الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 8 mai 1945 – Guelma –

Faculté des Mathématiques, d'Informatique et des Sciences de la Matière

Département d'Informatique

Mémoire de Fin d'Études Master

Filière: Informatique

Spécialité: Systèmes Informatiques

Thème:

Un schéma d'authentification sécurisé pour l'internet des véhicules

---

Encadré Par :
Dr. FARRAG Mohamed Amine

Présenté par :
MERZOUGUI Salah Eddine

-Octobre 2020-

Dédicaces

Je dédie ce mémoire,

À ma chère mère, qui a œuvré et prié pour ma réussite, par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie. Reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude, merci beaucoup maman.

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

À mes deux frères Mehdi et Ahmed, ma sœur Belkis pour leur présence dans ma vie, et à tout la famille.

À mes précieux amis Bilel, Lotfi, Oussama, Sami, Mehdi, Abdrezzak et Aymen pour leur bonne compagnie. À Maya et Imene pour leur soutien et encouragement. Merci infiniment les amis.

À vous mes camarades du parcours éducatif, et surtout Nebili Charafeddine qui a vraiment contribué à notre succès avec ses groupes éducatifs, ses conseils et son aide.

À Mes enseignants qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

À Othmane Friha doctorant à l'université de Badji Mokhtar, Annaba et à Leandros Maglaras, Leicester, UK pour leur aide dans la réalisation de l'article.

Encore merci à tout le monde du fond du cœur.

Mr. MERZOUGUI Salah Eddine

Remerciements

J’exprime à travers ces quelques phrases modestes toute ma gratitude pour tous ceux qui ont aidés à aboutir ce travail:

A Dieu Allah

L’éternel tout puissant, le Clément, le Miséricordieux.

A notre **Prophète MOHAMED** (PSSL).

A mon enseignant encadreur Monsieur **FERRAG Mohamed Amine** Docteur à l’Université, 8 mai 1945 Guelma.

Qui a accepté de m'encadrer avec disponibilité et bienveillance.

Pour son enseignement, sa patience, et ses précieux conseils.

Aux jurés qui ont acceptés d’examiner ce travail.

Pour m’avoir fait l’honneur de juger mon mémoire et de rapporter mon travail.

Je tiens aussi, à remercier toutes les personnes qui m'ont aidés à la réalisation de ce travail, en commençant par les enseignants de mon cursus universitaire, jusqu’à mes collègues.

الملخص

يسمح إنترنت المركبات (IoV) للمركبات التي تسافر على الطرق بتشكيل شبكة ذاتية التنظيم. حيث يوفر مزايا متعددة، مثل نظام التحذير المتكامل الذي ينبه السائقين في حالة وقوع حادث حتى يتمكنوا من اتخاذ قرار سريع بناءً على معلومات حركة المرور المقدمة. يمكن مشاركة المعلومات الأكثر تعقيدًا بين المركبات وتحسين سلامة ودقة السيارات ذات الطيار الآلي. ومع ذلك، في حالة **عدم** وجود إجراء فعال من أجل الأمان و الحفاظ الخصوصية، يمكن للخصم بسهولة جمع البيانات المرسلة عبر الشبكات التي تحتوي بشكل عام على البيانات الخاصة لمستخدمي المركبات. في هذه الأطروحة، نقترح نظام مصادقة آمن لـ (IoV) حيث يعتمد على Blockchain و Fog Computing. وبشكل أكثر تحديدًا، يستخدم النظام المقترح خمس مراحل متمثلات في**:** التهيئة، التسجيل، المصادقة، الإجماع وتحديث الشهادة. بالاستناد إلى تقنية التشفير بالمنحنى الإهليلجي ووظائف التجزئة، يمكن للنظام المقترح الحفاظ على السرية، النزاهة، الخصوصية، إخفاء الهوية وعدم الإنكار. أيضًا، يمكن للنظام المقترح أن يتحمل أكثر الهجمات شيوعًا مثل هجوم DDoS وهجوم man-in-the-middle والهجوم المقنع، ... إلخ. قمنا بتحليل أمن المخطط المقترح في إطار أداة المحاكاة (AVISPA)، ثم قمنا بتقييم الأداء من حيث تكاليف الحساب والاتصال. يوضح تقييم المخطط المقترح فعاليته مقارنة بالمقترحات ذات الصلة.

الكلمات المفتاحية: الأمان، المصادقة، إنترنت المركبات، شبكة المركبات المخصصة، الحوسبة السحابية، الحوسبة الضبابية، البلوك تشين، طرق التشفير، التشفير بالمنحنيات الاهليلجية.

Abstract

The Internet of Vehicles (IoV) allows vehicles on the road to form a self-organized network. It offers multiple advantages, such as an integrated warning system that warns drivers in the event of an accident so that they can quickly decide based on the traffic information provided. More sophisticated information can potentially be shared between vehicles and improve the safety and accuracy of autopilot vehicles. However, in the absence of an effective security and privacy measure, an adversary can easily collect data transmitted through networks which typically contain the private data of vehicle users. In this thesis, we propose a secure authentication scheme for IoV based on Blockchain and Fog Computing. More specifically, the proposed scheme uses five phases, namely, initialization, registration, authentication, consensus and certificate update. Based on elliptical curve cryptography technology and hash functions, the proposed scheme can preserve confidentiality, integrity, privacy, anonymity, and non-repudiation. Also, the proposed scheme can withstand the most frequent attacks like DDoS attack, man-in-the-middle attack, and disguise attack …etc. We analyze the security of the scheme proposed under the AVISPA simulator, and then we assess the performance in terms of computation and communication costs. The evaluation of the proposed scheme demonstrates its effectiveness compared to the relative proposals.

Keywords: Security, Authentication, Internet of vehicles, Vehicular ad hoc network, Cloud computing, Fog computing, Blockchain, Cryptographic methods, Elliptic curve cryptography.

Résumé

L'Internet des véhicules (IoV) permet aux véhicules qui circulent sur les routes de former un réseau auto-organisé. Il offre de multiples avantages, comme un système d'avertissement intégré qui avertit les conducteurs en cas d'accident afin qu'ils puissent décider rapidement en fonction des informations routières fournies. Des informations plus sophistiquées peuvent éventuellement être partagées entre les véhicules et améliorer la sécurité et la précision des véhicules autopilotés. Toutefois, en l'absence d'une mesure efficace de sécurité et de protection de la vie privée, un adversaire peut facilement recueillir les données transmises par des réseaux qui contiennent généralement les données privées des utilisateurs de véhicules. Dans ce mémoire, nous proposons un schéma d'authentification sécurisé pour l'IoV basé sur la Blockchain et le Fog Computing. Plus précisément, le schéma proposé utilise cinq phases, à savoir, initialisation, registration, authentification, consensus et mise à jour de certificat. Basé sur la technologie de la cryptographie à courbe elliptique et les fonctions de hachage, le schéma proposé peut préserver la confidentialité, l'intégrité, la vie privée, l'anonymat, et la non-répudiation. Aussi, le schéma proposé peut résister aux attaques les plus fréquentes comme l'attaque DDoS, l'attaque de l'homme du milieu, et l'attaque de déguise,…etc. Nous analysons la sécurité du schéma proposé sous le simulateur AVISPA, puis nous évaluons les performances en termes de coûts de calcul et de communication. L'évaluation du schéma proposé démontre son efficacité par rapport aux propositions relatives.

Mots Clés: Sécurité, Authentification, Internet des véhicules, Réseau véhiculaire ad hoc, Le calcul du Cloud, Le calcul du Fog, La Blockchain, Les méthodes cryptographiques, Cryptographie à courbe elliptique.

Table des matières

Liste des figures

Liste des tableaux

Liste des algorithmes

Liste des abréviations

AVISPA (Automated Validation of Internet Security Protocols and Applications): Validation automatisée des protocoles et applications de sécurité Internet.

CaaS (Cooperation as a Service): Coopération en tant que service.

CDHP (Computational Diffie-Hellman Problem): Problème computationnel de Diffie-Hellman.

