REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU-BEKR BELKAID – TLEMCEN

Laboratoire STIC

THÈSE LMD

Présentée à :

FACULTE DES SCIENCES – DEPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

DOCTORAT

Spécialité : *Informatique Distribuée et Réseaux (IDR)*

Par :

BENADLA Sarra

Sur le thème

Sécurité des données et protection de la vie privée des usagers dans les réseaux Fog véhiculaires

---

Soutenue publiquement le 25 novembre 2023 à Tlemcen devant le jury composé de :

Mr. BENMAMMAR Badr	Professeur	Université de Tlemcen	Président
Mr. MERAD BOUDIA Omar Rafik	Maître de Conférences A	Université d'Oran 1	Directeur de thèse
Mr. LEHSAINI Mohamed	Professeur	Université de Tlemcen	Co-Directeur de thèse
Mr. BELALEM Ghalem	Professeur	Université d'Oran 1	Examinateur
Mme. LABRAOUI Nabila	Professeur	Université de Tlemcen	Examinatrice
Mr. DEBBAL Mohammed	Maître de Conférences A	Université de Ain Temouchent	Examinateur

Laboratoire de Système et Technologie de l'Information et de la Communication (STIC)
BP 119, 13000 Tlemcen - Algérie

Remerciements

Tout d'abord, je souhaite adresser mes sincères remerciements à mon directeur de thèse, le Docteur **MERAD BOUDIA Omar Rafik**. Son encadrement, son expertise et son soutien constant ont été des facteurs déterminants dans la réalisation de cette thèse. Ses conseils avisés et sa volonté de partager ses connaissances m'ont permis de repousser mes limites et de mener à bien ce travail de recherche. Je tenais à prendre un moment pour lui exprimer ma profonde gratitude pour son rôle déterminant en tant que directeur de thèse.

Je voudrais remercier mon co-directeur, le Professeur **LEHSAINI Mohamed**. Son expertise et son mentorat ont eu un impact positif durable sur mon parcours académique et je suis honorée d'avoir pu bénéficier de sa précieuse guidance.

Je voudrais également remercier le Professeur **BENMAMMAR Badr** de l'université de Tlemcen, président du jury, pour avoir accepté de présider cette soutenance de thèse. Je souhaite exprimer ma gratitude envers les autres membres du jury, le Professeur **BELALEM Ghalem** de l'université d'Oran 1, le Professeur **LABRAOUI Nabila** de l'université de Tlemcen, et le Docteur **DEBBAL Mohammed** de l'université de Ain Temouchent pour avoir consacré leur temps, et leur attention à évaluer ma thèse.

Enfin, je souhaite adresser mes remerciements à ma famille, mes amis et tous ceux qui m'ont soutenu tout au long de ce parcours académique. Leurs encouragements, et leur soutien moral ont été d'une importance cruciale dans la réalisation de cette thèse.

Résumé

L'Internet des Véhicules (IoV) est un réseau qui considère les véhicules comme des machines intelligentes et permet leur interaction et leur communication mutuelles dans le but d'améliorer les performances et la sécurité du trafic routier. Bien que l'IoV apporte des solutions à certains problèmes, il présente également des limites, notamment en termes de temps de réponse. Cela a conduit les chercheurs à proposer l'intégration du Fog Computing dans les réseaux de véhicules afin de bénéficier de ses avantages. Ainsi, le Vehicular Fog Computing (VFC) émerge comme un paradigme pour les réseaux véhiculaires, offrant des services à la périphérie du réseau. Le VFC présente un ensemble d'avantages significatifs, tels que l'agilité, l'efficacité et la réduction de la latence. Cependant, il est également vulnérable à diverses attaques, et les mesures de sécurité existantes dans les réseaux véhiculaires traditionnels ne sont pas nécessairement applicables au VFC. Par conséquent, afin de garantir la satisfaction des utilisateurs du réseau, il est essentiel de garantir la sécurité et la confidentialité des données sensibles. Dans le cadre de ce projet de thèse, l'objectif est de relever les défis de sécurité associés au VFC. Pour atteindre cet objectif, deux contributions ont été proposées, axées sur la sécurité et la protection de la vie privée des utilisateurs au sein des réseaux VFC. La première contribution concerne un mécanisme de détection des attaques Sybil, tandis que la deuxième contribution est un nouveau mécanisme d'authentification. Ces mécanismes reposent sur l'utilisation des techniques cryptographiques avancés et de la technologie Blockchain. Ils ont été soigneusement analysés et comparés à d'autres travaux pertinents en termes de services de sécurité et de performances. Les résultats obtenus ont été extrêmement satisfaisants.

Mot clés : Sécurité, protection de la vie privée, VFC, blockchain, authentification, attaque Sybil.

Abstract

The Internet of Vehicles (IoV) is a network that treats vehicles as intelligent machines, enabling them to interact and communicate with each other to enhance road traffic performance and safety. While IoV offers solutions to certain challenges, it also has its limitations, particularly in terms of response time. As a result, researchers have proposed integrating Fog Computing into vehicular networks to leverage its benefits. Consequently, Vehicular Fog Computing (VFC) is emerging as a paradigm for vehicular networks, providing services at the network edge. VFC offers several significant advantages, including agility, efficiency, and reduced latency. However, it is also susceptible to various attacks, and the security measures employed in traditional vehicular networks may not be directly applicable to VFC. Therefore, ensuring the security and confidentiality of sensitive data is crucial to satisfying network users. The objective of this thesis project is to address the security challenges associated with VFC. To achieve this goal, two contributions have been proposed, focusing on security and user privacy within VFC networks. The first contribution involves a mechanism for detecting Sybil attacks, while the second is a novel authentication mechanism. These mechanisms rely on advanced cryptographic tools and Blockchain technology. They have undergone thorough analysis and comparison with other relevant works in terms of security services and performance. The obtained results have been extremely satisfactory.

Key words: Security, privacy, VFC, blockchain, authentication, Sybil attack.

ملخص

إنترنت السيارات هي شبكة تتعامل مع السيارات على أنها آلات ذكية، مما يتيح لها التفاعل والتواصل مع بعضها البعض لتعزيز أداء حركة المرور على الطرق. وبالرغم من أن إنترنت السيارات توفر حلاً لبعض التحديات، إلا أن لديها بعض القيود، لا سيما فيما يتعلق بزمن الاستجابة. وبناءً على ذلك، اقترح الباحثون دمج الحوسبة الضبابية في شبكات السيارات للاستفادة من فوائدها. يظهر الحوسبة الضبابية للسيارات كنموذج حديث لشبكات السيارات، حيث يوفر مجموعة من المزايا الهامة، بما في ذلك السرعة والكفاءة وتقليل التأخير. ومع ذلك، فإنها تتعرض أيضًا لمختلف أنواع الهجمات، وقد لا تكون التدابير الأمنية المستخدمة في شبكات السيارات التقليدية قابلة للاستخدام المباشر في الحوسبة الضبابية للسيارات. لذا، فإن ضمان أمان وسرية البيانات الحساسة أمر حاسم لإرضاء مستخدمي الشبكة. يهدف هذا المشروع البحثي إلى معالجة التحديات الأمنية المرتبطة بـالحوسبة الضبابية للسيارات. ولتحقيق هذا الهدف، تم اقتراح مساهمتين، تركز الأولى على آلية لاكتشاف هجمات سايبيل، في حين تقترح الثانية آلية للمصادقة. تعتمد هذه الآليات على أدوات تشفير متقدمة وتقنية البلوكشين. وقد تم تحليلها ومقارنتها بعناية مع الأعمال الأخرى ذات الصلة من حيث خدمات الأمان والأداء.

كلمات رئيسية: الأمان، الخصوصية، الحوسبة الضبابية للسيارات، البلوكشين، المصادقة، هجوم سايبيل.

Table des matières

Liste des figures

Liste des tableaux

Liste des acronymes

AaaS	Application as a Service
AD	Audit Department
AI	Artificial Intelligence
AIAA	AI Algorithms Approach
BB	Blockchain-Based
BC	Blockchain
BD	Base de Données
CA	Cryptography Approach
CaaS	Containers as a Service
CB	Certificate-Based
CC	Cloud Computing
CRL	Certificate Revocation List
DDoS	Distributed Denial of Service
DMV	Department of Motor Vehicles
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
DTM	Distributed Trust Management
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Event Data Recorder
ENaaS	Enterprise Network as a Service
FC	Fog Computing
FN	Fog Node
GIS	Geographic Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSB	Group Signature Based
IaaS	Infrastructure as a Service

IDB	IDentity-Based
INS	Inertial Navigation System
IoT	Internet of Things
IoV	Internet of Vehicle
ITS	Intelligent Transportation Systems
LA	Location Approach
MANET	Mobile Ad hoc NETwork
MCC	Mobile Cloud Computing
MIRACL	Multiprecision Integer and Rational Arithmetic C/C++ Library
MITM	Man In The Middle
NaaS	Network as a Service
NIST	National Institute of Standards and Technology
OBU	On-Board Unit
OMNet++	Objective Modular Network Testbed in C++
OSM	OpenStreatMap
P2P	Peer to Peer
PaaS	Platform as a Service
PB	Pseudonym-Based
PBFT	Practical Byzantine Fault Tolerance
PCM	Power Control Models
PKI	Public Key Infrastructure
PKIB	Public Key Infrastructure Based
PoS	Proof of Stake
PoW	Proof of Work
QoS	Quality of Service
RFID	Radio-Frequency IDentification
RSSI	Received Signal Strength Indicator
RSU	RaodSide Unit
SaaS	Software as a Service
SCB	Symmetrical Cryptography Based
SM	Service Manager

SSA	Signal Strength Approach
STaaS	Storage as a Service
SUMO	Simulation of Urban MObility
TA	Trusted Authority
TI	Technology Information
TMS	Traffic Management Server
TTA	Trusted Third-party Authority
V2H	Vehicle-to-Human
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Personal
V2R	Vehicle-to-Roadside unit
V2S	Vehicle-to-Sensor
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANET	Vehicular Ad hoc NETwork
VCC	Vehicular Cloud Computing
VFC	Vehicular Fog Computing
VFS	Vehicular Fog Services
WAVE	Wireless Access in Vehicular Environment
WP	Witness Peer

Introduction générale

Le développement de l'Internet des Objets (IoT) englobe plusieurs industries, notamment l'industrie automobile. Dans ce contexte, l'Internet des véhicules (IoV), également connu sous le nom d'Internet of Vehicles, est apparu. Son objectif principal est de proposer une multitude de services supplémentaires aux conducteurs, aux passagers et aux acteurs de l'industrie, afin d'améliorer la sécurité routière, d'offrir des divertissements et une connectivité Internet, d'optimiser la rentabilité des produits, ainsi que d'améliorer la fiabilité et la facilité de diagnostic des véhicules. Cependant, il existe des défis majeurs liés à l'adoption de ces services par les utilisateurs. L'une des raisons principales est la préoccupation croissante concernant la cybersécurité, car la connectivité des véhicules les expose à des attaques potentielles. D'autre part, le nombre croissant de véhicules connectés génère une quantité considérable de données à différents niveaux, ce qui pose un défi important. Les architectures à deux niveaux, telles que celle du VCC (Vehicular Cloud Computing), sont insuffisantes pour traiter efficacement ces données. En effet, le VCC est entièrement centralisé, ce qui entraîne des temps de réponse importants et une surcharge du réseau face à un tel volume de données.

Le Fog computing, également connu sous le nom d'informatique en brouillard, est un concept à trois niveaux qui vise à répondre aux besoins des applications en agissant comme un intermédiaire entre le Cloud et les véhicules connectés. Il fournit des services via des serveurs situés à proximité géographique des véhicules, ce qui permet une analyse en temps réel des données et des réponses rapides aux requêtes. Dans le cadre du Vehicular Fog Computing (VFC), les véhicules sont considérés comme des périphériques intelligents, mobiles et équipés de différents capteurs tels que le radar, le GPS et la caméra. Une partie de ces données est traitée localement, tandis que d'autres sont envoyées aux nœuds Fog à d'autres fins. Les nœuds Fog collectent, traitent et envoient les données (traitées) aux serveurs. Contrairement aux réseaux véhiculaires existants, les nœuds Fog offrent une plus grande variété de fonctions et de services aux véhicules, tels que la navigation, la diffusion vidéo et les feux de circulation intelligents. Les nœuds Fog ne se limitent pas à un rôle de relais, ils traitent et stockent également des données, prenant des décisions localement dans leur zone.

Dans une architecture VFC, les nœuds Fog sont déployés de façon régulière sur les routes publiques sans aucune isolation physique en raison de leur position géographique. Par conséquent, ces nœuds sont plus vulnérables aux attaques de compromission physique que les serveurs sur le Cloud qui sont généralement protégés physiquement. Dans le VFC, les données collectées sur l'environnement environnant, peuvent contenir de nombreuses informations sensibles. Des acteurs curieux tels que les fournisseurs de services et les pirates informatiques ont la capacité d'extraire différents types d'informations personnelles à partir de ces données, tels que la localisation ou les préférences. Afin de protéger ces informations sensibles contre de telles attaques, des algorithmes cryptographiques spécifiques basés sur les chiffrements asymétriques peuvent être utilisés comme une mesure de sécurité efficace.

La protection de la vie privée des utilisateurs est primordiale dans un VFC. En effet, les données collectées sur le milieu environnant sont nécessairement centrées sur les personnes et liées à certains aspects des conducteurs ou des passagers et de leur environnement social (par exemple, où se trouvent les conducteurs et les passagers et où ils vont, quels endroits ils visitent fréquemment et quelle trajectoire ils choisissent et quelle activité ils préfèrent faire dans des véhicules). Des solutions comme l'utilisation des pseudonymes, et la blockchain peuvent répondre à ce besoin, cependant, les solutions qui existent encourent une charge considérable de calcul et de communication. Rappelons que l'un des principaux avantages du VFC est sa rapidité de réponse. Ainsi, que ce soit pour assurer la confidentialité ou bien pour garantir la protection de la vie privée des utilisateurs, les algorithmes doivent être efficaces.

Au sein de cette thèse, nous présentons deux solutions axées sur la sécurité et la protection de la vie privée des utilisateurs au sein d'un réseau VFC, visant à relever les défis de sécurité mentionnés précédemment. La première solution propose un mécanisme de détection des attaques Sybil, tandis que la deuxième solution propose un mécanisme d'authentification. Le mécanisme de détection des attaques Sybil repose sur l'utilisation de la technologie blockchain. Ce mécanisme détecte les attaques Sybil à deux niveaux : le premier niveau est basé sur le RSSI (Received Signal Strength Indication) et le deuxième niveau est basé sur la trajectoire d'un véhicule. Nous prenons en compte un attaquant puissant qui cherche à compromettre le réseau en utilisant divers scénarios d'attaque pour mener à bien une attaque Sybil. Le mécanisme d'authentification repose également sur l'utilisation de la technologie blockchain et de la cryptographie sur les courbes elliptiques

(ECC). Ce mécanisme résout le problème du séquestre des clés en permettant au véhicule de choisir ses propres clés publiques et privées. De plus, le pseudonyme du véhicule peut être modifié simultanément avec les paires de clés, ce qui assure l'absence de corrélation entre eux.

Voici les contributions que nous apportons dans le cadre de cette thèse :

1. L'adoption de la technologie Blockchain permet d'atteindre une forme de décentralisation, ce qui peut améliorer les performances en matière de calcul et de temps de réponse, tout en évitant une surcharge excessive du réseau.
2. Pour garantir la sécurité, différentes techniques cryptographiques sont mises en œuvre, assurant ainsi des services tels que l'intégrité, la confidentialité et la protection de la vie privée.
3. Une comparaison a été effectuée entre les résultats obtenus en termes de coût de calcul, de communication et de services de sécurité, en les confrontant avec les travaux connexes.

La structure du présent manuscrit de thèse est la suivante :

Le premier chapitre de cette thèse présente une introduction aux réseaux véhiculaires, leur évolution et les problèmes de sécurité spécifiques au sein du VFC. Ce chapitre joue le rôle d'une préface qui établit les fondements de l'ensemble de la thèse. Le deuxième chapitre de cette thèse se concentre sur l'analyse des travaux existants, en mettant l'accent sur deux aspects majeurs. Le premier aspect concerne l'attaque Sybil au sein du réseau VFC, tandis que le deuxième aspect concerne l'authentification. Dans le troisième chapitre de cette thèse, nous abordons notre première contribution qui vise à détecter les attaques Sybil au sein du réseau VFC. Le quatrième chapitre, présente notre deuxième contribution qui consiste en un mécanisme d'authentification conditionnelle préservant la vie privée pour les réseaux VFC.

Chapitre I : Généralité sur les réseaux Fog véhiculaires

I.1. Introduction

L'évolution récente des technologies de communication a conduit à une évolution des différents appareils, qui deviennent de plus en plus intelligents et connectés. Le secteur des transports n'échappe pas à ce phénomène ; les véhicules deviennent intelligents et autonomes grâce à l'utilisation de capteurs et de techniques de communication. De ce fait, un nouveau domaine de recherche a été créé dans le secteur des transports. Dans ce chapitre, nous présentons l'évolution des réseaux de communication pour les véhicules, en commençant par une introduction aux réseaux véhiculaires, qui se décline en trois paradigmes : les réseaux VANET, l'IoV et le VCC. Ensuite, nous détaillons le paradigme VFC, qui est au cœur de cette thèse.

I.2. Introduction aux réseaux véhiculaires

Dans le monde entier, le nombre de personnes utilisant les systèmes de transport ne cesse de croître. Voelcker [1] a estimé que le nombre de véhicules en circulation dans le monde dépassera le milliard et pourrait atteindre deux milliards d'ici 2035. Cette croissance du nombre de véhicules sur la route a de nombreuses conséquences, notamment la congestion et les accidents mortels. Pour améliorer la sécurité routière, divers paradigmes de réseaux de véhicules ont été proposés, tels que les réseaux de véhicules ad hoc (Vehicular Ad hoc NETwork ou VANET), l'Internet des véhicules (Internet of vehicle ou IoV), le Cloud Computing Véhiculaire (Vehicular Cloud Computing ou VCC), et récemment le Fog Computing Véhiculaire (Vehicular Fog Computing ou VFC). Chaque paradigme a été proposé comme une évolution d'un autre pour améliorer l'efficacité [2].

I.2.1. Vehicular Ad hoc NETwork

I.2.1.1. Généralité

Le concept du réseau VANET a été proposé pour la première fois lors de la conférence de normalisation des communications automobiles de l'Union Internationale des Télécommunications - secteur de la normalisation des Télécommunications - (UIT-T) en 2003. Le réseau VANET est l'application du réseau mobile ad hoc (Mobile Ad hoc NETwork ou MANET[1]) dans

[1] MANET : Un réseau mobile ad hoc est défini comme un système distribué composé d'un groupe de nœuds mobiles similaires, capables de se déplacer de manière dynamique et arbitraire. Une telle collection autonome de nœuds

le domaine des transports. L'objectif principal des VANET est de construire des systèmes de transport routier plus sûrs. Plus précisément, les VANET sont conçus pour améliorer la sécurité et la gestion du trafic tout en offrant le confort et le plaisir aux conducteurs ainsi qu'aux passagers sur les routes publiques.

Dans les VANET, les véhicules sont équipés de systèmes de positionnement global (Global Positioning System ou GPS), de capteurs et d'unités embarquées (On-Board Unit ou OBU). Ils sont considérés comme des nœuds mobiles qui agissent comme une machine intelligente, ils peuvent communiquer avec d'autres véhicules, et avec des unités de bord de route (RSU) afin d'échanger des informations routières.

Le réseau VANET utilise l'accès sans fil dans l'environnement du véhicule (WAVE) pour échanger des informations entre les OBU équipés dans les véhicules, les RSU et un ensemble de nœuds de capteurs. Les unités de base impliquées dans la communication sont : l'UA, la RSU et l'OBU [4]. Elles sont abordées comme suit :

- **Unité d'application (UA) :** Il s'agit d'une interface graphique entre l'utilisateur et l'OBU. L'utilisateur peut récupérer les messages stockés, des informations complètes sur la vitesse de déplacement, les conditions de circulation, etc. afin de les analyser.
- **Unité de bord de route (RSU)** : Les RSU sont des unités stationnaires déposées le long de la route, telles que les feux de circulation ou les panneaux d'avertissement sur la route, qui fournissent une connectivité et une aide à l'information aux véhicules, y compris des avertissements de sécurité et des informations sur le trafic. Les RSU échangent des informations par le biais de moyens de communication avec ou sans fil.
- **Unité embarquée (On-Board Unit ou OBU) :** Il s'agit d'un dispositif électronique composé d'un processeur, d'un système de positionnement global (GPS), d'une mémoire vive, de nœuds de capteurs et de modules d'enregistrement de données d'événements (EDR). Parfois, ces modules peuvent être placés indépendamment à l'intérieur des véhicules. En général, les OBU sont montés à bord et échangent des informations avec les OBU et les RSU proches. Pour communiquer, l'OBU utilise la technologie radio IEEE 802.11p dans un environnement ad hoc. En revanche, dans un environnement basé sur

mobiles ne dispose pas d'une infrastructure spécifique, d'une administration centralisée ou de stations de base assignées, de sorte que la topologie du réseau est soumise à des changements rapides [3].

l'infrastructure, les OBU utilisent la technologie radio IEEE802.11 a/b/g. En outre, les OBU contrôlent la connexion ad hoc, le routage, la gestion de la mobilité basée sur IP, les problèmes de sécurité des données et la congestion du réseau. L'EDR est un dispositif électronique qui fait partie de l'OBU. Il stocke tous les messages transmis et reçus par les OBU et les RSU proches. Il enregistre également toutes les activités qui se sont produites dans l'environnement du véhicule pendant le trajet. Le module GPS est utilisé pour identifier l'emplacement physique, l'accélération et la direction du mouvement du véhicule à un intervalle de temps spécifique. Un dispositif informatique spécialisé est attaché à l'OBU. Il est chargé de prendre les mesures nécessaires en fonction des messages reçus d'autres OBU ou RSU. Des radars et des capteurs sont utilisés pour détecter les obstacles qui apparaissent pendant le déplacement du véhicule. Une antenne omnidirectionnelle est responsable de l'accès à l'information sur les canaux sans fil. Pour identifier un véhicule de manière unique, une plaque d'immatriculation électronique (ELP) est également associée à chaque véhicule.

I.2.1.2. Architecture

L'objectif de l'architecture de communication des VANET est de permettre aux véhicules de communiquer entre eux et avec les infrastructures routières fixes afin d'être mis à jour avec les informations routières [5]. Trois modes de communication sont possibles (comme le montre la figure I.1).

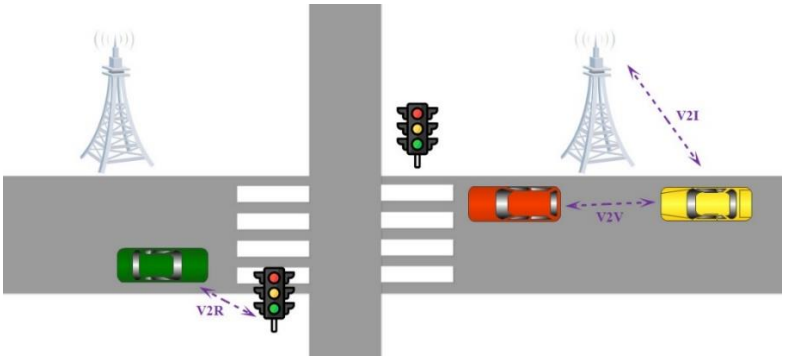

Figure I.1. Architecture de communication VANET.

- **Communication véhicule à véhicule (Vehicle-to-Vehicle ou V2V) :** Avec la communication V2V, chaque véhicule peut contacter ses voisins sans passer par un support d'infrastructure fixe (communication directe) et peut être principalement utilisé pour des

applications de sûreté, de sécurité et de diffusion. La communication V2V utilise la technique du saut unique ou la technique du saut multiple (avec l'aide de véhicules intermédiaires). En général, les messages liés à la sécurité sont transmis par un seul saut, tandis que les messages non liés à la sécurité sont transmis par plusieurs sauts. Le mode V2V est utilisé pour la diffusion de messages d'urgence tels que le freinage d'urgence, la décélération en cas de collision, l'alerte en cas d'embouteillage, etc. Parfois, la communication V2V est également utilisée dans le cadre d'une conduite coopérative.

- **Communication de véhicule à unité de bord de route (Vehicle-to-Roadside unit ou V2R) :** V2R fait référence aux informations échangées entre les véhicules et les RSU, où les RSU sont utilisées comme serveurs de stockage de données. La communication V2R peut atteindre de longues distances, contrairement à la communication V2V. De plus, les RSU peuvent jouer le rôle de sauts intermédiaires pour étendre la portée de la communication jusqu'à la destination.
- **Communication de véhicule à infrastructures (Vehicle-to-Infrastructure ou V2I) :** grâce à ce type de communication, les véhicules peuvent se connecter à l'internet et bénéficier de plusieurs services internet.

I.2.1.3. Caractéristiques

Les réseaux VANET diffèrent des autres réseaux par leurs comportements et leurs caractéristiques.

- **Mobilité :** les VANET fonctionnent dans un environnement très dynamique. Le trafic est plus dense aux heures de pointe, car les véhicules se déplacent à des vitesses différentes [6]. En raison de la vitesse variable du véhicule, des problèmes de communication se posent à des vitesses très basses et très élevées. En effet, les embouteillages importants ralentissent ou arrêtent le trafic, et les véhicules ont donc le temps d'échanger des messages.
- **Mobilité prévisible :** Les routes sont les seules voies où les mouvements des véhicules peuvent être prédits. Grâce au GPS, il est facile de trouver des informations sur les routes. La position d'un véhicule peut facilement être déterminée en regardant sa vitesse et sa trajectoire sur la route.
- **Connectivité et topologie du réseau :** La topologie change constamment lorsque les véhicules se déplacent. Les connexions et les déconnexions de nœuds sont courantes dans la topologie.

- **Disponibilité des ressources énergétiques :** La contrainte d'alimentation n'est plus un problème dans les VANET, car les véhicules ont des batteries solides qui fournissent une alimentation constante à l'OBU. En plus de leurs propres batteries, ils disposent d'ordinateurs extrêmement puissants pour traiter des calculs complexes. Les VANET permettent la transmission d'informations d'un véhicule à l'autre sans nécessiter de ressources énergétiques ou de calcul.
- **Densité réseau/trafic :** La densité du trafic varie dans les VANET en fonction de la densité du réseau. Par rapport aux zones urbaines ou aux autoroutes, les zones rurales ont un taux d'accidents plus faible.
- **Facilité du calcul :** Récemment, les fournisseurs de services ont doté les véhicules de capacités de calcul élevées, telles que la mémoire, des capteurs efficaces, de l'espace de stockage, un accès à Internet, une technologie d'antenne avancée et le GPRS (General Packet Radio Service).

VANET est un réseau de véhicules qui a amélioré la gestion des routes, et qui a apporté de nombreux avantages à ses utilisateurs. Cependant, il reste très limité quant au nombre de véhicules et aux contraintes de mobilité. Plus précisément, il ne peut pas fournir tous les services durables aux utilisateurs du réseau. Dans ce sens, un nouveau paradigme est apparu, connu sous le nom d'internet des véhicules.

I.2.2. Internet of Vehicle

I.2.2.1. Généralité

La nouvelle ère de l'Internet des Objets (Internet of Things ou IoT) a suscité l'évolution des réseaux ad hoc véhiculaires classiques (VANET) vers le paradigme de l'internet des véhicules (IoV). L'IoV est un domaine important des ITS qui fournit de nombreuses technologies et applications. Cependant, il n'existe pas de définition uniforme de l'IoV en raison de la compréhension différente de la connotation de l'IoV dans divers domaines de recherche [7]. Quelques définitions sont données ci-dessous :

L'IoV est considéré comme une intégration de l'IoT dans le système de transport selon Alam et al. [8]. Les auteurs ont considéré les véhicules comme des objets roulants qui détectent des informations. Pour un échange efficace d'informations dans l'IoV entre les différentes entités du réseau, de nombreuses technologies et applications sont intégrées, telles que la technologie de

communication sans fil et les capteurs intelligents. Yang et al. [7] ont considéré l'IoV comme un ensemble de véhicules connectés entre eux en formant un réseau basé sur le système d'information des véhicules. L'état du véhicule détecté par les équipements du véhicule est transmis aux conducteurs. Le trafic est contrôlé par les ITS au moyen de diverses interconnexions existantes dans les réseaux.

L'IoV est un réseau qui comprend plusieurs utilisateurs, véhicules et objets. Il s'agit d'un système intégré hautement contrôlable, opérationnel, gérable et crédible, qui fournit des services à de grandes villes, voire à un pays entier [9]. Il s'agit d'un système complexe plutôt que d'un simple réseau de services pour véhicules.

I.2.2.2. Architecture

Les technologies avancées dans les véhicules ont conduit à la création de plus de types de communications dans l'IoV par rapport au VANET. L'IoV se compose essentiellement de six types de connexion [10] comme illustre la figure I.2.

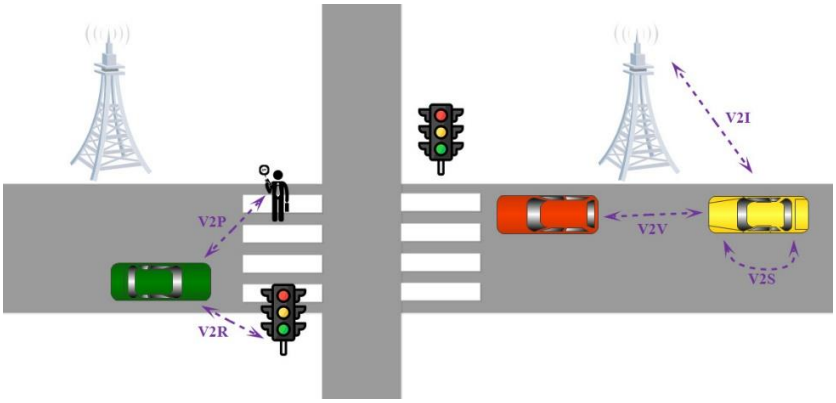

Figure I.2. Architecture de communication IoV.

- **Communication de véhicule à dispositif personnel (Vehicle-to-Personal ou V2P) :** c'est nommé aussi communication de véhicule à l'homme (Vehicle-to-Human ou V2H). Ce type de communication fait référence à l'interaction entre les véhicules et les dispositifs personnels qui appartiennent aux personnes (conducteurs, passagers, piétons, cyclistes), comme les tablettes, les téléphones intelligents, etc. Grâce à ce type de connexion, les véhicules peuvent partager avec les dispositifs mobiles différents services (partage de fichiers, musique, streaming vidéo).

- **Communication de véhicule à capteurs (Vehicle-to-Sensor ou V2S) :** ce type de communication permet aux véhicules de surveiller leur comportement lors leur déplacement en détectant leur vitesse, leur position, la pression des pneus, la pression d'huile moteur, etc.
- **Communication de véhicule à tout (Vehicle-to-Everything ou V2X) :** grâce à l'IoT, les véhicules peuvent se connecter à tout ce qui peut partager des informations sur l'environnement du véhicule.

I.2.2.3. Caractéristiques

L'émergence de "l'Internet des objets pour les véhicules" ou "Internet des véhicules" (IoV) corrige les lacunes du VANET et ouvre de brillantes perspectives pour le développement d'ITS à l'avenir. Nous avons analysé les avantages de l'IoV sous plusieurs angles :

- L'architecture de réseau hétérogène de l'IoV permet la coopération entre le réseau de communication du véhicule et d'autres réseaux de communication.
- La plupart des dispositifs de communication de la vie quotidienne sont compatibles avec l'IoV. La coopération mutuelle de différents types de réseaux et l'émergence de multiples modèles de communication (V2S, V2V, V2P, V2R, V2I, V2X) ont permis le partage de données volumineuses et la fiabilité de divers services de communication, tout en élargissant le champ d'application de la communication automobile. C'est l'un des avantages les plus importants de l'IoV. Plus précisément, V2S représente la communication entre capteurs embarqués via Ethernet et Wi-Fi. V2V et V2R qui représentent la communication entre véhicule et véhicule ou entre véhicule et RSU peuvent communiquer via WAVE. V2P représente la communication entre un véhicule et les terminaux portables d'une personne utilisant CarPlay d'Apple, le système Android ou NFC. V2I représente la communication entre les véhicules et l'infrastructure via Wi-Fi ou LTE/4G/5G/ B5G [10].

I.2.3. Vehicle Cloud Computing

I.2.3.1. Généralité

I.2.3.1.1. Cloud Computing

D'après l'institut national des normes et de la technologie (National Institute of Standards and Technology ou NIST), le Cloud Computing (CC) a été défini comme suit : « *Le Cloud est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de*

ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mises à disposition et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services » [11].

Comme l'ont souligné Foley [12] et Kim [13], la notion du CC est née de la prise de conscience du fait qu'au lieu d'investir dans l'infrastructure, les entreprises peuvent juger utile de louer l'infrastructure et parfois les logiciels nécessaires à l'exécution de leurs applications. Cette idée a été suggérée par l'omniprésence et le coût relativement faible de l'internet à haut débit, ainsi que par les progrès réalisés dans les domaines de la virtualisation, du calcul parallèle et distribué, et des bases de données distribuées. L'un des principaux avantages du CC est qu'il offre un accès évolutif aux ressources informatiques et aux services de technologie de l'information (TI).

