\text{ConnectivitéGPS}(\text{Véhicule}) = \text{Active} \vee \text{ConnectivitéV2V}(\text{Véhicule}) = \text{Active}) \\ &\wedge \text{PositionGéographique}() = \text{Ressource}(\text{Carte})) \end{aligned} \tag{3.2}$$

   En conséquence, pour obtenir l'autorisation Pr, l'utilisateur doit avoir une connectivité GPS ou V2V active, et sa position géographique doit correspondre à la carte demandée. Cette approche plus intégrée garantit une gestion d'accès plus précise et contextuelle au sein des réseaux VANETs.

3.6.3 Processus d'exécution

Le processus d'exécution comprend trois entités : le conducteur est le demandeur et le consommateur de service, le gestionnaire de sécurité du VANET gère la demande du conducteur, et le service de communication VANET est l'entité qui vérifie et satisfait cette demande. Les étapes du processus de contrôle d'accès sont détaillées ci-dessous :

a) **Décomposition de la demande**

La première étape de ce processus implique la décomposition de la demande, permettant ainsi de récupérer séparément les informations essentielles. Cela inclut les attributs du conducteur, les sous-requêtes en cas de services VANET multiples, ainsi que le plan de composition de la demande, qui sera utilisé ultérieurement. Une fois la demande décomposée, le gestionnaire de sécurité du VANET recueille des informations complémentaires, telles que les attributs environnementaux et les attributs du conducteur, pour établir le profil du conducteur. Pour chaque sous-requête, le gestionnaire de sécurité du VANET fusionne la sous-requête avec le profil du conducteur, créant ainsi une requête unique. Enfin, les résultats sont transmis aux services de communication VANET concernés pour vérifier les autorisations d'accès.

b) **Gestion des déconnexions et de disponibilité**

En raison de la mobilité des nœuds au sein de VANET, la gestion efficace des déconnexions et de la disponibilité des VCS est d'une importance cruciale. La mobilité des véhicules peut engendrer des déconnexions fréquentes et imprévisibles, potentiellement affectant la qualité du service offert.

Pour faire face à ce défi, nous avons développé un algorithme qui préalablement vérifie la disponibilité d'un VCS à l'aide de la fonction "isAvailable" avant d'envoyer une sous-requête. Si le VCS est disponible, la sous-requête est immédiatement transmise et traitée. En cas d'indisponibilité, la sous-requête est placée dans une file d'attente pour un traitement ultérieur. De plus, notre algorithme gère les déconnexions en utilisant la fonction "handleVCSDisconnection". Il tente de réenvoyer la sous-requête jusqu'à un nombre maximal de tentatives. Si le VCS demeure indisponible après avoir atteint ce nombre maximal de tentatives, la sous-requête peut alors être redirigée vers un autre VCS disponible, sous réserve d'obtenir l'autorisation de ce deuxième VCS. Cette approche garantit que les sous-requêtes sont traitées de manière efficace et opportune, même en présence des défis résultant de la mobilité des nœuds au sein de VANET. Les deux fonctions sont illustrées dans les algorithmes 5 et 4.

c) **Vérification des permissions**

La vérification des permissions est effectuée par les services de communication VANET qui contiennent l'opération demandée. Chaque service de communication VANET est chargé de définir et d'appliquer ses propres règles d'accès, adaptées à ses services particuliers, et il traite exclusivement la sous-requête qui lui est destinée, sans être conscient des autres services VANET.

Pour évaluer les autorisations d'accès accordées au conducteur, le service de communication VANET approprié utilise les attributs du profil du conducteur, qui ont préalablement été fournis par le gestionnaire de sécurité, conformément à notre modèle. En plus des attributs liés au conducteur et à son environnement, la vérification des autorisations d'accès prend également en considération les caractéristiques des véhicules connectés. Une autorisation d'accès est accordée si le conducteur répond aux critères définis par la règle d'accès spécifique au service et s'il dispose des équipements requis pour traiter la réponse à sa demande, sinon elle est refusée. Ce processus est clairement défini dans l'algorithme 1.