COaaS (Computing as a Service): Le calcul en tant que service.

DaaS (Data as a Service): Les données en tant que service.

DDoS (Distributed Denial of Service): Déni de service distribué.

DOS (Denial of Service): Déni de service.

DSRC (Dedicated Short-Range Communications): Communications à courte portée dédiées.

ECC (Elliptic Curve Cryptography): Cryptographie à courbe elliptique.

ECDLP (Elliptic Curve Discrete Logarithm Problem): Problème du logarithme discret de la courbe elliptique.

GaaS (Gateway as a Service): La passerelle en tant que service.

GIN (Gateway of Internetworking): Passerelle d'Inter-réseautage.

GPS (Global Positioning System): Système de positionnement global.

HLPSL (High Level Protocol Specification Language): Langage de spécification de protocole de haut niveau.

IEEE (Institute of Electrical and Electronics Engineers): Institut d'ingénieurs en électricité et électronique.

***iOS* (iPhone Operating System)**: Système d'exploitation iPhone.

IoT (Internet of Things): Internet des Objets.

IoV (Internet of Vehicles): Internet des véhicules.

ITS (Intelligent Transport Systems): Systèmes de transport intelligents.

LBS (Localization Based Service): Service basé sur la localisation.

LTE (Long Term Evolution): Évolution à long terme.

MAC (Message Authentication Code): Code d'authentification de message.

MOST (Media Oriented System Transport): Systèmes de transport orientés médias.

NaaS (Network as a Service): Le réseau en tant que service.

NFC (Near Field Communication): Communication de champs proche.

OAA (Open Automotive Alliance): Alliance automobile ouverte.

OBU (On Board Units): Unités embarquées.

OSI (Open Systems Interconnection): Interconnexion des systèmes ouverts.

PBFT (Practical Byzantine Fault Tolerance): Tolérance aux pannes byzantine pratique.

PIB: Produit Intérieur Brut.

PKI (Public Key Infrastructure): Infrastructure à clé publique.

RSU (Road Side Units): Unités côté route.

SHA (Secure Hash Algorithm): Algorithme de hachage sécurisé.

SNR (Signal to Noise Ratio): Rapport signal sur bruit.

SP (Service Provider): Fournisseur de services.

STaaS (Storage as a Service): Le stockage en tant que service.

STI: Service de technologie et l'information.

TA (Trusted Authority): Autorité de confiance.

TPD (Tamper Proof Device): Dispositif anti-sabotage.

TPNIO (Third Party Network Inter Operator): Interopérateur de réseau tiers.

V2I (Vehicle to Infrastructure): La communication véhicule-infrastructure.

V2P (Vehicle to Pedestrian): Les communications de véhicule à appareil.

V2R (Vehicle to Road): Les communications de véhicule à véhicule.

V2S (Vehicle to Sensors): Les communications de véhicule à capteur.

V2V (Vehicle to Vehicle): Les communications de véhicule à véhicule.

VANET (Vehicular Ad-Hoc Network): Réseau Ad-Hoc de véhicules.

VFC (Vehicular Fog Computing): Calcul du Fog véhiculaire.

WHO (World Health Organization): Organisation mondiale de la santé.

WiMAX (Worldwide Interoperability for Microwave Access): Interopérabilité mondiale pour l'accès micro-ondes.

WLAN (Wireless Local Area Network): Réseau local sans fil.

Introduction Générale

Grâce à l'évolution et à l'émergence des technologies de traitement des données et de communication, les véhicules ont été transformés en unités plus intelligentes. L'intégration de capteurs de détection, de capacités de communication et de mise en réseau dans les véhicules leur a donné la possibilité d'interagir entre eux et avec les unités routières (RSU) afin de partager des informations en temps réel de manière intelligente. La possibilité d'échanger des informations entre eux et d'autres véhicules a permis l'émergence de réseaux de véhicules ad hoc (VANET). Ces réseaux de véhicules urbains garantissent une grande variété de services généralement destinés aux véhicules exactement pour leurs utilisateurs, tels que les applications de sécurité routière, le contrôle intelligent du trafic, les services de divertissement, etc. Malheureusement, ces réseaux ne peuvent pas traiter des données de grande taille pour prendre des décisions intelligentes car ils n'ont pas la possibilité de traiter, d'analyser et d'évaluer les informations globales collectées auprès des véhicules et des infrastructures. Cela a conduit à l'émergence de l'Internet des véhicules (IoV), l'un des domaines révolutionnaires de l'Internet des objets (IoT), qui se développe à partir des VANET. Mais contrairement à eux, l'IoV intègre les véhicules, les humains, les choses et les réseaux en tant qu'unité intelligente via des technologies de réseau telles que le Deep Learning, le Cloud Computing, le Fog Computing, etc. Cependant, en raison de l'essor des véhicules intelligents sur le marché mondial, des équipements embarqués ont été fournis, qui collectent, gèrent et échangent des volumes de données massifs, entraînant une croissance très importante du trafic réseau. Et c'est pourquoi le concept de calcul du Fog véhiculaire (VFC) a été intégré. Il offre la possibilité de collecter, traiter, organiser et stocker des données de trafic en temps réel tout en améliorant l'efficacité de la communication et en minimisant la latence. De nombreux travaux antérieurs ont montré que les réseaux IoV font toujours face à de nombreuses menaces difficiles, en particulier des problèmes de sécurité et de confidentialité. Il est facile de provoquer des problèmes de sécurité tels que la falsification de données, la falsification d'identité et la divulgation

d'informations sensibles, ainsi que des problèmes de confidentialité tels que l'obtention d'informations privées de l'utilisateur, telles que sa véritable identité et son emplacement. Les deux peuvent endommager la vie privée et la sécurité personnelle des conducteurs et des passagers. Par conséquent, de nombreuses recherches sur la sécurité et la confidentialité ont été proposées. En plus de la sécurité personnelle et de la préservation de la vie privée, il existe d'autres objectifs de sécurité tels que la confidentialité des informations, l'authenticité mutuelle, l'intégrité, l'anonymat, etc. Afin de fournir ces fonctionnalités, Blockchain est devenu une technologie appropriée pour les environnements d'applications décentralisés. Grâce à ses fonctionnalités de consensus distribué, en particulier dans les environnements de réseaux de véhicules complexes où les véhicules ne se font pas confiance. Sous la protection de cette technologie, les données ne peuvent pas être facilement modifiées par les attaquants en raison des fonctionnalités cryptographiques offertes par cette technologie. Ainsi, la technologie Blockchain a été adaptée comme solution réalisable pour garantir les objectifs de sécurité. D'où, sur cette base, nous posons les questions suivantes: Comment intégrer le calcul du Fog dans un réseau IoV afin d'optimiser le trafic réseau? Et comment pouvons-nous adopter la technologie de cryptage Blockchain pour assurer l'authentification mutuelle tout en préservant la confidentialité des individus et en maintenant d'autres objectifs de sécurité afin de résoudre le problème des attaques malveillantes?

Ce travail a donc été réalisé pour concevoir un schéma d'authentification mutuelle basé sur la technologie Blockchain, tout en garantissant les objectifs de sécurité mentionnés. La mise en œuvre et l'évaluation du programme ont été effectuées à l'aide de l'outil AVISPA bien connu.

Chapitre I

Internet des véhicules (IoVs)

Chapitre I

Internet des véhicules (IoVs)

Dans ce chapitre, nous introduisons les réseaux d'internet des véhicules et ses différents concepts: motivation, technologies, applications et ses éléments afin que nous puissions comprendre la structure de ces réseaux intégrés.

1.1. Définition:

L'internet des véhicules (IoV) est un system ouvert de réseaux intégrés qui est connu par sa contrôlabilité, sa gestion et sa grande efficacité et sa fiabilité. Il fonctionne avec quatre composants principaux qui sont: Humain, Véhicule, Objet et Environnement; tous connecter l'un avec l'autre à travers plusieurs réseaux. L'humain représente l'utilisateur qui consomme des services ou applications de l'IoV fournis, et pas seulement les conducteurs des véhicules mais il représente tous les gens inclus dans l'environnement de l'IoV comme les piétons, les cyclistes et même les membres de famille des conducteurs. Le Véhicule représente tous les voitures ou drones qui consomment ou fournissent des services ou applications de l'IoV. L'Objet est une appareille qui peut être à l'intérieur ou à l'extérieur des véhicules. L'environnement est la combinaison des humains, véhicules et objets [1].