CC a introduit plusieurs caractéristiques nouvelles par rapport aux systèmes locaux traditionnels :

- Le CC présente un approvisionnement à la demande des ressources de calcul, de stockage et de services informatiques. Il met à la disposition des utilisateurs des ressources informatiques infinies ; par conséquent, les utilisateurs ne sont pas nécessairement tenus de planifier la fourniture de ressources physiques ;
- Les utilisateurs ont la possibilité de louer des services et des ressources en fonction de leurs besoins à un moment donné. Le CC peut offrir des alternatives flexibles permettant aux utilisateurs d'acheter des ressources matérielles supplémentaires uniquement en cas d'augmentation de leurs besoins.
- Le CC offre également aux utilisateurs la possibilité de louer des ressources informatiques pour une période donnée.

I.2.3.1.2. Mobile Cloud Computing

En 2007, une nouvelle technique est apparue, le Cloud computing mobile (Mobile Cloud Computing ou MCC), qui est devenue un domaine attrayant pour les entreprises en raison de l'utilisation généralisée d'applications mobiles à faible coût [14]. Lorsque le traitement et le stockage des données s'effectuent en dehors de l'appareil mobile, cette infrastructure est appelée MCC. Les applications ont été déplacées des téléphones mobiles vers le Cloud, afin de partager les applications, le stockage des données et l'informatique mobile entre les appareils mobiles. Ainsi, le MCC est utilisée dans un large éventail d'applications telles que l'informatique de masse,

le traitement du langage naturel, le partage de GPS, le traitement d'images, les applications de données de capteurs, les requêtes, le partage de l'accès à Internet et la recherche multimédia [15]. Le MCC présente plusieurs avantages :

a) Tous les utilisateurs, où qu'ils soient et à tout moment, peuvent accéder aux services ;

b) les services fournissent des informations aux utilisateurs, telles que la localisation et le contexte ;

c) elle améliore la puissance de traitement et la capacité de stockage des données ;

d) elle prolonge la durée de vie de la batterie ;

e) l'informatique mobile a trouvé de nombreuses solutions pour surmonter les problèmes liés au Cloud [16].

La plupart des applications mobiles, comme le commerce mobile, l'apprentissage mobile et les soins de santé mobiles, ont bénéficié des avantages des multinationales. L'architecture du MCC est classée en fonction de la couche des centres de données et du modèle standard de service en Cloud, qui comprend la plateforme en tant que service (PaaS), l'infrastructure en tant que service (IaaS) et le logiciel en tant que service (SaaS) [15]. Bien qu'elle offre de nombreux avantages et services aux utilisateurs, elle doit faire face à de nombreux défis tels que la faible bande passante, la qualité des services et la sécurité pour les utilisateurs mobiles.

I.2.3.1.3. Application du Cloud Computing aux réseaux véhiculaires

Le VCC est considéré comme une extension du MCC. Dans le VCC, les ressources et les services peuvent arriver en temps réel pour des informations provenant de n'importe où. Cela permet aux passagers et aux conducteurs d'accéder à un certain nombre de nouvelles applications pour fournir divers services [17]. Le VCC constitue donc la base de l'amélioration et du développement des systèmes de transport intelligents et un environnement riche pour les chercheurs. En outre, il joue un rôle majeur dans la vie des gens en assurant la sûreté, la sécurité, la confiance et le confort des passagers et des conducteurs. L'objectif fondamental du VCC est de fournir des services peu coûteux aux conducteurs et de réduire les accidents et les embouteillages. Le Cloud traditionnel fournit des services tels que des logiciels, du stockage et des ressources informatiques, mais dans le VCC, d'autres services sont apparus. La figure I.3 montre le VCC, qui

échange des informations entre les véhicules ou entre le centre de données Cloud et les véhicules par l'intermédiaire des RSU afin de calculer ou de stocker.

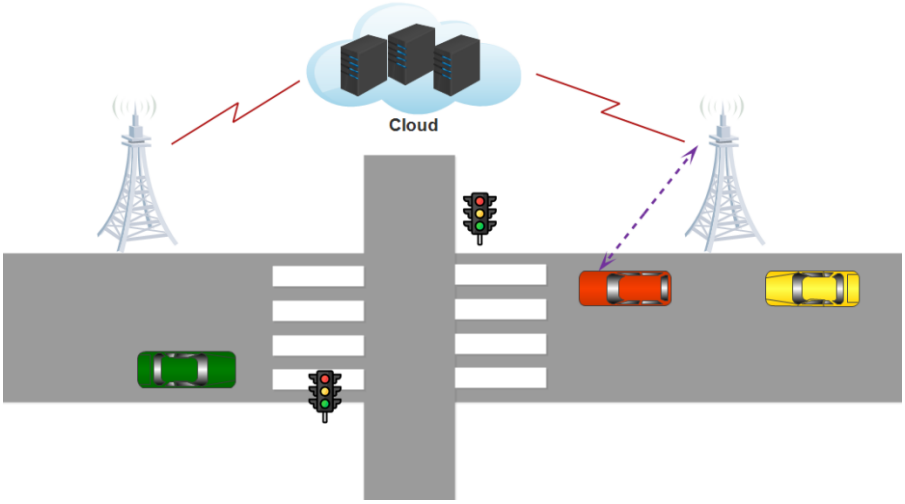

Figure I.3. Modèle de communication du VCC.

Le VCC fournit des services, comme l'infrastructure en tant que service (IaaS), la plateforme en tant que service (PaaS), l'application en tant que service (AaaS), le logiciel en tant que service (SaaS) et le stockage en tant que service (STaaS), aux utilisateurs de véhicules lorsqu'ils sont connectés via des OBU afin d'obtenir un stockage et une puissance de calcul illimités [18]. Le VCC améliore la gestion du trafic routier en réduisant les risques pour la vie, les coûts et les délais.

I.2.3.2. Architecture

L'architecture du VCC repose sur trois couches : véhicule, communication et Cloud. Comme l'illustre la figure I.4,

- Véhicule : La première couche est celle de l'intérieur du véhicule, qui est responsable de la surveillance de la santé et de l'humeur du conducteur ainsi que de la collecte d'informations à l'intérieur de la voiture, telles que la pression et la température, à l'aide de capteurs corporels, de capteurs environnementaux, de capteurs de smartphones, de capteurs internes du véhicule, de capteurs de navigation inertielle (INS) et de la reconnaissance du comportement du conducteur [19], [20], et cela afin de prédire les réflexes et les intentions du conducteur. Ensuite, les informations recueillies par les capteurs doivent être envoyées au Cloud pour être stockées ou utilisées comme données d'entrée pour divers logiciels de la couche d'application, par exemple

pour fournir des applications de reconnaissance de la santé et de l'environnement. Nous supposons que chaque véhicule est équipé d'un OBU qui comprend un système de navigation intégré, avec une carte et l'emplacement d'un RSU. Les OBU disposent d'une communication sans fil à large bande pour transférer des données par le biais de dispositifs de communication cellulaire 3G ou 4G, Wi-Fi, WiMAx, Wireless Access in Vehicular Environment (WAVE) [21], ou Dedicated Short Range Communication (DSRC) [22].

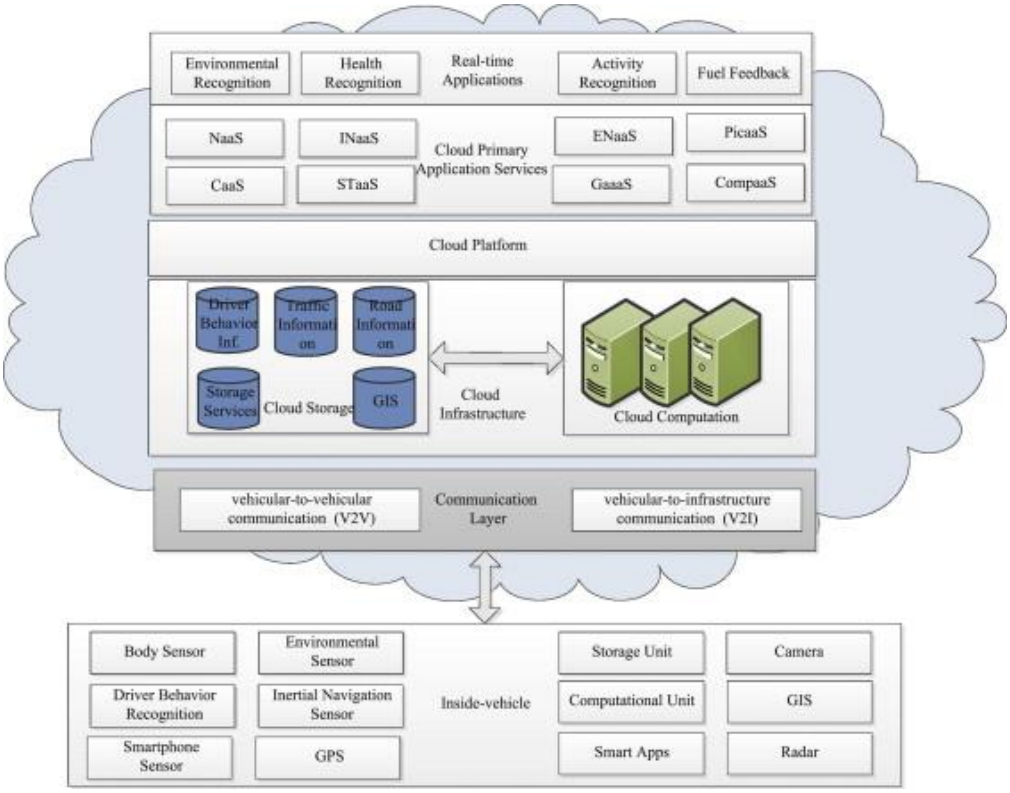

Figure I.4. Architecture du réseau VCC [23].

- Communication : La couche suivante de cette architecture est appelée communication, qui comprend deux parties :

- *La communication V2V via DSRC* : Si un conducteur fait preuve d'un comportement anormal sur la route, par exemple en changeant radicalement de direction, en dépassant la limite de vitesse ou en cas de défaillance mécanique majeure du véhicule, un message d'avertissement d'urgence (EWM) est généré et envoyé au stockage Cloud et aux véhicules environnants, contenant l'emplacement géographique, la vitesse, l'accélération et la direction de déplacement du contrevenant.

- *La communication V2I :* C'est le deuxième composant de la couche de communication qui est responsable de l'échange de données opérationnelles entre les véhicules, les infrastructures et le Cloud sur des réseaux sans fil tels que 3G, satellite ou Internet

- **Cloud** : La couche Cloud se compose de trois couches internes : l'application, l'infrastructure du Cloud et la plate-forme du Cloud.

- *Couche d'application :* Dans la couche application, diverses applications et services sont considérés comme des services en temps réel ou des services primaires en Cloud, accessibles à distance par les conducteurs, tels que le retour d'informations sur le carburant, la reconnaissance de l'activité humaine, la reconnaissance de la santé et la reconnaissance de l'environnement. La reconnaissance de l'activité humaine est utilisée pour une analyse (ou une interprétation) automatisée des événements en cours et de leur contexte dans les données vidéo. Dans les services primaires, plusieurs services sont déployés, tels que le réseau en tant que service (NaaS), le stockage en tant que service (STaaS), la coopération en tant que service (CaaS), l'information en tant que service (INaaS) et le divertissement en tant que service (ENaaS).
- *Couche d'infrastructure du Cloud :* L'infrastructure en Cloud se compose de deux parties : le stockage en Cloud et le calcul en Cloud. Les données recueillies par la couche intérieure du véhicule seront stockées dans le système d'information géographique (GIS), un dispositif de contrôle du trafic routier ou un système de stockage en fonction du type d'applications. La partie calcul est utilisée pour calculer les tâches de calcul qui fournissent des performances plus rapides, par exemple, les capteurs de reconnaissance de la santé envoient des données à la base de données du comportement du conducteur dans le stockage en Cloud.

I.3. Réseaux Fog véhiculaires : généralité

I.3.1. Fog computing : nouveau paradigme

Au cours des dernières années, le CC a offert de nombreuses possibilités aux entreprises en proposant à leurs clients une gamme de services informatiques. Le modèle actuel de "paiement à l'utilisation" est devenu une alternative efficace à la possession et à la gestion de centres de données privés pour les applications Web et les traitements par lots destinés aux clients [23]. Le

CC libère les entreprises et leurs utilisateurs finaux de la spécification de nombreux détails, tels que les ressources de stockage, la limitation des calculs et le coût des communications réseau. Cependant, cette flexibilité devient un problème pour les applications sensibles à la latence, qui nécessitent des nœuds à proximité pour répondre à leurs exigences en matière de délai [23]. Avec la prolifération des techniques et des appareils de l'IoT dans la vie quotidienne, le paradigme actuel du CC peut difficilement satisfaire les exigences en matière de mobilité, de localisation et de faible latence.

Le Fog Computing (ou FC) a été proposé en 2012 [24] comme un nouveau paradigme pour résoudre les problèmes liés au CC mentionnés ci-dessus. Le FC est une plateforme hautement virtualisée qui prend en charge le Cloud et fournit des services de stockage, de calcul distribué et de mise en réseau entre les utilisateurs finaux et les centres de données du Cloud.

Dans le FC, les services peuvent être hébergés sur des appareils terminaux tels que des décodeurs ou des points d'accès. L'infrastructure de cette nouvelle architecture informatique distribuée permet aux applications de fonctionner aussi près que possible des données massives et exploitables détectées provenant des personnes, des processus et des objets. Ce concept du FC, qui est en fait un CC proche du "terrain", crée une réponse automatisée qui génère de la valeur. Le CC et le FC fournissent tous les deux, des services de données, de calcul, de stockage et d'application aux utilisateurs finaux. Cependant, le Fog se distingue du Cloud par sa proximité aux utilisateurs finaux, sa distribution géographiquement dense et son soutien à la mobilité [25]. Le FC offre une faible latence, une connaissance de l'emplacement et améliore la qualité des services (QoS) pour les applications en continu et en temps réel. Les exemples typiques sont l'automatisation industrielle, les transports et les réseaux de capteurs et d'actionneurs. En outre, cette nouvelle infrastructure prend en charge l'hétérogénéité, car les dispositifs Fog comprennent des appareils d'utilisateurs finaux, des points d'accès, des routeurs de périphérie et des commutateurs. Le paradigme Fog est bien positionné pour l'analyse des données en temps réel, il prend en charge des points de collecte de données distribués de manière dense et offre des avantages dans les domaines du divertissement, de la publicité, de l'informatique personnelle et d'autres applications.

Nous adoptons une hiérarchie simple à trois niveaux dans la figure I.5. Dans ce cadre, chaque objet intelligent est attaché à l'un des dispositifs du Fog. Les dispositifs du Fog peuvent être interconnectés, et chacun d'entre eux est relié au Cloud.

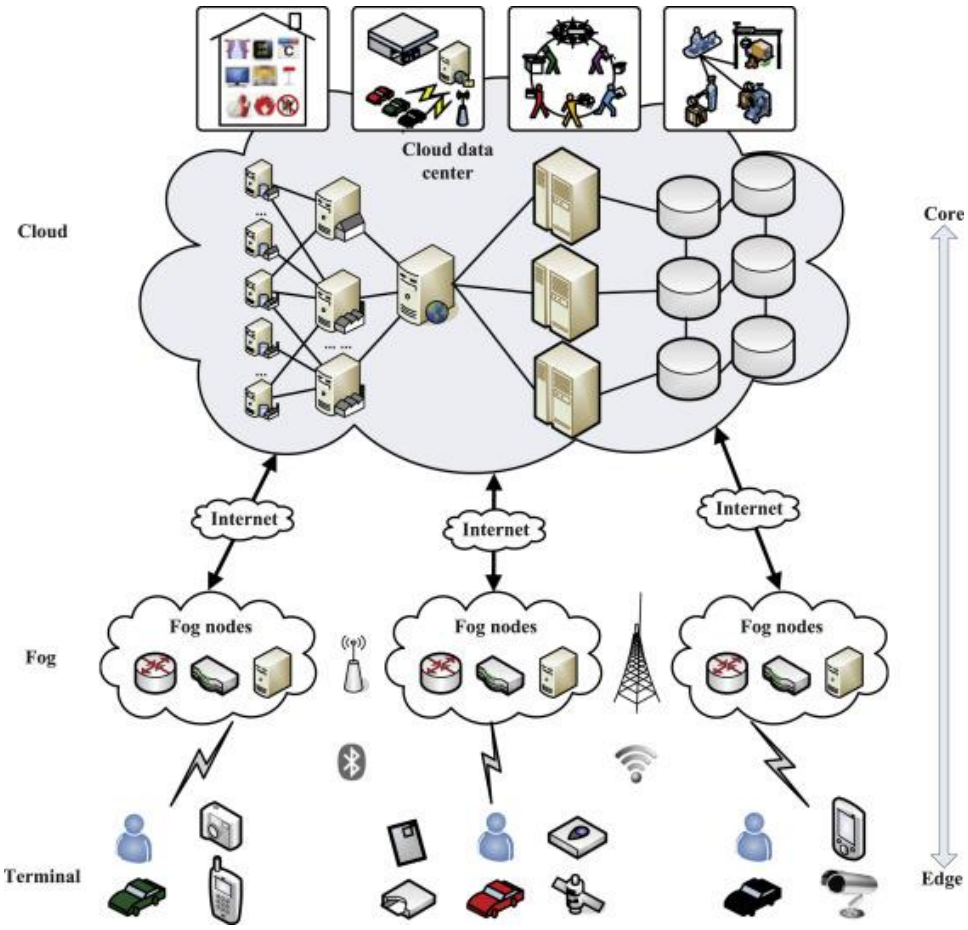

Figure I.5. Architecture du Fog Computing [26].

I.3.2. Vehicular Fog Computing

Le VCC présente de sérieuses limitations, notamment le fait qu'elle n'est pas adaptée aux nouveaux services de sécurité ou de l'infodivertissement, qui sont critiques en termes de temps, et ont des contraintes de latence beaucoup plus strictes. Afin de répondre à ses limites, le Vehicular Fog Computing (VFC) a été proposé. Le VFC représente l'application du FC sur les réseaux véhiculaires. L'objectif est de bénéficier des avantages du Fog sur le réseau véhiculaire.

Dans le VFC, les fournisseurs de services informatiques sont situés à proximité des véhicules afin de surmonter les contraintes de latence et autres [17]. Dans le VFC, une couche de serveurs Fog est déployée entre les véhicules et le serveur Cloud. Il se sert des dispositifs situés sur les véhicules ou les déploie à proximité de ces derniers afin de constituer cette couche de Fog intermédiaire. Les utilisateurs finaux et les véhicules sont également considérés comme faisant partie du « Fog ». Contrairement aux services de Cloud computing qui sont plus centralisés, le Fog

computing cible les applications avec des déploiements largement distribués. Les capteurs et autres dispositifs dans les véhicules collectent des données et ces données sont stockées et traitées à des niveaux Fog serveurs intermédiaires. Ainsi, les services offrent une communication à faible latence et une meilleure prise en compte du contexte [27].

Le Fog peut être constitué de plusieurs unités ou dispositifs situés au bord de la route dans des véhicules ou à proximité des véhicules ou bien il peut s'agir d'une agrégation des ressources abondantes du groupe de véhicules. En utilisant cette couche de Fog, la plupart des données des véhicules sont traitées et une réponse immédiate est fournie aux véhicules du réseau. La communication de la couche Fog au serveur Cloud n'a lieu que lorsque cela est nécessaire. Le Fog Computing est très bénéfique pour les applications à faible latence comme le streaming vidéo et les jeux. La proximité des utilisateurs et le soutien continu à la mobilité ont été les deux avantages uniques qui ont conduit à la popularité croissante du VFC dans la recherche et l'industrie.

Dans [17], le VFC est défini comme un type de véhicule de traitement utilisé comme infrastructure pour permettre une utilisation optimale de ses ressources de communication et de calcul. De plus, le VFC peut également fournir des services à faible latence et de localisation pour des applications en continu et en temps réel. Cependant, il n'existe pas encore de définition largement acceptée du VFC, ni des cas d'utilisation associés [28].

	VCC	**VFC**
Prise de décision	Distante	Locale
Emplacement	Distant	Proche
Mobilité	Elevée	Supportée
Latence	Elevée	Faible
Interactions en temps réel	Moyenne	Moyenne
Nombre de nœuds serveurs	Peu	Grand
Répartition géographique	Centralisée	Décentralisée et distribuée
Consommation de bande passante	Elevée	Faible
Capacités de calcul	Supérieure	Moyenne
Capacités de stockage	Forte	Faible

Tableau I.1. Comparaison entre le VCC et le VFC.

Le tableau I.1 montre la comparaison entre le VCC et le VFC. Bien que le VCC a offert de bonnes performances aux applications véhiculaires, la longue distance entre les appareils mobiles,

les véhicules et les centres de données distants a empêché la fourniture d'un service en temps réel à ces applications. Cela a entraîné un retard bien plus important dans la communication et le partage des ressources avec le VCC. De plus, le VFC offre un excellent support pour la mobilité alors que le VCC ne supporte que les applications qui sont moins mobiles. Le VCC est limité par la bande passante et son coût de déploiement est élevé. En revanche, le VFC a un faible coût de déploiement avec un équilibrage de la charge en temps réel et une prise de décision locale.

I.3.2.1. Architecture

L'architecture du VFC comprend trois types d'entités, à savoir les véhicules intelligents, qui constituent la couche de génération de données, les nœuds Fog, qui constituent la couche de Fog, et les serveurs Cloud, qui constituent la couche Cloud [29].

- Les Véhicules intelligents : Les véhicules intelligents jouent un rôle important en tant que principaux générateurs de données dans un système VFC, en raison de leurs capacités de calcul, de détection (par exemple, caméras, radars et GPS), de communication et de stockage en temps réel. La quantité de données collectées par les différents capteurs d'un véhicule intelligent a été estimée à environ 25 Go/h en une seule journée (par exemple, 20-60 Mo/s pour les caméras, 10 Ko/s pour les radars et 50 Ko/s pour le GPS) [29]. Certaines de ces données peuvent être traitées par le véhicule intelligent lui-même, afin d'éclairer la prise de décision en temps réel (c'est-à-dire au niveau du véhicule), tandis que d'autres données seront partagées et téléchargées vers les nœuds Fog pour être analysées et utilisées à d'autres fins (par exemple, la planification du trafic et des infrastructures, ainsi que la surveillance).

- Les nœuds Fog : Les RSU, généralement déployées dans différentes zones d'une ville, peuvent facilement être mises à niveau pour servir de nœuds Fog. Cela permettra la collecte des données envoyées par les véhicules intelligents, le traitement des données collectées et la communication des données (traitées) aux serveurs Cloud. Ces nœuds jouent également le rôle de dispositifs intermédiaires entre les serveurs Cloud et les véhicules intelligents dans le cadre d'un système VFC. Contrairement aux réseaux véhiculaires existants, ces nœuds (RSU) auront plus de fonctions et fourniront des services plus variés pour les véhicules intelligents, tels que la navigation, le streaming vidéo et les feux de circulation intelligents. En d'autres termes, ces nœuds ne sont pas seulement des relais ou des diffuseurs ; ils traitent également des données, stockent des

données et prennent des décisions en tant que couche Fog, (c'est-à-dire des décisions au niveau de la zone).

- Les serveurs Cloud : Ils assurent la surveillance au niveau de la ville et le contrôle centralisé à partir d'un site distant. Ces serveurs obtiendront les données téléchargées par les nœuds Fog tout en effectuant des analyses à forte intensité de calcul pour prendre des décisions optimales d'un point de vue holistique (par exemple, une décision au niveau de la ville). Par exemple, ils surveilleront, géreront et contrôleront les infrastructures routières de la ville afin de parvenir à un contrôle optimal du trafic au niveau de la ville. La couche Cloud est généralement constituée d'un serveur de gestion du trafic (TMS) et d'une autorité tierce de confiance (TTA). En général, le TMS est chargé de traiter les messages et d'informer les gestionnaires du trafic pour qu'ils prennent des mesures. Si tous les messages téléchargés par les véhicules sont traités par le TMS, celui-ci sera surchargé. Par conséquent, le TMS est simplement chargé de la réception des résultats et de l'attribution des récompenses dans notre travail. Les récompenses individuelles et l'équité du réseau sont gérées par le TTA.

I.3.2.2. Caractéristiques

L'architecture du VFC peut offrir de nombreux avantages et de nombreux systèmes VFC actuels puissent avoir des caractéristiques uniques.

- Temps de réponse : La plupart des applications destinés aux véhiculaires nécessitent une réponse en temps réel, notamment pour les applications de contrôle du trafic et d'amélioration de la sécurité. Cependant, l'architecture conventionnelle du VCC n'est pas conçue pour répondre à cette exigence de faible latence, puisque les données recueillies par les véhicules intelligents seront traitées à distance plutôt que localement. En raison du délai de transmission et de tout problème potentiel de connectivité (par exemple, hors de portée), le temps de réponse moyen des applications basées sur le Cloud et des applications traitées localement sera probablement supérieur à une seconde et inférieur à 10 ms, respectivement. Par conséquent, les nœuds Fog d'un système VFC, situés à proximité des véhicules intelligents, peuvent réduire considérablement le temps de réponse des applications embarquées.

- Communication : Dans un avenir prévisible, le nombre de véhicules intelligents (y compris les véhicules militaires intelligents) est susceptible d'augmenter et peut-être de devenir la norme. Ainsi, il est probable que la quantité de données générées et transmises par ces véhicules

augmentera de manière exponentielle à une fréquence élevée (similaire à la tendance actuelle du big data). Dans les scénarios classiques du VCC, les données brutes sont directement téléchargées vers les serveurs Cloud pour être traitées ultérieurement. Malgré les progrès potentiels des technologies de communication, la bande passante nécessaire à la transmission efficace d'un tel volume de données n'est pas garantie en raison d'un large éventail de facteurs logistiques, politiques et géographiques, en particulier dans une zone de conflit. Si les données sont trop volumineuses et trop fréquentes, les communications constitueront un goulot d'étranglement pour la plupart des applications véhiculaires. Par conséquent, les nœuds Fog d'un système VFC peuvent atténuer ces limitations en prétraitant les données collectées afin qu'elles puissent être agrégées/filtrées avant d'être téléchargées. Cela permet de réduire le volume et la fréquence des données.

- Le stockage : Dans l'architecture conventionnelle du VCC, presque toutes les données d'application seront stockées dans des serveurs Cloud distants. Cela peut ne pas être pratique en raison de la nature changeante des applications véhiculaires et des données collectées. Par exemple, les données et les applications véhiculaires sont de plus en plus sensibles à la localisation. Ainsi, la possibilité d'accéder aux données stockées en temps réel (par exemple, les données stockées dans des nœuds Fog décentralisés et sensibles à l'emplacement) réduira la charge de stockage sur les serveurs Cloud distants.

I.3.3. Problèmes de la Sécurité et de la protection de la vie privée dans les VFC

Le VFC étant un paradigme informatique encore relativement nouveau, les questions de sécurité restent inexplorées. Nous présentons ici plusieurs questions relatives à la sécurité et à la protection de la vie privée dans les VFC.

I.3.3.1. Les exigences de la sécurité et de la protection de la vie privée

- La confidentialité : La confidentialité est très importante dans le VFC. Une personne tierce ne doit pas intercepter le message ou les données envoyées par un véhicule ou un nœud Fog avant que le récepteur ne les reçoive. Tout accès non autorisé de ce type doit être détecté et empêché. Le chiffrement à clé publique ou symétrique peut être mis en œuvre pour obtenir la confidentialité requise [30].

- Intégrité : Tout message transmis dans un réseau VFC ne doit pas être modifié ou altéré par un tiers ou une entité malveillante. Pour garantir l'intégrité, toute modification du message doit être détectée avec le changement spécifique [29].

- Authentification : Chaque fois qu'un nœud Fog rejoint le réseau VFC, il doit être authentifié. Il devrait également y avoir un système d'authentification pour les véhicules clients qui demandent des services au réseau VFC.

- Validation de l'emplacement : La validation de l'emplacement doit être effectuée afin qu'aucun véhicule ne puisse prétendre être présent à cet endroit sans y être réellement présent.

- Autorisation et contrôle d'accès : Après être entrée dans le réseau VFC, une entité doit être autorisée et avoir accès pour effectuer une action. Un mécanisme de contrôle d'accès approprié doit être mis en œuvre pour empêcher toute activité non autorisée.

- Non-répudiation : La non-répudiation doit être mise en œuvre afin qu'un utilisateur puisse vérifier l'expéditeur de tout message et que l'expéditeur ne puisse pas nier avoir envoyé un message.

- Disponibilité : Le service du réseau VFC doit être disponible à tout moment. Il doit y avoir un mécanisme de protection approprié contre les attaques de disponibilité telles que le déni de service (Denial of Service ou DoS).

- Fiabilité : La fiabilité des services de la structure VFC doit être gérée, comme l'exactitude des calculs, et la capacité de stockage.

- Confidentialité des informations sur le véhicule : Les informations relatives au véhicule qui doivent être envoyées dans le réseau VFC, comme les informations d'enregistrement ou l'état de santé du véhicule, doivent rester privées et ne doivent pas être interceptées ou révélées à une entité malveillante.

- Confidentialité des informations personnelles : Les informations personnelles du conducteur, telles que son nom et son permis de conduire, ne doivent pas être révélées dans le réseau VFC.

- Confidentialité de l'emplacement : Les informations relatives à l'emplacement actuel et à l'itinéraire de destination des véhicules participants doivent être préservées afin que personne ne puisse suivre intentionnellement un véhicule.

I.3.3.2. Menaces et vulnérabilités

Nous allons identifier les menaces et les vulnérabilités de l'architecture du VFC en nous basant sur le modèle de sécurité STRIDE. Le terme STRIDE signifie Spoofing, Tempering, Repudiation, Information disclosure, Denial of service, et Elevation of privilege [31].

Le processus de modélisation des menaces STRIDE a été proposé pour la première fois par Microsoft pour identifier les menaces de sécurité d'un système. Chaque section du modèle STRIDE correspond à une propriété de sécurité souhaitable qui est l'authenticité, l'intégrité, la non-répudiation, la confidentialité, la disponibilité et l'autorisation. La figure I.6 donne un aperçu de la taxonomie des attaques selon ce processus de modélisation des menaces.

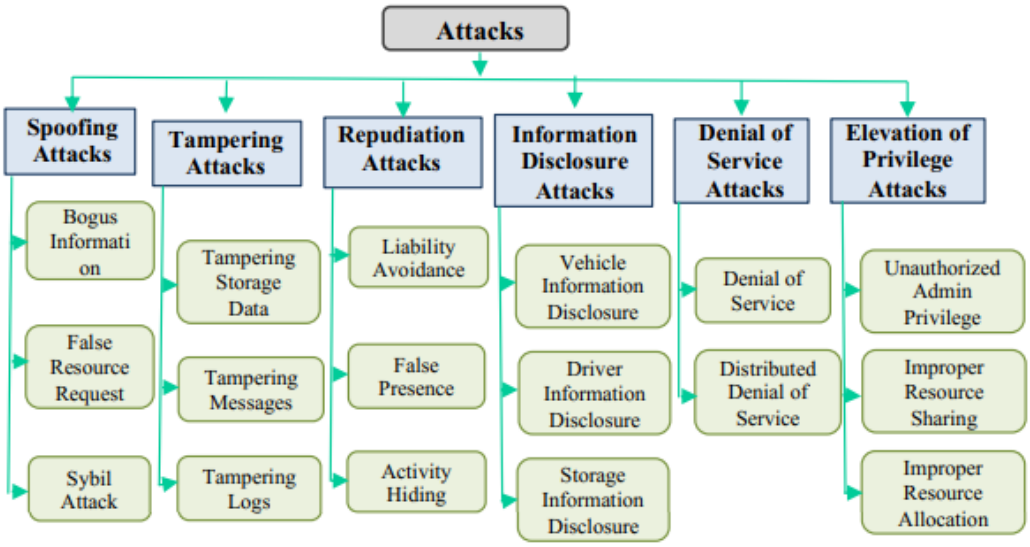

Figure I.6. Taxonomie des attaques basée sur STRIDE [30].

1) **Attaques par usurpation d'identité (spoofing attack) :** L'usurpation d'identité consiste à falsifier des données pour tromper un système et obtenir tout type d'accès non autorisé. Elle détruit l'authenticité qui est l'une des propriétés de sécurité les plus importantes. Voici quelques exemples d'attaques par usurpation :
   - *L'attaque par fausse information (Bogus information) :* Les véhicules malveillants qui utilisent le réseau VFC peuvent envoyer de fausses informations. Par conséquent,

les nœuds Fog risquent d'avoir des conclusions erronées, et par la suite, prendre des fausses décisions.

- *Fausses demandes de ressources (False ressource request) :* Un attaquant peut envoyer un grand nombre de fausses demandes de ressources au réseau VFC qui ne seront finalement pas utilisées par l'attaquant. Ces fausses demandes peuvent finir par épuiser les ressources du système.
- *Attaque Sybil (Sybil attack) :* Dans l'attaque Sybil, l'attaquant diffuse des messages à partir de plusieurs identités de nœuds qui prétendent provenir de plusieurs véhicules [32]. Le nœud Fog et les autres véhicules pensent que tous les messages proviennent de différents véhicules.

2) **Attaques de falsification (Tampering attack) :** Les attaques de falsification consistent à effectuer des mises à jour ou des modifications non autorisées de tout contenu dans le réseau VFC. Il s'agit d'attaques contre l'intégrité du système. Voici quelques exemples d'attaques par falsification :
   - *Falsification des données de stockage (Tampering storage data) :* Les véhicules ayant des contraintes de stockage peuvent externaliser leurs données aux nœuds Fog les plus proches. Un attaquant peut avoir accès aux données et effacer ou insérer des blocs de données.
   - *Falsification des messages (Tampering messages) :* Les messages transmis entre les entités constituent l'atout le plus important de l'architecture du VFC. Une entité malveillante peut attraper et altérer le message avant qu'il n'atteigne sa destination.
   - *Falsification des logs (Tampering logs) :* Les nœuds Fog ou le serveur Cloud distant peuvent stocker les fichiers logs de tout ce qui se passe dans l'architecture du VFC. L'attaquant peut obtenir un accès non autorisé aux logs et les modifier à diverses fins, par exemple pour essayer de tromper l'enquêteur après avoir effectué des activités malveillantes.
3) **Attaques par répudiation (Repiduation attack) :** Les attaques par répudiation se produisent lorsqu'un attaquant répudie l'exécution d'une action intentionnelle.
   - *Évitement de la responsabilité (liability avoidance) :* Du point de vue des nœuds Fog, l'attaquant peut nier avoir commis un incident tel qu'un accident de la route, avoir

fourni des informations erronées, avoir supprimé des données de stockage externalisées, etc.