Algorithm 1: Permission Checking VANET

```
Input: driverAttributes : DriverAtt;
environmentAttributes : environmentAtt;
vehicleSoftwareAttributes : vehicleAtt;
request : subRequest;
Output: permission : DriverPermission;
1  foreach operation ∈ subRequest do
       // Récupère les règles applicables pour l'opération
          spécifiée
2      rules ← getRule(operation, rules);
3      foreach rule ∈ rules do
           // Obtient l'autorisation en comparant les attributs
              du conducteur et de l'environnement avec les
              règles
4          permission = rule.getPermission(driverAtt, environmentAtt);
5          if permission = "Allowed" then
6              if capability(operation, vehicleAtt) = true then
                   // Vérifie si le véhicule a la capacité
                      d'effectuer l'opération
7                  permission = "allowed";
8                  return permission;
9              else
10                 if adapt(operation, vehicleAtt) = true then
                       // Vérifie si l'opération peut être adaptée
                          aux caractéristiques du véhicule
11                     permission = "allowed";
12                     return permission;
13                 else
14                     permission = "deny";
15                     return permission;
16         else
17             permission = "deny";
18             return permission;
```

Dans cet algorithme, **getRule** est une fonction qui renvoie les règles applicables pour une opération spécifique, **getPermission** est une fonction qui renvoie l'autorisation de la règle en comparant la condition de la règle avec les attributs de l'utilisateur ou du conducteur et les attributs environnementaux. **Capability** vérifie si le vehicule peut effectuer le résultat de l'opération. Enfin, **adapt** vérifie si le résultat de l'opération peut être adapté aux caractéristiques du vehicule.

d) **Résolution des conflits**

Le modèle de contrôle d'accès que nous avons proposé permet à chaque Service de Communication VANET (VCS) de fournir ses propres autorisations d'accès en fonction de sa propre politique de contrôle d'accès pour l'opération demandée. Cependant, cette approche peut parfois entraîner des conflits au sein du VANET, ce qui nécessite une gestion appropriée.

Afin de résoudre les problèmes de conflits dans le VANET, nous avons développé un mécanisme de résolution des conflits. Ce mécanisme garantit une réponse adéquate au conducteur tout en préservant la sécurité du VCS. Lorsque le Gestionnaire de Sécurité du VANET (VSM) reçoit toutes les autorisations des VCS impliqués dans la demande du conducteur, la résolution des conflits n'est pas nécessaire si toutes les autorisations sont soit accordées, soit refusées de manière cohérente. Cependant, en cas de permissions contradictoires, le VSM utilise le plan de composition de la demande initiale pour élaborer un schéma d'autorisation d'accès composite, en substituant les sous-requêtes par leurs autorisations respectives.

Le processus est illustré par l'algorithme 2.

Algorithm 2: Conflict Resolution VANET

Input: $plan, permissionSet$
Output: $permission$

```
permissions ← list(permissionSet);
options ← list(set(CompositionOption));
permission ← "deny";
if allPermissions = "permit" then
    //Si toutes les autorisations sont "permit", autorise l'accès;
    permission ← "permit";
else if allPermissions = "deny" then
    //Si toutes les autorisations sont "deny", refuse l'accès;
    permission ← "deny";
else
    //En cas d'autorisations contradictoires, utilisez le plan de composition initial
     ConflictSummary ← join(plan, subRequest);
    i ← 0;
    operationLog ← [];
    result ← True;
    while i < len(permissions) do
        if permissions[i] = "permit" then
            append(operationLog, 'True');
            currentResult ← True;
        else
            append(operationLog, 'False');
            currentResult ← False;
        if i < len(options) then
            if options[i] = "Or" then
                append(operationLog, '∨');
                result ← result ∨ currentResult;
            else
                append(operationLog, '∧');
                result ← result ∧ currentResult;
        i ← i + 1;
    if result then
        //Si le résultat est vrai, autorise l'accès;
        permission ← "permit";
    else
        //Sinon, refuse l'accès;
        permission ← "deny";
return permission;
```

e) **Exécution du processus**

L'exécution du processus comprend plusieurs étapes essentielles visant à garantir un traitement efficace des sous-requêtes au sein du réseau VANET. Tout d'abord, chaque sous-requête est dirigée vers un Véhicule à Service de Communication (VCS) disponible. Avant l'envoi, nous effectuons une vérification de la disponibilité du VCS à l'aide de la fonction "isAvailable". Cette fonction détermine si un signal provenant du VCS est reçu dans un délai spécifié. Si le VCS est disponible, la sous-requête est immédiatement envoyée pour traitement, et les informations requises sont obtenues en retour. En cas d'indisponibilité d'un VCS, par exemple en raison d'une déconnexion, la sous-requête est mise en file d'attente pour un traitement ultérieur. Une logique de gestion des déconnexions est alors appliquée, pouvant inclure des tentatives de réenvoi après un certain laps de temps ou la redirection vers un autre VCS disponible. Ce processus se répète jusqu'à ce que toutes les sous-requêtes soient traitées. Ensuite, nous utilisons l'ensemble des permissions obtenues pour résoudre d'éventuels conflits entre les autorisations reçues des différents VCS. Enfin, les résultats de toutes les sous-requêtes sont agrégés pour former la réponse finale, qui est ensuite transmise au demandeur initial, tel que le conducteur ayant initié la demande. L'algorithme 3 illustre ce processus de manière détaillée.