Le réseau IoV combine les calculs des données et la communication entre humain, véhicule et objet d'une façon coopérative pour optimiser le transport, minimiser le trafic, améliorer la qualité des services fourni par les villes et ainsi pour assurer la satisfaction et le plaisir des humains quand ils utilisent leur véhicules.

1.2. Motivations, Technologies et applications:

Au cours de la dernière décennie, les chercheurs des deux domaines industriel et académique ont soumis beaucoup de technologies sophistiquées pour mettre en œuvre le système de réseau IoV. Ces technologies ont été proposées pour les différentes couches IoT: application, physique et liaison de données, transport et réseaux.

1.2.1. Motivations de l'IoV:

La motivation pour la conception et le développent de l'IoV est divisée pour trois raisons principales. Premièrement, les problèmes liés à la commercialisation des VANET sont signalés. Deuxièmement, le volume croissant des accidents de la circulation est examiné. Troisièmement, l'énorme opportunité du marché à venir pour l'IoV est évaluée.

1.2.1.1. Les problèmes de commercialisation dans les VANET:

Malgré l'énorme potentiel des VANET pour adresser les problèmes de sécurité et d'efficacité du trafic à moindre coût opérationnel, il n'a pas pu attirer l'intérêt commercial des industries au cours des deux dernières décennies [2]. Certaines des raisons d'un moindre intérêt commercial pour les VANET sont décrites ci-dessous.

- Le cadre des VANET ne pouvait garantir les services globaux et durables des applications de service de technologie et l'information (STI). Cela est dû à l'architecture réseau pure ad hoc. Une fois qu'un véhicule est déconnecté d'un réseau ad hoc, il perd les services du réseau malgré la présence du véhicule sur la route. Cela est dû à l'incapacité de collaborer avec d'autres réseaux alternatifs accessibles [3].
- Dans le cadre actuel des VANET, la connectivité internet ne pouvait pas être garantie. Par conséquent, les applications commerciales ne sont pas disponibles pour les conducteurs et les passagers. Cela est dû à la dépendance des applications commerciales à une connectivité internet fiable [4].
- Malgré la croissance considérable des appareils personnels dans notre vie quotidienne, les appareils ne sont pas en mesure de communiquer avec les VANET dû à l'architecture réseau incompatible [5].
- Décisions intelligentes basées sur les calculs basés sur l'extraction de données volumineuses ne sont pas possibles dans l'architecture VANET actuelle. Cela est dû aux contraintes de calcul et de stockage et indisponibilité des services de calcul du Cloud sur les véhicules [6].
- La précision des services dans les applications de service de technologie et l'information (STI) est nettement inférieure, considérant le risque lié à

l'utilisation des services pour une meilleure expérience de conduite. Cela est dû au calcul basé sur des informations locales liées à des environnements de trafic dans les VANET.

- Les opérations du réseau de véhicules dépendent fortement de la coopération des utilisateurs du réseau. La dépendance diminue la fiabilité des services des VANETs [7].

Paramètres	VANET	IoV
Commercialisation	Non	Oui
Collaboration avec d'autres réseaux	Non	Oui
Le service Internet	Non	Oui
Les types de communication	Deux types	Cinq types
La taille des données	Limité	N'est pas limité
La décision	Basée sur un calcul simple et logique	Basée sur les algorithmes d'apprentissage automatique
Cloud Computing	Non	Oui
Fog Computing	Non	Oui
Scalabilité	Non	Oui
Connectivité	Faible	Très fort

Tableau 1.1. Une comparaison entre les réseaux véhiculaires VANET et IoV.

1.2.1.2. Le nombre croissant de victimes de la circulation:

Les trois principaux problèmes liés à la circulation routière sont la sécurité, l'efficacité et la pollution. Ce sont les principales causes de préoccupation concernant la conception et le développement de l'IoV. L'IoV fournirait un cadre plus fiable pour les communications véhiculaires, par rapport aux VANET pour les applications de service de technologie et l'information (STI) intelligentes. La communications véhiculaires fiables permettrait de réduire efficacement les accidents de la circulation [8]. Le nombre croissant de victimes de la circulation dans le monde a été signalé dans diverses enquêtes [9], [10]. Les faits principaux de certains rapports sont indiqués ci-dessous.

Selon un rapport de l'organisation mondiale de la santé (WHO), le nombre total de décès sur la route dans le monde en raison des divers accidents de la circulation sur la route est de 1,25 million par an [9]. Le nombre moyen de décès par jour est de près de 32876. En ne considérant que les jeunes (15≤âge≤29), les accidents de la route ont causé le plus grand nombre de décès en 2012 parmi les dix principales causes de pertes. Selon un autre rapport, les accidents de la route entraînent des coûts économiques énormes; 3% du Produit Intérieur Brut (PIB) mondial [10]. L'énorme croissance du nombre de véhicules sur route est l'une des principales causes de la pollution de l'air, en particulier dans les capitales. Les rapports suggèrent qu'il existe un besoin urgent de réduire les accidents de la circulation sur la route en utilisant une communication véhiculaire plus fiables basée sur des applications de sécurité.

1.2.1.3. Opportunités de marché:

L'IoV offre une énorme opportunité de marché non seulement pour l'industrie automobile, mais aussi pour une gamme d'autres industries, y compris la fabrication d'équipements informatiques, l'industrie du logiciel et les fournisseurs de services internet. Il y'a une prédiction qui dit que le nombre de véhicules sur la route va augmenter dans le monde [11]. En raison du taux de motorisation plus élevé, la congestion des routes entraînerait un accroissement du temps de déplacement dans les années à venir. Même si 5 minutes du temps perdu à voyager dans le monde sont monétisées, cela devrait générer 25 milliards d'euros de revenus par an d'ici 2030 [12]. L'industrie automobile devrait augmenter la marge bénéficiaire de 54 milliards d'euros en 2012 à 79 milliards d'euros d'ici 2020 [13]. L'utilisation efficace du temps de déplacement est également l'un des principaux objectifs de l'IoV. Un autre facteur clé pour la conception et le développement de l'IoV est les progrès récents et le taux plus élevé de pénétration du marché de l'IoT [14]. Dans le développement de l'IoT, l'industrie automobile est l'une des industries ayant une croissance très rapide. La vente de voitures connectées atteindrait jusqu'à 81 millions par an et la vente de 80% des nouvelles voitures aurait une forme de technologie de conduite connectée d'ici 2025 (voir Fig. 1) [15]. La valeur économique potentielle produite par l'IoV est estimée entre 210 et 740 milliards de dollars par an d'ici 2025.

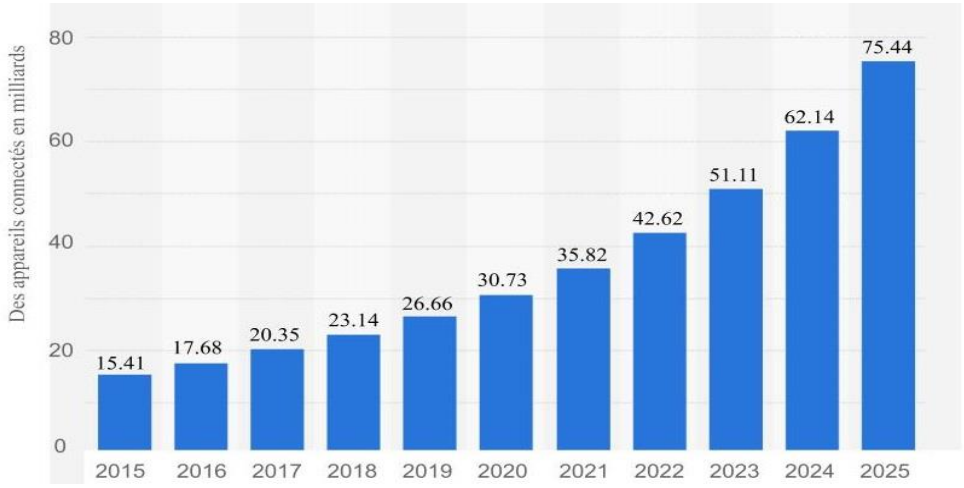

Figure 1.1. La prévision des ventes de voitures avec une certaine forme de connectivité jusqu'en 2025 [15].