- *Fausse présence (False presence) :* L'attaquant peut prétendre être présent à un endroit à un moment donné sans y être réellement présent. Ces attaques sont très graves dans les architectures du VFC car les applications sont généralement très sensibles à la localisation.
- *Dissimulation d'activité (Activity hiding) :* Lors de l'exécution d'une attaque, l'attaquant peut essayer de cacher l'activité en ne laissant pas ces événements être enregistrés afin qu'il ne puisse pas être reconnu coupable dans une enquête future.

4) **Attaques de divulgation d'informations (Information disclosure attack) :** Dans les attaques par divulgation d'informations, l'attaquant peut dissimuler son identité pour acquérir des informations sensibles spécifiques sur un utilisateur ou un véhicule, puis les utiliser ou les divulguer à l'extérieur. Par exemple :
   - *Divulgation d'informations sur le véhicule et le conducteur (Vehicle and driver information disclosure) :* l'attaquant peut capturer et divulguer des informations confidentielles sur le véhicule et le conducteur, telles que les données des capteurs, la localisation, les informations d'enregistrement, le kilométrage, le permis de conduire, la trajectoire, l'assurance, etc.
   - *Divulgation des informations de stockage (Storage information disclosure) :* les véhicules utilisateurs peuvent externaliser leurs données vers le stockage des nœuds Fog les plus proches. Cependant, ces données peuvent contenir des informations sensibles sur les utilisateurs. Un attaquant ou un nœud Fog malveillant peut révéler ces informations à des entités extérieures.
5) **Attaques par déni de service (Denial of service attack) :** Les attaques par déni de service peuvent être réalisées pour perturber la disponibilité, les performances et l'efficacité du système.
   - *Déni de service (Denial of service) :* Dans l'attaque par déni de service, l'attaquant consomme les ressources disponibles par le biais d'une usurpation ou d'une utilisation avide, ce qui pousse les utilisateurs légitimes à se battre pour accéder à ces ressources. Comme cette attaque est généralement réalisée par un seul attaquant, un trop grand

nombre de messages ou de demandes de ressources peuvent être refusé pour empêcher l'attaque et assurer un partage logique des ressources entre les utilisateurs.

- *Déni de service distribué (Distributed denial of service) :* L'attaque par déni de service distribué est réalisée par plusieurs véhicules malveillants contre les nœuds Fog, en envoyant des messages sans signification ou de demandes de ressources pour épuiser les ressources.

6) **Attaques par élévation de privilèges (Elevation of privilege attack) :** L'élévation de privilèges consiste à obtenir, après s'être introduit dans le système, des privilèges non autorisés que l'attaquant n'est pas censé avoir. Ces attaques ruinent l'autorisation, qui est une propriété de sécurité critique.

- *Privilège d'administrateur non autorisé (Unauthorized admin privilege) :* L'attaquant peut élever son privilège pour obtenir l'accès au niveau administrateur du système VFC afin de contrôler différents composants de l'architecture, tels que les nœuds Fog et les centres de données distants.
- *Partage inapproprié des ressources (Improper resource sharing) :* Les nœuds Fog partagent leurs ressources qui doivent être réparties de manière optimale entre les utilisateurs pour garantir l'équité. Cependant, l'attaquant peut élever le privilège pour augmenter l'utilisation de ses ressources plus que les autres véhicules.
- *Allocation inappropriée des ressources (Improper resource allocation) :* Les ressources hétérogènes disponibles sont allouées de manière optimale en fonction des besoins. Tous les véhicules utilisateurs s'attendent à recevoir une part équitable des ressources disponibles. Cependant, l'attaquant peut élever son privilège pour obtenir plus de ressources de stockage, de calcul ou de réseau.

I.4. Conclusion

Dans ce chapitre, nous avons présenté les différents paradigmes des réseaux véhiculaires : VANET, IoV, VCC et VFC en donnant leurs caractéristiques. Le VFC, comme tout nouveau paradigme, est vulnérable aux différentes menaces. La sécurité et la protection de la vie privée sont des aspects très importants pour l'établissement et le maintien de la confiance des utilisateurs dans le VFC. Cependant, nous avons détaillé les problèmes de la sécurité et de la protection de la vie privée dans les réseaux VFC, en identifiant les exigences de la sécurité et en classant les menaces et les vulnérabilités.

Chapitre II : État de l'art : Analyse et discussion des travaux existants connexes

II.1. Introduction

L'objectif premier des réseaux VFC est de garantir des conditions de circulation sûres et d'assurer la sécurité des conducteurs en diffusant des messages d'information dans le réseau. Cependant, les attaquants peuvent violer la sécurité et la confidentialité accordées aux propriétaires de véhicules en raison de l'utilisation d'un support sans fil ouvert. Comme nous l'avons souligné dans le premier chapitre, le réseau VFC est comme tout nouveau paradigme vulnérable à diverses attaques. Les réseaux VFC doivent fournir des services fiables et sécurisés aux utilisateurs, et les entités VFC doivent avoir un certain niveau de confiance. Dans ce chapitre, nous allons analyser et examiner des travaux existants en se basant sur deux aspects, le premier concerne l'attaque Sybil au sein du réseau VFC et le deuxième concerne l'authentification.

II.2. L'attaque Sybil dans les réseaux véhiculaires

II.2.1. Définition de l'attaque Sybil

Le concept d'attaque Sybil a été introduit pour la première fois par Douseur [33]. Il s'agit d'une menace qui vise à perturber un réseau. Dans l'attaque Sybil, l'attaquant utilise des identités multiples afin d'envoyer des messages à d'autres nœuds appartenant au même réseau. Ces identités qui peuvent être créées ou usurpées par l'attaquant sont appelées les nœuds Sybil. Une illusion est créée dans le réseau par l'envoi d'un message indiquant des fausses alertes ; par exemple ; un accident ou un embouteillage a déjà eu lieu afin d'obliger les autres véhicules à changer d'itinéraire et à emprunter celui de l'attaquant. De plus, de fausses informations peuvent être injectées dans le réseau par l'attaquant Sybil [34]. Les différents types d'attaques Sybil possibles sont présentés dans la figure II.1. La figure II.1 montre clairement que la classification des attaques Sybil est effectuée sur la base de l'identité, de la participation au réseau, et du type de communication [35]. Ces caractéristiques sont expliquées dans les paragraphes suivants.

a) **Catégorie d'identité** : Dans cette catégorie, une nouvelle identité Sybil est créée par l'attaquant. Cette identité peut être générée aléatoirement avec un nombre entier, ou volée des nœuds voisins.

b) **Catégorie de participation** : Dans cette catégorie, il existe deux types de participation au réseau, participation simultanée et participation non simultanée. Dans la participation simultanée, l'attaquant essaye de faire en sorte que ses identités Sybil participent

toutes au réseau en même temps. Dans la participation non simultanée, l'attaquant tente de présenter un nombre énorme d'identités sur une période donnée, tout en n'agissant que pour un nombre plus restreint d'identités à un moment donné. Pour ce faire, il peut faire en sorte qu'une identité semble quitter le réseau et qu'une autre la remplace. Une autre possibilité est que l'attaquant dispose de plusieurs dispositifs physiques sur le réseau et qu'il fasse en sorte que ces dispositifs échangent leurs identités. Si le nombre d'identités utilisées par l'attaquant est égal au nombre de dispositifs physiques, chaque dispositif présente des identités différentes à des moments différents.

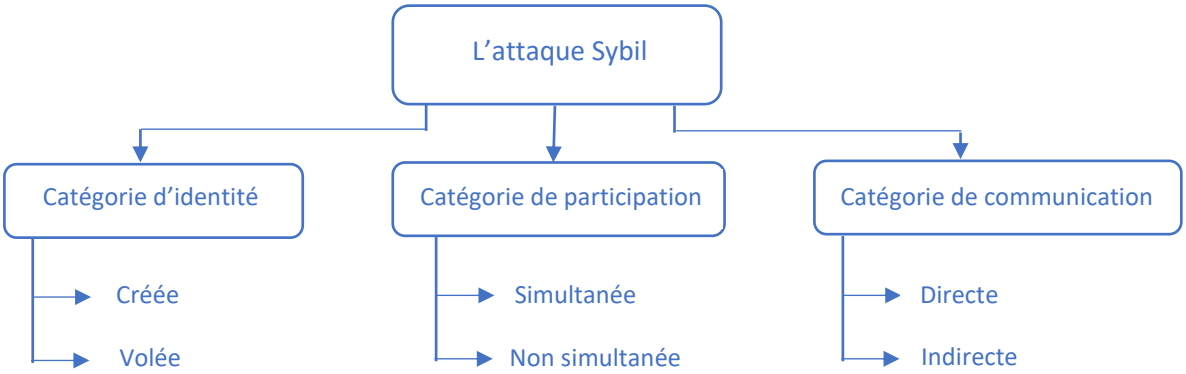

Figure II.1. Les différentes catégories d'attaques Sybil.

c) **Catégorie de communication :** L'un des moyens de réaliser l'attaque Sybil consiste à faire en sorte que les nœuds Sybil communiquent directement avec les nœuds légitimes. Lorsqu'un nœud légitime envoie un message radio à un nœud Sybil, l'un des dispositifs malveillants écoute le message. De même, les messages envoyés par les nœuds Sybil sont en fait envoyés par l'un des dispositifs malveillants. Cette manière de communication est considéré comme communication directe. Pour la communication indirecte, aucun nœud légitime ne peut communiquer directement avec les nœuds Sybil. Au lieu de cela, un ou plusieurs dispositifs malveillants prétendent être en mesure d'atteindre les nœuds Sybil. Les messages envoyés à un nœud Sybil sont acheminés via l'un de ces nœuds malveillants, qui prétend transmettre le message à un nœud Sybil.

II.2.2. L'impact de l'attaque Sybil sur les réseaux VFC

Comme nous avons vu dans le premier chapitre, chaque paradigmes des réseaux véhiculaires est caractérisé par ses types de communication. Par conséquent, l'attaque Sybil ne concerne pas uniquement la communication V2V mais aussi la communication V2R et V2I. Dans

le réseau VFC, l'attaquant peut viser les nœuds FN afin de partager les informations routières comme le montre la figure II.2.

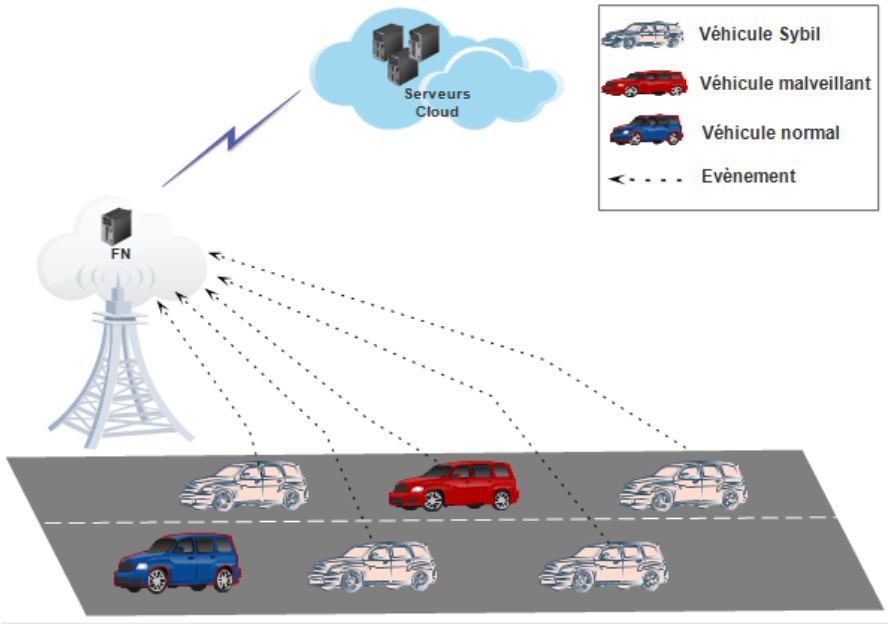

Figure II.2. Modèle d'attaque Sybil dans le réseau VFC.

Un véhicule malveillant peut lancer une attaque Sybil à des fins personnelles, par exemple un conducteur égoïste qui souhaite se déplacer rapidement sur une route sans être coincé dans un embouteillage lance l'attaque Sybil en donnant des fausses alertes au FN (accident, trafic routier, travaux, etc.) afin que les véhicules victimes soient contraints de modifier leurs trajectoires.

Le succès de l'attaque Sybil entraîne le succès d'autres types d'attaques telles que l'attaque DoS et DDoS. L'objectif de ces deux attaques est de rendre un service indisponible et d'empêcher les utilisateurs légitimes de l'utiliser. Avec l'attaque Sybil, il est possible de lancer une attaque DoS en envoyant des requêtes avec différentes identités et en laissant le FN effectuer des vérifications et des calculs, de sorte que le FN peut tomber en panne et devenir hors service. L'attaquant peut réussir l'attaque DoS et l'attaque DDoD dans les deux types de réseaux (VCC et VFC), mais dans le réseau VFC, il peut réussir avec un très petit nombre de requêtes envoyées et en un temps minimal par rapport à celles sur le VCC.

La réussite de l'attaque DoS peut avoir de graves répercussions sur le fonctionnement du réseau VFC. Le FN peut effectuer des analyses réduites sur les données reçues et les envoyer au serveur Cloud pour des analyses à l'échelle du réseau [36]. Par exemple, le serveur doit faire des

statistiques sur la disponibilité des parkings dans le réseau pour rediriger les véhicules, ou voir les routes les moins fréquentées par les véhicules pour définir le trajet d'une ambulance. L'attaque DoS et l'attaque DDoS peuvent avoir un impact sur la décision prise par le serveur Cloud après l'analyse et les statistiques si toutes les régions ne sont pas disponibles pour participer aux rapports envoyés au serveur, ce qui entraîne un dysfonctionnement du réseau.

II.2.3. Classification des méthodes de détection de l'attaque Sybil

De nombreux travaux ont été réalisés pour détecter l'attaque Sybil au sein des réseaux véhiculaires. En fait, les approches proposées peuvent être classées en quatre catégories [37] : les approches basées sur la cryptographie, les approches basées sur la localisation, les approches basées sur l'intensité du signal et les approches basées sur les algorithmes d'intelligence artificielle.

a) **Approches basées sur la cryptographie (CA) :** Pour un meilleur contrôle du réseau, les utilisateurs doivent s'authentifier avant de bénéficier des services du réseau. Zhou et al. [36] ont proposé un mécanisme de détection des nœuds Sybil basé sur les certificats. Un ensemble de pseudonymes à utiliser par les véhicules est obtenu auprès du département des véhicules à moteur (Department of Motor Vehicles ou DMV), qui représente l'autorité de certification. Les pseudonymes associés à chaque véhicule sont hachés à une valeur commune à l'aide d'une fonction de hachage. En calculant les valeurs de hachage des pseudonymes obtenus, une RSU décidera si les pseudonymes proviennent du même pool. Si une RSU suspecte une attaque Sybil, elle en informe le DMV, qui décide si les deux pseudonymes obtenus proviennent de la même voiture.

Dans [38], les auteurs ont utilisé un protocole d'authentification à clé publique pour effectuer la vérification du véhicule, qui est nécessaire pour que le véhicule puisse envoyer un message. Pour transmettre le message, l'expéditeur utilise la clé d'authentification et la méthode de cryptage. Le récepteur vérifie l'identité du membre en examinant sa signature.

Anwar et al. [39] proposent une approche de détection de l'attaque Sybil qui comprend un système d'authentification basé sur le Cloud. Ils disposent d'un algorithme de détection des nœuds malveillants, ainsi que des nœuds Sybil, qui utilise la cryptographie avec l'authentification HMAC et le positionnement en temps réel.

b) **Approches basées sur la localisation (LA) :** Pour cette approche, il existe deux méthodes de localisation. La première est basée sur les voisins du véhicule et la seconde sur la trajectoire du véhicule. Baza et al. [40] ont proposé un schéma de détection d'attaque Sybil pour les réseaux VANET utilisant la preuve de travail et de localisation. La trajectoire est formée par une série de preuves de localisation obtenues auprès des RSU. Les véhicules doivent exécuter l'algorithme de preuve de travail lorsqu'ils se déplacent vers une nouvelle RSU afin d'empêcher l'attaquant de créer plusieurs trajectoires simultanément et de contrer ainsi l'attaque DoS. Les trajectoires sont utilisées pour signaler des évènements. La solution permet d'obtenir un taux de détection élevé, mais elle entraîne des coûts de calcul importants.

Dans [41], les auteurs proposent un système d'authentification préservant la vie privée afin de détecter l'attaque Sybil pour l'internet des véhicules. La proposition identifie un véhicule avec sa trajectoire qui consiste en des étiquettes horodatées émises par les RSU rencontrées sur son chemin. Le véhicule doit résoudre une série d'énigmes informatiques générées par l'une des RSU voisines afin d'obtenir une trajectoire authentifiée et d'empêcher les véhicules malveillants de générer plusieurs trajectoires simultanément. En outre, et puisque le véhicule peut utiliser le service Cloud, il doit signer les résultats intermédiaires de l'énigme informatique à l'aide d'une signature agrégée séquentielle. La solution présente une grande similitude avec la solution mentionnée dans [40], sauf que cette proposition contre l'attaque Sybil ne prend pas en compte la limitation de la longueur de la trajectoire, même lorsque l'attaquant est autorisé à utiliser les services en Cloud.

Chang et al. [42] proposent une solution pour détecter l'attaque Sybil dans les zones urbaines. L'idée de leur algorithme est de positionner les véhicules en mouvement en formant une trajectoire. La position du véhicule est obtenue à partir de l'unité RSU qui délivre un message signé comme preuve de localisation à cet endroit et à ce moment-là. La solution présente certaines limites en termes de sécurité puisqu'elle suppose la RSU fiable pour créer les trajectoires, ce qui n'est pas toujours le cas.

Hamdan et al. [43] proposent une solution hybride pour contrer l'attaque Sybil dans les réseaux VANET. L'algorithme combine les méthodes d'empreinte et de détection d'abus de pseudonyme préservant la vie privée (P2DAP). L'idée de cette combinaison est d'appliquer la méthode de l'empreinte dans le cas de véhicules se déplaçant à grande vitesse et d'appliquer la

méthode P2DAP dans le cas d'un grand nombre de véhicules dans le réseau. Le taux de détection de l'algorithme hybride est plus élevé que celui de la méthode P2DAP et de la méthode de l'empreinte, mais il est limité au seuil de vitesse qui n'a pas encore été fixé.

c) **Approches basées sur l'intensité du signal (SSA) :** La technologie utilisée dans cette approche est l'indication de l'intensité du signal reçu (Received Signal Strength Indicator ou RSSI) qui mesure la puissance présente dans le signal radio reçu. Lorsque l'écart entre l'émetteur et le récepteur augmente, l'intensité du signal s'affaiblit et le débit de données ralentit, ce qui se traduit par une baisse du débit moyen. La technique basée sur RSSI a suscité l'intérêt de nombreux chercheurs en raison des avantages liés aux faibles coûts de calcul et à l'absence d'installation d'équipement. Garip et al. [44] ont proposé un mécanisme de localisation basé sur le RSSI pour détecter l'attaque Sybil dans les réseaux VANET. Dans cette méthode, les nœuds mobiles sont utilisés pour localiser un autre nœud mobile, qui se modifie ensuite en fonction des niveaux d'interruption hétérogènes de l'environnement.

Les auteurs de [45] proposent des modèles de contrôle de la puissance (Power Control Models ou PCM) potentiels pour effectuer des attaques Sybil dans les réseaux VANET, puis suggèrent un schéma de détection des attaques Sybil par identification du contrôle de la puissance qui détecte les anomalies dans les séries temporelles RSSI et utilise un classificateur SVM linéaire pour identifier les nœuds Sybil.

Li et al. [46] proposent un mécanisme basé sur les séries RSSI et de la matrice de conduite des véhicules pour détecter les nœuds Sybil. Pour détecter les nœuds Sybil, le mécanisme utilise une correspondance de distance dynamique pour déterminer l'écart entre la série RSSI et la matrice de conduite. La proposition a l'avantage de ne pas dépendre des réseaux VANET, des nœuds adjacents ou d'un matériel spécifique.

d) **Approches basées sur des algorithmes d'IA (AIAA) :** Dans cette approche, les chercheurs se sont basés sur des algorithmes d'intelligence artificielle (IA) tels que les k-voisins les plus proches (k-Nearest Neighbors ou k-NN) et l'algorithme d'apprentissage automatique. Gu et al. [47] ont utilisé l'approche k-NN pour identifier les attaques Sybil en comparant la ressemblance des modèles de conduite des véhicules bénins et en identifiant les différences entre les modèles de conduite des nœuds bénins et malveillants.

Dans [48], les auteurs ont proposé un mécanisme de détection de l'attaque Sybil à l'aide de la blockchain. Tout d'abord, le véhicule doit classer ses voisins comme normaux ou malveillants, puis les RSU vérifient et collaborent pour former un mécanisme de gestion de la confiance distribuée (Distributed Trust Management ou DTM) basé sur l'utilisation de la blockchain pour partager la liste de confiance des véhicules et identifier la classe de chaque véhicule traversant le réseau.

II.2.4. Discussion

Comme nous l'avons vu plus haut, il existe différentes méthodes pour traiter les attaques Sybil dans les réseaux véhiculaires, nous discutons de la possibilité d'adapter ces approches aux réseaux VFC.

Les approches basées sur la cryptographie peuvent être appliquées au réseau VFC pour détecter les attaques de Sybil sans aucun changement de performance si l'approche adoptée est une approche centralisée (l'authenticité de confiance est responsable de la vérification des pseudonymes). Cependant, de cette manière, nous ne pouvons pas mettre en évidence l'avantage de l'utilisation des FN dans le réseau. En fait, dans la littérature, les propositions de solutions d'authentification pour les réseaux VFC sont divisées en deux catégories, il y a des chercheurs qui ont gardé une authentification centralisée dans leurs protocoles de telle sorte que les FN ont un rôle de relais pendant la phase d'authentification (et ils offrent des services aux utilisateurs authentifiés). D'autres chercheurs ont donné un rôle aux FN afin qu'ils interviennent dans la phase d'authentification de manière décentralisée.

Les approches basées sur la localisation peuvent être appliquées au réseau VFC dans quelques cas. Dans les réseaux VFC, le FN peut intervenir pour vérifier la validité des listes de voisins par exemple (ou de la trajectoire dans le cas d'une localisation basée sur la trajectoire) avant de contacter le serveur en Cloud pour la suite du traitement. Le véhicule malveillant qui lance une attaque Sybil peut en profiter pour effectuer une attaque DoS et neutraliser facilement le FN. Lorsque les FN n'effectuent pas de gros volumes de traitement par rapport à leur capacité ou ne participent pas à l'audit, l'approche peut être appliquée avec succès.

De même, les deux autres approches, à savoir les approches basées sur l'intensité du signal et les approches basées sur les algorithmes d'IA, peuvent être appliquées avec succès si les FN n'interviennent pas dans le processus de vérification et de calcul.

Les trois approches (LA, SSA et AIAA) ont une limite commune qui est le coût du calcul. Cette limite est liée à la complexité des algorithmes considérés, en particulier les approches AIAA. Le FN peut effectuer les étapes de vérification et de calcul pour un nombre limité de véhicules ; l'augmentation du nombre de véhicules dans une telle zone peut facilement surcharger le FN.

Solution	Techniques utilisées	Avantages	Limites
[36]	- Fonction de hachage à sens unique	- Facile à mettre en œuvre. - Presque impossible de confondre entre un véhicule légitime et un véhicule Sybil.	- Faites entièrement confiance au serveurs
[38]	- HMAC - Clé d'authentification.	- Faible coût de calcul. - Facile à mettre en œuvre.	- La détection échoue si le nœud malveillant utilise l'identité d'un nœud victime dans le même groupe.
[39]	- Cryptographie symétrique - GPS - HMAC	- Des ressources informatiques et un espace de stockage intéressants	- Temps de réponse élevé.
[40]	- Partage du secret. - Signatures à seuil. - Preuve de travail.	- La compromission de la RSU est détectable. - Contrer l'attaque DoS.	- Coût de calcul élevé.
[41]	- Seuil de signature sans distributeur de confiance. - Code d'authentification du message. - Énigme informatique.	- La proposition contre l'attaque Sybil sans limitation de la longueur de la trajectoire	- Coût de calcul élevé.
[42]	- Signature de l'anneau liant.	- Haute précision	- Considérer les RSU comme des entités de confiance. - Coût de communication et de calcul élevés
[43]	- Algorithme de l'empreinte - Algorithme P2DAP	Détecter les nœuds Sybil même si les véhicules se déplacent à grande vitesse.	- Coût de calcul élevé.
[44]	- RSSI	- Il n'est pas nécessaire d'installer un matériel spécifique. - Faible coût de calcul.	Nécessité d'utiliser de nombreux véhicules voisins pour réussir à détecter l'attaque.

[45]	- RSSI - Méthode de classification par machine à vecteur de support.	- Identifier les nœuds Sybil avec des forces de transmission variables. - Détection des nœuds Sybil à l'aide de cinq modèles d'attaque.	- La solution n'est pas efficace si l'attaquant utilise plusieurs appareils depuis le même véhicule.
[46]	- Séquence RSSI. - Matrice de conduite	- La scalabilité. - Approche décentralisée.	- Les facteurs environnementaux peuvent influencer la précision des nœuds. - L'efficacité diminue si la vitesse du véhicule augmente
[47]	- Machine à vecteur de support (SVM)	-Haute précision de détection.	- La solution n'est pas efficace si la densité du trafic est faible.
[48]	- Blockchain. - Apprentissage automatique.	- Haute précision.	- Considérer les RSU comme des entités fiables. - Coût de calcul élevé.

Tableau II.1. Comparaison entre les travaux de détection de l'attaque Sybil dans les réseaux véhiculaires.

Le tableau II.1 présente une comparaison entre les travaux susmentionnés. Il existe une relation étroite entre les techniques utilisées, le temps de calcul et la précision de la détection. Un taux de précision élevé nécessite une combinaison de plusieurs techniques, ce qui implique une augmentation du temps de calcul. Afin de réduire le temps de calcul, de nombreux auteurs ont limité dans leurs propositions les scénarios d'attaquants qui peuvent exister. Ils ont donc proposé leurs solutions en se basant sur des hypothèses qui ne sont pas proches de la réalité, telles que la fiabilité des RSU et l'exclusion des cas d'attaquants dotés de grandes capacités. En effet, nous avons besoin d'une solution qui contre l'attaque Sybil dans plusieurs scénarios d'attaquants, qui prenne en compte des hypothèses qui existent dans la réalité et dont le coût de calcul soit minimal.

II.3. L’authentification dans les réseaux véhiculaires

L'authentification est l'un des principaux problèmes de sécurité des réseaux véhiculaires en général et aux réseaux VFC en particulier, car une authentification faible peut conduire à plusieurs attaques, telles que l'attaque DoS, l’attaque DDoS, l'attaque par rejeu, l'attaque de l'homme du milieu (man-in-the middle ou MITM) [49].

II.3.1. Classification des mécanismes d'authentification et de la protection de la vie privée

L'authentification et la protection de la vie privée sont deux aspects principaux de la sécurité qui sont nécessaires à l'établissement de la confiance entre les véhicules dans un réseau véhiculaire. L'utilisation de systèmes d'authentification appropriés garantit la sécurité d'un réseau véhiculaire et facilite l'identification des nœuds non légitimes et des faux messages.

De nombreux chercheurs ont proposé des systèmes d'authentification pour répondre aux attaques courantes contre les réseaux véhiculaires et garantir la sécurité des communications. Dans cette section, nous catégorisons les systèmes d'authentification dans les réseaux véhiculaires. Les types de systèmes d'authentification peuvent être classés en sept catégories : les systèmes d'authentification basés sur la cryptographie symétrique (SCB), les systèmes d'authentification basés sur l'infrastructure à clé publique (PKIB), les systèmes d'authentification basés sur les signatures de groupe (GSB), les systèmes d'authentification basés sur les signatures sans certificats (CB), les systèmes d'authentification basés sur les pseudonymes (PB), les systèmes d'authentification basés sur l'identité (IDB), et les systèmes d'authentification basés sur la blockchain (BB) [50].

a) Les systèmes d'authentification basés sur la cryptographie symétrique (SCB)

Cette catégorie dépend des schémas de cryptographie à clé symétrique dans lesquels une clé symétrique est principalement utilisée pour assurer la sécurité dans les réseaux véhiculaires. L'expéditeur et le destinataire peuvent calculer efficacement la clé symétrique et l'utiliser pour assurer la confidentialité des communications. En outre, le code d'authentification des messages (MAC) est également utilisé pour authentifier les messages dans ces systèmes. Pour chaque message, l'expéditeur produit un MAC à l'aide de la clé secrète partagée. Un membre du réseau possédant la même clé peut vérifier le MAC reçu avec le message. Ces systèmes sont utilisés dans les réseaux véhiculaires car ils ont des coûts de calcul et de communication moindres et la vérification peut être effectuée rapidement.

Dans [51], deux techniques, à savoir la double authentification et la gestion des clés, ont été proposées pour assurer la transmission sécurisée des données dans les réseaux VANET. Dans le cas de la première technique, les membres fournissent leurs informations essentielles telles que

leur identité, leur adresse électronique et leur adresse à la TA lors de l'enregistrement hors ligne. Le véhicule est authentifié à l'aide de l'empreinte digitale stockée dans la carte à puce. Ensuite, l'authentification de la TA est effectuée et le code d'authentification est également généré. Dans la seconde technique, La TA produit deux clés doubles différentes pour deux groupes distincts opérant dans le réseau. Lors de la phase initiale de configuration, La TA choisit les valeurs de la clé de groupe et de la clé secrète d'un groupe multiplicatif. Ensuite, les membres du groupe s'inscrivent auprès de la TA et reçoivent les clés de groupe. Les véhicules peuvent alors communiquer en toute sécurité avec d'autres véhicules et avec la TA. De même, lorsqu'un utilisateur principal rejoint ou quitte le réseau, la clé de groupe correspondante est mise à jour et communiquée à tous les membres du groupe. Toutefois, ce système ne fournit pas d'informations sur le taux de perte de paquets et le délai de bout en bout dans les réseaux VANET.

Dans [52], des techniques d'authentification et de distribution de clés préservant la vie privée ont été proposées. Dans la première approche, un protocole d'authentification anonyme a été proposé pour préserver la vie privée et assurer l'intégrité des messages diffusés. L'expéditeur produit un certificat anonyme temporaire et transmet une signature avec le message. Par la suite, le récepteur peut authentifier la source et le message en vérifiant le certificat et la signature. Dans la seconde approche, un processus sécurisé de distribution de clés est mis en œuvre, dans lequel chaque membre du réseau reçoit une clé de groupe anonyme. Même si une RSU est impliquée dans une activité malveillante, la TA peut déterminer son identité réelle. Ce système permet le suivi conditionnel, la non-répudiation et la résistance aux attaques de l'homme du milieu (MITM). Toutefois, il n'offre pas de résistance aux attaques par rejeu et par usurpation d'identité.

Dans [53], un système d'authentification anonyme, efficace, et basé sur l'appariement bilinéaire a été proposé et nommé EABA. Il utilise un code d'authentification de message basé sur le hachage (HMAC) et un schéma basé sur le groupe pour éliminer l'exigence de mémoire des listes de révocation de certificats (CRL) et l'énorme surcharge de communication. Il garantit que seuls les véhicules autorisés entrent dans le groupe et qu'il n'est pas nécessaire de consacrer du temps au processus de vérification des listes de révocation de certificats. Il utilise également des pseudonymes et des signatures basées sur l'identité pour garantir la préservation conditionnelle de la vie privée et la vérification des messages par lots, respectivement. Le principal avantage de HMAC est qu'il augmente les performances du réseau en supprimant le besoin de CRL. Cependant,

le délai de transmission de l'EABA est élevé et la perte de paquets augmente également avec la vitesse.

b) Les systèmes d'authentification basés sur l'infrastructure à clé publique (PKIB)

Cette catégorie dépend des systèmes basés sur la cryptographie à clé publique dans lesquels la TA contrôle la composition des paires de clés publique-privée et leur distribution aux membres valides à des fins de communication. Cette infrastructure contient la clé publique du véhicule et la signature numérique de l'autorité de certification pour l'authentification. Ces systèmes sont utilisés pour déployer une méthode robuste et sûre pour l'authentification des véhicules dans le respect de la vie privée. La traçabilité est assurée par des certificats délivrés par l'autorité de certification.

Dans [54], un protocole d'authentification de messages anonymes utilisant l'identité locale (LIAP) a été proposé. Un véhicule demande une clé maîtresse locale à une RSU enregistrée dans son rayon d'action au cours de la phase de récupération de la clé maîtresse. Après avoir obtenu la clé, un véhicule génère son identité anonyme pour produire une signature sur le message. Par la suite, l'identité réelle du véhicule malveillant peut être retrouvée et le véhicule correspondant peut-être révoquer du réseau. Ce système assure l'authentification et l'intégrité des messages, la non-répudiation et la préservation conditionnelle de la vie privée. Il résiste également aux attaques de collusion et aux attaques par rejeu. Toutefois, la distribution des certificats, la gestion des CRL et la révocation des membres augmentent les coûts de calcul et de communication.