Algorithm 3: ProcessVANET

```
Input: driver request : Request
Output: Response : Answer
Var sub request set : set of sub request
permission set : set of permission
plan : Execution plan
missing : set of missing information
queue : set of sub requests (initially empty)
Receive(driver request)
plan ← requestDecomposition(driver request)
foreach VCS in VANET do
    if isAvailable(VCS) then
        // Envoie la sous-requête pour traitement
        send(sub-request, VCS)
        wait(VCS)
        inf ← receive()
    else
        // Met la sous-requête en file d'attente en cas de
           non-disponibilité du VCS
        queue.add(sub-request)
        // Gère la déconnexion du VCS
        handleVCSDisconnection(VCS, sub-request)
while queue is not empty do
    // Récupère la première sous-requête dans la file
       d'attente
    sub-request ← queue.removeFirst()
    foreach VCS in VANET do
        if isAvailable(VCS) then
            // Envoie la sous-requête au premier VCS disponible
            send(sub-request, VCS)
foreach VCS ∈ VCSAsker do
    if isAvailable(VCS) then
        // Envoie des informations au VCS
        send(inf, VCS)
        while Expired(session) and (received Permission ≤ sub request set.length) do
            // Attends la réception des permissions et gère les
               déconnexions
            Permission set.add(permission)
    else
        // Handle VCS disconnection
Result ← conflictResolutionVANET(Permission set, plan) //Résout les conflits d'autorisation
Send(Result, driver) //Envoie la réponse finale au conducteur
```

Algorithm 4: isAvailable(VCS)

Input: VCS
Output: true if available, false otherwise

```
Initialize a timer with a certain timeout value;
while timer has not expired do
    if a beacon is received from VCS then
        return true;
return false;
```

Algorithm 5: handleVCSDisconnection

Input: VCS, sub-request

```
queue.add(sub-request);
max_retries ← 3;
// Maximum number of retries
wait_time ← 5;
// Time to wait in seconds
for i from 1 to max_retries do
    sleep(wait_time);
    // Wait for a certain period of time
    if isAvailable(VCS) then
        sub-request ← queue.pop();
        // Remove the sub-request from the queue
        send(sub-request, VCS);
        // Send it back to the reconnected VCS
        return ;
// If reached here, all retries failed. // You may want to send the sub-request to another //
  available VCS or log the failure.
```

3.7 Scénario

Nous avons une ville avec une circulation dense où de nombreux véhicules sont équipés de VCS (services de communication connectés). Les conducteurs de ces véhicules souhaitent recevoir des informations de navigation en temps réel pour éviter les embouteillages et optimiser leurs trajets, tout en obtenant des informations sur les stations-service à proximité pour assurer un ravitaillement en carburant efficace. Plusieurs services de communication VANET (VCS) offrent des informations de navigation en temps réel, tels que des mises à jour sur le trafic, les accidents, les travaux routiers, etc.

Dans ce scénario, imaginons que Bob, un conducteur, souhaite obtenir des informations sur l'état du trafic et localiser les restaurants, un parking à proximité et les stations d'essence, car son véhicule nécessite du carburant. Bob utilise son véhicule équipé de capteurs et de communication VANET pour effectuer cette demande.