1.2.2. Technologies de l'IoV:

Vu que l'environnement du réseau en IoV est hétérogène, une gamme de technologies d'accès sans fil sera disponible pour l'application client, pour établir des connexions avec des serveurs intelligents basés sur le Cloud. Les technologies d'accès sans fil sont divisées en trois catégories: communications véhiculaires, mobiles cellulaires et statiques à petite portée basées sur le réseau de communication. Ces technologies ont été développées pour des différents types de réseaux de communication. Par conséquent, leurs caractéristiques puissance et limite sont différentes. Une préférence prioritaire des technologies accès sans fil est dérivée dans le tableau 1 basée sur les six paramètres qui caractérisent efficacement ces technologies. Les six paramètres importants des technologies d'accès sans fil comprennent le débit de données, portée de communication, support de mobilité, délai de communication, support de sécurité et scalabilité. Cette préférence serait utilisée pour sélectionner la technologie d'accès sans fil approprié pour chaque application client. La sélection de la technologie appropriée serait utile pour maintenir la qualité du service.

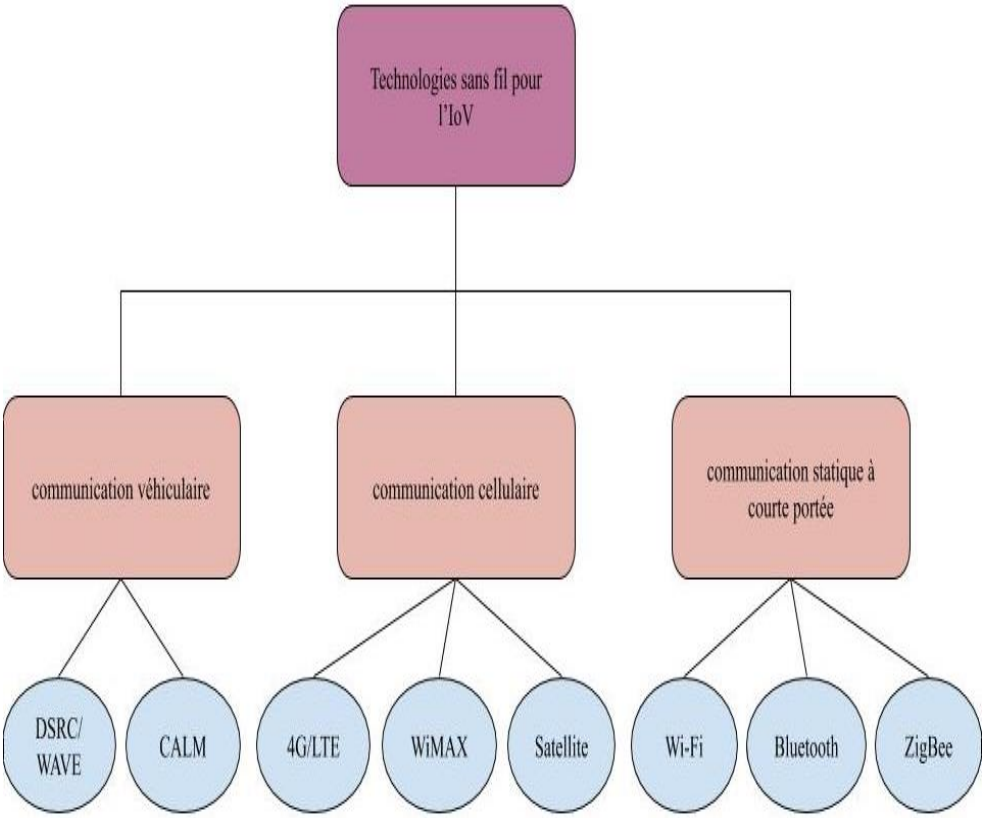

Figure 1.2. Classification de technologie d'accès sans fil pour les applications de l'IoV [16].

Aujourd'hui, il existe de nombreuses technologies d'accès sans fil et méthodes connues telles que les WLAN, WiMAX, cellulaire sans fil, etc. Ces technologies sont utilisées pour assurer la connexion entre les différents composants du réseau de l'IoV et surtout l'insertion des véhicules dans le réseau intégré de l'IoV.

Technologie d'accès sans fil	Débit de données	Portée de communication	Support de mobilité	Délai de communication	Support de sécurité	Scalabilité
DSRC/WAVE	Moyen	Moyen	Très élevé	Très élevé	Très bas	Moyen
CALM	Bas	Moyen	Élevé	Élevé	Très bas	Moyen
4G/LTE	Élevé	Élevé	Moyen	Moyen	Très élevé	Élevé
WiMAX	Moyen	Très élevé	Moyen	Très bas	Élevé	Très élevé
Wifi	Très élevé	Bas	Bas	Bas	Moyen	Bas
Bluetooth	Très bas	Très bas	Très bas	Très bas	Bas	Très bas
ZigBee	Très bas	Très bas	Très bas	Moyen	Moyen	Très bas

Tableau 1.2. Une préférence prioritaire des technologies d'accès sans fil pour IoV [16].

Technologie	Standards	Bande passante	Zone de couverture
WLAN	IEEE 802.11 a/b/g/n	100 Mbps	courte portée
WiMAX	IEEE 802.16 a/e/m	72 Mbps	50 km
3G, 4G, & LTE	IEEE 802.11p / WAVE	Véhicule en mouvement: 384 kbps Nœud fixé: 2 Mbps	1 km

Tableau 1.3. Comparaison entre les technologies de communication les plus connues pour IoV.

Le WLAN contient les normes IEEE 802.11a/b/g/n/p. Il a obtenu une grande acceptation sur le marché, et prend en charge la transmission des données à courte portée à une vitesse relativement élevée. Le débit de données maximal réalisable dans la dernière version (802.11n) est d'environ 100 Mbps. IEEE 802.11p est une nouvelle norme de communication dans la famille IEEE 802.11 qui est basée sur IEEE 802.11a. IEEE 802.11p est conçu pour un accès sans fil dans l'environnement véhiculaire afin de prendre en charge les applications de systèmes de transport intelligentes. L'utilisation des réseaux locaux sans fil dans les VANET nécessite des recherches supplémentaires. Par exemple, *Wellens et al.* [17] ont présentés les résultats d'une vaste campagne de mesure évaluant les performances des normes IEEE 802.11a, b et g dans des scénarios de communication automobile, et ont montrés que la vélocité a un impact négligeable, testé sur une vitesse maximal de 180 km/h. *Yuan et al.* [18] ont évalué les performances du protocole MAC IEEE 802.11p appliqué aux communications de sécurité V2V dans un environnement routier typique. WiMAX contient les normes IEEE 802.16 a/e/m est capable de couvrir une grande zone géographique, jusqu'à 50 km, et peut fournir une bande passante importante aux utilisateurs finaux, jusqu'à 72 Mbps théoriquement. Alors que la norme IEEE 802.16 prend en charge uniquement les communications sans fil à haut débit fixes, La norme IEEE 802.16e/WiMAX mobile prend en charge des vitesses allant jusqu'à 160 km/h et des classes différentes de qualité de service, même pour les transmissions sans visibilité directe.

En comparant les technologies WiMAX et WLAN, nous constatons que le principal avantage est que la méthode d'accès aux canaux dans WiMAX utilise un algorithme de planification où la station d'abonné ne sera en

concurrence avec les autres qu'une seule fois lors de la première tentative de connexion au réseau.