De même, un schéma de révocation efficace basé sur le Fog computing a été proposé dans [55], qui utilise l'arbre de hachage de Merkle au lieu de la CRL. L'arbre de Merkle élimine le temps nécessaire à la vérification de la CRL. Les routes sont divisées en différentes régions, dans lesquelles des nœuds Fog supervisent tous les véhicules localement et font office de passerelle de confiance. Le nœud Fog est chargé de délivrer des certificats à tous les véhicules se trouvant dans son rayon d'action et transmet la demande de délivrance de certificat du véhicule à l'autorité de certification. Le nœud Fog met à jour le véhicule lorsqu'il reçoit le certificat. L'autorité de certification construit l'arbre de Merkle pour conserver l'enregistrement de la révocation des certificats, et les certificats révoqués sont conservés dans les nœuds feuilles. Par la suite, le nœud Fog diffuse l'arbre aux véhicules pendant leur fonctionnement. Toutefois, il est difficile de conserver une copie fraîche de l'arbre à chaque nœud.

c) Les systèmes d'authentification basés sur l'identité (IDB)

Cette catégorie dépend des systèmes de cryptographie basés sur l'identité. Dans ce cas, les informations nécessaires au véhicule (par exemple, le numéro de téléphone, l'adresse électronique) sont utilisées pour générer sa clé publique. Il n'est donc plus nécessaire de gérer et de distribuer des certificats.

Sutrala et al. [56] proposent un mécanisme d'authentification conditionnelle préservant la vie privée dans l'environnement IoV à l'aide de la cryptographie à courbe elliptique (ECC). La proposition permet l'authentification de deux types de communications, V2V et V2I. Plus précisément, un véhicule peut authentifier ses voisins et la RSU peut également authentifier les véhicules dans sa zone de couverture sur la base d'une vérification par lots. Le système proposé offre une meilleure sécurité contre les attaques actives et passives, mais il considère les RSU comme des entités de confiance, ce qui n'est pas proche de la réalité.

Dans [57], les auteurs présentent un protocole d'authentification mutuelle basé sur le Cloud dans le réseau IoV. La proposition est basée sur une architecture technologique d'identification par radiofréquence (RFID) avec une préservation efficace de la vie privée. Les auteurs ont utilisé l'exponentiation modulaire pour crypter les informations dans la communication. Ils ont réussi à empêcher le suivi malveillant par des attaquants externes, mais la solution reste limitée aux faiblesses du Cloud.

FBIA est un nouveau système d'authentification pour les réseaux véhiculaires basés sur le Fog, proposé par Song et al. [58]. La proposition se compose de deux couches : la couche d'authentification de sécurité pour les véhicules en dehors du Fog et la couche de contrôle de sécurité pour le reste des véhicules. Les auteurs ont réussi à prouver la précision de l'authentification et l'adaptabilité à un environnement de réseau mobile à grande vitesse dans l'IoV.

Zhong et al. [59] présentent un système d'authentification conditionnel préservant la vie privée pour les réseaux véhiculaires basés sur le Fog. La solution permet aux véhicules de générer leurs clés privées, leurs clés publiques et leurs pseudonymes. Les clés privées ne sont connues que du véhicule, ce qui permet au système de résister au problème du dépôt de clés. La proposition présente certaines limites, notamment le problème du traitement centralisé par la TA et la traçabilité des nœuds Fog compromis.

Dans [60], un système d'authentification sûr et préservant la vie privée a été proposé pour le réseau VANET basé sur le Fog. Les auteurs utilisent le filtre de quotient (Quotient Filter ou QF) pour l'authentification des nœuds, tandis que l'authentification des messages est basée sur l'ECC. La proposition se caractérise par une latence réduite et une meilleure sécurité.

d) Les systèmes basés sur les signatures sans certificats (CB)

Cette catégorie dépend des systèmes basés sur la signature sans certificat, dans lesquels la nécessité de certificats est supprimée. Ces systèmes éliminent le problème de la gestion des CRL dans les systèmes traditionnels basés sur la PKI. En outre, ces systèmes ne nécessitent pas la distribution de certificats aux véhicules ni leur révocation par le réseau.

Un système de signature basé sur la courbe elliptique sans appariement bilinéaire a été proposé dans [61]. Dans ce schéma, un centre de génération de clés (Key Generation Center ou KGC) fournit une clé privée partielle à un véhicule généré à l'aide de son identité réelle. Ensuite, le véhicule choisit au hasard une valeur secrète et produit sa clé privée complète à l'aide des paramètres publics, de la clé privée partielle et de la valeur secrète. De même, le véhicule génère sa clé publique à l'aide des paramètres publics et de la valeur secrète. Un véhicule signe le message à l'aide de la clé privée et le récepteur vérifie la paire message-signature à l'aide de la clé publique. Toutefois, l'analyse comparative et les coûts de communication et de calcul du système proposé ne sont pas fournis.

Dans [62], un système de signature courte sans certificat et basé sur l'appariement bilinéaire a été proposé. Il prend en charge les dispositifs à faible largeur de bande et à faible capacité de stockage. En outre, les coûts de génération et de vérification de la signature sont moindres. En outre, ce système n'utilise pas l'opération de hachage MapToPoint et la longueur de la signature n'est que d'un seul élément de groupe. En outre, il est sûr contre les super adversaires de type I et II dans le cadre de l'algorithme ROM (Random Oracle Model).

e) Les systèmes basés sur les pseudonymes (PB)

Cette catégorie dépend de systèmes basés sur des pseudonymes. Tout d'abord, le véhicule envoie son identité réelle et les informations connexes à la TA par l'intermédiaire de la RSU en utilisant le canal sécurisé. Après avoir vérifié les détails, la TA transmet la pseudo-identité et sa validité au véhicule correspondant. La pseudo-identité est utilisée pour réaliser l'authentification

et l'anonymat complet pendant la communication entre véhicules. Deux pseudonymes du même véhicule ne peuvent pas être liés l'un à l'autre pour obtenir l'identité réelle ou pour découvrir le véhicule exact, ce qui contribue à garantir l'impossibilité d'établir un lien. En outre, la TA peut révéler l'identité réelle du véhicule à l'aide du pseudonyme si celui-ci est impliqué dans une activité malveillante.

Dans [63], un système d'authentification basé sur les pseudonymes (PASS) a été proposé pour préserver la vie privée dans les réseaux VANET. Il assure une grande confidentialité car les attaquants ne peuvent pas déterminer l'identité réelle du véhicule. Après avoir vérifié l'identité réelle, la TA fournit les ensembles de clés secrètes, les certificats pseudonymes et les certificats de signature au véhicule. Ensuite, la TA enregistre le lien entre un véhicule et ses pseudo-identités. La TA conserve les informations sur les véhicules révoqués dans les CRL. En outre, lorsque la TA supprime une RSU R_j, elle ajoute le certificat de R_j à la CRL. Au même temps, les certificats émis par R_j sont automatiquement révoqués du réseau. Ce système assure l'authentification, la révocation de l'identité, la préservation conditionnelle de la vie privée et la non-répudiation. Cependant, il souffre d'une lourde charge de gestion des CRL.

Un système d'authentification préservant la vie privée conditionnellement basé sur l'identité pour les réseaux VANET (CPAV) a été proposé dans [64]. Il résout les problèmes de l'opération d'appariement bilinéaire qui est une opération cryptographique qui prend du temps. Il utilise une fonction de hachage résistante aux collisions et l'ECC pour augmenter les performances et l'efficacité du réseau. En outre, ce système offre une sécurité contre les attaques par signature choisie adaptative et par message choisi dans le cadre du modèle ROM. L'avantage de ce système est que la vérification des messages par lots prend moins de temps, même si le nombre de messages augmente. La taille du message et de la signature n'a pas d'incidence sur les coûts de transmission. Toutefois, cela n'explique pas le taux de vérification des messages.

f) Les systèmes basés sur la signature de groupe (GSB)

Cette catégorie dépend de la signature des membres d'un groupe. Normalement, le groupe se compose d'un responsable et de membres. Chaque membre du groupe dispose d'une clé publique et d'une clé privée individuelle. Les algorithmes de signature de groupe se composent de quatre algorithmes principaux : KeyGen, Sign, Verify et Find. L'algorithme KeyGen génère une paire de clés publique-privée, l'algorithme Sign produit une signature sur le message, l'algorithme Verify

vérifie la paire message-signature et l'algorithme Find révèle le véhicule malveillant. Un adversaire ne peut pas relier deux signatures produites par le même véhicule en utilisant son identité réelle, ce qui garantit l'impossibilité de les relier. Lors de la vérification, seule la clé publique est utilisée, ce qui permet de garantir l'évolutivité. Aucun membre ne peut produire une signature au nom d'un autre membre du groupe.

Shao et al. [65] ont proposé un schéma d'authentification anonyme à seuil utilisant un modèle de groupe décentralisé pour minimiser les couts en termes de chargement et de vérification des CRL. Dans ce schéma, les RSU peuvent tracer la position du véhicule. Il utilise la cryptographie basée sur l'appariement bilinéaire pendant le processus de diffusion. Néanmoins, il présente certaines limites, telles que l'absence de sécurité de transmission et d'inversion, de contrôle des collisions et d'impossibilité d'établir des liens. En outre, il est également vulnérable aux attaques par rejeu.

Wang et al. [66] ont étudié un schéma d'authentification efficace basé sur la préservation conditionnelle de la vie privée afin de fournir le processus de vérification par lots pour les communications V2V et V2I. Ils ont donc proposé un schéma d'authentification efficace à préservation conditionnelle de la vie privée (ECPB) basé sur la signature de groupe pour améliorer l'efficacité de la procédure d'authentification dans les réseaux VANET. Toutefois, le délai de la réponse moyenne lors de la vérification devrait être réduit davantage.

g) Les systèmes d'authentification basés sur la blockchain (BB)

Cette catégorie dépend des cadres d'authentification et de révocation d'identité basés sur la blockchain. L'autorité de certification (Certification Authority ou CA) attribue un pseudo-identité ou un certificat aux véhicules qui sont stockés dans la blockchain. En outre, les informations sur le pointeur d'entrée sont fournies au destinataire pour vérification. Les avantages les plus significatifs de l'utilisation de la blockchain sont la décentralisation et la transparence [67]. Les informations ajoutées à la blockchain sont immuables, c'est-à-dire qu'une fois qu'elles sont enregistrées dans la blockchain, personne ne peut les modifier. En outre, la CA ne souffre pas d'une charge de gestion et de distribution des CRL

Yao et al. [68] ont proposé un mécanisme d'authentification anonyme léger pour les services de Fog véhiculaire distribués basé sur BC et nommé BLA. Leur contribution vise

l'authentification entre les centres de données à l'aide de l'ECC. La proposition réduit considérablement le temps d'authentification mais ne prend pas en charge l'authentification mutuelle entre le véhicule et le gestionnaire de service (SM).

Kaur et al. [69] présentent un système efficace d'authentification des centres de données et d'échange de clés utilisant la blockchain et l'ECC. La proposition a permis de contrer diverses attaques et de réduire considérablement le temps de communication.

EASBF est un mécanisme d'authentification basé sur le Fog pour les réseaux IoV proposé par Merzougui et al. [70]. Les auteurs ont utilisé l'ECC pour authentifier les véhicules et la BC pour stocker les informations d'authentification des véhicules. La proposition a permis d'améliorer la sécurité en contrant diverses attaques.

II.3.2. Discussion

Un mécanisme d'authentification tente de garantir l'exactitude d'un message en authentifiant sa source, et de préserver la vie privée d'un véhicule. Chaque mécanisme cryptographique utilisé présente des avantages et des inconvénients. Le déploiement d'un mécanisme particulier dépend des exigences spécifiques des autorités et des membres du réseau.

Les systèmes basés sur la cryptographie à clé symétrique ont moins de coûts de communication et de calcul. Toutefois, l'utilisation de MAC ou d'une clé identique lors de la génération et de la vérification de la signature peut facilement permettre à l'attaquant de porter atteinte à la sécurité et à la vie privée.

Dans les systèmes basés sur l'infrastructure à clé publique, chaque membre possède une paire de clés publique-privée et un certificat. L'autorité de certification reçoit les demandes d'émission de certificats des RSU et des véhicules, et n'émet le certificat qu'après avoir vérifié les détails correspondants. Contrairement aux systèmes basés sur la cryptographie à clé symétrique, deux clés différentes sont utilisées du côté de l'émetteur et du récepteur, c'est-à-dire qu'une clé privée est utilisée lors de la génération de la signature et une clé publique lors de la vérification. En outre, la sécurité du réseau peut être améliorée en même temps que les performances. Toutefois, le problème de la distribution et de la révocation des certificats affecte la propriété d'évolutivité. De plus, la vérification et la gestion des CRL augmentent le coût de communication du réseau.

Dans les systèmes de cryptographie basés sur l'identité, les informations personnelles de chaque membre sont utilisées lors de la génération de la clé publique. Le principal avantage de ces systèmes est qu'ils éliminent la charge de gestion et de distribution des certificats. Le KGC ou la TA gère le processus de génération et de distribution des clés et surveille l'ensemble du réseau. Dans ces systèmes, la TA aide les membres du réseau à assurer l'anonymat de la source, la non-répudiation et l'authentification des messages. Il peut également révéler l'identité du véhicule malveillant à l'aide de la clé publique et des informations. Dans ces systèmes, l'attaquant peut obtenir l'identité réelle de l'expéditeur en analysant la clé publique et les paires message-signature.

Dans les systèmes de signature sans certificat, l'expéditeur ne transmet aucun type de certificat avec le message. D'autres mécanismes cryptographiques sont utilisés lors de la génération ou de la vérification des signatures à la place des certificats. Cependant, le coût de calcul augmente considérablement en raison de l'agrégation et du stockage des signatures. De même, la pseudo-identité est utilisée dans les systèmes basés sur les pseudonymes pour l'authentification de la source. L'attaquant ne peut pas obtenir les informations privées de l'expéditeur par l'analyse de la pseudo-identité. Toutefois, le véhicule doit stocker à l'avance plusieurs pseudo-identités dans la TA. En plus, la TA doit maintenir la base de données du lien entre la pseudo-identité et l'identité réelle de chaque membre afin d'identifier les véhicules malveillants en cas de besoin.

Dans les systèmes basés sur les pseudonymes, une pseudo-identité pour chaque membre du réseau est utilisée à la place de l'identité réelle. Le PID est obtenu auprès de la TA en fournissant l'identité originale et la clé publique. Il est également utilisé lors de la génération de la signature du message. Un véhicule transmet le PID avec la signature du message lors de la communication avec les véhicules adjacents. Un récepteur peut vérifier le PID pour réaliser l'authentification de la source avec l'aide de la TA. Le principal avantage de ces systèmes est que l'adversaire ne peut pas extraire l'identité réelle de l'expéditeur à partir de l'analyse de son PID ou de la paire message-signature. Un véhicule peut assurer l'anonymat complet, l'authentification de la source, la non-liaison et la non-répudiation dans le réseau. Toutefois, la gestion et la recherche d'une solution à l'attaque Sybil sont complexes.

Dans les systèmes basés sur les signatures de groupe, les véhicules forment un groupe et produisent leur paire de clés publique-privée pour la communication. L'expéditeur signe le message à l'aide de clés privées et publiques, et le récepteur vérifie la signature à l'aide des clés

publiques de chacun. Le principal problème de ces systèmes est que la vérification de la signature de groupe est généralement une opération qui prend du temps, ce qui les rend inadaptés aux dispositifs à durée limitée des réseaux véhiculaires.

Dans les systèmes d'authentification basés sur la blockchain, la transparence et l'immutabilité sont garanties à chaque membre du réseau. Tout membre du réseau peut vérifier les opérations effectuées par l'autorité de confiance. Le principal avantage du déploiement de la blockchain est qu'aucun membre ne peut modifier ou supprimer les informations enregistrées dans la blockchain. De plus, les systèmes d'authentification basés sur la blockchain sont décentralisés, ce qui signifie qu'ils ne dépendent pas d'une autorité centrale unique pour vérifier l'identité. Cela permet d'éliminer les points de défaillance uniques et les vulnérabilités potentielles associées à une autorité centrale. Les méthodes actuelles basées sur la blockchain sont limitées, car il faut faire confiance à certaines entités pour mettre à jour la blockchain.

Le tableau II.2 récapitule les principaux avantages et limites de chaque catégorie d'authentification étudiée.

Catégorie	Avantages	Limites
SCB	- Faible coût de calcul et de communication	- Facilité des compromission des clés
PKIB	- Utilisation des clés publique et privée	- Dépendance à l'autorité de certification - Gestion des CRL coûteuse
GSB	- Anonymat des membres du groupe	- Taille du groupe limité - Temps de vérification de signature élevé
CB	- Protection de la vie privée (anonymat)	- Coût de calcul élevé - Gestion des pseudo-identité complexe (par la TA)
PB	- Protection de la vie privée (anonymat et la non-liaison)	- Gestion centralisée
IDB	- Protection de la vie privée (anonymat et la non-liaison)	- Control des pseudonymes complexe (risque de l'attaque Sybil)
BB	- Décentralisation - Traçabilité et transparence - l'immutabilité	- Confidentialité des données sensibles

Tableau II.2. Comparaison entre les catégories d'authentification existantes dans les réseaux véhiculaires.

II.4. Conclusion

Le réseau VFC est un nouveau domaine de recherche qui est apparu après certaines limitations des réseaux véhiculaires traditionnels. Pour prouver son efficacité, il doit assurer des services de sécurité à ses utilisateurs et préserver leur vie privée. Dans ce chapitre, nous avons abordé deux aspects reliés à la sécurité, et qui sont l'attaque Sybil et l'authentification. Nous avons décrit l'attaque Sybil et son impact sur les réseaux VFC. Le succès de l'attaque Sybil est considéré comme plus dangereux que dans les réseaux traditionnels, ce qui s'explique par la capacité limitée des nœuds Fog. Elle peut provoquer un dysfonctionnement du réseau plus rapidement et avec moins d'efforts de la part de l'attaquant. Les méthodes existantes de détection des attaques Sybil dans les réseaux véhiculaires peuvent être appliquées avec succès dans les réseaux VFC si le FN n'est pas impliqué dans la vérification et le calcul de l'algorithme de détection. Nous avons aussi étudié différents schémas d'authentification et de préservation de la vie privée, ainsi que les techniques de pointe utilisées dans les réseaux véhiculaires. Nous constatons qu'un mécanisme cryptographique unique ne peut pas répondre à tous les besoins de sécurité et qu'il est nécessaire d'élaborer un ensemble de techniques. Les principales limites des mécanismes cryptographiques actuels et l'objet des études en cours sont l'efficacité du calcul et de la communication, l'absence d'entités centralisées, les besoins importants en mémoire pour les certificats et les listes de révocation correspondantes, et la possibilité de non-répudiation en rendant la protection de la vie privée conditionnelle. En outre, la robustesse face à diverses attaques et le respect de toutes les exigences de sécurité font également l'objet d'études. Ces observations ont conduit à la proposition de deux contributions distinctes. La première contribution se concentre sur la détection de l'attaque Sybil, tandis que la deuxième se focalise sur l'authentification. Les détails de ces contributions seront présentés en profondeur dans les deux chapitres suivants.

Chapitre III : Première contribution : Détection de l'attaque Sybil dans les réseaux VFC

III.1. Introduction

Le réseau VFC est encore en phase d'évolution, ce qui implique qu'il est primordial de prêter attention aux défis de sécurité, car une simple défaillance de la sécurité peut entraîner des dommages économiques et humains au sein du réseau. Comme tout nouveau réseau, le VFC est vulnérable à une variété d'attaques qui compromettent les critères de sécurité du réseau tels que la non-répudiation, la confidentialité, l'intégrité et la disponibilité des services. Parmi les attaques classées comme les plus dangereuses, l'attaque Sybil. Dans ce chapitre, nous présentons notre première contribution [71] qui permet la détection de l'attaque Sybil dans le réseau VFC. Notre solution a pu contrer l'attaque Sybil dans plusieurs scénarios d'attaquant avec un taux de détection élevé.

III.2. Motivation

Comme nous avons vu dans notre état de l'art, de nombreux travaux ont été proposés pour contrer l'attaque Sybil au sein des réseaux véhiculaires, en s'appuyant sur différentes méthodologies telles que la cryptographie, l'indicateur de puissance du signal reçu (RSSI) et l'analyse du comportement du véhicule. La détection par cryptographie se caractérise par une grande précision car les solutions sont entièrement centralisées, mais cette centralisation facilite la tâche de l'attaquant en ciblant une seule entité pour provoquer des dysfonctionnements dans le réseau. Le RSSI a intéressé de nombreux chercheurs en raison de sa simplicité et du fait qu'il ne nécessite pas l'installation d'un matériel spécifique. L'attaque Sybil est détectée à l'aide de RSSI en évaluant la distance de l'émetteur du signal et en analysant la cohérence de la position autodéclarée du véhicule. Bien que cette stratégie soit facile à appliquer, elle reste inefficace car l'attaquant peut modifier la puissance du signal. D'autres chercheurs se sont concentrés sur la similarité des trajectoires des véhicules pour détecter l'attaque Sybil. Lorsqu'un véhicule construit sa trajectoire, il doit demander une preuve de position à chaque RSU rencontrée sur son chemin. Cette approche permet de détecter les nœuds Sybil avec une grande précision, mais avec l'évolution de la capacité des OBU, un attaquant peut générer plusieurs trajectoires en parallèle. Les travaux [40] et [41] peuvent empêcher les OBU malveillants de générer plusieurs trajectoires en parallèle, mais cela augmente le coût de calcul des OBU, ce qui nuit à leur utilisation d'autres applications dans le réseau véhiculaire.

Dans ce qui suit, nous allons présenter notre première contribution qui consiste en un mécanisme de détection de l'attaque Sybil dans le réseau VFC. Notre mécanisme de détection utilise le RSSI, la trajectoire d'un véhicule et la technologie blockchain. Notre solution assure un taux élevé de détection des nœuds Sybil avec un coût minimal par rapport aux travaux existants.

III.3. Contexte

III.3.1. Cryptographie sur les courbes elliptiques

La cryptographie sur les courbes elliptiques (ECC) est un groupe de méthodes cryptographiques qui utilisent une ou plusieurs caractéristiques des courbes elliptiques. En 1985, Koblitz [72] et Miller [73] ont tous les deux proposé séparément l'utilisation des courbes elliptiques en cryptographie. Ces qualités peuvent être utilisées pour créer des primitives cryptographiques afin d'améliorer des primitives cryptographiques existantes, par exemple en réduisant la taille des clés cryptographiques.

Dans le domaine de la sécurité des réseaux sans fil, l'ECC est devenue la meilleure alternative pour garantir des services de sécurité tels que l'intégrité et l'authentification avec une efficacité notable. En effet, l'ECC utilise des clés plus petites que les approches traditionnelles à clé publique. Cela permet une génération rapide des clés, un accord rapide sur les clés et des signatures rapides [74]. Pour produire une courbe elliptique qui est un ensemble de points, l'équation mathématique suivante est utilisée :

$$y^2 = x^3 + Ax + B \qquad (III.1)$$

Où le discriminant (Δ = -($4A^3$ + $27B^2$)) de (1) est différent de 0. Notez que cette courbe inclut le point O à l'infini. La cryptographie à clé publique est basée sur l'insolubilité de certains problèmes mathématiques. Le problème du logarithme discret de la courbe elliptique (ECDLP) est donné par le problème suivant. Soit deux points arbitraires et précis Q et P, le calcul scalaire : $Q = xP$ signifie que le point de la courbe elliptique P est ajouté à lui-même x fois. L'ECDLP consiste à trouver le plus petit nombre naturel x satisfaisant $Q = xP$.

L'avantage pour un adversaire de calculer x en temps polynomial (t) est le suivant : $Adv^{ECDLP}(t)$ = [$(Q, P) = x$]. L'hypothèse ECDLP conclut que $Adv^{ECDLP}(t) \leq \epsilon$ [75].

III.3.2. La blockchain

La BC est un grand livre distribué proposé par Satoshi Nakamoto dans le contexte financier [76]. Elle est sous forme d'une chaine qui permet à plusieurs nœuds du réseau de conserver les mêmes informations sans avoir besoin d'une autorité de confiance centrale. Les participants de la BC sont appelés nœuds. La BC fournit un réseau décentralisé dans lequel tous les nœuds du réseau participent activement à la validation et à la vérification des données. Les données qui seront stockées dans la BC seront cryptées à l'aide de la cryptographie. Chaque bloc contient un hachage crypté, un horodatage et un hachage du bloc précédent de la chaîne par lequel le bloc sera connecté [77], comme le montre la figure III.1.

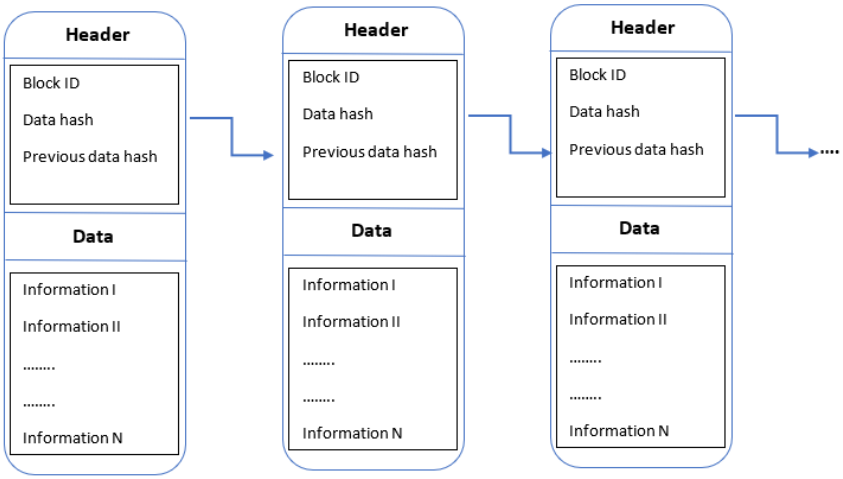

Figure III.1. Architecture d'une blockchain.

Les nœuds du réseau doivent être en mesure d'accepter ou de rejeter l'ajout d'un nouveau bloc sans provoquer de conflit ; cette phase est réalisée par le processus consensus. Il existe de nombreux algorithmes de consensus tels que : Proof of Work (PoW), Proof of Stake (PoS), Casper, et Practical Byzantine Fault Tolerance (PBFT). Chaque algorithme de consensus présente ses propres avantages et inconvénients, ainsi que la capacité de s'adapter à diverses conditions [78].

La BC a connu un énorme succès en tant que technologie émergente de pair à pair (Peer to Peer ou P2P) au cours des dernières années en raison de ses avantages. Par conséquent, elle a été appliquée dans presque tous les domaines de l'IoT dans ces différents contextes (tels que le secteur de l'énergie, l'industrie, les soins de santé et la sécurité) [79]. Le terme "sécurité" englobe divers services tels que l'autorisation, l'authentification, la protection de la vie privée, et la résilience face

à différentes attaques. L'utilisation de la BC comme ressource de stockage garantit la transparence, l'immutabilité, la traçabilité et la non-répudiation, ce qui répond efficacement aux exigences de sécurité des réseaux véhiculaires. L'application de la BC dans le domaine de la sécurité a permis non seulement de garantir une meilleure sécurité, mais aussi d'améliorer les performances des systèmes en réduisant le temps de traitement [80].

Trois types de systèmes de blockchain sont actuellement utilisés : la blockchain publique, la blockchain privée et la blockchain de consortium. La différence entre ces trois types se résume au degré d'ouverture disponible pour la participation des nœuds [78]. Le tableau III.1 résume la différence entre ces trois types.

- **Blockchain publique :** La blockchain publique (ou blockchain sans permission) est une blockchain entièrement décentralisée. Elle permet à ses participants de consulter toutes les données du grand livre, d'exécuter des transactions avec d'autres nœuds de la chaîne et de participer au processus de consensus.

- **Blockchain privée :** La blockchain privée (ou blockchain de permission) n'est pas ouverte au monde extérieur. Les autorisations de lecture et d'écriture des données sur la blockchain privée et les droits de comptabilisation des blocs sont attribués selon les règles de l'organisation.

- **Blockchain de consortium :** La blockchain de consortium est une combinaison des deux autres architectures de blockchain (publique et privée) afin de bénéficier des avantages des deux. Il s'agit d'une blockchain basée sur des autorisations, dans laquelle la participation est limitée à un consortium de membres.

Propriété	BC publique	BC privée	BC de consortium
Infrastructure	Décentralisée	Distribuée	Semi décentralisée
Validation	Mineurs	Un ensemble des nœuds autorisés	Un ensemble des nœuds autorisés
Performance	Faible	Haute	Moyenne
Scalabilité	Haute	Faible	Moyenne
Exemples de consensus	PoW, PoS	PBFT, PAXOS	PBFT, SCP, PoET

Tableau III.1. La différence entre les types de blockchain.

Dans notre mécanisme, nous avons considéré une blockchain de consortium, car elle est semi-décentralisée, seule une petite partie des nœuds étant autorisée à exécuter le consensus, ce qui la rend plus efficace.

III.3.3. RSSI

Le RSSI est une mesure de l'intensité du signal sur la liaison radio et est exprimé en dBm. Il est utilisé pour localiser les nœuds d'un réseau en convertissant les signaux RSS bruts en informations utiles (coordonnées de positionnement). Comme le montre la figure III.2, pour réaliser le processus de positionnement, des nœuds d'ancrage sont placés le long des itinéraires. L'algorithme de localisation peut être résumé en quatre phases. La première phase consiste à collecter les valeurs RSS du nœud mobile de référence. La force du signal reçu est une formule de la puissance d'émission et de la distance entre l'émetteur et le récepteur. La deuxième phase caractérise l'environnement. Les valeurs RSS aident à trouver les paramètres appropriés pour une région spécifique en effectuant une caractérisation de l'environnement. Ensuite, les paramètres environnementaux et les valeurs RSS sont envoyés à un serveur pour obtenir la distance à l'aide d'un modèle de perte de chemin [81]. Enfin, la technique de trilatération ou de multi-latération permet d'obtenir les coordonnées de l'emplacement [82]. Dans notre mécanisme, les FN sont chargés de calculer les coordonnées de localisation à partir des nœuds d'ancrage et de la technique de trilatération.

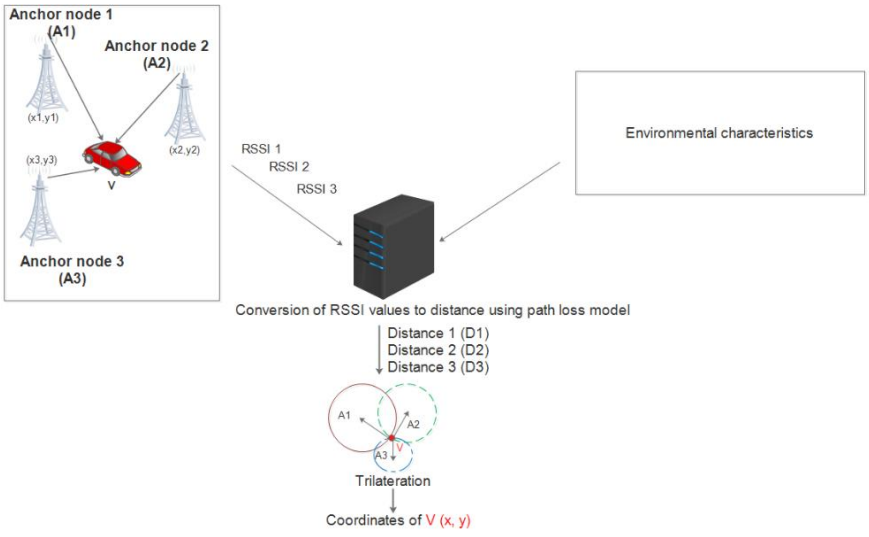

Figure III.2. Positionnement à l'aide de RSSI.

III.3.4. Modèle du réseau

Le modèle du réseau considéré dans cette contribution est constitué de 6 entités comme le montre la figure III.3. La description de ses entités est comme suit :

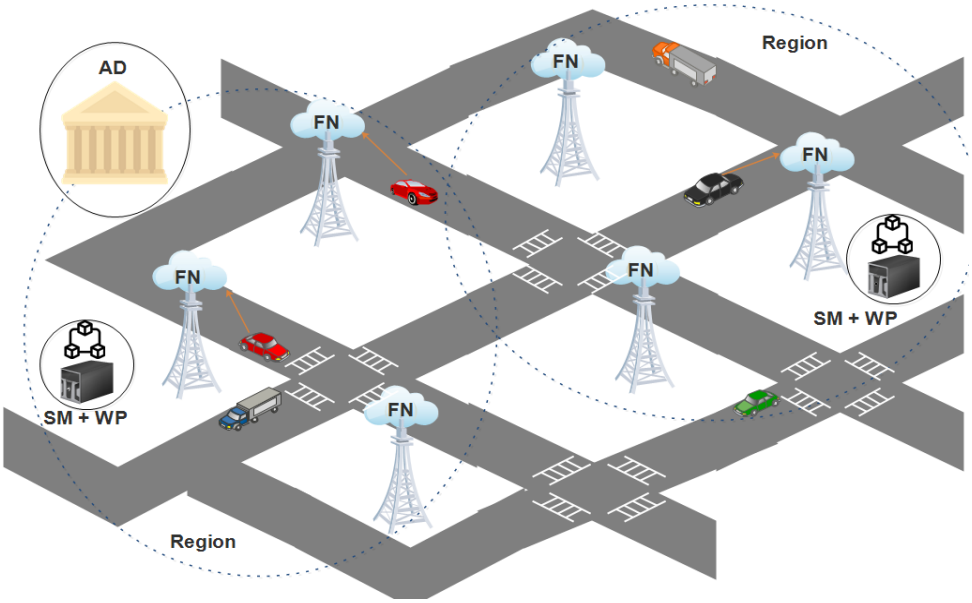

Figure III.3. Modèle du réseau considéré.