Demande de Bob :

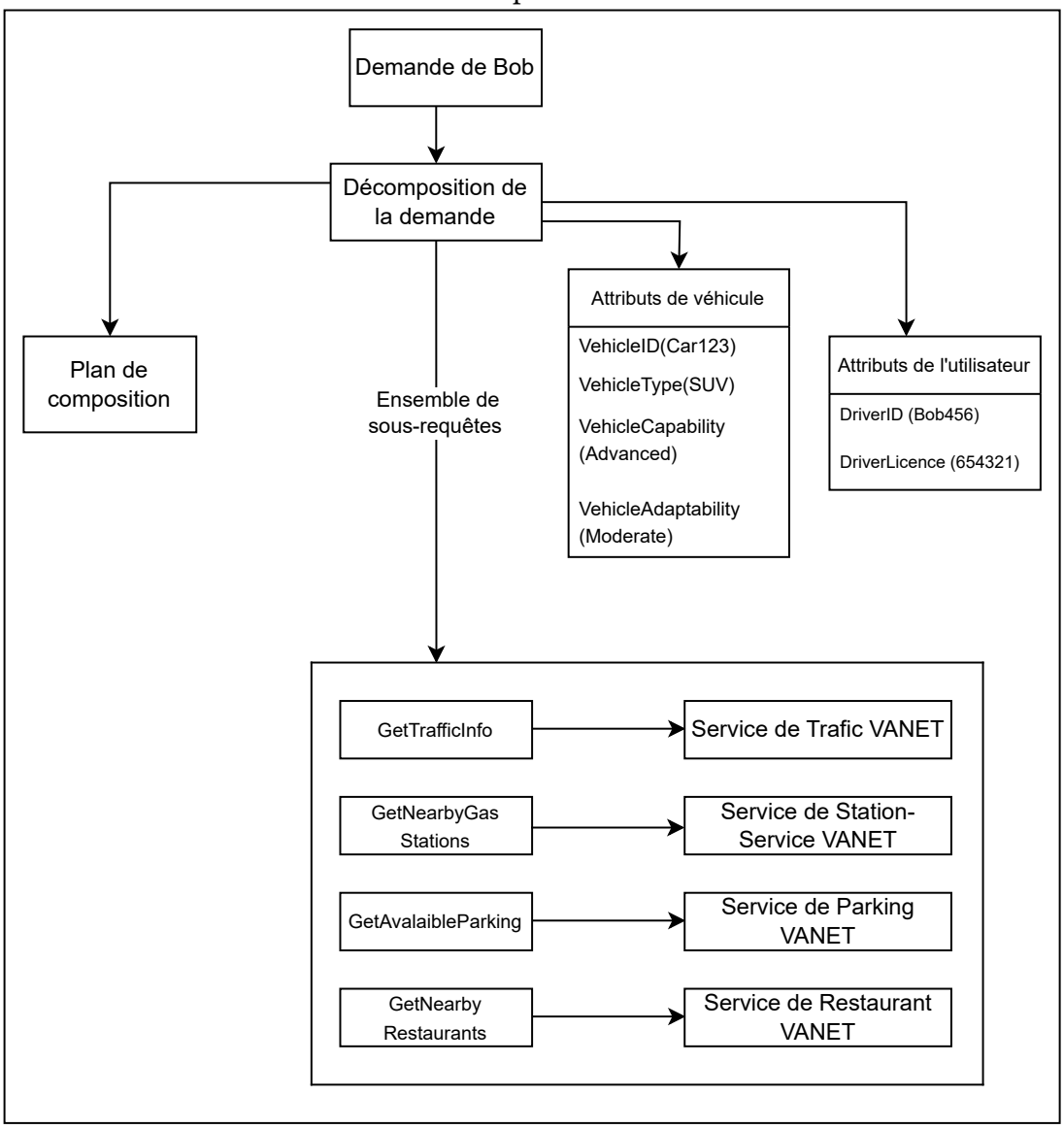
```
REQ = {
    DriverID(Bob456),
    DriverLicense(654321),
    VehicleID(Car123),
    VehicleType(SUV),
    VehicleCapability(Advanced),
    VehicleAdaptability(Moderate),
    [
        (Sname(TrafficService), Operation(GetTrafficInfo), Location
            (GPS), Action(Read)),
        (Sname(GasStationService), Operation(GetNearbyGasStations),
             Location(GPS), Action(Read)),
        (Sname(ParkingService), Operation(GetAvailableParking),
            Location(GPS), Action(Read)),
        (Sname(RestaurantService), Operation(GetNearbyRestaurants),
             Location(GPS), Action(Read))
    ],
    CompositionOps(+)

}
```

La demande de Bob est complexe car elle nécessite l'accès à quatre services VANET distincts. Le processus se déroule comme suit :

a) **Décomposition de la demande**

La demande de Bob est d'abord décomposée en sous-requêtes par le Gestionnaire de Sécurité du VANET (VSM). Cette décomposition permet de récupérer séparément les informations essentielles, notamment les attributs du conducteur, les sous-requêtes, ainsi que le plan de composition de la demande, qui sera utilisé ultérieurement. Chaque sous-requête est ensuite envoyée au Service de Communication VANET (VCS) approprié, Voir figure 3.2.