La technologie sans fil cellulaire contient la 3G, la 4G et la LTE. Les réseaux 3G d'aujourd'hui fournissent des données à un débit de 384 kbps aux véhicules lorsqu'ils se déplacent, et peut aller jusqu'à 2 Mbps pour les nœuds fixes. Les systèmes 3G offrent un transfert plus fluide par rapport aux systèmes WLAN et WiMAX [5], [6].

En regardant les technologies d'accès sans fil décrites ci-dessus, la 4G ou LTE devrait être la technologie la plus efficace pour lancer le réseau inter-véhicules et activer l'IoV. Parce que, Premièrement, la 4G ou LTE est la norme de communication la plus utilisée, et a été déployée par la plupart des pays pour fournir des services d'accès. Par conséquent, n'importe quel véhicule peut l'utiliser pour se connecter à l'IoV. Deuxièmement, dans le contexte de bâtiments élevés et d'un environnement urbain complexe, les performances de la 4G ou du LTE sont les meilleures de toutes les technologies d'accès sans fil [19], [20].

1.2.3. Applications d'IoV:

Le développement énorme et rapide du réseau et des technologies de l'information numérique, ont conduit à rendre les véhicules plus intelligents et automatiques. Et a donné naissance à de nombreuses applications qui combinent à la fois la sécurité de conduite et la prestation de services. Les applications IoV peuvent être classées en deux catégories principales: les applications de sécurité et les applications utilisateur. Les applications de sécurité visent à augmenter et améliorer la sécurité des conducteurs et des passagers connectés à l'IoV en envoyant des notifications aux véhicules sur l'état de l'environnement autour d'eux [21]. Les applications utilisateur fournissent aux utilisateurs des différents services utiles. Par exemple, Apple CarPlay, introduit à l'origine comme un system iOS dans les véhicules, offre une intégration automobile complète pour les cartes d'Apple et la navigation détaillée, téléphone, message et service de musique. Semblable à CarPlay, Google Android Auto fournit une interface sans distraction qui permet aux conducteurs de profiter des services en connectant des appareils Android au véhicule. Chinese Tencent a récemment lancé son application de navigation

locale Lubao qui propose des contenus générés par les utilisateurs et des fonctions sociales.

Les technologies visant à améliorer la sécurité des véhicules et des passagers présentent un grand intérêt, l'une des applications la plus importantes est la prévention des collisions. À l'heure actuelle, les technologies anticollision sont en grande partie des systèmes basés sur les véhicules proposés par les fabricants d'équipement d'origine sous forme de packages autonomes qui servent globalement deux fonctions, l'avertissement de collision et l'assistance au conducteur. Le premier prévient le conducteur lorsqu'une collision semble imminente, tandis que le second contrôle partiellement le véhicule soit en régime permanent, soit en tant qu'intervention d'urgence [22]. Pour être plus précis, l'avertissement de collision comprend des notifications concernant un accident de voiture à chaîne, des avertissements sur les conditions routières telles qu'une route glissante et un avertissement de véhicule en approche [20]. D'une part, des avertissements de collision pourraient être utilisés pour avertir les voitures d'un accident survenu le long de la route, empêchant ainsi un empilement de se produire. D'un autre côté, ils pourraient également être utilisés pour avertir rapidement les conducteurs et éviter qu'un accident ne se produise en premier lieu. Notez que la conduite à proximité et à travers des intersections est l'un des défis les plus complexes auxquels les conducteurs sont confrontés car deux ou plusieurs flux de trafic se croisent et la possibilité de collision est élevée [23]. Le domaine d'intersection intelligent, où les dispositifs de contrôle de la circulation conventionnels tels que les panneaux d'arrêt et les feux de circulation sont supprimés, a été un domaine de recherche très vivant ces dernières années. Les véhicules coordonnent leur mouvement à travers l'intersection grâce à une combinaison de prise de décision en temps réel centralisée et distribuée, utilisant le positionnement global, les communications sans fil, la détection et le calcul embarqués.

Les applications utilisateur sont assez variées, allant du streaming multimédia en temps réel ou non en différé et des communications interactives telles que la vidéoconférence, les informations de météo ou l'accès à internet comme le transfert de données, la navigation sur le Web, le téléchargement de

musique et les jeux interactifs, et les applications de service routier, telles que l'emplacement et les listes des prix des restaurants ou des stations d'essence [20]. D'une manière générale, les applications utilisateur fournissent deux services de base liés à l'utilisateur: les services locaux coopératifs et les services Internet mondiaux. Les services locaux coopératifs sont des applications axées sur l'information et le divertissement qui peuvent être obtenues à partir des services locaux tels que la notification de points d'intérêt, le commerce électronique local et le téléchargement de médias. Les services Internet mondiaux se concentrent sur les données qui peuvent être obtenues auprès des services communautaires tels que les assurances et les services financiers, la gestion de la flotte et la gestion des zones de stationnement [24].

1.3. Les éléments réseaux de l'IoV:

Ce modèle d'IoV est proposé en identifiant les principaux éléments du réseau. Les parties constitutives de l'IoV en termes d'éléments de réseau expriment plus efficacement la signification et les fonctionnalités de l'IoV en tant que réseau complètement hétérogène. Les quatre principaux éléments du réseau de l'IoV sont identifiés, notamment: Cloud, Fog, Connexion et Client (voir figure 1.3.). Une vue logique du modèle de réseau IoV proposé est présentée sur la figure 1.4 avec les composants internes de chaque élément.

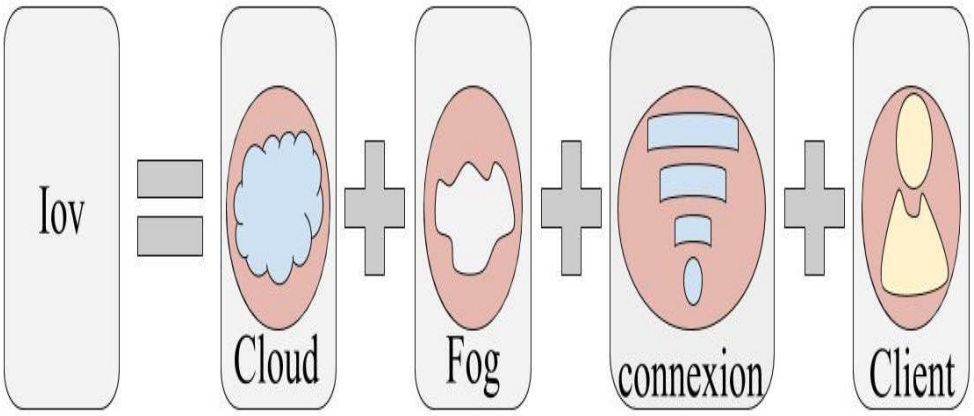

Figure 1.3. Les éléments du réseau de l'IoV [16].

Le premier élément de l'IoV est le Cloud qui représente le cerveau de l'IoV où une gamme de services liés au calcul et traitement intelligents sont proposés en tant que services principaux. Les services sont proposés sur une

plateforme fournie par une infrastructure Fog qui est le deuxième élément de l'IoV. Ces services sont accessibles via une Connexion fiable qui est le troisième élément de l'IoV. Les différents types de communications véhiculaires de l'IoV représentent une connexion différente en raison de l'utilisation de différentes technologies d'accès sans fil. Ces différents types de connexions sont utilisés par des applications Client intelligentes qui constituent le quatrième élément de l'IoV. Chaque application client a des exigences de service qui peuvent être différentes des autres, et qui sont définies en termes de caractéristiques d'une technologie d'accès sans fil.