- **Unité embarquée (OBU) :** Il s'agit d'une unité équipée de fonctions de calcul et de communication comprenant un récepteur GPS, un ordinateur intégré et une interface de réseau sans fil intégrée dans le véhicule.
- **Nœud Fog (FN) :** Il valide la localisation d'un OBU et donne une étiquette aux OBU qui confirment son positionnement. Le FN peut également collecter, stocker et traiter les données reçues des véhicules.
- **Région** : Le réseau peut être divisé en différentes régions. Chaque région est composée de plusieurs nœuds d'ancrage, de plusieurs nœuds Fog (FN), d'un seul gestionnaire de services (SM) et d'un pair témoin (WP).
- **Gestionnaire de services (SM) :** Il permet de tenir un registre public dans chaque FN. Un SM est principalement responsable de la gestion de tous les FN de sa région. Chaque SM tient une BC qui contient tous les enregistrements d'accès aux véhicules et les informations relatives à leurs positions.
- **Pair témoin (WP) :** il s'agit d'un pair qui utilise un algorithme de consensus pour publier les résultats du positionnement dans la BC. Chaque région a son propre WP. WP et SM ont collaboré pour établir une blockchain de consortium.
- **Département d'audit (AD) :** Il s'agit d'une autorité de confiance, qui est responsable de l'enregistrement des OBU et des FN.

III.3.5. Hypothèses de sécurité

Pour simuler un scénario d'attaque Sybil typique dans les réseaux VFC, nous prenons en compte les hypothèses suivantes :

- L'AD est considéré comme une entité de confiance.
- Les SM sont considérés comme des entités de confiance, ils sont physiquement protégés et disposent d'une grande capacité de calcul.
- La BC n'est accessible qu'à l'AD, au SM et au WP.
- La communication entre le FN et le SM se fait par l'intermédiaire d'un canal sécurisé.
- Chaque véhicule peut changer de pseudonyme à tout moment et à sa volonté.
- Le véhicule malveillant peut s'enregistrer plusieurs fois, il peut voler le pseudonyme et le certificat d'un autre véhicule pour demander une validation de position, il peut générer de fausses trajectoires et il peut voler les étiquettes de preuve de position d'un autre véhicule obtenues auprès des FN.
- Le nœud malveillant peut modifier arbitrairement la puissance de transmission de signal uniquement pour lui-même et pour les nœuds Sybil fabriqués.
- Deux nœuds différents existant simultanément dans le réseau ne peuvent pas avoir la même identité.
- Les véhicules doivent demander une preuve de leur position à chaque FN rencontré sur leur chemin.

III.3.6. Objectifs de conception

Notre proposition devrait permettre d'atteindre les objectifs suivants :

- **Anonymat** : Permettre au véhicule de choisir son pseudonyme, qu'il définit lui-même et qu'il peut modifier si nécessaire.
- **Authentification** : Pour obtenir une preuve de position ou pour signaler un événement, il est essentiel de s'assurer de la légitimité de la demande faite par un véhicule. Les véhicules qui ne sont pas enregistrés dans le réseau ne sont pas autorisés à obtenir une preuve de position ou à signaler un événement.
- **Protection de la vie privée** : Les informations privées d'un OBU doivent être cachées aux autres utilisateurs du réseau. Dans notre mécanisme, l'identité de l'OBU et la clé privée

sont des informations privées qui ne doivent jamais être connues par des personnes non autorisées.

- **Attaque par rejeu** : Les demandes envoyées par les entités du réseau ne doivent pas être réutilisées plus d'une fois afin d'empêcher les adversaires d'itérer sur ces demandes et d'accéder illégalement aux services et ressources du réseau.
- **Attaque par usurpation d'identité** : Le vol du certificat d'un OBU légitime par un véhicule malveillant doit être détecté par le FN afin de ne pas valider la position du véhicule malveillant.
- **Attaque de compromission des FN** : Dans notre proposition, les FN sont responsables de la validation des positions des véhicules, de sorte que la solution proposée doit être résistante aux attaques de compromission des FN.
- **Attaque par déni de service** : Étant donné que le FN participe au processus de détection de l'attaque Sybil, il est important de résister à l'attaque DoS.

III.4. Notre mécanisme proposé de détection de l'attaque Sybil

III.4.1. Description générale

Dans cette section, nous décrivons notre mécanisme basé sur la blockchain pour détecter les attaques Sybil dans les réseaux VFC. Dans notre proposition, le véhicule doit demander aux FN rencontrés sur son chemin une preuve de sa position pour former sa trajectoire. Cette trajectoire est ensuite utilisée pour signaler un événement. La demande contient un certificat délivré par l'AD qui prouve son enregistrement dans le système, un pseudonyme auto-généré et un horodatage. À la réception d'une demande de position envoyée par un véhicule, le FN doit procéder à une série de vérifications avant de valider la position. La première vérification à effectuer est basée sur le RSSI. Elle vérifie si la demande de position est envoyée par le même véhicule. Cette vérification est considérée comme premier niveau de détection, elle permet de détecter l'attaque Sybil dans le cas le plus simple. Si ce n'est pas le cas, le FN contacte le SM pour demander les informations d'enregistrement car le FN n'est pas autorisé à accéder au BC. Si le véhicule est correctement enregistré, le FN délivre une preuve de position au véhicule et demande au SM d'enregistrer cette preuve dans la BC. À chaque FN rencontré sur le chemin du véhicule, celui-ci doit envoyer une nouvelle demande contenant le même pseudonyme et un nouvel horodatage.

Pour signaler un événement, le véhicule doit envoyer une requête qui contient son pseudonyme, le nombre d'étiquettes obtenus lors de son parcours, et le hash de la concaténation de ces étiquettes. Le FN contacte le SM pour vérifier ces informations dans la BC. Le SM vérifiera si ces étiquettes existent dans la BC et si ce véhicule a une trajectoire. Plus précisément, un ensemble d'étiquettes de position ne signifie pas nécessairement une trajectoire. La construction de la trajectoire à partir des étiquettes de position est effectuée par le SM selon un algorithme que nous avons proposé pour contrer l'attaque de compromission des FN. Si le FN reçoit plusieurs rapports simultanément, il doit comparer chaque paire de demandes de rapport pour détecter l'attaque Sybil. Cette étape est considérée comme un deuxième niveau de détection. Nous détaillons chaque étape dans la sous-section suivante.

III.4.2. Les phases de notre mécanisme

Le processus de détection des attaques se compose de cinq phases : Phase d'initialisation, phase d'enregistrement, phase d'échange de messages, phase de consensus, et phase de rapport d'événement et de détection des nœuds Sybil. Les détails de chacune de ces phases sont présentés ci-dessous :

1) Phase d'initialisation *:* La figure III.4 détaille les étapes de cette phase. Cette phase est utilisée pour initialiser les paramètres du système ; elle est exécutée par l'AD en effectuant les opérations suivantes :

- Choisir une courbe elliptique avec ses paramètres : (E, n, q, P) où E est la courbe elliptique sur le corps premier q avec le point de base P d'ordre n. P est le générateur du groupe cyclique G.

- Générer la clé privée SK_{AD}, qui est un nombre aléatoire appartenant à $\mathbb{Z}_n^*$.

- Calculer $PK_{AD} = SK_{AD}.P$, où PK_{AD} est la clé publique de l'AD.

- Choisir deux fonctions de hachage H_0 et H_1 telles que :

$H_0 : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$

$H_1 : G, \mathbb{Z}_n^*, \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$

- Publier les paramètres du système : <E, n, PK_{AD}, q, H_0).

- D'autre part, pour contrer l'attaque de compromission du FN, l'AD définit un nombre aléatoire 'y' qui représente le nombre à atteindre pour construire une trajectoire :

y appartient à $\mathbb{N}^* \setminus \{1\}$. Ce nombre ne doit être connu que par les SM et n'est pas stocké dans la mémoire de l'AD.

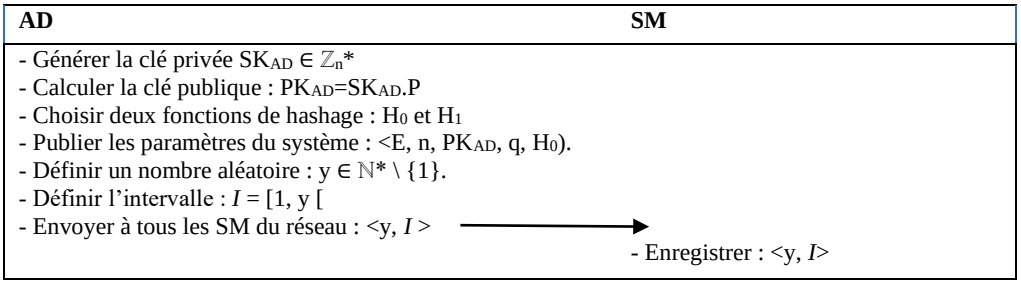

Figure III.4. Phase 1 : Phase d'initialisation.

- L'AD doit également définir l'intervalle '*I*' qui doit être utilisé par les SM pour définir les coefficients des FN qui sont dans leur région : *I* appartient à $\mathbb{N}$ tel que :

I = [1, y [avec un pas égal au reste de la division euclidienne de y sur 10.

- L'AD informe tous les SM par le nombre y et l'intervalle *I*.

2) Phase d'enregistrement : Cette phase permet à l'AD d'enregistrer les OBU et les FN via un canal sécurisé. La procédure d'enregistrement est la même pour les FN et les OBU, à l'exception de l'étape 4 qui concerne les FN. Les détails de cette phase sont présentés à la figure III.5 et sont les suivants :

- **Étape 1 :**

- Chaque OBU a sa propre identité unique (ID_{OBU}). L'OBU chiffre l'ID_{OBU} avec la clé publique de l'AD :($E = Enc\text{-}PK_{AD}(ID_{OBU})$)

- L'OBU l'envoie E à l'AD via un canal sécurisé.

- **Étape 2 :**

Pour enregistrer les OBU, l'AD effectue les opérations suivantes :

- Décrypter "E" reçu de l'OBU avec sa clé privée SK_{AD}.

- Choisir au hasard un nombre SK_{OBU} appartenant à $\mathbb{Z}_n^*$, ce SK_{OBU} représente la clé privée de l'OBU.

- Calculer la clé publique PK_{OBU} : ($PK_{OBU} = SK_{OBU}.P$).

- Générer un pseudonyme pour l'OBU afin de cacher sa véritable identité ; il sélectionne un nombre aléatoire "x" qui appartient à $\mathbb{Z}_n^*$, le concatène avec ID_{OBU} puis le hache à l'aide de H_0 : ($PID1_{OBU} = H_0(ID_{OBU} \| x)$).

- Délivrer un certificat à l'OBU comme preuve d'enregistrement. Pour calculer ce certificat, l'AD hache PK_{OBU}, SK_{OBU} et $PID1_{OBU}$ à l'aide de H_1, puis chiffre le résultat à l'aide de la clé publique : ($Cert_{OBU} = H_0(H_1(PK_{OBU}, SK_{OBU}, PID1_{OBU}))$

- Envoyer à l'OBU via un canal sécurisé : < (PK_{OBU}, SK_{OBU}), $PID1_{OBU}$, $Cert_{OBU}$ >

- Enregistrement sur la BC : <PK_{OBU}, $PID1_{OBU}$, $Cert_{OBU}$ >

Les clés publiques des FN et des OBU sont visibles par toutes les entités du réseau.

- **Étape 3 :**

- L'OBU stocke les informations reçues de l'AD dans sa mémoire : < (PK_{OBU}, SK_{OBU}), $PID1_{OBU}$, $Cert_{OBU}$>

Il convient de noter que les mêmes étapes sont suivies pour enregistrer les FN. Par conséquent, chaque FN stocke dans sa mémoire les informations reçues de l'AD : <(PK_{FN}, SK_{FN}), $PID1_{FN}$, $Cert_{FN}$>.

OBUi / FNj	**AD**
- Choisir ID_{OBU}. - Calculer E = Enc-PK_{AD}(ID_{OBU}) - Envoyer <E> via un canal sécurisé →	
	- Décrypter E : Dec-SK_{AD}(E) - Générer la clé privée : $SK_{OBU} \in \mathbb{Z}_n$* - Calculer la clé publique : PK_{OBU}= SK_{OBU}.P - Générer un pseudonyme : $PID1_{OBU} = H_0(ID_{OBU} \| x)$. - Calculer la preuve d'enregistrement : $Cert_{OBU} = H_0(H_1(PK_{OBU}, SK_{OBU}, PID1_{OBU}))$)
←	- Envoyer < (PK_{OBU}, SK_{OBU}), $PID1_{OBU}$, $Cert_{OBU}$ >Via un canal sécurisé
	- Enregistrer sur la BC : <PK_{OBU}, $PID1_{OBU}$, $Cert_{OBU}$ >
- Enregistrer : < (PK_{OBU}, SK_{OBU}), $PID1_{OBU}$, $Cert_{OBU}$ >	

Figure III.5. Phase 2 : Phase d'enregistrement des OBU et des FN.

- **Étape 4 :**

Le processus de cette étape est illustré à la figure III.6.

- l'AD doit envoyer au SM de droite le $PID1_{FN}$ et la clé publique PK_{FN} du FN enregistré < $PID1_{FN}$, PK_{FN} >

- Le rôle du SM dans cette étape est de générer un coefficient "coeff" pour ce nouveau FN. Un coefficient est un nombre aléatoire qui appartient à l'intervalle *I*.

- Le SM stocke dans sa mémoire interne : < $PID1_{FN}$, PK_{FN}, coeff> et transmet ensuite ces trois informations à tous les SM du réseau.

AD	**SM**
- Envoyer < $PID1_{FN}$, PK_{FN} > via un canal sécurisé ⟶	- Générer un coefficient : coeff ∈ I - Enregistrer : < $PID1_{FN}$, PK_{FN}, coeff> - Envoyer ces trois informations à tous les SMs.

Figure III.6. Phase 2 : Génération des coefficients par SM.

3) ***Phase d'échange de messages*** *:* L'OBU en mouvement doit échanger des messages avec le FN pour valider sa position. La validation de la position se fait en trois étapes, dont la figure III.7 présente les détails :

- **Étape 1 :**

L'OBU mobile effectue les opérations suivantes :

- Choisir un nombre aléatoire "m" qui appartient à $\mathbb{Z}_n^*$. Ce "m" est utilisé pour générer un nouveau pseudonyme "PID_{OBU}", le calcul de ce PID_{OBU} étant le suivant : $PID_{OBU}=H_0$ ($PID1_{OBU}$ || m).

- Sélectionnez l'horodatage TMP_{OBU}. Cet horodatage permet de valider le message relayé et de s'assurer qu'il ne sera pas relayé à nouveau prochainement.

- Concaténer le certificat obtenu de l'AD avec le PID_{OBU} et le TMP_{OBU} générés : S = ($Cert_{OBU}$ || PID_{OBU} || TMP_{OBU}).

- Calculer une signature sur "S" pour garantir l'intégrité et l'authenticité du message. La signature est calculée à l'aide de sa clé privée : Sig_SK_{OBU} (S).

- Préparer une requête composée de "S" avec la signature et l'envoyer au FN : Req = (S || Sig_SK_{OBU} (S)).

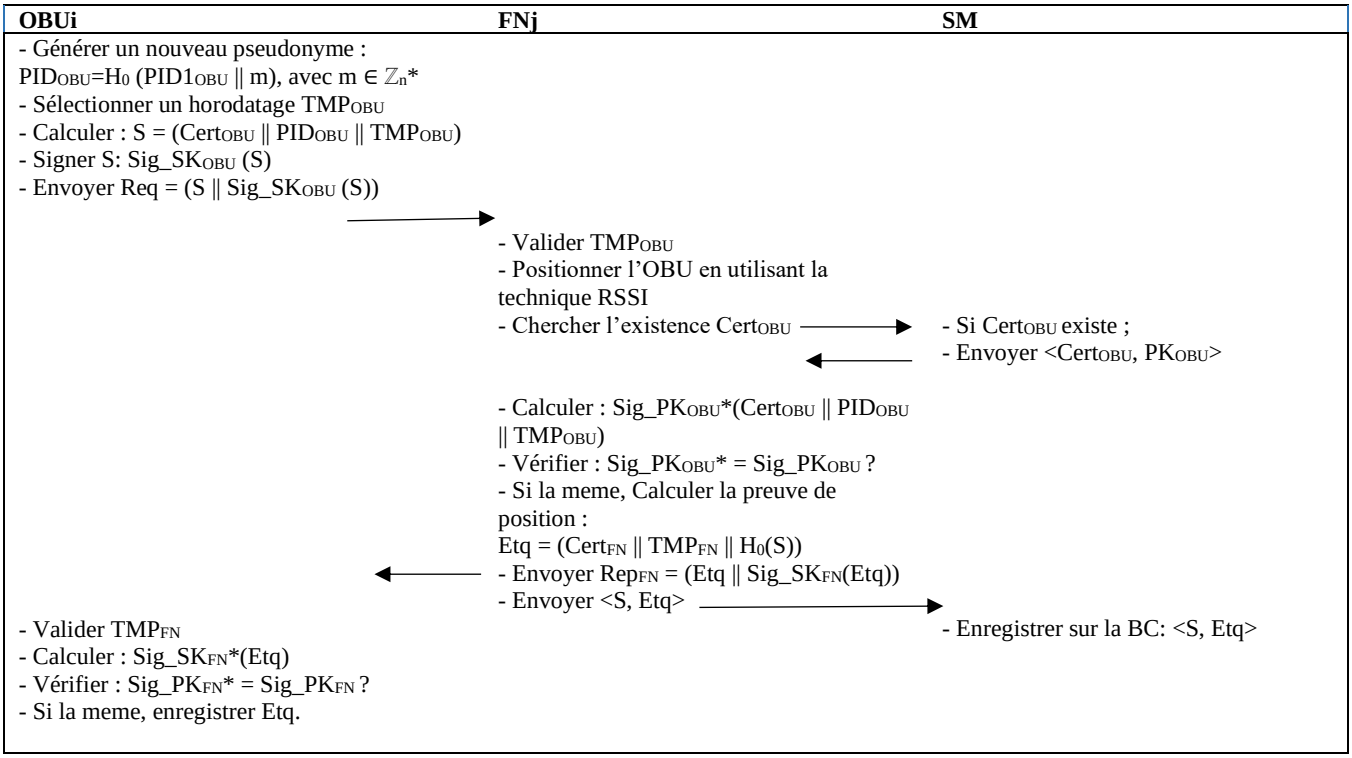

Figure III.7. Phase 3 : Phase d'échange de messages.

- **Étape 2 :**

- Après la réception de "Req", le FN vérifie la validité de TMP_{OBU} ; s'il n'entre pas dans la fenêtre temporelle autorisée, le FN met fin à la connexion, sinon il poursuit ses vérifications.

- Le FN positionne l'OBU en utilisant la technique RSSI. Pour ce faire, la valeur RSS est extraite du message envoyé par l'OBU. En utilisant le modèle de perte de chemin, la valeur RSS sera convertie en distance :

$$P_r = \frac{p(d_0)}{(d/d_0)^n} \qquad (III.2)$$

Où $P(d_o)$ est la puissance reçue mesurée à la distance d_o. Généralement, la valeur de d_o est fixée comme constante d_o = 1 m. n est l'indice de perte de chemin qui est un paramètre pour l'évaluation des caractéristiques de l'environnement.

$$P_{r(d)} = P_{r(d_0)} - 10 \times n \times log_{10}\left(\frac{d}{d_0}\right) \quad (III.3)$$

- Deux paramètres environnementaux majeurs, n et $Pr(d_o)$, sont acquis. En conséquence, la distance entre le FN et l'OBU est obtenue à l'aide de la formule (III.3) :

$$d = d_0 \exp\left(\frac{p_{r(d0)} - p_{r(d)}}{10n}\right) \quad (III.4)$$

- En utilisant la formule (III.4), et en fonction des coordonnées de position (x_v,y_v) déclarées par l'OBU et des coordonnées actuelles de FN (x_F,y_F), la distance d' est calculée :

$$d' = \sqrt{(x_F - x_v)^2 + (y_F - y_v)^2} \quad (III.5)$$

- La différence entre les deux distances (d et d') est calculée à l'aide de la formule (III.6) :

$$|d' - d| = \alpha \quad (III.6)$$

- Le FN considère un OBU comme un nœud normal si la valeur α obtenue à partir de la formule (III.6) est comprise dans la fourchette d'écart β (α < β). Étant donné que β doit être résumé en fonction de l'environnement expérimental.

- Si le FN reçoit deux ou plusieurs "Reqs" en même temps, il doit comparer les distances calculées à l'aide de la formule (III.3) pour chaque paire de requêtes. Par exemple, pour comparer la Req1 et la Req2 reçues, le FN doit calculer la différence entre les distances (d1 et d2) après les avoir calculées :

$$|d1 - d2| = \gamma \quad (III.7)$$

Si γ est inférieur à δ (γ < δ), il considère ces Reqs comme des nœuds Sybil et met fin à la connexion. Sinon, il continue ses vérifications. δ est un seuil prédéfini qui indique la distance minimale qui peut séparer deux véhicules. Cette partie de l'étape 2 permet de détecter l'attaque Sybil à un premier niveau, plus précisément dans le cas d'attaque le plus simple (un attaquant envoie deux "Req" ou plus à partir du même endroit, de la même période et avec le même pseudonyme ou des pseudonymes différents).

- Après avoir localisé l'OBU, le FN doit vérifier le $Cert_{OBU}$ reçu et l'intégrité du "Req", pour cela il doit contacter le SM de sa région et lui demander de vérifier l'existence du $Cert_{OBU}$ dans la BC.

- Le SM informe le FN du résultat de la recherche du $Cert_{OBU}$ dans la BC. Si le $Cert_{OBU}$ existe, le SM envoie la clé publique au FN. Dans le cas contraire, il envoie une réponse négative.

- Le FN met fin à la connexion si la réponse du SM est négative ; sinon, il vérifie l'intégrité de " Req" en calculant Sig_PK_{OBU} ($Cert_{OBU}$ || PID_{OBU} || TMP_{OBU}) et en le comparant avec le Sig reçu. Le calcul est effectué à l'aide de la clé publique reçue du SM.

- Si les deux signatures sont différentes, le FN met fin à la connexion ; dans le cas contraire, il doit envoyer une étiquette à l'OBU pour prouver sa localisation. Cette étiquette est une concaténation de la $Cert_{FN}$ reçue de l'AD, de l'horodatage TMP_{FN} et du hachage de "S" (reçu de l'OBU) à l'aide de la fonction de hachage H_0 : Etq = ($Cert_{FN}$ || TMP_{FN} || H_0(S)).

- Le FN envoie Rep_{FN} à l'OBU, qui contient Etq et la signature de Etq : Rep_{FN} = (Etq || Sig_SK_{FN} (Etq)).

- Le FN contacte le SM pour l'enregistrement sur la BC : (S, Etq).

- **Étape 3 :**

- Après la réception de "Rep_{FN}", l'OBU vérifie la validité du TMP_{FN}, s'il n'entre pas dans la fenêtre temporelle autorisée, l'OBU met fin à la connexion, sinon il poursuit ses vérifications.

- L'OBU doit vérifier l'intégrité du "Rep_{FN}" reçu. Pour ce faire, il calcule Sig_PK_{FN} (Etq)) et le compare avec le Sig reçu. S'ils sont identiques, il enregistre dans sa mémoire : "Etq".

- A chaque FN rencontré dans la trajectoire de l'OBU, il doit envoyer une nouvelle requête avec le même certificat "$Cert_{OBU}$", le même pseudonyme utilisé dans sa première requête "PID_{OBU}", et un nouveau TMP_{OBU}.

4) Phase de consensus : Le résultat de la localisation validé par le FN doit être enregistré dans la BC. Le FN ne peut pas enregistrer directement sur la BC, il doit contacter le SM pour cela. Nous utilisons un algorithme de consensus PBFT dans notre proposition. Nous supposons qu'il y a n nombre de WP ayant la capacité d'écrire un bloc dans la BC. Comme le montre la figure 8, l'un des WP prend le rôle de "Speaker", qui est chargé de lancer le processus de consensus, tandis que les autres agissent comme des membres du congrès qui participent au mécanisme de vote lancé par le Speaker. L'algorithme PBFT se déroule en trois étapes. Le processus de consensus est le suivant :

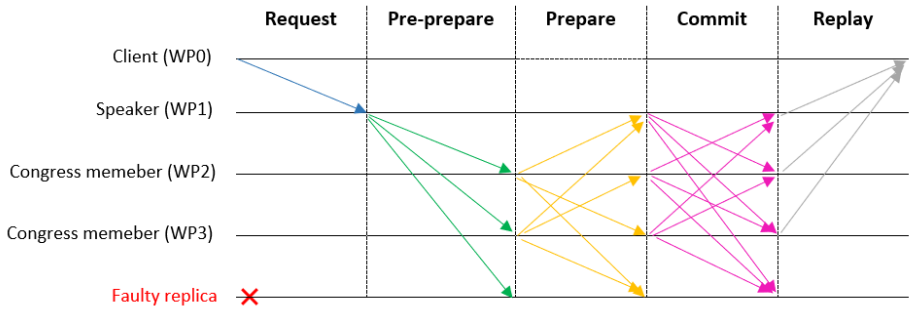

Figure III.8. Phase 4 : Phase de consensus.

- **Étape 1 :**

- Sélectionner le speaker "SP" à l'aide de l'évaluation suivante : SP = (*ind* mod n) + 1 (8) Où *ind* fait référence à l'indice du bloc actuel.

- Après avoir prouvé la position d'un OBU par le FN et transféré l'étiquette de preuve de position au SM de sa région, le SM partage cette preuve avec tous les WPs. Les WP stockent les étiquettes reçues dans leurs mémoires internes. Après un temps t qui représente le temps de génération d'un bloc, un nouveau bloc est constitué.

- **Étape 2 :**

- Après la création du bloc, le processus de vote commence. Le SP demande aux membres du congrès de voter en leur adressant une requête. La demande est envoyée sous la forme d'un message de Pre-Prepare. Elle contient l'identifiant du SP, l'index du bloc, le bloc créé et la signature du bloc à l'aide de sa clé privée : <Request_v, SP, ind, New_bloc, Sig_{SP}(New_bloc) >. Request_v représente la demande de vote. Une réponse est envoyée par les WP correctes sous la forme d'un message de préparation à tous les autres membres.

- Après avoir reçu 2f messages de préparation des autres membres et le Pre-Prepare associé, les membres du congrès ont accepté la demande du SP. En conséquence, ils envoient à tous les autres membres un message de validation.

- **Étape 3 :**

- Le nième groupe de travail envoie sa demande de vote après avoir reçu 2f + 1 messages de validation associés. La demande contient l'identifiant du WP, la signature du bloc avec sa clé

privée : < Request_r, WPn, ind, New_bloc, Sig_{WP}(New_bloc) >. Request_r est la demande de réponse.

- Une fois que le SP a reçu les réponses des membres du congrès, le bloc est ajouté à la blockchain et les mémoires internes des WP sont vidées.

5) la phase de signalement des événements et de détection des nœuds Sybil : Dans notre proposition, les OBU malveillants peuvent modifier le signal de transmission ; plus précisément, un OBU malveillant peut s'enregistrer plusieurs fois ou générer plusieurs pseudonymes, et envoyer plusieurs demandes de positionnement en modifiant la force du signal de transmission ; cela implique que la détection des nœuds Sybil ne sera pas possible dans la phase d'échange de messages - phase 3, étape 2 (étant donné que le FN se base sur le RSSI pour positionner l'OBU). Pour isoler les nœuds "Sybil" non détectés lors de la phase 3, nous avons ajouté cette phase en tant que deuxième niveau de détection. Dans notre solution, pour signaler tout type d'événement (accident, congestion, travail, etc.), l'OBU doit envoyer une requête qui prouve sa trajectoire. Le processus de signalement est illustré à la figure III.9 et se déroule comme suit :

- **Étape 1 :**

- L'OBU doit construire une requête qui contient le pseudonyme qu'il a utilisé pendant son déplacement pour valider sa position "PID_{OBU}", son certificat "$Cert_{OBU}$", le nombre d'étiquettes obtenues pendant son déplacement "NbrTags", le hash de la concaténation de toutes les étiquettes obtenues à l'aide de la fonction H_0. Nous avons utilisé la fonction H_0 pour cacher le chemin du véhicule aux autres membres du réseau. La requête sera la suivante :

$Trg = (PID_{OBU} \| Cert_{OBU} \| TMP_{OBU} \| NbrTags \| H_0 (Path))$.

- L'OBU signe Trg à l'aide de sa clé privée et signale l'événement à FN : Event = (Trg || Sig_SK_{OBU}(Trg)).

- **Étape 2 :**

- Lorsque le FN reçoit le rapport d'événement "Event", il commence à vérifier la validité du TMP_{OBU}, s'il n'entre pas dans la fenêtre temporelle autorisée, le FN ne prend pas en compte ce rapport. Dans le cas contraire, il procède à la vérification de la signature reçue avec l'événement.

- Il calcule $Sig\_PK_{OBU}(Trg)$, s'il n'est pas identique à la signature reçue, il ignore le rapport, sinon, il contacte le SM de sa région pour vérifier l'existence et la validité des autres informations envoyées dans la demande d'événement en consultant la BC et voir si ce véhicule a une trajectoire.

- **Étape 3 :**

- Le SM doit vérifier que le $Cert_{OBU}$ existe et que le PID_{OBU} correspond au $Cert_{OBU}$. Cette vérification permet de s'assurer que ces informations ne sont pas volées ou générées aléatoirement. Si ces deux conditions sont vérifiées, il sélectionne, en fonction des NbrTags envoyés dans la requête, les derniers NbrTags enregistrés sur la BC. Après avoir trouvé ces étiquettes, il les trie par ordre croissant sur la base du TMP, les concatène et hache cette concaténation à l'aide de la fonction H_0. Si le résultat de ce hachage n'est pas similaire au hachage envoyé dans le rapport, le rapport est ignoré, sinon il passe à l'étape suivante.

- Le SM doit vérifier si cet OBU a au moins une trajectoire car, dans notre proposition, pour signaler un événement, il faut avoir au moins une trajectoire. Une trajectoire est définie dans notre proposition comme un ensemble de preuves de position obtenues à partir de plusieurs FN. Le nombre défini par l'AD "y" lors de la phase d'initialisation représente le nombre à atteindre pour former une trajectoire. Le nombre "y" n'est connu ni par les OBU ni par les FN. Lorsque la somme des coefficients de plusieurs FN est égale à "y", on dit qu'une trajectoire est formée. Cette étape permet de contrer l'attaque de compromission des FNs. Un OBU malveillant peut compromettre un FN pour obtenir une preuve de position, mais cela ne suffit pas pour signaler un événement. Une trajectoire est une collaboration de plusieurs FN en fonction des coefficients attribués par le SM. Même si l'OBU malveillant compromet plusieurs FN, cela ne garantit pas qu'il ait formé une trajectoire, cette propriété étant garantie par la propriété d'aléatoire des coefficients.

- Le SM ne sélectionne que les étiquettes récentes selon une période définie, par exemple les étiquettes des deux dernières heures. Ensuite, il calcule le nombre de trajectoires construites. Le nombre de trajectoires est égal à la somme des coefficients des FN qui ont livré des preuves divisées par le nombre fixé par l'AD.

$$Nombre\ de\ trajectoires\ =\ somme\ des\ Coeff\ (FN)/y \qquad (III.9)$$

- Si le résultat est supérieur à 1, cela signifie que le véhicule peut construire au moins une trajectoire, et on passe à l'étape suivante. Dans le cas contraire, le rapport n'est pas pris en compte.