FIGURE 3.2 – Décomposition de la demande



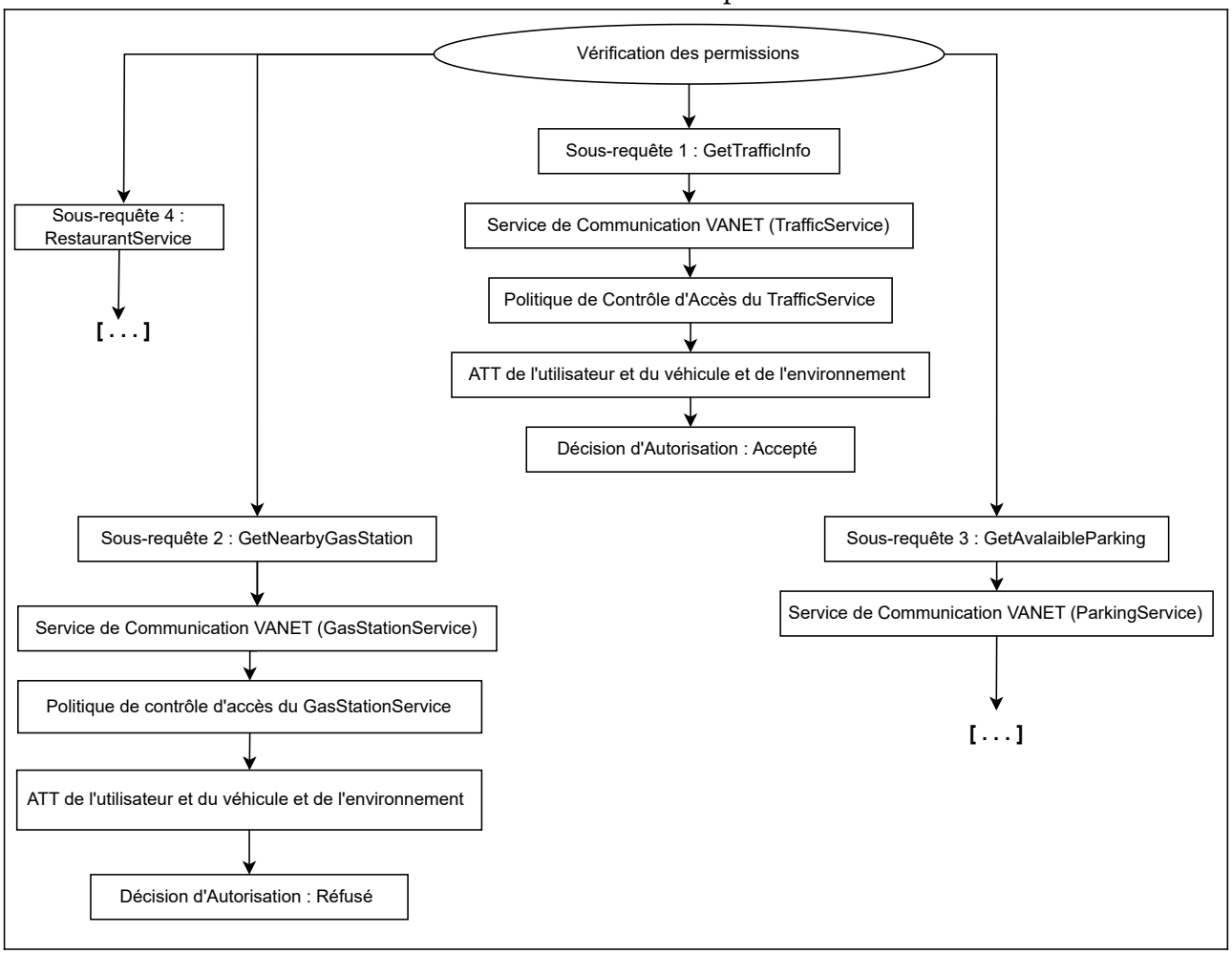
b) **Gestion des déconnexions et de disponibilité**