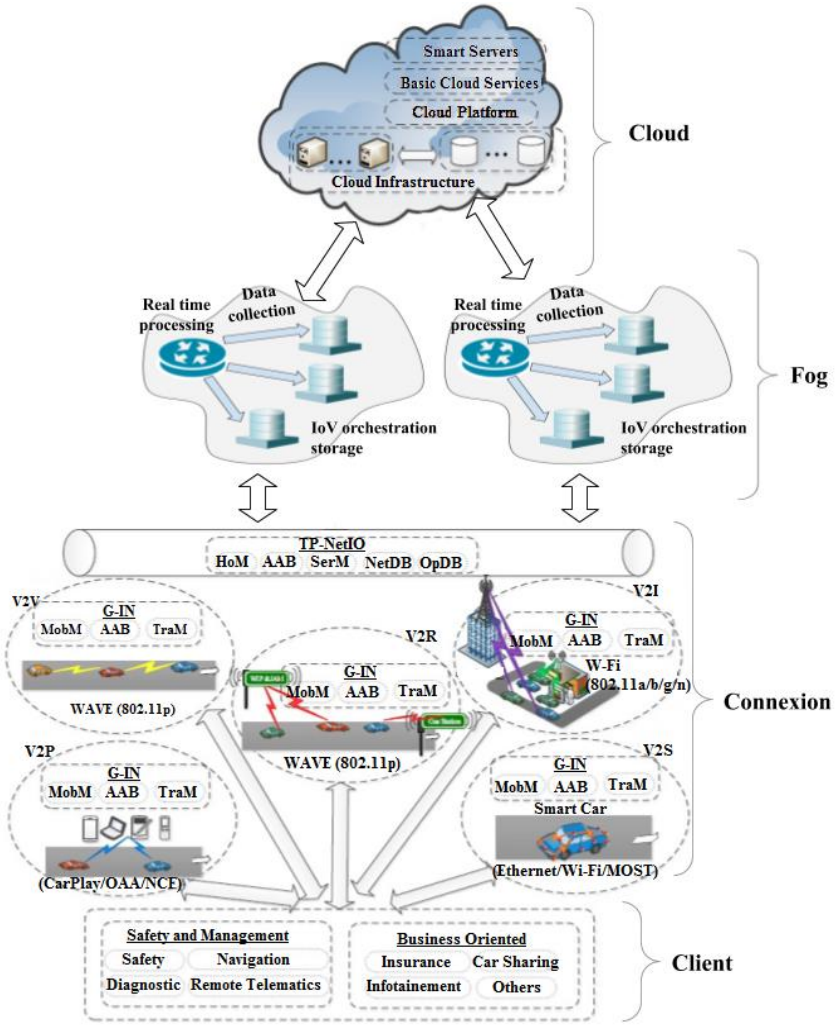

Figure 1.4. Le modèle réseau de l'IoV [16].

1.3.1. Calcul du Cloud:

L'importance des informations liées au trafic augmenterait considérablement avec la réalisation de l'IoV. Ceci est dû à l'intégration de différents types de réseaux avec le réseau des véhicules. Pour collecter, traiter et diffuser dynamiquement des informations sur le trafic en temps réel, il faudrait un système de traitement de l'information à une échelle de péta-octet [25]. Et pour gérer des informations de cette ampleur, le calcul du Cloud Framework est le meilleur environnement. Un Framework est proposé pour mettre en œuvre le rôle du calcul du Cloud en tant qu'élément de l'IoV en utilisant le concept d'applications serveurs basés sur le Cloud (voir figure 1.4). Ce Framework comporte trois niveaux opérationnels principaux: les services Cloud de base, les serveurs d'applications intelligents et les consommateurs et producteurs d'informations.

1.3.1.1. Services Cloud de base:

Les services Cloud de base incluent les services offerts aux applications serveurs intelligentes de trafic, y compris la coopération en tant que service (CaaS), le stockage en tant que service (STaaS), la passerelle en tant que service (GaaS), le calcul en tant que service (COaaS), le réseau en tant que service (NaaS), les données en tant que service (DaaS) [26].

1.3.1.2. Applications Serveurs intelligentes:

Les applications serveurs intelligentes de l'IoV sont divisés en quatre catégories, notamment la sécurité du trafic, la gestion du trafic, l'abonnement aux services et le divertissement [24]. Deux moteurs de traitement: moteurs internes et externes sont pris en compte pour les serveurs intelligents. Le moteur interne comprend une unité de stockage des Big Data, une unité de traitement des Big Data et une unité d'analyse des Big Data traitées. Toutes les opérations de ces trois unités sont effectuées à l'aide des services Cloud de base offerts sur la plateforme Cloud. Le moteur externe comprend une unité de diffusion d'informations chargée de la fourniture de services de bout en bout aux applications clients et une unité de collecte d'informations chargée de la collecte des données source.

1.3.1.3. Consommateur et producteur d'informations (les plateformes du Cloud):

Le rôle susmentionné du calcul du Cloud fait de lui l'un des éléments les plus importants dans la conception et le développement de l'IoV. Les services offerts par les quatre applications serveurs intelligentes sont la base de l'intelligence en IoV [27]. La responsabilité principale des serveurs Cloud est de traiter et d'appliquer l'intelligence artificielle en temps réel sur des données de trafic massives pour prendre des décisions intelligentes pour les applications client intelligentes [28]. L'effort de Google pour développer un système en temps réel basé sur Android pour l'IoV avec l'aide de l'alliance automobile ouverte (OAA) est l'un des meilleurs candidats.

1.3.2. Calcul du Fog:

Le calcul du Fog est un appendice de l'environnement du calcul du Cloud qui fournit divers services au bord du réseau. Il prend en charge les services de données, de stockage, de calcul et d'application pour les utilisateurs finaux tout comme le calcul du Cloud [29]. Il comble également l'écart entre les véhicules/appareils intelligents dans l'IoV et les centres de données distants. De plus, il offre d'autres avantages, tels qu'une bande passante réduite, une latence minimisée et une sécurité renforcée. *Huang et al.* [30] ont conçu trois protocoles dans les IoV qui peuvent améliorer les performances de collecte de données et de diffusion de code en optimisant le déploiement des centres de données. *Yao et al.* [31], et *Asuquo et al.* [32] ont discuté des problèmes de fiabilité, de sécurité et de confidentialité dans l'environnement des IoV. Ainsi, l'environnement de communication IoV présente plusieurs problèmes de sécurité et de confidentialité, tels que la divulgation de données, les fuites de clés de session, la relecture, les attaques d'homme au milieu et d'usurpation d'identité, ainsi que le manque d'anonymat et de traçabilité. Par conséquent, pour sécuriser ce type de communication, nous avons besoin des schémas légers d'authentification et de gestion des clés déployés par le calcul du Fog [33].

1.3.3. Connexion:

La Connexion est utilisée pour établir et maintenir la communication entre le Cloud ou le Fog et les véhicules permettant d'accéder aux services intelligents basés sur le Cloud en IoV. En raison de l'utilisation de plusieurs

technologie d'accès sans fil pour réaliser des réseaux, l'interconnexion entre ces réseaux est très difficile [34]. Il existe deux principaux composants d'une connexion: Interopérateur de réseau tiers (TPNIO) et passerelle d'interconnexion de réseaux (GIN).

1.3.3.1. Interopérateur de réseau tiers (TPNIO):

La nécessité d'un accord de niveau de service (SLA) direct entre les opérateurs des réseaux est réduite en IoV en raison de la considération de TPNIO [35]. Le SLA direct est une contrainte difficile pour tous les réseaux hétérogènes mais TPNIO permet une itinérance transparente sans compromettre la qualité et la sécurité des services des opérateurs de réseau.

1.3.3.2. Passerelle d'Inter-réseautage (GIN):

En raison des environnements de réseau hétérogènes en IoV, différentes technologies d'accès sans fil sont utilisées pour établir des connexions. Il existe cinq types de réseaux de véhicules en IoV, notamment **V2V**, **V2R**, **V2I**, **V2P** et **V2S**:

- **V2V** (Les communications de véhicule à véhicule): Comprennent un réseau sans fil où les automobiles s'envoient des messages avec des informations sur ce qu'elles font. Ces données incluraient la vitesse, l'emplacement, le sens de la marche, le freinage et la perte de stabilité. V2V utilise des communications dédiées à courte portée (DSRC) par le standards 802.11p/WAVE [36].
- **V2R** (Les communications de véhicule à route): Comprennent un réseau sans fil où les véhicules peuvent communiquer avec les marques de voie, panneaux de signalisation et feux de circulation le long de la route afin de connaitre l'état de la route. cette communication est faite via 802.11p/WAVE [37].
- **V2I** (La communication véhicule-infrastructure): Représente l'échange sans fil de données entre les véhicules et l'infrastructure routière afin de fournir des services de communication et d'information aux utilisateurs. Cette communication est faite via Wifi (802.11a/b/g/n) ou 4G / LTE [36].