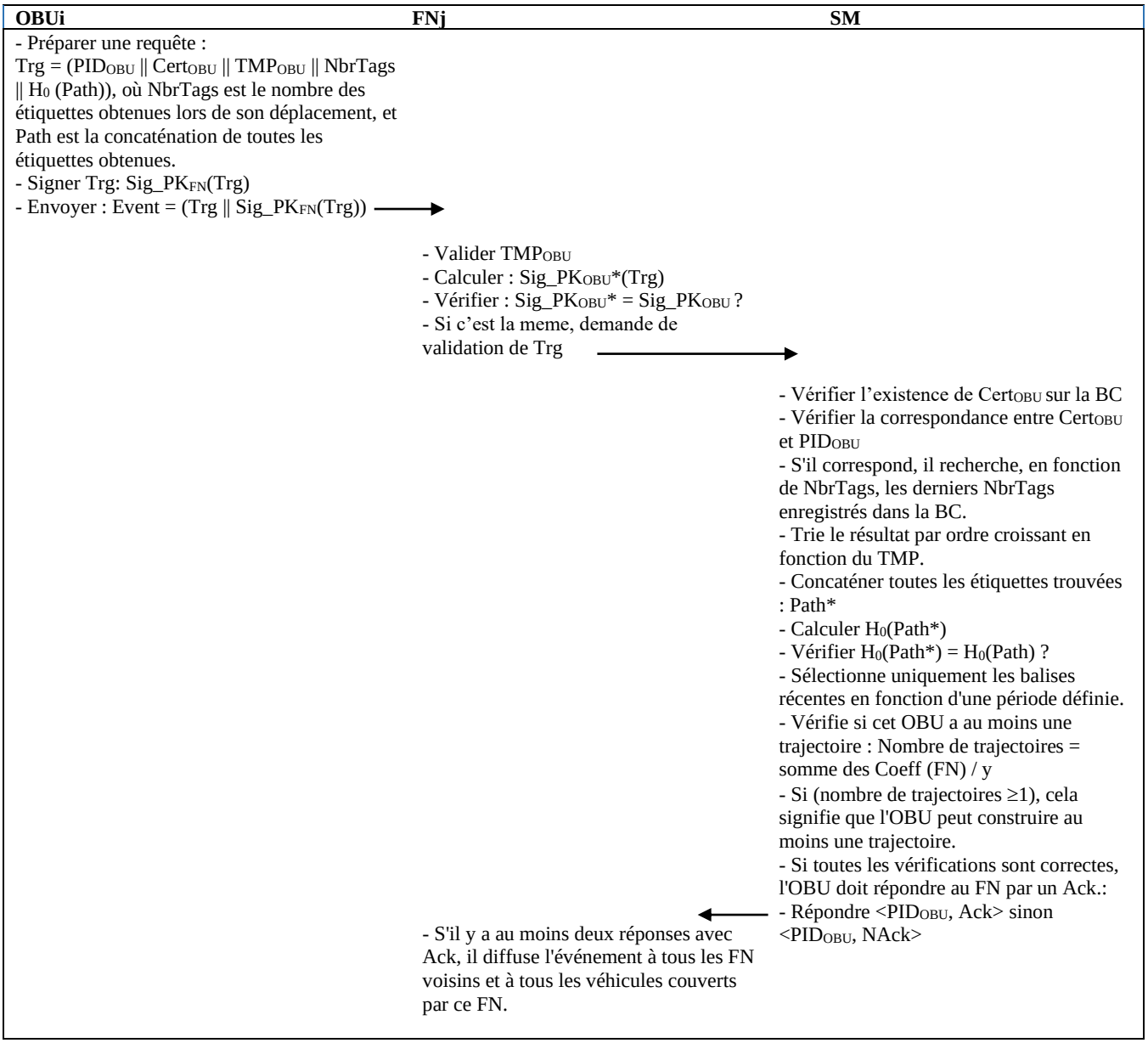

Figure III.9. Phase 5 : la phase de signalement des événements et de détection des nœuds Sybil.

- Dans le scénario où il y a plusieurs rapports d'événements en même temps, le SM doit faire un ensemble de comparaisons pour chaque paire de trajectoires. Il compare d'abord la longueur de la trajectoire calculée ci-dessus. Si deux trajectoires ont une longueur différente, il accepte le rapport, sinon il vérifie la similarité des preuves de position dans les deux trajectoires. Si les deux trajectoires ont des preuves de position provenant de FN différents, le signal est accepté, sinon il vérifie les horodatages de toutes les preuves de position des deux trajectoires. Pour chaque preuve de position émise par le FN pour les deux trajectoires, il fait la différence entre les TMP

des deux preuves de position. Si la différence entre les deux valeurs appartient à un intervalle de temps défini, par exemple [0, 2] minute, ces deux trajectoires seront considérées comme des attaques Sybil ; sinon, le signal est accepté.

- **Étape 4 :**

- Le SM doit répondre au FN qui a reçu les rapports d'événements en lui communiquant le résultat des vérifications. La réponse contient le PID de l'OBU qui a envoyé le rapport avec un Ack pour le rapport accepté et un NAck dans le cas contraire.

- Pour que le rapport soit pris en compte, il doit y avoir au moins deux réponses avec Ack. S'il y en a au moins deux, le FN diffuse l'événement à tous les FN voisins et à tous les véhicules couverts par ce FN.

III.5. Analyse de la sécurité

Dans cette section, nous analysons la sécurité du mécanisme proposé et présentons nos résultats de simulation en utilisant OMNET++, SUMO et le framework Veins.

III.5.1. Détection des attaques

- **Attaque Sybil** : L'attaque Sybil peut être détectée dans plusieurs scénarios :
  - Pour former une demande de position par l'OBU, l'attaquant peut générer différents pseudonymes avec la même localisation ; dans ce cas, l'attaque sera détectée avec la technique RSSI dans la phase d'échange de messages et la preuve de position ne sera pas délivrée.
  - Si l'attaquant modifie la transmission du signal, utilise plusieurs types d'équipement du même véhicule ou génère des pseudonymes à différents endroits, l'attaque sera détectée dans la phase de signalement des événements et de détection des nœuds Sybil grâce à la comparaison des trajectoires.
- **Attaque par rejeu** : Dans notre proposition et dans les deux phases : "phase d'échange de messages" et "phase de signalement d'événements et de détection de nœuds Sybil", chaque message transmis est accompagné d'un horodatage. Lorsqu'il reçoit le message, le récepteur doit comparer cet horodatage avec la fenêtre temporelle autorisée ; si cet horodatage est compris dans la fenêtre, il considère le message comme récent. Si l'attaquant A modifie

l'horodatage avec un nouvel horodatage valide, la modification sera détectée après vérification de la signature du message reçu.

- **Attaque par usurpation d'identité** : Dans la phase d'échange de messages, l'attaquant A peut voler un certificat à un OBU légitime, générer un nouveau pseudonyme PID_A et un horodatage TMP_A, et signer le message avec sa clé privée pour former la demande. Le FN contactera le SM de sa région pour vérifier la correspondance entre le certificat obtenu auprès de l'AD et la clé publique de l'OBU. Cette attaque sera détectée en calculant Sig_{PKA} ($Cert_{OBU}$ || PID_A || TMP_A) et en le comparant au Sig reçu.
- **Anonymat** : Dans la phase d'échange de messages, l'OBU peut générer son pseudonyme sur la base du pseudonyme obtenu auprès de l'AD, ainsi que changer son pseudonyme à tout moment.
- **Authentification** : Le FN doit demander au SM de vérifier l'enregistrement d'un OBU, soit dans sa demande de preuve de position, soit au moment de la notification de l'événement.
- **Confidentialité** : Lors de la phase d'enregistrement, l'OBU/FN envoie son identité à l'AD sous forme cryptée et dans un canal sécurisé. A la réception, l'AD génère un nombre entier aléatoire et l'utilise pour créer un pseudonyme afin de masquer l'identité de l'OBU/FN. D'autre part, un attaquant ne peut pas obtenir la clé privée de l'OBU/FN à partir de la clé publique, ce qui revient à utiliser le problème de logarithme discret de la courbe elliptique. D'autre part, la trajectoire des conducteurs est cachée aux autres entités du réseau. Au moment de la demande de preuve de position, l'OBU n'est pas tenu d'envoyer les preuves de position déjà obtenues. Au moment de la notification de l'événement, l'OBU envoie sa trajectoire hachée à l'aide de la fonction de hachage H_0 : H_0 (Path).
- **Attaque par compromission des nœuds FN** : Dans notre proposition, le nombre à atteindre pour former une trajectoire est caché aux OBU. En outre, chaque FN a un coefficient variable qui est également caché aux OBU. Même si un OBU malveillant compromet plusieurs FN, il ne sera pas sûr d'avoir formé une trajectoire.
- **Attaque par déni de service** : L'un des avantages des réseaux Fog véhiculaires est la capacité du nœud Fog. Un nœud FN a une capacité de calcul et de stockage intéressante par rapport aux RSU. Un OBU malveillant ne peut pas mettre un FN hors service car la capacité d'un OBU est considérablement plus petite que celle d'un FN. En outre, dans notre proposition, la majeure partie du traitement est effectuée par le SM.

Services de sécurité	[42]	[40]	[41]	[83]	[84]	**Notre mécanisme**
Privacy	✓	✓	✓	✗	✗	✓
Anonymat	✗	✗	✗	✗	✗	✓
Authentification	✓	✓	✓	✗	✗	✓
Attaque par rejeu	✓	✓	✓	✗	✗	✓
Attaque par usurpation d'identité	✗	✗	✗	✗	✗	✓
Attaque DoS	✗	✓	✓	✗	✗	✓
Compromission des FN/RSU	✗	✓	✓	✗	✗	✓
Attaque Sybil	✓	✓	✓	✓	✓	✓

Tableau III.2. Comparaison entre les services de sécurité.

Le tableau III.2 présente une comparaison entre notre proposition et celles de [42], [40], [41], [83] et [84] en ce qui concerne la résistance à différentes attaques. Notre proposition peut contrer plusieurs attaques telles que l'attaque par rejeu, l'attaque par usurpation d'identité, l'attaque par déni de service et l'attaque par compromission des FN. Ce n'est pas le cas des autres propositions. La solution [42] ne peut faire face qu'à l'attaque par rejeu, tandis que les solutions [40] et [41] ne peuvent pas faire face à l'attaque par usurpation d'identité. En ce qui concerne l'anonymat, notre proposition permet aux OBU de choisir leurs pseudonymes et de les modifier à tout moment, ce qui n'est pas le cas des autres systèmes. Dans les travaux [83] et [84], les auteurs n'ont pas utilisé de techniques cryptographiques. C'est pourquoi leurs propositions n'ont contré aucune des attaques énumérées dans le tableau III.2, à l'exception de l'attaque Sybil.

III.5.2. Simulation

Le système de simulation est composé d'un simulateur de réseau OMNeT ++ 5.6.2, d'un framework Veins 5.2 et d'un générateur de trafic SUMO 1.8.0. OMNeT++ est un simulateur d'événements discrets qui peut être utilisé pour évaluer la performance du réseau [85], Veins est un framework libre pour effectuer des simulations de réseaux de véhicules [86] et SUMO est un simulateur d'événements de trafic libre qui suit les mouvements des véhicules tels que la vitesse, l'emplacement, l'accélération et d'autres paramètres [87]. Comme le montre la figure III.10, nous avons sélectionné une section de la carte de la ville d'Oran, en Algérie, avec des dimensions de 80,66 X 38,52 Km^2 en utilisant le projet OpenStreetMap [88] et les routes sont générées aléatoirement à l'aide de SUMO. Les autres paramètres de simulation sont configurés dans OMNeT++ et sont illustrés dans le tableau III.3.

Paramètres de simulation	Valeur
Temps de simulation	800 s
Taille de la carte	80,66 X 38.52 km^2
Nombre des véhicules	150
Portée de la transmission	300 m
Protocole	802.11p
Puissance de transmission (mW)	20

Tableau III.3. Paramètres de notre simulation.

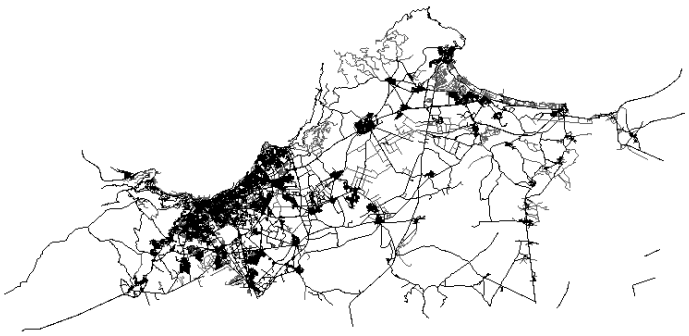

Figure III.10. Partie de la carte choisie pour la simulation : la ville d'Oran, Algérie.

III.5.2.1. Métrique

Pour évaluer notre proposition, nous avons pris en compte les paramètres suivants :

- **Le taux de faux positifs (FPR) :** représente le taux de nœuds distincts qui sont identifiés comme des nœuds Sybil. Le taux de faux positifs est calculé comme suit :

$$\frac{FP}{FP + TN} \qquad (III.10)$$

Où FP est le nombre de faux positifs (nombre de nœuds distincts considérés à tort comme Sybil) et TN est le nombre de vrais négatifs (nombre de nœuds Sybil correctement détectés comme Sybil).

- **Le taux de faux négatifs (FNR) :** représente le taux de nœuds Sybil identifiés comme nœuds distincts. Il est calculé comme suit :

$$\frac{FN}{FN + TP} \qquad (III.11)$$

Où FN est le nombre de faux négatifs (le nombre de nœuds Sybil considérés à tort comme des nœuds distincts) et TP est le nombre de vrais positifs (le nombre de nœuds distincts correctement identifiés comme des nœuds distincts).

- **Le taux de vrais négatifs (TNR) :** représente le taux de détection des nœuds Sybil correctement identifiés comme nœuds Sybil. Il est calculé comme suit :

$$\frac{TN}{TN + FP} \qquad (III.12)$$

- **Le taux de vrais positifs (TPR) :** représente le taux de détection des nœuds distincts correctement identifiés comme nœuds distincts. Il est calculé comme suit :

$$\frac{TP}{TP + FP} \qquad (III.13)$$

Pour prouver l'efficacité de notre proposition en termes de taux de détection, nous simulons tous les scénarios qui peuvent être lancés par les véhicules et nous voyons dans quelle phase la détection a lieu. Pour cela, dans notre expérience, nous avons simulé 150 véhicules avec des trajectoires aléatoires. Nous avons fixé la taille minimale de la trajectoire à 5 (y=5). Nous avons choisi 1/3 du nombre total de véhicules comme véhicules malveillants. Un véhicule dans le réseau peut avoir un comportement bénin ou malveillant. Un véhicule malveillant peut exécuter plusieurs scénarios pour réussir son attaque. Les scénarios possibles sont les suivants.

- Scénario 1 : un véhicule bénin s'enregistre une seule fois, demande une preuve de position à chaque FN qu'il rencontre sur son chemin et utilise les étiquettes qu'il a obtenues pour signaler un événement.

- Scénario 2 : le véhicule malveillant s'enregistre une seule fois, génère plusieurs pseudonymes simultanément et envoie des demandes de position à la FN pour chaque pseudonyme généré.

- Scénario 3 : le véhicule malveillant s'enregistre plusieurs fois pour obtenir plusieurs certificats, génère des pseudonymes pour chaque certificat obtenu auprès de l'AD, modifie la puissance du signal transmis et demande une preuve de position pour chaque pseudonyme généré.

- Scénario 4 : le véhicule malveillant vole un certificat à un véhicule légitime, envoie une demande de position avec le certificat volé ou l'utilise pour signaler un événement.

- Scénario 5 : le véhicule malveillant s'enregistre plusieurs fois pour obtenir plusieurs certificats, génère des pseudonymes pour chaque certificat obtenu auprès de l'AD, modifie la puissance du signale transmis et demande une preuve de position pour chaque pseudonyme généré. Au moment de signaler l'événement, il modifie sa trajectoire. Plus précisément, il supprime certaines preuves de position de sa trajectoire.

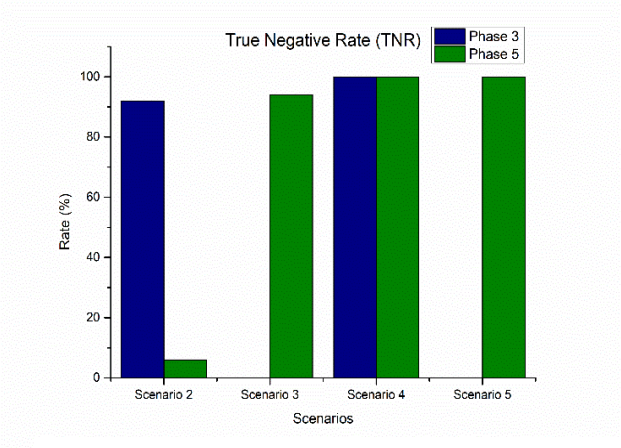

Figure III.12. Taux de vrais négatifs pour les différents scénarios d'attaque.

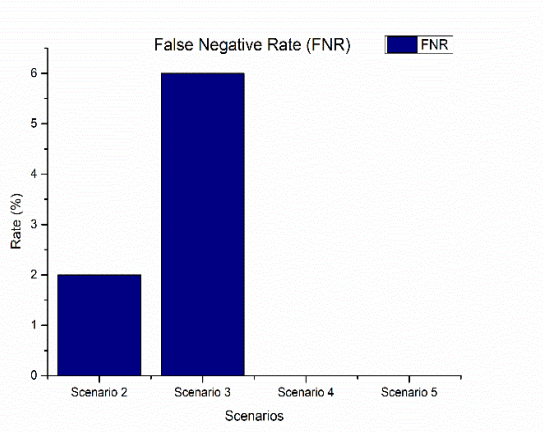

Figure III.11. Taux de faux négatifs des différents scénarios d'attaque.

Les figures III.11 et III.12 montrent respectivement le taux de vrais négatifs et le taux de faux négatifs. Pour le scénario 2, notre proposition a permis d'atteindre un taux de 98 %. Plus précisément, 92 % sont détectés au premier niveau de la solution et 6 % au deuxième niveau de la solution. Dans le scénario 2, l'attaquant peut lancer son attaque de différentes manières. Dans le premier cas, il peut envoyer ses demandes de preuve de position à partir du même endroit et au même moment. Dans le deuxième cas, il peut demander des preuves de position à partir de différents endroits. Le premier cas sera détecté automatiquement au cours de la phase 3. Le deuxième cas sera détecté lors de la phase 5. Les 2 % restants représentent le taux de faux négatifs. Pour le scénario 3, la phase 3 n'a pas pu détecter les nœuds Sybil. En revanche, les nœuds Sybil sont détectés en phase 5 avec un taux de 94 %. Dans ce scénario, l'attaquant réussira à obtenir des preuves de position pour chaque pseudonyme généré puisque la phase 3 s'appuie sur l'intensité du signal pour le positionner. D'autre part, les trajectoires de Sybil sont détectées au moment de la déclaration de l'événement. Le taux de faux négatifs pour le scénario 3 est de 6 %. Pour le scénario

4, notre mécanisme peut détecter les nœuds Sybil dans les deux phases avec un taux de vrais négatifs égal à 100 % et un taux de faux négatifs égal à 0 %. Ce scénario englobe deux cas d'attaque. Dans le premier, l'attaquant demande une preuve de position dans la phase 3 en volant un certificat à un véhicule légitime. Dans notre proposition, avant que le FN ne délivre une preuve de position, il doit contacter le SM pour vérifier la correspondance du certificat envoyé avec la clé publique de cet OBU. S'il n'y a pas de correspondance, cet OBU n'aura pas de preuve de position. Dans le deuxième cas d'attaque suivant, l'attaquant utilise un certificat volé dans la demande de rapport d'événement. Parmi les vérifications qui seront effectuées par le SM figurent la correspondance entre le pseudonyme, le certificat et la clé publique. Le scénario 4 se caractérise par une grande précision grâce à l'immuabilité de la BC. Le scénario 5 est à peu près similaire au scénario 3, mais il est davantage lié à la phase 5. La solution peut détecter les trajectoires Sybil avec un taux de vrais négatifs égal à 100 % et un taux de faux négatifs égal à 0 %. Un attaquant peut chercher à modifier ses trajectoires (générées avec ses pseudonymes) en supprimant certaines preuves de position afin de ne pas être détecté comme une trajectoire Sybil. Dans notre proposition, la vérification de la similarité des trajectoires signalant un événement figure parmi les vérifications à effectuer pour détecter les trajectoires Sybil. Dans notre proposition, toutes les preuves de position seront stockées dans la BC. En outre, une trajectoire envoyée pour signaler un événement sera validée par le SM. L'OBU ne décide pas de la trajectoire utilisée pour le rapport. Le scénario 1 peut être représenté par le taux de vrais positifs (TPR) et le taux de faux positifs (FPR). Dans la phase 3, le taux de vrais positifs peut atteindre 98 % et le taux de faux positifs 2 %. Dans la phase 5, le taux de vrais positifs peut atteindre 97%, et le taux de faux positifs est égal à 3%. Nous avons

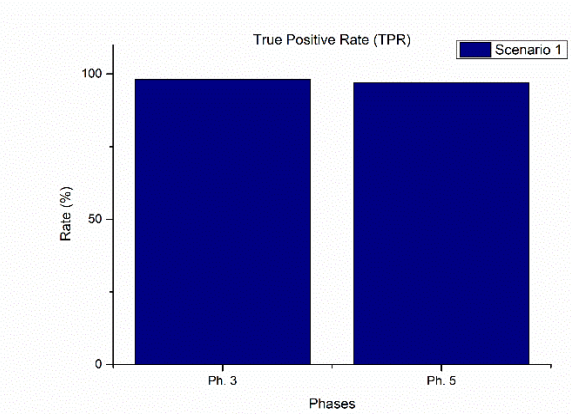

Figure III.14. Taux de vrais positifs du scénario 1**.**

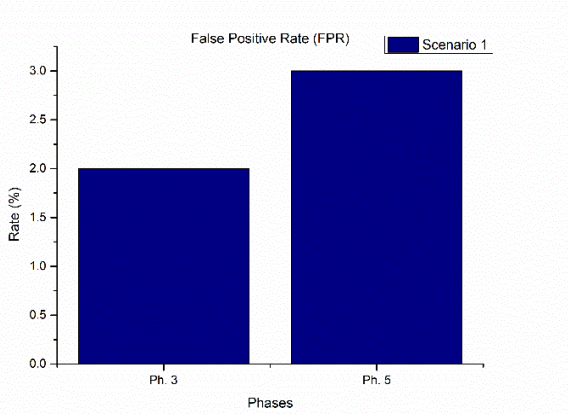

Figure III.14. Taux de faux positifs du scénario 1.

considéré que tous les véhicules bénins formaient au moins une trajectoire. Le TPR et le FPR sont présentés respectivement dans les figures III.13 et III.14.

III.5.2.2. Discussion

Notre proposition peut contrer l'attaque Sybil dans différents scénarios d'attaque, ce qui n'est pas le cas des solutions [42], [40], [41], [83] et [84]. Pour le scénario 1, la détection de l'attaque est possible dans les 6 propositions, mais notre proposition donne une meilleure précision. Le scénario 2 est détecté dans notre solution, dans [83] et [84] ; nous pouvons remarquer que notre proposition peut détecter les nœuds Sybil plus rapidement que les deux solutions [83] et [84]. En outre, la précision de notre proposition est supérieure à celle des deux travaux. Le scénario 3 est détecté dans notre solution, dans [42], [40] et [41]. Ces trois solutions n'utilisent pas le RSSI. Par conséquent, nous considérons le fait d'enregistrer un véhicule malveillant plusieurs fois (par exemple, en utilisant plusieurs matériels du même véhicule) pour obtenir des preuves de position. Ce scénario n'est détecté ni par [83] ni par [84]. Dans ces deux références, la construction des trajectoires des véhicules dépend des valeurs RSS. Plus précisément, toute erreur dans les valeurs RSS peut influencer la trajectoire des véhicules et, par conséquent, la précision de détection des nœuds Sybil. Les deux solutions ne tiennent pas compte de la modification de l'intensité du signal par l'attaquant. Dans le scénario 4, l'attaque n'est détectée que par notre proposition. Dans notre proposition, le message de demande de preuve de position et le message de rapport d'événement sont accompagnés d'une signature sur le message. Contrairement à d'autres solutions : [42], [40] et [41] où la signature n'est utilisée que pour l'horodatage du message. En outre, dans notre proposition, les certificats sont stockés dans la BC, ce qui signifie qu'ils ne seront ni modifiés ni

supprimés. Dans [83] et [84], il n'y a pas de contrôle centralisé sur les identifiants des véhicules. L'usurpation d'identité est difficile à détecter.

Scenario	[42]	[40]	[41]	[83]	[84]	Notre mécanisme
Scenario 1	✓	✓	✓	✓	✓	✓
Scenario 2	✗	✗	✗	✓	✓	✓
Scenario 3	✓	✓	✓	✗	✗	✓
Scenario 4	✗	✗	✗	✗	✗	✓
Scenario 5	✗	✗	✗	✓	✓	✓

Tableau III.4. Comparaison entre la détection dans différents scénarios.

Dans le scénario 5, les travaux [42], [40] et [41] ne détectent pas ce scénario d'attaque. Dans ces trois solutions et dans la phase de signalement des événements, il n'y a pas de contrôle sur l'historique d'une trajectoire. Plus précisément, un attaquant qui crée deux trajectoires simultanément, puis supprime une preuve de position de l'une des trajectoires, ne sera pas détecté comme une trajectoire Sybil. Dans les travaux [83] et [84], le contrôle et la détection des nœuds Sybil sont effectués uniquement par les RSU. Les OBU ne jouent aucun rôle. Une comparaison est donnée dans le tableau III.4.

III.6. Analyse des performances

Dans cette section, nous présentons, par le biais d'une comparaison approfondie, une analyse des performances en termes de communication et de coût de calcul. Le coût en temps est simulé sur la base de la bibliothèque MIRACL [89], nous menons les expériences sur un ordinateur portable équipé d'un processeur Intel(R) Core(TM) i7-8550U à 1,80 GHz et de 8,0 Go de RAM. Nous comparons notre solution avec la proposition de Baza et al. [40]. Pour une meilleure sécurité, nous utilisons SHA-256 pour H_0 et H_1, et l'algorithme de signature numérique à courbe elliptique (ECDSA) pour la signature avec une taille de clé égale à 160 bits.

III.6.1. Coût de calcul

Nous considérons la phase d'échange de messages et nous mesurons, à l'aide de la bibliothèque MIRACL, le coût de la signature utilisée dans notre travail, à savoir ECDSA, et le coût de la signature BLS à seuil utilisée dans la proposition [40]. Les résultats sont présentés dans le tableau III.5.

Protocole	**Opération**	**Temps (ms)**
ECDSA	Signature	0.15
	Vérification	0.86
BLS	Signature	0.29
	Vérification	15.88

Tableau III.5. Coût de la signature et de la vérification en ms.

Dans le mécanisme proposé, l'OBU signe une seule fois sa demande au moment où il demande une preuve de position et effectue une seule vérification après avoir reçu la preuve du FN. Cela signifie que la charge totale de l'OBU dans cette phase est de 0,15 ms + 0,86 ms. Il en va de même pour le FN qui doit vérifier la signature après avoir reçu la demande de l'OBU et procéder à une signature unique de la preuve de position, ce qui donne une surcharge de 0,15 ms + 0,86 ms. Dans [40], le RSU nécessite un coût de 16,17 t ms. En effet, le RSU doit effectuer t vérifications et t signatures pour un véhicule, ce qui représente un total de (0,29 t + 15,88 t) ms. Dans notre solution, la surcharge de calcul est fixe ; FN a besoin de 1,01 ms pour émettre une preuve de position (c'est-à-dire 990 véhicules/seconde). Contrairement à la solution [40], où la charge de calcul dépend du choix de t. Plus précisément, la charge de calcul augmente linéairement avec la valeur de t. Pour t = 4, une RSU a besoin de 64,68 ms pour émettre une preuve de position (c'est-à-dire 15 véhicules/seconde).

III.6.2. Coût de communication

Pour calculer le surcoût de communication, il est nécessaire de prendre en compte tout paquet dans le réseau effectué par une entité du réseau. Dans notre proposition, le surcoût de communication peut être divisé en deux parties principales : la communication entre les véhicules et les FN et la communication entre les FN et les véhicules. Ces résultats ont été validés pour les phases 3 et 5. Le surcoût est mesuré en octets. Le tableau III.6 présente les coûts de communication pour chaque solution.

Dans la phase 3, un message envoyé par l'OBU doit contenir un certificat obtenu auprès de l'AD de 32 octets, un pseudonyme de 32 octets, un TMP de 4 octets et une signature de demande de 40 octets. Le total du message envoyé sera donc de 108 octets. De même, dans [40], l'overhead est de 48 l + 40 t + 32 octets, où l est le nombre de RSU qu'un véhicule rencontre et t est le seuil

du protocole de signature de seuil (t, n). Une réponse du FN à l'OBU doit comprendre un certificat de 32 octets, un TMP de 4 octets, un hachage de 32 octets de la demande de l'OBU avec H_0 et une signature de 40 octets, soit un total de 108 octets. Pour la solution [40], le surcoût est de 24 *l* + 20 t.

Solution	**Taille (octet)**		
	Phase	**OBU**	**RSU / FN**
[40]	Ph. 3	48 *l* + 40 *t* + 32	24 *l* + 20 *t*
	Ph. 5	24 *l* + 20 *t* + 120 *k* + 20	/
Notre mécanisme	Ph. 3	32 + 32 + 4 + 40	32 +32+4 + 40
	Ph. 5	32 + 32 + 4 + 2 + 32 + 40	/

Tableau III.6. Comparaison des coûts de communication.

Dans la phase 5, pour rapporter un événement, l'OBU doit envoyer une requête au FN qui contient son pseudonyme de 32 octets, son certificat de 32 octets, un TMP de 4 octets, le nombre de chemins de 2 octets, le hachage de son chemin de 32 octets et une signature de 40 octets, soit un total de 142 octets. De même, le surcoût dans [40] est de 24 *l* + 20 t + 120 k + 20 octets où k représente le nombre de RSU rencontrées de telle sorte que le seuil du protocole de signature de seuil est atteint.

Dans notre proposition, la taille du message est fixe dans les deux phases 3 et 5 et ne dépend pas du nombre de FN rencontrées par l'OBU, alors que dans [40], la taille du message dépend du nombre de RSU rencontrées par l'OBU dans son trajet et dépend également du seuil défini par le protocole de signature de seuil.

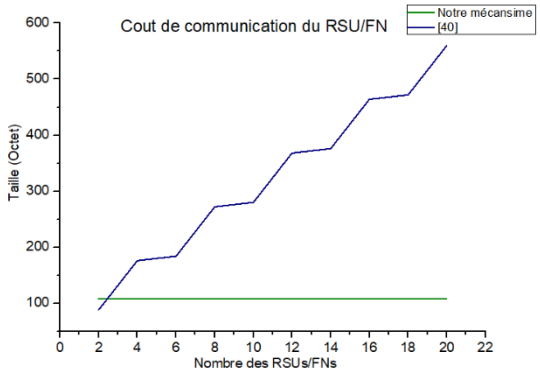

Figure III.16. Coût de communication des RSU/FN.

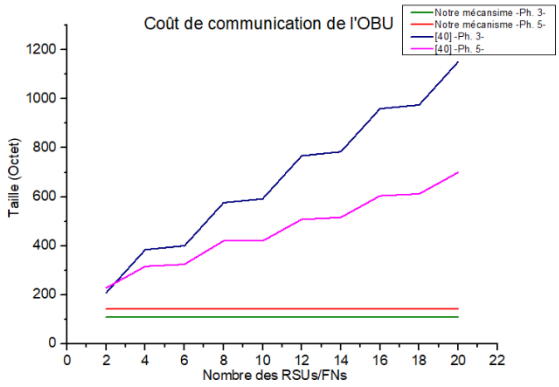

Figure III.15. Coût de communication de l'OBU.

Nous pouvons noter que notre proposition a considérablement réduit les coûts de communication pour les deux entités (FN et OBU), comme le montrent clairement les figures III.15 et III.16. Nous utilisons une valeur de 4 pour le protocole de signature de seuil (t=4).

III.7. Conclusion

L'attaque Sybil est considérée comme une attaque très dangereuse car elle peut causer des dommages mortels et des pertes financières dans les réseaux VFC. Dans ce chapitre, nous avons présenté notre mécanisme de détection de l’attaque Sybil dans les réseaux VFC. Nous avons utilisé le RSSI, la trajectoire des véhicules ainsi que la technologie Blockchain. Le FN est responsable de la fourniture de preuves de position pour les véhicules afin de former des trajectoires, qui seront utilisées dans les rapports d'événements. Avant de fournir les preuves de position, le FN doit positionner le véhicule à l'aide du RSSI. D'une part, l'utilisation du RSSI permet de détecter le cas simple d'une attaque Sybil, d'autre part, l'utilisation de la trajectoire permet de détecter une attaque Sybil dans le cas où l'attaquant modifie la valeur de transmission du signal. Cette combinaison nous permet de tirer parti des deux méthodes, ce qui accroît la précision de la détection. Notre proposition peut contrer l'attaque de compromission des FN et détecter d'autres types d'attaques telles que les attaques par rejeu et par usurpation d'identité. De plus, l'analyse des performances montre la rentabilité du mécanisme proposé en termes de calcul et de communication.

Chapitre IV : Deuxième contribution : Mécanisme d’authentification préservant conditionnellement la vie privée

IV.1. Introduction

Avec l'émergence des réseaux VFC, le système de transport améliore de plus en plus la gestion du trafic et la sécurité routière. Cependant, des transmissions de données sûres et fiables sont devenues cruciales pour garantir une meilleure qualité de service. Dans ce contexte, plusieurs systèmes d'authentification conditionnelle préservant la vie privée ont été proposés. Dans ce chapitre, nous présentons notre deuxième contribution [90] qui représente un mécanisme d'authentification conditionnelle préservant la vie privée pour les réseaux VFC. L'évaluation des performances et l'analyse de la sécurité montrent que notre mécanisme proposé fournit des caractéristiques de sécurité améliorées par rapport aux travaux connexes avec une réduction des coûts de calcul et de communication.

IV.2. Motivation

Parmi les exigences de sécurité des réseaux VFC, on trouve l'intégrité, la confidentialité, la disponibilité, l'anonymat et l'authentification [91]. Les véhicules doivent utiliser des identités anonymes à la place de leurs identités réelles afin d'éviter la compromission du conducteur. L'anonymat doit être conditionnel, ce qui signifie que seule l'autorité de confiance (Trusted Authority ou TA) peut identifier un véhicule qui agit de manière malveillante [92]. La fonction qui permet de cacher l'identité d'un véhicule à tout le monde, sauf à l'autorité de confiance, est appelée préservation conditionnelle de la vie privée. Dans la littérature, la plupart des schémas souffrent de problèmes de séquestre de clés. Même les schémas qui répondent à cette préoccupation se heurtent au problème du stockage et de la centralisation, puisque l'autorité de confiance doit enregistrer pour chaque véhicule tous les pseudonymes qui seront utilisés. De même, le véhicule doit stocker tous les pseudonymes et les clés qui seront utilisés dans sa mémoire.