Lors de l'envoi des sous-requêtes, une indisponibilité du RestaurantService est détectée. Le mécanisme de gestion de la disponibilité intégré au VSM s'active alors pour identifier un autre VCS capable d'offrir un service similaire. Heureusement, un VCS alternatif pour la localisation de restaurants est identifié et sollicité. Par ailleurs, les VCS pour TrafficService, GasStationService et ParkingService confirment leur disponibilité et sont prêts à traiter leurs sous-requêtes respectives.

c) **Vérification des permissions**

Avant de traiter les sous-requêtes, chaque VCS effectue une vérification des permissions. TrafficService et ParkingService, après vérification, accordent l'accès à Bob pour les opérations demandées. Néanmoins, la demande adressée au GasStationService est refusée suite à la vérification des permissions. Par chance, le VCS alternatif pour le RestaurantService autorise l'accès de Bob suite à sa vérification, Voir figure 3.3.

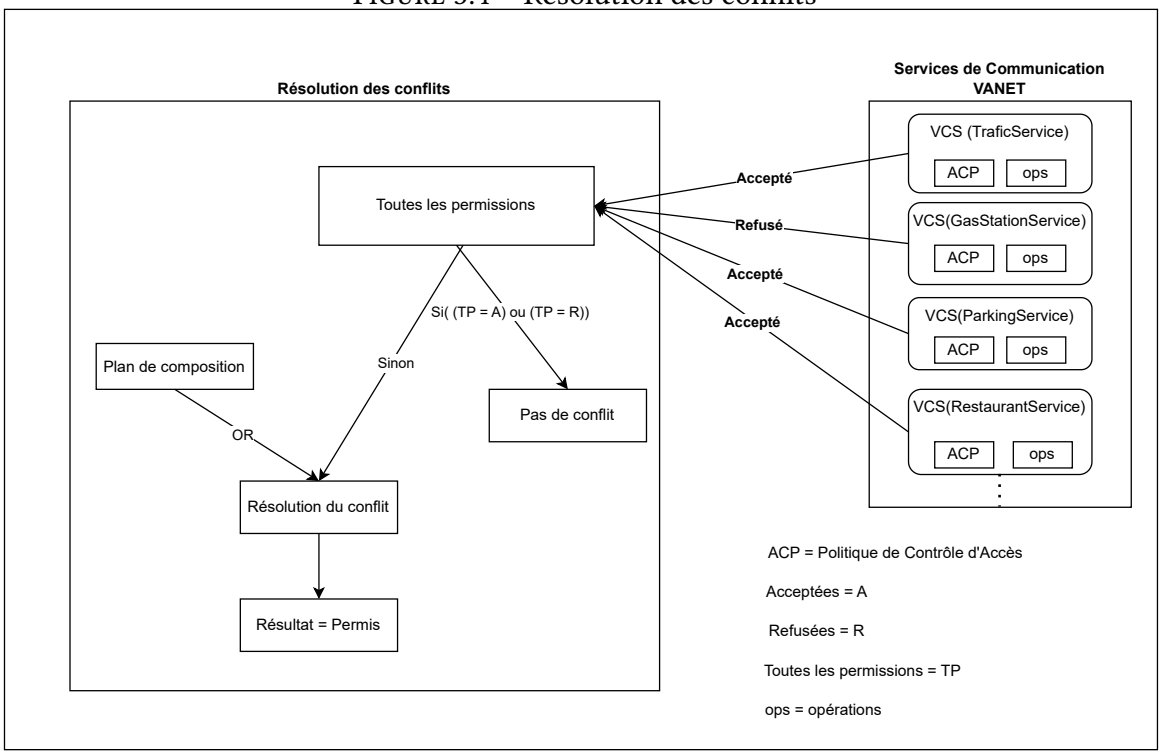
FIGURE 3.3 – Vérification des permissions



d) **Résolution des conflits**

Suite à cette phase de vérification, le VSM est confronté à un ensemble de réponses mixtes : certaines autorisations ont été accordées, tandis que d'autres ont été refusées. Dans ce cas, la stratégie de résolution des conflits adoptée par le VSM est basée sur les options de composition. Dans ce scénario, les options de composition sont définies par l'opérateur logique (+), qui représente l'opérateur "OU". Cela signifie que le VSM traitera les sous-requêtes pour lesquelles l'autorisation a été accordée, en ignorant celles pour lesquelles l'autorisation a été refusée, comme illustré dans la figure 3.4.