- **V2P** (Les communications de véhicule à appareil): Représente les communications des appareils personnels des véhicules utilisant CarPlay d'Apple ou le système Android de OAA ou Communication de champ proche (NFC) [38].
- **V2S** (Les communications de véhicule à capteur): Représente les communications des capteurs dans le véhicule via Ethernet, Wifi ou systèmes de transport orientés médias (MOST) [38].

Ces réseaux sont utilisés par les applications clientes pour accéder aux services des serveurs intelligents à l'aide de passerelle d'Inter-réseautage (GIN).

1.3.4. Client:

Les services des serveurs intelligents basés sur le Cloud sont utilisés par les applications Clients à l'aide d'une connexion réseau. Les applications clients ou les clients en IoV peuvent être largement divisés en deux catégories: axé sur la sécurité et la gestion, et axé sur les affaires ou business.

1.3.4.1 Sécurité et gestion:

Les applications ITS liées à la sécurité et à la gestion du trafic sont largement divisées en quatre groupes: sécurité, navigation, diagnostic et télématique à distance.

- **Sécurité:** Les applications ITS liées à la sécurité routière sont des applications basées sur la communication de machine à machine. Les performances et la qualité des opérations pourraient être considérablement améliorées en intégrant des serveurs intelligents basés sur le Cloud [39]. L'une de ces applications est présentée ci-dessous:

– **Prévention d'accident:** Elle empêche les accidents grâce à l'échange d'informations en temps réel entre les véhicules. Elle permet diverses opérations automatiques, notamment le contrôle de la vitesse, le changement de voie, l'arrêt, la commande de direction, etc.

- **Navigation:** Les applications ITS liées à la navigation sont des services basés sur la localisation [40]. Les performances de ces applications dépendent principalement de la précision des informations de localisation. Les informations sont obtenues à partir du récepteur GPS attaché aux

véhicules. Ces applications aident à gérer le trafic et améliorent ainsi l'efficacité du trafic. L'une de ces applications est présentée ci-dessous:

Informations sur le trafic en temps réel: Elle fournit des informations de circulation en direct à l'aide d'un capteur vidéo attaché aux véhicules et de réseaux de communication hétérogènes. Ce système repose sur une diffusion en ligne efficace des informations sur le trafic à l'aide de réseaux de véhicules hétérogènes.

- **Diagnostic:** Les applications liées au diagnostic des véhicules fonctionnent comme consultant en santé personnelle pour les véhicules [41]. Outre la surveillance en temps réel de l'état général des véhicules, la gestion des données en Cloud sur l'état des véhicules est l'une des opérations clés de ces applications. L'une de ces applications est présentée ci-dessous:

– Autoréparation: Il s'agit d'un système de guidage de réparation étape par étape basé sur le Cloud. Il aide le propriétaire du véhicule à résoudre les problèmes matériels / logiciels du véhicule. Le système repose sur une base de données basée sur le Cloud. Des conseils clairs sont disponibles pour tous les types de véhicules grâce aux technologies audio et vidéo.

- **Télématique à distance:** L'accès à distance à certaines opérations non routières de véhicules pourrait être rendu possible grâce à des applications télématiques à distance hautement sécurisées [42]. Les applications sont basées sur des méthodes précises de suivi à distance, d'authentification et d'autorisation.

1.3.4.2. Business:

Les applications ITS pour IoV axées sur les affaires peuvent être largement divisées en quatre catégories: assurance, auto-partage, info-divertissement et autres applications.

- **Assurance:** Les applications ITS basées sur l'assurance utilisent des différents modèles pour fournir une assurance. Les modèles sont basés sur une analyse statistique des informations, y compris l'utilisation des véhicules, le comportement de conduite, le lieu d'utilisation et la durée d'utilisation [43]. L'une de ces applications est présentée ci-dessous:

– Assurance sur les statistiques de conduite: Elle calcule automatiquement les frais d'assurance en utilisant les informations des statistiques de conduite. Les informations incluent la durée de conduite quotidienne / mensuelle / annuelle ou combien vous conduisez et les violations quotidiennes / mensuelles / annuelles des règles de circulation ou comment vous conduisez.

- **Partage de voiture:** Les applications ITS d'auto-partage reposent sur le concept de l'amélioration de l'utilisation des ressources lors de l'utilisation des voitures et donc de la réduction des coûts de transport. Cela peut être réalisé en voyageant en voiture en groupe. L'une de ces applications est présentée ci-dessous:

– covoiturage: Il s'agit d'une application d'auto-partage basée sur une plateforme Cloud. Elle attribue les demandeurs de services automobiles au propriétaire de la voiture. L'allocation est basée sur l'optimisation des critères d'appariement des passagers. Les critères incluent l'adresse locale, le lieu de travail, le moment, le sexe, l'âge et la position d'emploi.

- **Info-divertissement:** Évoluant des concepts de maison connectée, de bureau et de mobilité, il est maintenant temps de conduire connecté. C'est le concept de base des applications ITS d'info-divertissement de l'IoV [44]. L'une de ces applications est présentée ci-dessous:

– Conduite connectée: Il s'agit d'un système de synchronisation d'appareils pour les véhicules. Il connecte l'ordinateur de bord du véhicule à un ordinateur de bureau ou domestique, à un smart phone et à d'autres appareils en ligne. Le système est basé sur une connexion à distance dans différents types d'appareils en ligne avec des informations d'identification de sécurité.

Chapitre II

La sécurité des réseaux véhiculaires (VANET et IoV)

Chapitre II

La sécurité des réseaux véhiculaires (VANET et IoV)

Dans ce chapitre, nous introduisons les différentes notions et objectifs de sécurité des réseaux véhiculaires et les différentes attaques réalisés contre ces objectifs. Nous avons ensuite rassemblé certains des travaux connexes concernant la préservation de la vie privée dans les réseaux VANET et des travaux connexes concernant l'authentification dans les réseaux IoV. Cela nous permettra de nous positionner par rapport à ces différents aspects et d'avoir une idée générale sur les principaux défis auxquels ces réseaux sont confrontés.

2.1. Sécurité d'un réseau véhiculaire:

La sécurité est l'état d'être libre de tout danger ou menace. La sécurité signifie la sûreté, ainsi que les mesures prises pour être sain et sauf ou protégées. En réseaux véhiculaires, il est essentiel de se défendre contre les activités d'utilisation abusive et de bien définir l'architecture de sécurité car il s'agit d'une communication sans fil ayant une topologie très dynamique et de nombreux types de participants qui sont très difficiles à sécuriser. Tout cela a conduit à des menaces potentielles pour la sécurité des communications et de la vie privée des individus. Par conséquent, les solutions préservant la confidentialité de la diffusion de contenus sont devenues extrêmement difficiles et nécessaires, et de nombreuses recherches ont été menées récemment [45], [46].

2.1.1. Objectif de sécurité:

L'authentification et la confidentialité dans les réseaux véhiculaires sont des termes très larges liés à différentes exigences de sécurité. L'une des étapes les plus importantes dans les réseaux véhiculaires est le processus d'authentification par lequel les messages liés au trafic envoyés par des entités autorisées sont acceptés. Le processus d'authentification comprend deux phases principales: la signature et la vérification. Le véhicule émetteur signe les messages et le véhicule récepteur vérifie les messages signés [47]. Ces

données liées au trafic sont très sensibles pour les véhicules. Pour cela on cherche à protéger et à augmenter la sécurité du traitement et l'échange de ces données en respectant les exigences de sécurité. Ces exigences de sécurité comprennent:

2.1.1.1. La confidentialité:

Dans les réseaux véhiculaires, la définition de la confidentialité fait référence à la communication confidentielle [48]. Un ensemble de règles qui limite les restrictions d'accès à certaines ressources. Dans un groupe, ses membres seuls sont en mesure de décrypter les messages qui sont diffusés à chaque membre, et seul un membre récepteur dédié est capable de déchiffrer le message qui lui est consacré. Cela se fait en utilisant le cryptage ou en échangeant un message spécial entre les unités embarquées dans les véhicules (OBU) et les unités côté route (RSU) comme une forme de vérification des données [49].