Dans ce qui suit, nous allons présenter notre mécanisme d'authentification conditionnelle préservant la vie privée, qui permet au véhicule de générer ses propres clés privées/publiques avec son pseudonyme, sans qu'elles soient stockées auprès de la TA. La proposition utilise la cryptographie sur les courbes elliptiques pour l'authentification et la technologie blockchain pour stocker les résultats d'enregistrement et d'authentification.

IV.3. Contexte

IV.3.1. Chaine de hachage

Une fonction de hachage à sens unique *h* est une fonction qui fait correspondre un message m de taille arbitraire à un message de taille fixe appelé condensé d : d= *h*(m). L'une de ses caractéristiques est la non-réversibilité ; plus précisément, un adversaire qui connaît m peut facilement calculer son hachage : d= *h* (m), mais un adversaire qui connaît d ne peut jamais calculer m : m= h^{-1}(d).

Une chaîne de hachage est l'application successive d'une fonction de hachage à un message m. Une chaîne de hachage de longueur L, notée h^{L}(m), est l'application de la fonction de hachage au message m, L fois [93]. Par exemple, si L=3, le calcul sera le suivant : h^{3}(m) = d3 ; tel que :

h(m)=d1

h(d1)=d2

h(d2)=d3.

IV.3.2. Modèle du réseau

Notre modèle de réseau est présenté par la figure IV.1. Le système se compose de cinq entités :

- **Autorité de confiance (TA) :** Son rôle est d'initialiser le système et d'enregistrer les OBU et les SM. La TA est la seule entité qui connait la véritable identité d'un OBU, ce qui lui permet d'identifier les OBU malveillants. Elle se caractérise par une grande capacité de calcul et de communication.

- **Unité embarquée (OBU) :** Les équipements et les capteurs qui sont déployés dans les véhicules pour effectuer différentes interactions sont connus sous le nom d'OBU. Ils permettent le stockage des données, le calcul et la communication avec différentes entités du réseau. Dans ce chapitre, les OBU font référence aux véhicules qui doivent être enregistrés et authentifiés pour utiliser les services offerts par les FN.

- **Nœud Fog (FN) :** Il s'agit d'une infrastructure déployée sur le bord de la route. Il dispose de capacités de calcul et de stockage suffisantes. Il fournit des services de Fog véhiculaire (Vehicular Fog Services ou VFS) aux véhicules authentifiés.

•**Gestionnaire de services (SM) :** Le réseau est divisé en régions. Le SM est le gestionnaire de service d'une région et doit être enregistré auprès de la TA. Il est principalement responsable de l'authentification des OBU dans sa région. Chaque SM tient un registre public qui contient tous les enregistrements des véhicules.

•**Pair témoin (WP) :** Le WP est un pair qui utilise un algorithme consensus pour écrire les résultats de l'authentification dans la BC. Une BC de consortium est formée par tous les WP et SM. Chaque région a son propre WP ; chaque région contient un SM, un WP et plusieurs FN.

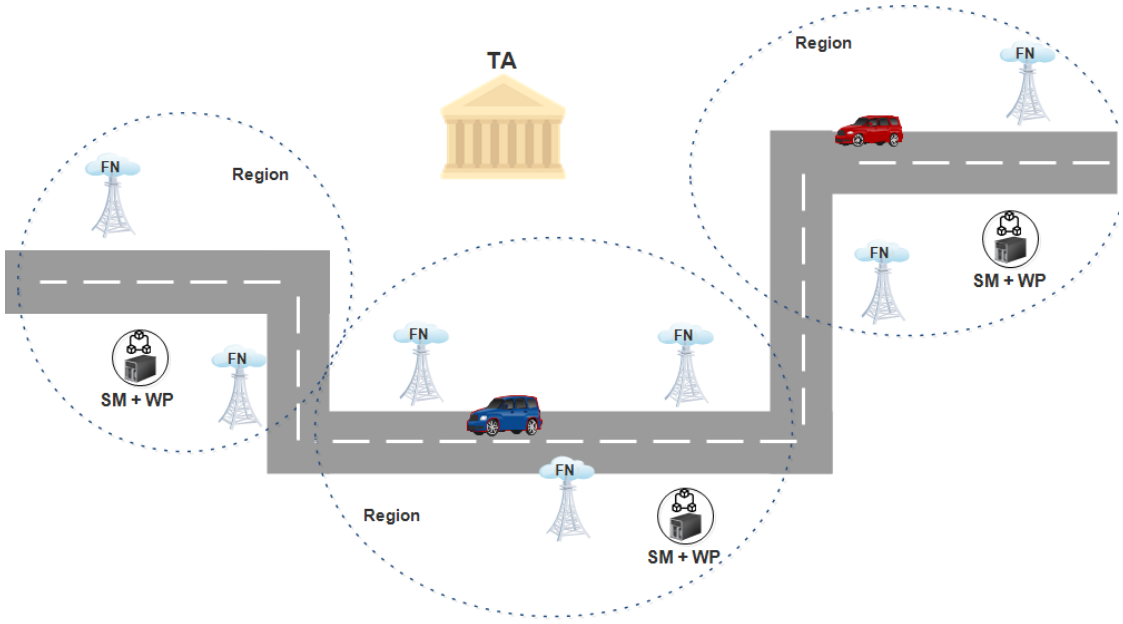

Figure IV.1. Le modèle de réseau utilisé dans notre mécanisme.

IV.3.3. Modèle de sécurité

Dans notre mécanisme, nous prenons en compte les hypothèses suivantes :

- Les SM sont considérés comme des entités de confiance, ils sont physiquement protégés et disposent d'une grande capacité de calcul.
- La BC n'est accessible qu'à la TA, au SM et au WP.
- La communication entre les différentes entités du réseau est publique et non sécurisée.
- Un adversaire Adv peut lancer différentes attaques, notamment des attaques par rejeu, des attaques Sybil et des attaques DDoS.

IV.4. Notre mécanisme proposé

Le mécanisme d'authentification comprend cinq phases : la phase d'initialisation, la phase d'enregistrement, la phase d'authentification, la phase de consensus et la phase de prestation de services.

a) Phase d'initialisation :

Dans cette phase, la TA exécute les étapes suivantes pour produire et publier les paramètres publics du système.

- **Étape 1 :**

- La TA choisit une courbe elliptique E définie par (IV.1) :

$$E : y^2 = x^3 + ax + b \ (mod\ p) \qquad (IV.1)$$

- **Étape 2 :**

- La TA génère aléatoirement une clé secrète SK_{TA} qui appartient à $\mathbb{Z}_q^*$. Elle calcule la clé publique : $PK_{TA}=SK_{TA}.P$

- **Étape 3 :**

- Elle choisit une fonction de hachage : h_0 et h_1 telle que :

$h_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$

$h_1 : \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$.

- TA garde le SK_{TA} secret et publie les paramètres suivants : Para = (p, q, P, G, PK_{TA}, h_0), tel que P est le point de base d'ordre q et P le générateur du groupe cyclique G.

b) **Phase d'enregistrement :**

- La TA est responsable de l'enregistrement des OBU et des SM via un canal sécurisé. Les détails de cette phase sont montrés sur les figures IV.2 et IV.3 respectivement et sont les suivants :

1) Enregistrement de l'OBU :

- **Étape 1 :**

- En utilisant PK_{TA}, l'OBU chiffre son identité réelle RID et l'envoie à la TA : E_{OBU} = Enc_PK_{TA} (RID).

- **Étape 2 :**

- La TA décrypte E_{OBU} à l'aide de la SK_{TA} pour extraire le RID.

- Elle choisit deux nombres aléatoires r_1 et r_2 qui appartiennent à $\mathbb{Z}_q^*$. r_1 et r_2 sont deux nombres qui seront utilisés pour générer les pseudonymes de l'OBU. La paire (r_1, r_2) est unique.

- Elle calcule un jeton (Tk) comme suit : $Tk = h_1 (SK_{TA} \| r_1 \| r_2) \oplus h_0(RID)$

- La TA enregistre dans sa base de données (BD) : <RID, r_1, r_2 et Tk>.

- Elle enregistre dans la BC : <r_1, r_2 et Tk>.

- La TA envoie à l'OBU : <r_1, r_2 et Tk>.

- **Étape 3 :**

- L'OBU enregistre dans son BD <r_1, r_2 et Tk>.

OBU	**TA**
- Crypter RID : E_{OBU}=Enc_PK_{TA}(RID) - Envoyer E_{OBU} →	
	- Décrypter : $Dec\_SK_{TA}(E_{OBU})$ - Choisir (r_1, r_2) ∈ $\mathbb{Z}_q$* - Calculer : Token = $h_1(SK_{TA} \| r_1 \| r_2) \oplus h_0(RID)$ - Enregistrer sur son Base de données : <RID, r_1, r_2, Token) - Enregistrer dans la BC : <r_1, r_2, Token> - Envoyer <r_1, r_2, Token> ←
- Enregistrer <r_1, r_2, Token>	

Figure IV.2. Phase d'enregistrement - Enregistrement des OBU -.

2) Enregistrement du SM :

- **Étape 1 :**

- RID_{SM} est l'identifiant du SM

- Il choisit aléatoirement sa clé privée SK_{SM}.

- Il calcule la clé publique : $PK_{SM}=SK_{SM}.P$

- Il calcule : $E_{SM} = Enc\_PK_{TA} (RID_{SM} || PK_{SM})$, et il envoie E_{SM} à la TA.

- **Étape 2 :**

- La TA décrypte E_{SM} pour récupérer le RID_{SM} et le PK_{SM}.

- Elle calcule un Tk pour le SM comme suit : $Tk_{SM} = h_1 (SK_{TA} || PK_{SM}) \oplus h_0(RID_{SM})$

- Elle stocke dans la BC : $<RID_{SM}, PK_{SM}, Tk_{SM}>$.

- Elle envoie Tk_{SM} à SM.

- **Étape 3 :**

- SM enregistre dans sa base de données $<Tk_{SM}>$.

SM	**TA**
- Générer la clé privée $SK_{SM} \in \mathbb{Z}_n^*$ - Calculer la clé publique $PK_{SM}=SK_{SM}.P$ - Crypter son RID_{SM}: $E_{SM}=Enc\_PK_{TA}(RID_{SM} \| PK_{SM})$ - Envoyer E_{SM} →	
	- Décrypter : $Dec\_SK_{TA}(E_{SM})$ - Calculer : $Token_{SM} = h_1(SK_{TA} \| PK_{SM}) \oplus h_0(RID_{SM})$ - Enregistrer dans la BC: $<RID_{SM}, PK_{SM}, Token_{SM}>$ - Envoyer $<Token_{SM}>$ ←
- Enregistrer $< Token_{SM} >$	

Figure IV.3. Phase d'enregistrement - Enregistrement des SM -.

c) Phase d'authentification

Un OBU qui souhaite accéder aux services fournis par les FN doit être authentifié. Les FN ne sont pas protégés physiquement, ce qui les rend plus vulnérables aux attaques par compromission physique [91]. Toutefois, les FN jouent le rôle de relais entre les OBU et les SM dans cette phase. Le SM diffuse le résultat de l'authentification à tous les WP pour qu'ils l'inscrivent dans la BC. Les étapes à suivre par un OBU pour être authentifié sont illustrées à la figure IV.4 et elles sont les suivantes :

- **Étape 1 :**

- L'OBU génère ses clés ; il choisit au hasard un nombre SK_{OBU} qui appartient à $\mathbb{Z}_q^*$.

- Il calcule : $PK_{OBU} = SK_{OBU}.P$

- Il génère son pseudonyme :

$W = PK_{OBU} \bmod r_1$

$S1 = h_0(r_1)$

$S2 = h_0^w (r_2)$

$PID_{OBU} = h_0(S1 \oplus S2)$. Lorsque l'OBU génère de nouvelles clés, le pseudonyme change également sans être lié.

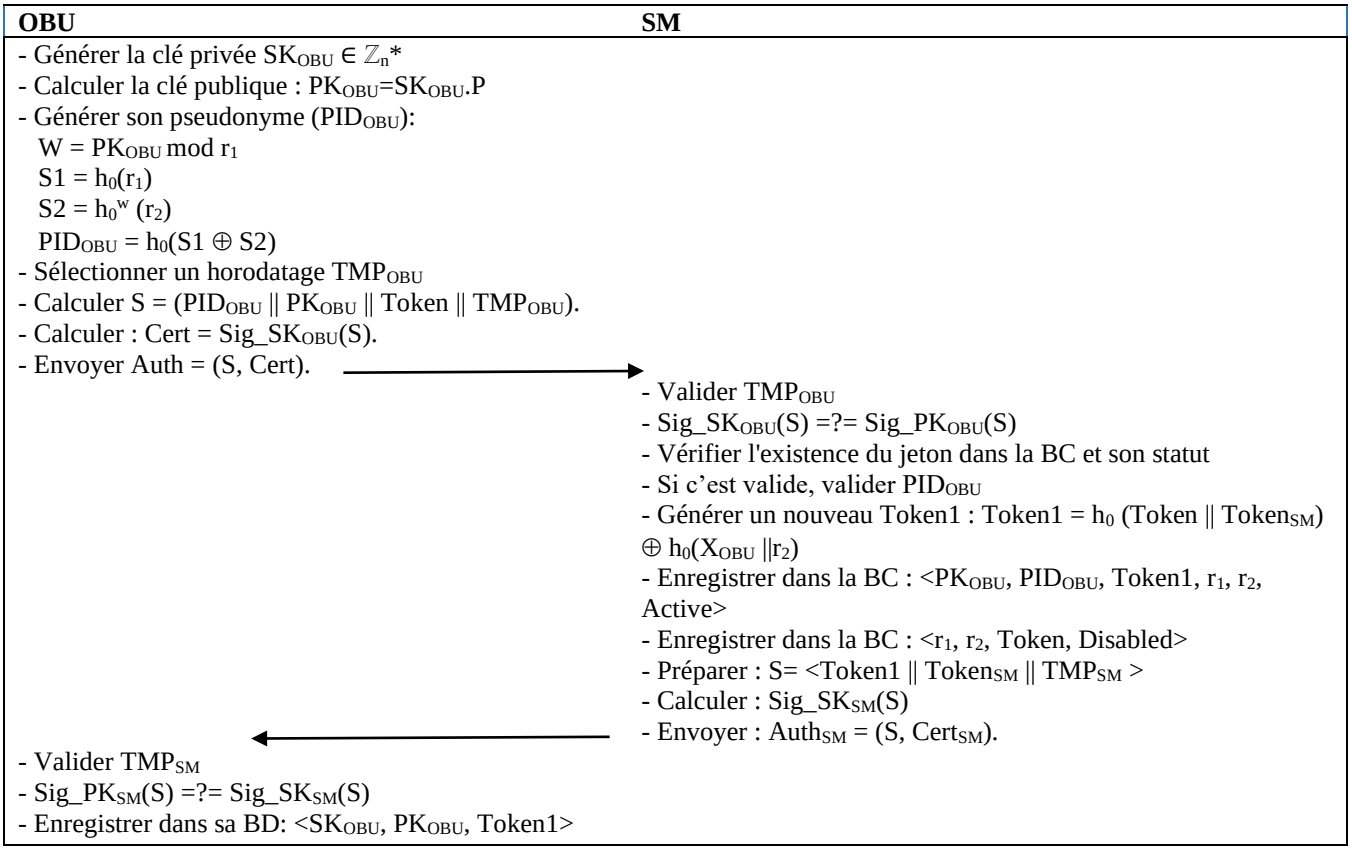

Figure IV.4. Phase d'authentification.

- Sélectionnez l'horodatage TMP_{OBU}. Cet horodatage permet de dater le message relayé et de s'assurer qu'il ne sera pas relayé à nouveau prochainement.

- Il concatène le pseudonyme généré, avec PK_{OBU}, et le TMP : $S = (PID_{OBU} || PK_{OBU} || Tk || TMP_{OBU})$.

- Pour garantir l'intégrité du message, l'OBU calcule une signature sur S : Cert = $Sig\_SK_{OBU}(S)$.

- Il envoie une demande d'authentification au SM qui contient S et la signature : Auth = (S, Cert).

- **Étape 2 :** À la réception de Auth, le SM effectue une série de vérifications :

- Tout d'abord, il vérifie la validité du TMP_{OBU}, s'il n'entre pas dans la fenêtre temporelle autorisée, la connexion est interrompue, sinon, il poursuit ses vérifications.

- Sur la base de la PK_{OBU} reçue dans Auth, il calcule $Sig\_PK_{OBU}(S)$ pour vérifier l'intégrité du message. S'il est égal à $Sig\_SK_{OBU}(S)$, il poursuit ses vérifications, sinon il met fin à la connexion.

- Il recherche dans la BC le Tk reçu pour savoir si cet OBU est déjà enregistré et, s'il existe, il vérifie l'état de la ligne. L'état peut être "actif", "désactivé" ou "révoqué". Actif signifie que cet OBU a déjà un jeton et des clés en cours d'utilisation. Désactivé signifie que cet OBU utilise un autre Tk et que le Tk recherché n'est plus valide. Révoqué signifie que cet OBU a été signalé à la TA et qu'il est révoqué.

- S'il est révoqué ou désactivé, il met fin à la connexion, sinon il suit les étapes pour enregistrer une nouvelle ligne.

- Il calcule le PID' (sur la base de r_1, r_2 et du PK_{OBU} reçu) si PID' = PID_{OBU}, l'OBU est marqué comme étant authentifié.

- Il génère un nouveau $Tk_1 = h_0 (Tk \,||\, Tk_{SM}) \oplus h_0(X_{OBU} \,||r_2)$ où X_{OBU} est l'abscisse du point PK_{OBU}.

- Il enregistre dans la BC : (PK_{OBU}, PID_{OBU}, Tk_1, r_1, r_2, Active).

- Il enregistre dans la BC la ligne du premier Tk avec un état désactivé pour éviter que l'OBU n'utilise plusieurs pseudonymes en parallèle.

- Il prépare S : $S= <Tk_1 \,||\, Tk_{SM} \,||\, TMP_{SM} >$

- Il calcule une signature sur S en utilisant son SK_{SM} : $Cert_{SM} = Sig\_SK_{SM}(S)$ pour garantir l'intégrité du message.

- Il envoie à l'OBU : $Auth_{SM} = (S, Cert_{SM})$.

- **Étape 3 :**

- A la réception de $Auth_{SM}$, l'OBU vérifie la validité du TMP_{SM}.

- Il vérifie l'intégrité du message et calcule $Sig\_PK_{SM}(S)$. S'il est égal à $Sig\_SK_{SM}(S)$ reçu dans le message, il enregistre dans sa base de données : SK_{OBU}, PK_{OBU} et Tk_1.

d) Phase de consensus :

Après avoir reçu les résultats de l'authentification, les WP les enregistrent dans la BC par le biais de l'algorithme de consensus. Dans notre mécanisme, nous utilisons la blockchain du consortium avec l'algorithme de consensus PBFT. Cet algorithme est considéré comme un algorithme efficace pour l'authentification sécurisée dans les réseaux véhiculaires [94]. Nous supposons qu'il y a x WP dans le réseau ; l'initiateur du processus de consensus est un WP nommé "Speaker", tandis que les autres sont des membres du congrès qui participent au vote initié par le "Speaker". Les étapes du consensus sont les suivantes :

- **Étape 1 :** la formule suivante permet de sélectionner un speaker Sp : $Sp = (Bloc_i \bmod x) + 1$, $Bloc_i$ représentant l'indice de bloc actuel.

- **Étape 2 :** après l'authentification d'un OBU, le SM diffuse les résultats de l'authentification aux WP pour qu'ils les stockent dans leurs mémoires. Après un temps t, qui est déjà défini comme le temps nécessaire pour générer un bloc, un nouveau bloc est généré.

- **Étape 3 :** Sp demande aux membres du congrès de voter en utilisant la requête suivante : <request, $Bloc_i$, Sp, Block, Sig_SK_{WP}(Block)> où "request" désigne la demande de vote, "Block" désigne le bloc lui-même, et Sig_SK_{WP}(Block) désigne la signature créée sur le bloc.

- **Étape 4 :** La demande est envoyée aux membres du congrès sous la forme d'un message de préparation. Une réponse est envoyée par le bon WP sous la forme d'un message Prepare à tous les autres membres.
- **Étape 5 :** Après 2m messages de préparation, les membres du congrès se prononcent contre la demande Sp et envoient un message de validation f à tous les autres membres.
- **Étape 6 :** après avoir reçu 2f + 1 messages de validation associés, le ième WP partage son vote : <Vote, $Bloc_i$, WP, Block, Sig_SK_{WP}(Block)> où vote représente la décision du vote, WP est l'identifiant du WP.
- **Étape 7 :** Lorsque le Sp reçoit la réponse des membres du congrès, le nouveau bloc est ajouté.

e) Phase de prestation du service :

Lorsqu'un OBU se déplace à une autre région, il doit rester authentifié de manière transparente. Dans ce cas, l'OBU doit envoyer une demande qui prouve son authentification.

- **Étape 1 :**

- L'OBU doit sélectionner un nouveau TMP.

- Il le concatène avec le dernier token utilisé : D = <Tk_1 || TMP>

- Il calcule la signature de D : Cert=Sig_SK_{OBU} (D)

- Il envoie au nouveau SM : Auth = <D || Cert>.

- **Étape 2 :**

- Le SM doit vérifier la validité de la TMP reçue. S'il est valide, il continue les vérifications, sinon il met fin à la connexion.

- Il vérifie l'intégrité du message en calculant Sig_PK_{OBU}(D), s'il est égal à Sig_SK_{OBU}(D) reçu avec le message il passe à l'étape suivante, sinon il met fin à la connexion.

- Il recherche dans la BC le Tk_1 envoyé par l'OBU et vérifie l'état de la ligne. S'il est désactivé ou révoqué, il met fin à la connexion, sinon il authentifie l'OBU.

Au cours du processus d'authentification, si un véhicule illégal est signalé à la TA, la TA accède au BC, découvre son identité réelle et enregistre une nouvelle ligne avec le dernier Tk' (r_1, r_2, Tk, Révoqué). En révoquant les deux nombres r_1 et r_2, l'OBU ne peut plus accéder au réseau.

IV.5. Analyse de la sécurité et de la protection de la vie privée

- **Anonymat :** Pour garantir l'anonymat, chaque véhicule est supposé utiliser un pseudonyme au lieu de son identité réelle. Lors de la phase d'authentification, le véhicule génère un pseudonyme qui n'a aucun rapport avec son identité réelle. Par conséquent, un Adv ne peut jamais extraire l'identité réelle du véhicule. En outre, lorsqu'un SM veut vérifier la validité du pseudonyme généré, il se base sur (r_1, r_2). Il n'a pas besoin de connaître l'identité réelle du véhicule, ce qui satisfait à la préservation conditionnelle de la vie privée.

- **Traçabilité et révocation :** Dans notre proposition, lorsqu'un véhicule avec un comportement malveillant est signalé à la TA, la TA accède à la BC et enregistre (r_1, r_2) comme révoqué.
- **Non-liaison :** Les pseudonymes et les clés privées/publiques sont fréquemment mis à jour par le véhicule. Mais la paire (r_1, r_2) reste non modifiable et n'est connue que de la TA, des SM et du véhicule lui-même. Un Adv ne peut pas distinguer si deux messages (contenant un pseudonyme et une clé publique) envoyés à l'instant t et t+1 sont envoyés par le même véhicule ou non.

- **Confidentialité :** Dans la phase d'enregistrement, la TA envoie au véhicule une paire (r_1, r_2) pour générer des pseudonymes. r_1 et r_2 sont envoyés via un canal sécurisé et ne sont connus que par la TA, des SM et du véhicule. Dans la phase d'authentification, r_1 et r_2 sont utilisés pour la génération de pseudonymes et ne seront jamais envoyés. Un Adv qui tenterait d'analyser un pseudonyme pour en extraire r_1 et r_2 n'y parviendrait jamais en raison de la fonction de hachage à sens unique utilisée.

- **Résilience du séquestre des clés :** La seule entité qui connaît la clé privée de l'OBU est le véhicule lui-même. Personne d'autre n'est capable d'imiter le véhicule.

- **Authentification mutuelle :** Dans la phase d'authentification, le SM authentifie le véhicule après avoir vérifié l'intégrité du message, l'existence du jeton et la validité du pseudonyme généré. Le véhicule vérifie l'authenticité du message reçu du SM en calculant $Sig\_PK_{SM}(S)$ s'il est égal à la signature reçue avec le message, le SM est authentique.

- **Attaque par rejeu :** Chaque message envoyé dans notre proposition est lié à un horodatage. Le destinataire du message doit vérifier la validité de cet horodatage dans un premier temps. Un Adv qui utilise un message déjà envoyé et change l'horodatage par un autre plus récent sera détecté par la signature du message authentique jointe à la demande.

- **Attaque DDoS :** Dans notre proposition, le modèle de réseau considéré consiste en plusieurs SM formant un réseau distribué. Par conséquent, le succès d'une attaque DDoS n'a pas d'influence sur l'ensemble du réseau, elle peut ne toucher qu'un seul nœud.

- **Attaque de l'homme du milieu :** Dans la phase d'authentification, un véhicule doit envoyer une demande d'authentification qui contient un pseudonyme généré, une clé publique, le jeton obtenu de la TA et un horodatage. Un Adv qui voudrait lancer une attaque de type "man-in-the-middle" n'y parviendrait pas. Il ne peut générer au hasard ni le pseudonyme ni le jeton d'authentification. Le SM recalculera le pseudonyme sur la base de r_1 et r_2 ; il vérifiera l'existence du jeton dans la BC. En outre, Adv ne peut modifier ou supprimer aucune information de la demande car toute modification sera détectable en raison de la signature attachée à la demande.

	[59]	**[70]**	**Notre mécanisme**
Confidentialité	✓	✓	✓
Anonymat	✓	✓	✓
Traçabilité	✓	✓	✓
Non-liaison	✓	✗	✓
Authentification mutuelle	✗	✓	✓
Attaque de l'homme du milieu	✓	✓	✓
Attaque par rejeu	✓	✓	✓
Résilience du séquestre des clés	✓	✗	✓
Attaque DDoS	✗	✓	✓
Attaque Sybil	✗	✗	✓

Tableau IV.1. Comparaison des caractéristiques de sécurité entre le mécanisme que nous proposons, [59] et [70].

- **Attaque Sybil :** Chaque véhicule peut générer un nouveau pseudonyme (avec des clés privées/publiques) à tout moment. Cette caractéristique peut encourager les véhicules malveillants

à l'exploiter pour lancer une attaque Sybil et, par conséquent, faire échouer le réseau VFC très rapidement. Dans notre proposition, après chaque nouvelle demande d'authentification, le SM marque l'ancien pseudonyme dans la BC comme désactivé afin qu'il ne soit jamais utilisé dans les communications futures.

Le tableau IV.1 représente une comparaison en termes de sécurité de notre système avec [59] et [70]. Nous pouvons noter que notre mécanisme offre plus de caractéristiques de sécurité que les autres. Pour la solution [59], il manque l'authentification mutuelle et l'attaque DDoS. Pour la solution [70], il manque la dissociabilité et le séquestre des clés. En outre, aucune de ces solutions ne permet de contrer l'attaque Sybil.

IV.6. Evaluation des performances

Dans cette section, nous analysons le coût de calcul et de communication de notre mécanisme par rapport à [59] et [70]. À cette fin, nous considérons les trois phases suivantes : la phase d'enregistrement, la phase d'authentification et la phase de prestation du service. Pour évaluer les performances, nous utilisons la bibliothèque MIRACL [89]. Les expériences sont réalisées sur un ordinateur portable équipé d'un Intel(R) Core(TM) i7-8550U @ 1,80 GHz et de 8,0 Go de RAM.

IV.6.1. Coût de calcul

Pour mesurer les coûts de calcul, le temps d'exécution des opérations prises en compte dans cette sous-section est indiqué dans le tableau IV.2. Les opérations qui ne figurent pas dans le tableau sont considérées comme négligeables. Nous utilisons la fonction de hachage SHA-256 et l'algorithme de signature numérique à courbe elliptique (ECDSA) pour la signature avec une taille de clé de 160 bits.

Dans notre proposition, l'OBU ne doit effectuer que $2T_h$ pour s'enregistrer. Cela donne un temps total égal à 0,024 ms. Pour la solution [59], un OBU doit effectuer $4T_h + 3T_{Mecc} + 1T_{Aecc}$, soit un total de 1,97 ms. Dans la solution [70], l'OBU doit effectuer $5T_h + 2T_{Mecc}$, ce qui donne un coût total en temps de 1,3 ms.

Abréviation	Description	Temps (ms)
T_h	Fonction de hachage à sens unique	0.012
T_{Mecc}	Multiplication de points ECC	0.62
T_{Aecc}	Addition de points ECC	0.062
Sig	Signature ECDSA	0.14
Ver	Vérification ECDSA	0.84
Kdf	Fonction de dérivation de clé	0.048

Tableau IV.2. Le coût de calcul des opérations cryptographiques.

Pour authentifier un OBU dans notre proposition, il doit effectuer $8T_h + T_{Mecc} + 2Sig + 2Ver$. Le coût total est donc de 2,676 ms. Pour la proposition [59], l'OBU doit effectuer $4T_{Mecc} + 5T_{Aecc} + 3T_h$ avec un total égal à 2,826 ms. Dans la proposition [70], l'OBU doit effectuer $5T_h + 6T_{Mecc} + 2Kdf$, ce qui donne un coût total égal à 3,876 ms.

Les opérations à effectuer par un OBU dans la phase de prestation du service sont seulement 1Sig + 1Ver. Le coût de ces deux opérations est de 0,98 ms. Contrairement à la solution [70] qui nécessite $8T_h + 2T_{Mecc} + 2Kdf$, avec un total égal à 1,432 ms.

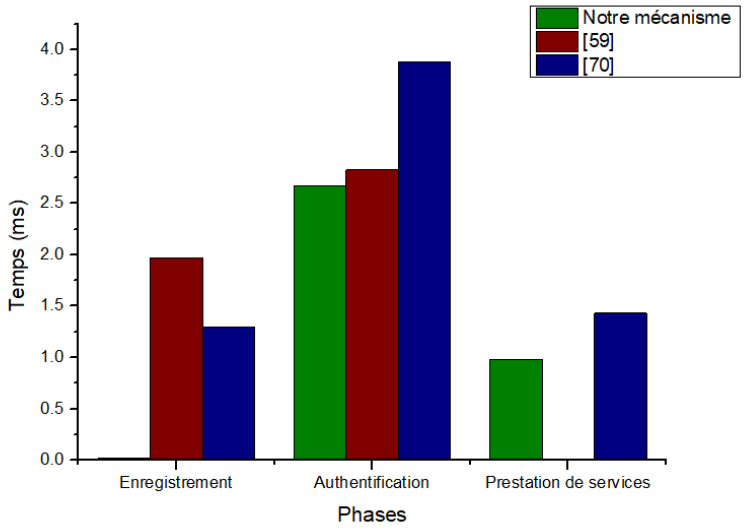

Figure IV.5. Comparaison des coûts de calcul.

Comme montre la figure IV.5, nous pouvons noter que notre proposition a un coût de calcul minimal par rapport aux deux autres propositions pour les trois phases.

IV.6.2. Coût de communication

Pour évaluer les coûts de communication, nous considérons le nombre de jetons transmis entre les nœuds au cours des trois phases. Dans cette section, le mot "jeton" ne fait pas référence au jeton d'authentification que nous avons utilisé, mais plutôt à la quantité d'informations par demande. Pendant la phase d'enregistrement, les jetons envoyés dans notre proposition sont les suivants : <RID, r_1, r_2, Token>. Par conséquent, le nombre total de jetons envoyés est de 4 jetons. Contrairement à la solution [59] qui envoie 6 jetons et à la solution [70] qui en envoie 7. Dans la phase d'authentification, les jetons envoyés dans notre proposition sont les suivants : <S, Tk, Tk_1, Tk_{SM}, TMP_{SM}>. Cela donne un total de 5 jetons. Dans la proposition [59], le nombre de jetons envoyés est de 4 jetons ; et dans la proposition [70], le nombre de jetons envoyés est de 7 jetons. Dans la phase de prestation de services, il n'y a qu'un seul jeton envoyé dans notre proposition, à savoir : <D>. En revanche, il y a 10 jetons dans la solution [70]. Nous comparons le nombre total de jetons échangés dans notre mécanisme avec les deux autres propositions. Notre mécanisme nécessite 10 jetons au total pour les trois phases. Dans [59], la proposition nécessite 10 jetons au total, mais nous ne considérons que deux phases. Le mécanisme EASBD [70] nécessite 24 jetons pour les trois phases. Nous pouvons noter que notre proposition est capable de réduire le nombre de jetons échangés par rapport aux autres. La comparaison est illustrée à la figure IV.6.

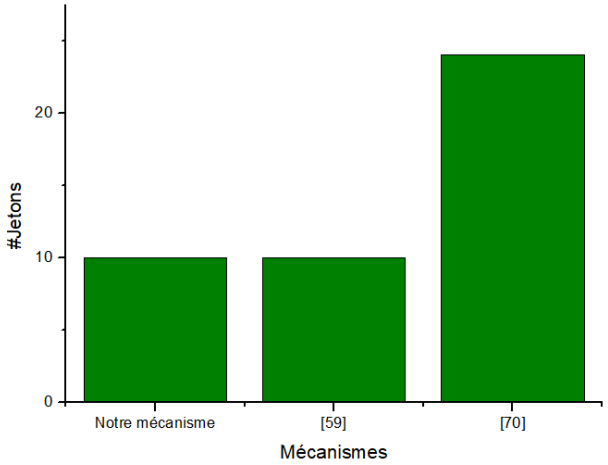

Figure IV.6. Comparaison des coûts de communication.