FIGURE 3.4 – Résolution des conflits



e) **Exécution du processus**

Enfin, le processus s'exécute en envoyant les sous-requêtes aux VCS appropriés, en vérifiant les permissions d'accès, en résolvant les conflits si nécessaire, et en agrégeant les résultats des sous-requêtes autorisées pour former une réponse complète.

Dans le cas de Bob, le résultat de ce processus serait que Bob a la permission d'accéder à GetTrafficInfo,GetAvailableParking et GetNearbyRestaurants mais pas à GetNearbyGasStations, ce qui génère un conflit. Le mécanisme de résolution des conflits pourrait impliquer de traiter uniquement les sous-requêtes pour lesquelles Bob a la permission et d'ignorer ou de refuser celle pour laquelle il n'a pas la permission. En fin de compte, la réponse envoyée à Bob inclurait les informations sur le trafic, le restaurant le plus proche et un parking ou il peut se garer mais exclurait les informations sur les stations-service à proximité en raison du manque de permission. Ainsi, le modèle de contrôle d'accès garantit que Bob reçoit des informations appropriées tout en maintenant la sécurité des services VANET et du conducteur.

3.8 Conclusion

Ce chapitre présente un modèle de contrôle d'accès conçu pour l'environnement des VANETs. L'objectif principal de ce modèle est d'introduire une nouvelle approche de gestion des autorisations d'accès au sein des réseaux de véhicules ad hoc. Plus spécifiquement, ce modèle vise à gérer efficacement les demandes adressées aux services VANET en prenant en compte les attributs du conducteur ainsi que les attributs environnementaux, tout en intégrant les capacités des véhicules connectés du conducteur dans le processus de contrôle d'accès.

Conclusion générale et perspectives

Ce mémoire s'inscrit dans le contexte du grave problème des accidents de la route qui coûtent chaque année des vies humaines et ont un impact économique et social significatif. Dans ce contexte, nous avons exploré les réseaux de communication véhiculaire (VANET) comme une solution prometteuse pour améliorer la sécurité routière tout en préservant la vie privée des conducteurs.

Le processus de contrôle d'accès est décomposé en trois étapes, soigneusement adaptées au contexte dynamique des VANETs. Tout d'abord, la phase de décomposition de la demande permet une distribution des tâches et renforce la sécurité grâce à la présence de plusieurs points de contrôle. Ensuite, dans la deuxième étape, chaque service de communication VANET impliqué dans la requête examine les autorisations d'accès à ses opérations en se basant sur les attributs du conducteur et les attributs des véhicules connectés du conducteur. Enfin, la troisième et dernière étape concerne la résolution des conflits. Une fois que les services de communication VANET concernés ont émis leurs autorisations d'accès, le gestionnaire de sécurité prend une décision finale quant à la demande du conducteur, en se fondant sur ces permissions.

Cependant, il est essentiel de noter que ce modèle présente des opportunités d'amélioration, notamment en ce qui concerne la gestion des politiques hétérogènes et la résolution des conflits. De plus, la validation dans des scénarios plus complexes est nécessaire. Une perspective prometteuse consiste à intégrer des dispositifs Internet des objets (IoT) dans les VANETs pour les adapter aux villes intelligentes. Cela ouvrirait la voie à de nouvelles possibilités de collecte de données en temps réel et de prise de décision automatisée. Enfin, bien que nous n'ayons pas encore simulé notre travail, l'introduction des IoT dans les VANETs reste une perspective d'avenir passionnante pour relever les défis de la mobilité urbaine.

Bibliographie

[1] Maria Azees, Pandi Vijayakumar et Lazarus Jegatha Deborah. « Comprehensive survey on security services in vehicular ad-hoc networks ». In : *IET Intelligent Transport Systems* 10.6 (2016), p. 379-388.

[2] Walid Bouksani. « Gestion de la protection de la vie privée dans les réseaux véhiculaires (VANET) ». Thèse de doct. Université du Québec à Trois-Rivières, 2017.

[3] Fangbo Cai et al. « Survey of access control models and technologies for cloud computing ». In : *Cluster Computing* 22 (2019), p. 6111-6122.

[4] Ines Chihi. « Étude de l'attaque «Black Hole» sur le protocole de routage VADD (Vehicule-Assisted Data Delivery) ». Thèse de doct. Université du Québec à Trois-Rivières, 2017.

[5] Djamil Aissani DJEBARI Nabil Hassina Nacer. « Composite Web Access Control Model Applied to the Internet of things ». In : ().

[6] Richard Gilles Engoulou et al. « VANET security surveys ». In : *Computer Communications* 44 (2014), p. 1-13.

[7] Amrita Ghosal et Mauro Conti. « Security issues and challenges in V2X : A Survey ». In : *Computer Networks* 169 (2020), p. 107093. issn : 1389-1286. doi : https://doi.org/10.1016/j.comnet.2019.107093. url : https://www.sciencedirect.com/science/article/pii/S1389128619305857.

[8] Guillaume Harry. « IAM-Gestion des identités et des accès : concepts et états de l'art ». In : (2013).

[9] Maxim Kalinin et al. « Role-based access control for vehicular adhoc networks ». In : *2018 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE. 2018, p. 1-5.

[10] Amira Kchaou et al. « Smart contract-based access control for the vehicular networks ». In : *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE. 2020, p. 1-6.

[11] Yue Li et al. « GNC-MAC : Grouping and Network Coding-assisted MAC for Reliable Groupcasting in V2X ». In : *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*. IEEE. 2020, p. 1-6.

[12] Marvy B Mansour et al. « VANET security and privacy-an overview ». In : *International Journal of Network Security & Its Applications (IJNSA) Vol* 10 (2018).

[13] Lewis Nkenyereye et al. « A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control for VANETs. » In : *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 6.2 (2015), p. 98-112.

[14] Dadoun Ouiza et Guendouz Ouiza. « Le routage dans les réseaux véhiculaires VANETs ». Thèse de doct. Université Mouloud Mammeri, 2017.

[15] Alisson Barbosa de Souza et al. « An adaptive mechanism for access control in vanets ». In : *Proceedings of the 10th international conference on networks. Mongol City, California, USA : ICN.* 2011, p. 183-188.

[16] Yuanxin Sun et al. « VIMAC : A Vehicular Information Medium Access Control Protocol for High Reliable and Low Latency Transmissions in VANET ». In : *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP).* 2019, p. 1-6. doi : 10.1109/WCSP.2019.8927945.

[17] Tao Wang, Li Kang et Jiang Duan. « A secure access control scheme with batch verification for VANETs ». In : *Computer Communications* 205 (2023), p. 79-86.

[18] Tao Wang, Li Kang et Jiang Duan. « Dynamic fine-grained access control scheme for vehicular ad hoc networks ». In : *Computer Networks* 188 (2021), p. 107872.

[19] Business Wire. *Siemens' ESCos Roadside Unit.* 2018.

[20] Yingjie Xia et al. « A Policy Enforcement Framework for Secure Data Dissemination in Vehicular Ad Hoc Network ». In : *IEEE Transactions on Vehicular Technology* 70.12 (2021), p. 13304-13314.

[21] Peng Zhang et al. « A Survey on Access Control in Fog Computing ». In : *IEEE Communications Magazine* 56.2 (2018), p. 144-149. doi : 10.1109/MCOM.2018.1700333.

Résumé

Le projet de fin de cycle se concentre sur l'amélioration de la sécurité routière dans les Réseaux de Véhicules Ad Hoc (VANET) en développant une solution de contrôle d'accès basée sur les attributs, intégrée dans une architecture en trois couches. La couche de demande gère les demandes de communication entre les utilisateurs, la couche de surveillance assure la disponibilité des services et la connectivité, tandis que la couche de sécurité vérifie les permissions et résout les conflits en prenant en compte des attributs tels que la vitesse, la direction et le statut d'urgence des véhicules. Cette approche proactive vise à minimiser les risques d'accidents en assurant une priorisation intelligente des messages au sein des VANET.

Mots clés : VANET, ABAC, Contrôle d'accès, VCS, VSM, Gestion de la mobilité, Vitesse de communication

Abstact

The end-of-cycle project focuses on enhancing road safety in Vehicular Ad Hoc Networks (VANETs) by developing an attribute-based access control solution integrated into a three-layer architecture. The request layer manages communication requests among users, the monitoring layer ensures service availability and connectivity, while the security layer verifies permissions and resolves conflicts, considering attributes like speed, direction, and emergency status of vehicles. This proactive approach aims to minimize accident risks by ensuring intelligent prioritization of messages within VANETs.

Keywords : VANET, ABAC, Acess control, VCS, VSM, Mobility Management, Communication speed