IV.7. Conclusion

Dans ce chapitre, nous avons présenté notre mécanisme d'authentification pour les réseaux VFC avec une préservation conditionnelle de la vie privée. La proposition utilise la cryptographie à courbe elliptique pour l'authentification et la technologie blockchain pour stocker les résultats de l'authentification. Notre mécanisme a pu résoudre le problème du séquestre de clés, il donne aussi un ensemble d'avantages, en particulier en ce qui concerne les attaques contrées, ce qui a été démontré par une analyse de sécurité. L'évaluation des performances a montré que notre mécanisme est efficace en termes de communication et de coût de calcul.

Conclusion générale et perspectives

Les réseaux VFC sont conçus principalement pour assurer la sécurité et la sûreté des conducteurs en diffusant des informations vitales dans le réseau. Cependant, l'utilisation de communications sans fil ouvertes expose les propriétaires de véhicules à des risques de sécurité et de violation de la confidentialité. Les réseaux VFC, en tant que nouveau paradigme, sont vulnérables à diverses attaques potentielles. Afin de garantir la confiance des utilisateurs, il est crucial que les réseaux VFC offrent des services fiables et sécurisés. Dans le cadre de cette thèse, nous avons proposé deux solutions axées sur la sécurité et la préservation de la vie privée des utilisateurs au sein d'un réseau VFC. La première solution consiste en un mécanisme de détection des attaques Sybil, tandis que la deuxième solution offre un mécanisme d'authentification.

L'attaque Sybil est largement reconnue comme une menace grave dans les réseaux VFC, pouvant entraîner des dommages considérables, tant sur le plan humain que financier. Dans notre première contribution, nous avons développé un mécanisme de détection de l'attaque Sybil spécifiquement conçu pour les réseaux VFC. Pour ce faire, nous avons utilisé une approche combinant le RSSI, la trajectoire des véhicules et la technologie Blockchain. Cette combinaison offre plusieurs avantages. D'une part, l'utilisation du RSSI permet de détecter les cas simples d'attaques Sybil. D'autre part, l'utilisation de la trajectoire permet de détecter les attaques Sybil plus sophistiquées, où l'attaquant altère la valeur de transmission du signal. En combinant ces deux méthodes, nous améliorons considérablement la précision de la détection. De plus, nos évaluations de performance ont démontré que le mécanisme proposé est à la fois rentable en termes de calcul et de communication, ce qui en fait une solution efficace pour contrer les attaques Sybil au sein des réseaux VFC.

Dans notre deuxième contribution, nous avons développé un mécanisme d'authentification pour les réseaux VFC, qui assure une préservation conditionnelle de la vie privée. Notre proposition repose sur l'utilisation de la cryptographie à courbe elliptique pour l'authentification des entités, ainsi que sur la technologie blockchain pour stocker de manière sécurisée les résultats de l'authentification. Nous avons réussi à résoudre le problème du séquestre de clés, qui est une préoccupation majeure dans le contexte d’authentification. L'évaluation des performances de notre mécanisme d'authentification a révélé son efficacité en termes de communication et de coût de

calcul. Il s'est avéré être une solution pratique et rentable pour assurer l'authentification sécurisée des entités au sein des réseaux VFC.

Comme perspective, nous envisageons d'explorer l'incidence de l'utilisation de la technologie blockchain sur nos propositions, en mettant l'accent sur le temps de réponse. Notre objectif principal sera d'étudier spécifiquement le temps nécessaire à la blockchain pour effectuer une recherche d'informations, en particulier lorsque le réseau s'étend (c'est-à-dire la scalabilité). Cette perspective nous permettra d'évaluer l'efficacité et les performances de l'utilisation de la blockchain dans nos propositions, tout en tenant compte des défis liés à l'expansion du réseau. Nous avons également pour objectif d'incorporer d'autres techniques cryptographiques dans le mécanisme d'authentification afin de simplifier le processus d'authentification et de l'adapter aux nouvelles générations des réseaux, tels que la 5G.

Liste des publications

- **Articles de revues internationales**

  - S. Benadla, O. R. Merad-Boudia, S. M. Senouci, et M. Lehsaini, « Detecting Sybil Attacks in Vehicular Fog Networks Using RSSI and Blockchain », *IEEE Trans. Netw. Serv. Manag.*, vol. 19, nº 4, p. 3919-3935, déc. 2022, doi: 10.1109/TNSM.2022.3216073. Revue de classe A (Impact Factor = 4.758).

- **Articles d'actes de conférences internationales**

  - S. Benadla et O. R. Merad-Boudia, « The Impact of Sybil Attacks on Vehicular Fog Networks », in *2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI)*, Tebessa, Algeria: IEEE, sept. 2021, p. 1-6. doi: 10.1109/ICRAMI52622.2021.9585965.

  - S. Benadla, O. R. Merad-Boudia, et M. Lehsaini, « Blockchain-Based Conditional Privacy-Preserving Authentication Mechanism for Vehicular Fog Networks », *in 2022 3rd International Conference on Embedded & Distributed Systems (EDiS)*, Oran, Algeria: IEEE, nov. 2022, p. 81-86. doi: 10.1109/EDiS57230.2022.9996473.

Références

[1] J. Voelcker, « “It’s Official: We Now Have One Billion Vehicles on the Planet ». [En ligne]. Disponible sur: https://www.greencarreports.com/news/1065070_its-official-we-now-have-one-billion-vehicles-on-the-planet

[2] Richa, T. P. Sharma, et A. K. Sharma, « Heterogeneous-Internet of Vehicles (Het-IoV) in Twenty-First Century: A Comprehensive Study », in *Handbook of Computer Networks and Cyber Security*, B. B. Gupta, G. M. Perez, D. P. Agrawal, et D. Gupta, Éd., Cham: Springer International Publishing, 2020, p. 555-584. doi: 10.1007/978-3-030-22277-2_22.

[3] S. Giordano, « Mobile Ad Hoc Networks », in *Wiley Series on Parallel and Distributed Computing*, I. Stojmenović, Éd., New York, USA: John Wiley & Sons, Inc., 2002, p. 325-346. doi: 10.1002/0471224561.ch15.

[4] Department of Computer Applications, KIET Group of Institutions, Ghaziabad, 201206, India, A. K. Goyal, G. Agarwal, et A. K. Tripathi, « Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey », *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, nº 10, p. 37-44, oct. 2019, doi: 10.5815/ijcnis.2019.10.05.

[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, et H. Zedan, « A comprehensive survey on vehicular Ad Hoc network », *J. Netw. Comput. Appl.*, vol. 37, p. 380-392, janv. 2014, doi: 10.1016/j.jnca.2013.02.036.

[6] H. Hartenstein et K. P. Laberteaux, « A tutorial survey on vehicular ad hoc networks », *IEEE Commun. Mag.*, vol. 46, nº 6, p. 164-171, juin 2008, doi: 10.1109/MCOM.2008.4539481.

[7] F. Yang, J. Li, T. Lei, et S. Wang, « Architecture and key technologies for Internet of Vehicles: a survey », *J. Commun. Inf. Netw.*, vol. 2, nº 2, p. 1-17, juin 2017, doi: 10.1007/s41650-017-0018-6.

[8] K. M. Alam, M. Saini, et A. El Saddik, « Toward Social Internet of Vehicles: Concept, Architecture, and Applications », *IEEE Access*, vol. 3, p. 343-357, 2015, doi: 10.1109/ACCESS.2015.2416657.

[9] F. Yang, S. Wang, J. Li, Z. Liu, et Q. Sun, « An overview of Internet of Vehicles », *China Commun.*, vol. 11, nº 10, p. 1-15, oct. 2014, doi: 10.1109/CC.2014.6969789.

[10] O. Kaiwartya *et al.*, « Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects », *IEEE Access*, vol. 4, p. 5356-5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[11] P. Mell et T. Grance, « The NIST Definition of Cloud Computing », 2011.

[12] J. FOLEY, *Private Clouds Take Shape*, InformationWeek., vol. 1104. 2008.

[13] W. Kim, « Cloud Computing: Today and Tomorrow. », *J. Object Technol.*, vol. 8, nº 1, p. 65, 2009, doi: 10.5381/jot.2009.8.1.c4.

[14] G. Huerta-Canepa et D. Lee, « A virtual cloud computing provider for mobile devices », in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, San Francisco California: ACM, juin 2010, p. 1-5. doi: 10.1145/1810931.1810937.

[15] A. Alzahrani, N. Alalwan, et M. Sarrab, « Mobile cloud computing: advantage, disadvantage and open challenge », in *Proceedings of the 7th Euro American Conference on Telematics and Information Systems*, Valparaiso Chile: ACM, avr. 2014, p. 1-4. doi: 10.1145/2590651.2590670.

[16] S. S. Qureshi, T. Ahmad, K. Rafique, et Shuja-ul-islam, « Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues », in *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, Beijing: IEEE, sept. 2011, p. 467-471. doi: 10.1109/CCIS.2011.6045111.

[17] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, et S. Chen, « Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures », *IEEE Trans. Veh. Technol.*, vol. 65, nº 6, p. 3860-3873, juin 2016, doi: 10.1109/TVT.2016.2532863.

[18] A. Boukerche et R. E. De Grande, « Vehicular cloud computing: Architectures, applications, and mobility », *Comput. Netw.*, vol. 135, p. 171-189, avr. 2018, doi: 10.1016/j.comnet.2018.01.004.

[19] T.-Y. Chung, Y.-M. Chen, et C.-H. Hsu, « Adaptive Momentum-Based Motion Detection Approach and Its Application on Handoff in Wireless Networks », *Sensors*, vol. 9, nº 7, p. 5715-5739, juill. 2009, doi: 10.3390/s90705715.

[20] N. Oliver et A. P. Pentland, « Graphical models for driver behavior recognition in a SmartCar », in *Proceedings of the IEEE Intelligent Vehicles Symposium 2000 (Cat. No.00TH8511)*, Dearborn, MI, USA: IEEE, 2000, p. 7-12. doi: 10.1109/IVS.2000.898310.

[21] D. Jiang et L. Delgrossi, « IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments », in *VTC Spring 2008 - IEEE Vehicular Technology Conference*, Marina Bay, Singapore: IEEE, mai 2008, p. 2036-2040. doi: 10.1109/VETECS.2008.458.

[22] Qing Xu, D. Jiang, R. Sengupta, et D. Chrysler, « Design and analysis of highway safety communication protocol in 5.9 GHZ dedicated short range communication spectrum », in *The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC 2003-Spring.*, Jeju, Korea: IEEE, 2003, p. 2451-2455. doi: 10.1109/VETECS.2003.1208831.

[23] M. Sookhak *et al.*, « Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing », *IEEE Veh. Technol. Mag.*, vol. 12, nº 3, p. 55-64, sept. 2017, doi: 10.1109/MVT.2017.2667499.

[24] F. Bonomi, R. Milito, J. Zhu, et S. Addepalli, « Fog computing and its role in the internet of things », in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, Helsinki Finland: ACM, août 2012, p. 13-16. doi: 10.1145/2342509.2342513.

[25] H. Zhang, Y. Xiao, S. Bu, D. Niyato, R. Yu, et Z. Han, « Fog computing in multi-tier data center networks: A hierarchical game approach », in *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia: IEEE, mai 2016, p. 1-6. doi: 10.1109/ICC.2016.7511146.

[26] P. Hu, S. Dhelim, H. Ning, et T. Qiu, « Survey on fog computing: architecture, key technologies, applications and open issues », *J. Netw. Comput. Appl.*, vol. 98, p. 27-42, nov. 2017, doi: 10.1016/j.jnca.2017.09.002.

[27] Y. Xiao et Chao Zhu, « Vehicular fog computing: Vision and challenges », in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI: IEEE, mars 2017, p. 6-9. doi: 10.1109/PERCOMW.2017.7917508.

[28] V. G. Menon et J. Prathap, « Vehicular Fog Computing: Challenges Applications and Future Directions », *Int. J. Veh. Telemat. Infotain. Syst.*, vol. 1, nº 2, p. 15-23, juill. 2017, doi: 10.4018/IJVTIS.2017070102.

[29] C. Huang, R. Lu, et K.-K. R. Choo, « Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges », *IEEE Commun. Mag.*, vol. 55, nº 11, p. 105-111, nov. 2017, doi: 10.1109/MCOM.2017.1700322.

[30] M. A. Hoque et R. Hasan, « Towards a Threat Model for Vehicular Fog Computing », in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York City, NY, USA: IEEE, oct. 2019, p. 1051-1057. doi: 10.1109/UEMCON47517.2019.8993064.

[31] P. Torr, « Demystifying the Threat-Modeling Process », *IEEE Secur. Priv. Mag.*, vol. 3, nº 5, p. 66-70, sept. 2005, doi: 10.1109/MSP.2005.119.

[32] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, et M. Younis, « Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs », in *2015 IEEE International Conference on Communications (ICC)*, London: IEEE, juin 2015, p. 7298-7303. doi: 10.1109/ICC.2015.7249492.

[33] J. R. Douceur, « The Sybil Attack », in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, et A. Rowstron, Éd., in Lecture Notes in Computer Science, vol. 2429. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, p. 251-260. doi: 10.1007/3-540-45748-8_24.

[34] Y. Zhang, B. Das, et F. Qiao, « Sybil Attack Detection and Prevention in VANETs: A Survey », in *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3*, K. Arai, S. Kapoor, et R. Bhatia, Éd., in Advances in Intelligent Systems and Computing, vol. 1290. Cham: Springer International Publishing, 2021, p. 762-779. doi: 10.1007/978-3-030-63092-8_51.

[35] B. K. Pattanayak, O. Pattnaik, et S. Pani, « Dealing with Sybil Attack in VANET », in *Intelligent and Cloud Computing*, D. Mishra, R. Buyya, P. Mohapatra, et S. Patnaik, Éd., in Smart Innovation, Systems and Technologies, vol. 194. Singapore: Springer Singapore, 2021, p. 471-480. doi: 10.1007/978-981-15-5971-6_51.

[36] T. Zhou, R. R. Choudhury, P. Ning, et K. Chakrabarty, « P2DAP — Sybil Attacks Detection in Vehicular Ad Hoc Networks », *IEEE J. Sel. Areas Commun.*, vol. 29, nº 3, p. 582-594, mars 2011, doi: 10.1109/JSAC.2011.110308.

[37] S. Benadla et O. R. Merad-Boudia, « The Impact of Sybil Attacks on Vehicular Fog Networks », in *2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI)*, Tebessa, Algeria: IEEE, sept. 2021, p. 1-6. doi: 10.1109/ICRAMI52622.2021.9585965.

[38] M. Rahbari et M. A. Jabreil Jamali, « Efficient Detection of Sybil attack Based on Cryptography in Vanet », *Int. J. Netw. Secur. Its Appl.*, vol. 3, nº 6, p. 185-195, nov. 2011, doi: 10.5121/ijnsa.2011.3614.

[39] A. Anwar, T. Halabi, et M. Zulkernine, « Cloud-based Sybil Attack Detection Scheme for Connected Vehicles », in *2019 3rd Cyber Security in Networking Conference (CSNet)*, Quito, Ecuador: IEEE, oct. 2019, p. 114-121. doi: 10.1109/CSNet47905.2019.9108923.

[40] M. Baza *et al.*, « Detecting Sybil Attacks Using Proofs of Work and Location in VANETs », *IEEE Trans. Dependable Secure Comput.*, vol. 19, nº 1, p. 39-53, janv. 2022, doi: 10.1109/TDSC.2020.2993769.

[41] J. Li, Z. Song, Y. Li, C. Cao, et Y. He, « Trajectory as an Identity: Privacy-Preserving and Sybil-Resistant Authentication for Internet of Vehicles », *Secur. Commun. Netw.*, vol. 2021, p. 1-10, déc. 2021, doi: 10.1155/2021/8251697.

[42] S. Chang, Y. Qi, H. Zhu, J. Zhao, et X. Shen, « Footprint: Detecting Sybil Attacks in Urban Vehicular Networks », *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, nº 6, p. 1103-1114, juin 2012, doi: 10.1109/TPDS.2011.263.

[43] S. Hamdan, A. Hudaib, et A. Awajan, « Detecting Sybil attacks in vehicular ad hoc networks », *Int. J. Parallel Emergent Distrib. Syst.*, vol. 36, nº 2, p. 69-79, mars 2021, doi: 10.1080/17445760.2019.1617865.

[44] M. T. Garip, P. H. Kim, P. Reiher, et M. Gerla, « INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks », in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV: IEEE, janv. 2017, p. 1-6. doi: 10.1109/CCNC.2017.8013424.

[45] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang, et X. Zhou, « Power Control Identification: A Novel Sybil Attack Detection Scheme in VANETs Using RSSI », *IEEE J. Sel. Areas Commun.*, vol. 37, nº 11, p. 2588-2602, nov. 2019, doi: 10.1109/JSAC.2019.2933888.

[46] W. Li et D. Zhang, « RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET », in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Chongqing, China: IEEE, juin 2019, p. 763-767. doi: 10.1109/ICCSN.2019.8905261.

[47] P. Gu, R. Khatoun, Y. Begriche, et A. Serhrouchni, « k-Nearest Neighbours classification based Sybil attack detection in Vehicular networks », in *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*, Miami Beach, FL, USA: IEEE, févr. 2017, p. 1-6. doi: 10.1109/MOBISECSERV.2017.7886565.

[48] A. Haddaji, S. Ayed, et L. C. Fourati, « Blockchain-based Multi-Levels Trust Mechanism Against Sybil Attacks for Vehicular Networks », in *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, Guangzhou, China: IEEE, déc. 2020, p. 155-163. doi: 10.1109/BigDataSE50710.2020.00028.

[49] N. Keshari, D. Singh, et A. K. Maurya, « A survey on Vehicular Fog Computing: Current state-of-the-art and future directions », *Veh. Commun.*, vol. 38, p. 100512, déc. 2022, doi: 10.1016/j.vehcom.2022.100512.

[50] P. Mundhe, S. Verma, et S. Venkatesan, « A comprehensive survey on authentication and privacy-preserving schemes in VANETs », *Comput. Sci. Rev.*, vol. 41, p. 100411, août 2021, doi: 10.1016/j.cosrev.2021.100411.

[51] P. Vijayakumar, M. Azees, A. Kannan, et L. Jegatha Deborah, « Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks », *IEEE Trans. Intell. Transp. Syst.*, vol. 17, nº 4, p. 1015-1028, avr. 2016, doi: 10.1109/TITS.2015.2492981.

[52] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, et B. Balusamy, « Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks », *Clust. Comput.*, vol. 20, nº 3, p. 2439-2450, sept. 2017, doi: 10.1007/s10586-017-0848-x.

[53] S. Jiang, X. Zhu, et L. Wang, « An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs », *IEEE Trans. Intell. Transp. Syst.*, vol. 17, nº 8, p. 2193-2204, août 2016, doi: 10.1109/TITS.2016.2517603.

[54] S. Wang et N. Yao, « LIAP: A local identity-based anonymous message authentication protocol in VANETs », *Comput. Commun.*, vol. 112, p. 154-164, nov. 2017, doi: 10.1016/j.comcom.2017.09.005.

[55] A. Alrawais, A. Alhothaily, B. Mei, T. Song, et X. Cheng, « An Efficient Revocation Scheme for Vehicular Ad-Hoc Networks », *Procedia Comput. Sci.*, vol. 129, p. 312-318, 2018, doi: 10.1016/j.procs.2018.03.081.

[56] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, et P. Lorenz, « On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment », *IEEE Trans. Veh. Technol.*, vol. 69, nº 5, p. 5535-5548, mai 2020, doi: 10.1109/TVT.2020.2981934.

[57] K. Fan, W. Jiang, Q. Luo, H. Li, et Y. Yang, « Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV », *J. Frankl. Inst.*, vol. 358, nº 1, p. 193-209, janv. 2021, doi: 10.1016/j.jfranklin.2019.02.023.

[58] L. Song, G. Sun, H. Yu, X. Du, et M. Guizani, « FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles », *IEEE Trans. Veh. Technol.*, vol. 69, nº 5, p. 5403-5415, mai 2020, doi: 10.1109/TVT.2020.2977829.

[59] H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina, et L. Liu, « Secure and Lightweight Conditional Privacy-Preserving Authentication for Fog-Based Vehicular Ad Hoc Networks », *IEEE Internet Things J.*, vol. 9, nº 11, p. 8485-8497, juin 2022, doi: 10.1109/JIOT.2021.3116039.

[60] S. Goudarzi *et al.*, « A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET », *Ad Hoc Netw.*, vol. 128, p. 102782, avr. 2022, doi: 10.1016/j.adhoc.2022.102782.

[61] K.-H. Yeh, K.-Y. Tsai, et C.-Y. Fan, « An efficient certificateless signature scheme without bilinear pairings », *Multimed. Tools Appl.*, vol. 74, nº 16, p. 6519-6530, août 2015, doi: 10.1007/s11042-014-2154-4.

[62] J.-L. Tsai, « A New Efficient Certificateless Short Signature Scheme Using Bilinear Pairings », *IEEE Syst. J.*, vol. 11, nº 4, p. 2395-2402, déc. 2017, doi: 10.1109/JSYST.2015.2490163.

[63] Y. Sun, R. Lu, X. Lin, X. (Sherman) Shen, et J. Su, « An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications », *IEEE Trans. Veh. Technol.*, vol. 59, nº 7, p. 3589-3603, sept. 2010, doi: 10.1109/TVT.2010.2051468.

[64] D. He, S. Zeadally, B. Xu, et X. Huang, « An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks », *IEEE Trans. Inf. Forensics Secur.*, vol. 10, nº 12, p. 2681-2691, déc. 2015, doi: 10.1109/TIFS.2015.2473820.

[65] J. Shao, X. Lin, R. Lu, et C. Zuo, « A Threshold Anonymous Authentication Protocol for VANETs », *IEEE Trans. Veh. Technol.*, vol. 65, nº 3, p. 1711-1720, mars 2016, doi: 10.1109/TVT.2015.2405853.

[66] Y. Wang, H. Zhong, Y. Xu, et J. Cui, « ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs », 2016.

[67] J. Golosova et A. Romanovs, « The Advantages and Disadvantages of the Blockchain Technology », in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius: IEEE, nov. 2018, p. 1-6. doi: 10.1109/AIEEE.2018.8592253.

[68] Y. Yao, X. Chang, J. Misic, V. B. Misic, et L. Li, « BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services », *IEEE Internet Things J.*, vol. 6, nº 2, p. 3775-3784, avr. 2019, doi: 10.1109/JIOT.2019.2892009.

[69] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, et S. H. Ahmed, « Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure », in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China: IEEE, mai 2019, p. 1-6. doi: 10.1109/ICCW.2019.8757184.

[70] M. S. Eddine, M. A. Ferrag, O. Friha, et L. Maglaras, « EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles », *J. Inf. Secur. Appl.*, vol. 59, p. 102802, juin 2021, doi: 10.1016/j.jisa.2021.102802.

[71] S. Benadla, O. R. Merad-Boudia, S. M. Senouci, et M. Lehsaini, « Detecting Sybil Attacks in Vehicular Fog Networks Using RSSI and Blockchain », *IEEE Trans. Netw. Serv. Manag.*, vol. 19, nº 4, p. 3919-3935, déc. 2022, doi: 10.1109/TNSM.2022.3216073.

[72] N. Koblitz, « Elliptic curve cryptosystems », *Math. Comput.*, vol. 48, nº 177, p. 203-209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[73] V. S. Miller, « Use of Elliptic Curves in Cryptography », in *Advances in Cryptology — CRYPTO '85 Proceedings*, H. C. Williams, Éd., in Lecture Notes in Computer Science, vol. 218. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, p. 417-426. doi: 10.1007/3-540-39799-X_31.

[74] M. Suárez-Albela, T. Fernández-Caramés, P. Fraga-Lamas, et L. Castedo, « A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications », *Sensors*, vol. 17, nº 9, p. 1978, août 2017, doi: 10.3390/s17091978.

[75] S. A. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, et M. K. Khan, « An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography », *Wirel. Pers. Commun.*, vol. 96, nº 4, p. 5355-5373, oct. 2017, doi: 10.1007/s11277-016-3745-3.

[76] S. NAKAMOTO, « Bitcoin: a Peer-to-Peer Electronic Cash System », in *Decentralized business review*, 2008, p. 21260. [En ligne]. Disponible sur: https://bitcoin.org/bitcoin.pdf

[77] M. Xu, Y. Guo, Q. Hu, Z. Xiong, D. Yu, et X. Cheng, « A trustless architecture of blockchain-enabled metaverse », *High-Confid. Comput.*, vol. 3, nº 1, p. 100088, mars 2023, doi: 10.1016/j.hcc.2022.100088.

[78] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, et G. Das, « Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems », *IEEE Consum. Electron. Mag.*, vol. 7, nº 4, p. 6-14, juill. 2018, doi: 10.1109/MCE.2018.2816299.

[79] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, et H. Janicke, « Blockchain Technologies for the Internet of Things: Research Issues and Challenges », *IEEE Internet Things J.*, vol. 6, nº 2, p. 2188-2204, avr. 2019, doi: 10.1109/JIOT.2018.2882794.

[80] D. Mahmudnia, M. Arashpour, et R. Yang, « Blockchain in construction management: Applications, advantages and limitations », *Autom. Constr.*, vol. 140, p. 104379, août 2022, doi: 10.1016/j.autcon.2022.104379.

[81] O. Katircioglu, H. Isel, O. Ceylan, F. Taraktas, et H. B. Yagci, « Comparing ray tracing, free space path loss and logarithmic distance path loss models in success of indoor localization with RSSI », in *2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers*, Belgrade, Serbia: IEEE, nov. 2011, p. 313-316. doi: 10.1109/TELFOR.2011.6143552.

[82] I. Qasim, N. Habib, U. Habib, Q. F. Usman, et M. Kamal, « Comparison of Localization Algorithms for Unmanned Aerial Vehicles », in *Intelligent Technologies and Applications*, I. S. Bajwa, T. Sibalija, et D. N. A. Jawawi, Éd., in Communications in Computer and Information Science, vol. 1198. Singapore: Springer Singapore, 2020, p. 258-269. doi: 10.1007/978-981-15-5232-8_23.

[83] J. Grover, M. S. Gaur, N. Prajapati, et V. Laxmi, « RSS-based Sybil Attack Detection in VANETs », *Proc. Int. Conf. TENCON2010*, p. 2278-2283, 2010.

[84] J. Grover, M. S. Gaur, et V. Laxmi, « Multivariate verification for sybil attack detection in VANET », *Open Comput. Sci.*, vol. 5, nº 1, p. 60-78, déc. 2015, doi: 10.1515/comp-2015-0006.

[85] « OMNeT++ Discrete Event Simulator ». https://omnetpp.org/ (consulté le 14 juin 2023).

[86] C. Sommer *et al.*, « Veins: The Open Source Vehicular Network Simulation Framework », in *Recent Advances in Network Simulation*, A. Virdis et M. Kirsche, Éd., in EAI/Springer Innovations in Communication and Computing. Cham: Springer International Publishing, 2019, p. 215-252. doi: 10.1007/978-3-030-12842-5_6.

[87] P. A. Lopez *et al.*, « Microscopic Traffic Simulation using SUMO », in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, Maui, HI: IEEE, nov. 2018, p. 2575-2582. doi: 10.1109/ITSC.2018.8569938.

[88] « OpenStreetMap », *OpenStreetMap*. https://www.openstreetmap.org/ (consulté le 13 mai 2023).

[89] « MIRACL », *GitHub*. https://github.com/miracl (consulté le 13 mai 2023).

[90] S. Benadla, O. R. Merad-Boudia, et M. Lehsaini, « Blockchain-Based Conditional Privacy-Preserving Authentication Mechanism for Vehicular Fog Networks », in *2022 3rd International Conference on Embedded & Distributed Systems (EDiS)*, Oran, Algeria: IEEE, nov. 2022, p. 81-86. doi: 10.1109/EDiS57230.2022.9996473.

[91] M. A. Hoque et R. Hasan, « Towards an Analysis of the Architecture, Security, and Privacy Issues in Vehicular Fog Computing », in *2019 SoutheastCon*, Huntsville, AL, USA: IEEE, avr. 2019, p. 1-8. doi: 10.1109/SoutheastCon42311.2019.9020476.

[92] M. Azees, P. Vijayakumar, et L. J. Deboarh, « EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks », *IEEE Trans. Intell. Transp. Syst.*, vol. 18, nº 9, p. 2467-2476, sept. 2017, doi: 10.1109/TITS.2016.2634623.

[93] C. P. Schnorr, « Efficient signature generation by smart cards », *J. Cryptol.*, vol. 4, nº 3, p. 161-174, janv. 1991, doi: 10.1007/BF00196725.

[94] S. Hafeez, M. R. Shahid, A. Sohail, S. Jabbar, M. Suleman, et M. Zafar, « Blockchain based Competent Consensus Algorithm for Secure Authentication in Vehicular Networks », in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Sukkur, Pakistan: IEEE, janv. 2020, p. 1-6. doi: 10.1109/iCoMET48670.2020.9073900.

Résumé

L'Internet des Véhicules (IoV) est un réseau qui considère les véhicules comme des machines intelligentes et permet leur interaction et leur communication mutuelles dans le but d'améliorer les performances et la sécurité du trafic routier. Bien que l'IoV apporte des solutions à certains problèmes, il présente également des limites, notamment en termes de temps de réponse. Cela a conduit les chercheurs à proposer l'intégration du Fog Computing dans les réseaux de véhicules afin de bénéficier de ses avantages. Ainsi, le Vehicular Fog Computing (VFC) émerge comme un paradigme pour les réseaux véhiculaires, offrant des services à la périphérie du réseau. Le VFC présente un ensemble d'avantages significatifs, tels que l'agilité, l'efficacité et la réduction de la latence. Cependant, il est également vulnérable à diverses attaques, et les mesures de sécurité existantes dans les réseaux véhiculaires traditionnels ne sont pas nécessairement applicables au VFC. Par conséquent, afin de garantir la satisfaction des utilisateurs du réseau, il est essentiel de garantir la sécurité et la confidentialité des données sensibles. Dans le cadre de ce projet de thèse, l'objectif est de relever les défis de sécurité associés au VFC. Pour atteindre cet objectif, deux contributions ont été proposées, axées sur la sécurité et la protection de la vie privée des utilisateurs au sein des réseaux VFC. La première contribution concerne un mécanisme de détection des attaques Sybil, tandis que la deuxième contribution propose un mécanisme d'authentification. Ces mécanismes reposent sur l'utilisation des techniques cryptographiques avancés et de la technologie Blockchain. Ils ont été soigneusement analysés et comparés à d'autres travaux pertinents en termes de services de sécurité et de performances. Les résultats obtenus ont été extrêmement satisfaisants.

Mot clés : Sécurité, protection de la vie privée, VFC, blockchain, authentification, attaque Sybil.

Abstract

The Internet of Vehicles (IoV) is a network that treats vehicles as intelligent machines, enabling them to interact and communicate with each other to enhance road traffic performance and safety. While IoV offers solutions to certain challenges, it also has its limitations, particularly in terms of response time. As a result, researchers have proposed integrating Fog Computing into vehicular networks to leverage its benefits. Consequently, Vehicular Fog Computing (VFC) is emerging as a paradigm for vehicular networks, providing services at the network edge. VFC offers several significant advantages, including agility, efficiency, and reduced latency. However, it is also susceptible to various attacks, and the security measures employed in traditional vehicular networks may not be directly applicable to VFC. Therefore, ensuring the security and confidentiality of sensitive data is crucial to satisfying network users. The objective of this thesis project is to address the security challenges associated with VFC. To achieve this goal, two contributions have been proposed, focusing on security and user privacy within VFC networks. The first contribution involves a mechanism for detecting Sybil attacks, while the second proposes an authentication mechanism. These mechanisms rely on advanced cryptographic tools and Blockchain technology. They have undergone thorough analysis and comparison with other relevant works in terms of security services and performance. The obtained results have been extremely satisfactory.

Key words: Security, privacy, VFC, blockchain, authentication, Sybil attack.

ملخص

إنترنت السيارات هو شبكة تتعامل مع السيارات على أنها آلات ذكية، مما يتيح لها التفاعل والتواصل مع بعضها البعض لتعزيز أداء حركة المرور على الطرق. وبالرغم من أن إنترنت السيارات يوفر حلاً لبعض التحديات، إلا أن لديها بعض القيود، لا سيما فيما يتعلق بزمن الاستجابة. وبناءً على ذلك، اقترح الباحثون دمج الحوسبة الضبابية في شبكات السيارات للاستفادة من فوائدها. يظهر الحوسبة الضبابية للسيارات كنموذج حديث لشبكات السيارات، حيث يوفر مجموعة من المزايا الهامة، بما في ذلك السرعة والكفاءة وتقليل التأخير. ومع ذلك، فإنها تتعرض أيضًا لمختلف أنواع الهجمات، وقد لا تكون التدابير الأمنية المستخدمة في شبكات السيارات التقليدية قابلة للاستخدام المباشر في الحوسبة الضبابية للسيارات. لذا، فإن ضمان أمان وسرية البيانات الحساسة أمر حاسم لإرضاء مستخدمي الشبكة. يهدف هذا المشروع البحثي إلى معالجة التحديات الأمنية المرتبطة بالحوسبة الضبابية للسيارات. ولتحقيق هذا الهدف، تم اقتراح مساهمتين، تركز الأولى على آلية لاكتشاف هجمات سايبيل، في حين تقترح الثانية آلية للمصادقة. تعتمد هذه الآليات على أدوات تشفير متقدمة وتقنية البلوكشين. وقد تم تحليلها ومقارنتها بعناية مع الأعمال الأخرى ذات الصلة من حيث خدمات الأمان والأداء.

كلمات رئيسية: الأمان، الخصوصية، الحوسبة الضبابية للسيارات، البلوكشين، المصادقة، هجوم سايبيل.