2.1.1.2. L'intégrité:

Elle garantit que les données ou les messages transmis entre les nœuds ne sont pas modifiés par les attaquants. C.-à-d. aucune altération des données. Ce concept dans les réseaux véhiculaires se combine souvent avec le concept **d'authenticité** pour garantir qu'un nœud doit pouvoir vérifier qu'un message est bien envoyé et signé par un autre nœud sans être modifié par personne. Afin d'obtenir cette propriété, la vérification des données est également requise. Une fois que le véhicule de l'expéditeur est authentifié, le véhicule du récepteur effectue des vérifications des données pour vérifier si le message contient les données correctes ou corrompues. Cela est assuré avec la signature numérique [50], [51].

2.1.1.3. L'authenticité:

Elle garantit que le message est généré par un utilisateur légitime ayant un certificat. Où le destinataire identifie l'expéditeur d'un message via un pseudonyme [52].

2.1.1.4. La disponibilité:

Le réseau doit être disponible et fonctionnel même s'il fait l'objet d'une attaque sans affecter ses performances. Parce qu'un retard en secondes rend le message insignifiant. Ce concept dans les réseaux véhiculaires n'est pas

différent de la disponibilité dans d'autres types de réseaux mais pas facile à assurer en raison de la mobilité à grande vitesse des véhicules [53].

2.1.1.5. La vie privée et l'anonymat:

La vie privée signifie cacher les données personnelles de l'utilisateur contre les nœuds non autorisés à l'aide de clés temporaires et anonymes. On distingue deux cas:

- **Les communications entre les véhicules et les unités côté route(RSU):** la vie privée signifie qu'il est impossible pour un espion de décider si deux messages différents proviennent du même véhicule.
- **Les communications entre véhicules:** la vie privée signifie que déterminer si deux messages valides différents provenant du même véhicule est extrêmement contraignant pour tout le monde, sauf un composant légitime par exemple, le gestionnaire de traçage [54].

L'anonymat signifie que l'identité physique de l'expéditeur d'un message devrait être coûteuse en termes de calcul. Assurer c'est deux concepts offre une vie privée totale de l'emplacement, et personne ne peut donc suivre la trajectoire d'un nœud [55].

2.1.1.6. La non-répudiation:

Les conducteurs doivent être identifiés de manière fiable en cas d'accident. Un expéditeur devrait avoir la responsabilité obligatoire de transmettre les messages de l'enquête qui déterminera la séquence et le contenu corrects des messages échangés avant un accident ou une attaque [56]. Et donc cet expéditeur ne peut pas nier l'envoi d'un message car il est déjà connu d'une autorité de confiance [53]. Ils peuvent récupérer l'identité de l'attaquant même après un dommage via un dispositif anti-sabotage (TPD).

2.2. Les attaques contre les réseaux véhiculaires:

Comme tout autre système de communication et de traitement de données, les réseaux véhiculaires sont exposés à des différents types de menaces et d'attaques. L'absence du problème d'énergie et de capacité d'un OBU à accueillir des dizaines de microprocesseurs confèrent au véhicule une capacité de traitement et de calcul importante. Comparé à un réseau régulier [57], cela représente deux avantages importants pour les nœuds d'un réseau

véhiculaire. En raison de la grande mobilité de ces réseaux, les deux avantages mentionnés affectent la faisabilité des attaques. Ainsi, il existe des attaques possibles dans un réseau régulier qui seront impossibles pour les réseaux véhiculaires et vice versa.

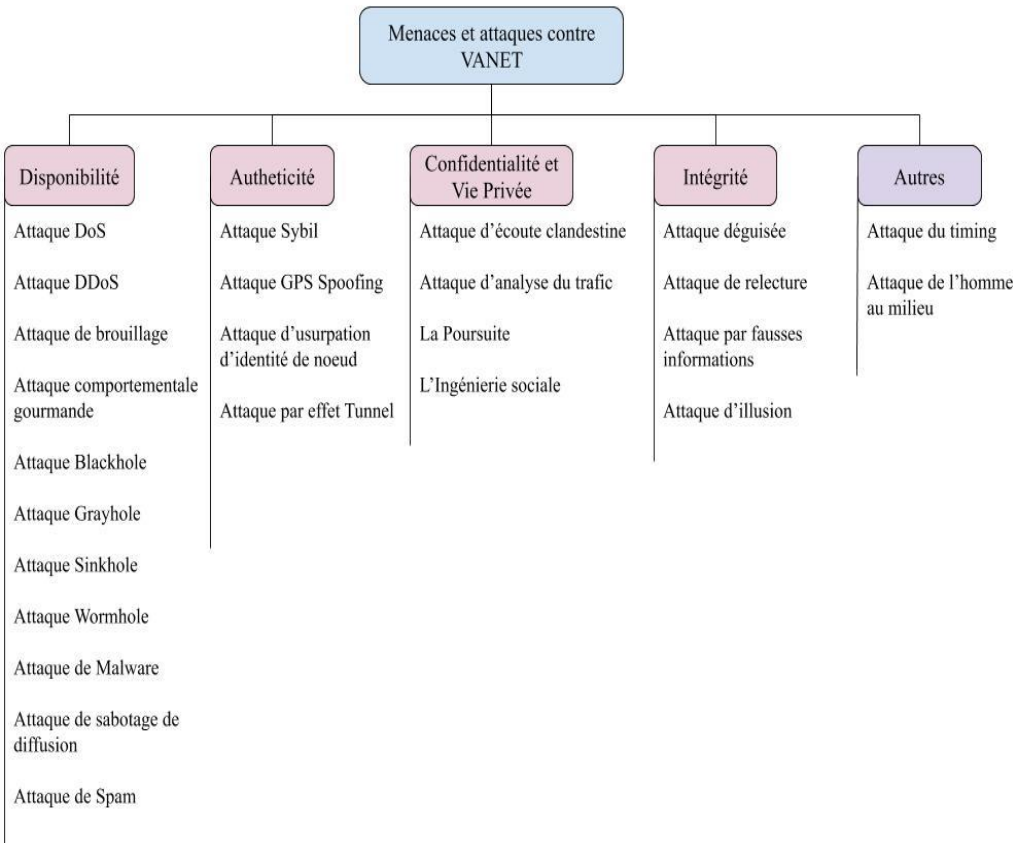

Figure 2.1. Exemples d'attaques contre les réseaux véhiculaires [154].

2.2.1. Attaques contre la disponibilité:

– Attaques par déni de service (DOS): Les attaques DOS sont classées comme une classe d'attaques dangereuses. Elles peuvent être effectuées par des nœuds malveillants internes ou externes au réseau [57]. Dans ces attaques, l'attaquant tente de bloquer les principaux moyens de communication et vise à interrompre les services afin qu'ils ne soient pas disponibles pour les utilisateurs légitimes [58]. Par exemple, inonder le canal de contrôle avec des volumes élevés de messages [59] pour que les nœuds du réseau (OBU et RSU) ne soient pas en mesure de gérer l'énorme quantité de données reçues.

– Attaque Déni de service distribué (DDoS): DDoS est une variante des attaques DOS, c'est une attaque distribuée commandée par un attaquant

principal qui joue le rôle de gérant d'attaque avec d'autres agents qui peuvent également être des victimes sans le savoir [60].

– Attaque de brouillage: Il s'agit d'un niveau physique d'attaque par déni de service. Le brouillage dans sa définition de base est la transmission d'un signal pour perturber le canal de communication, il est généralement intentionnel [61]. Cela réduit le rapport signal / bruit (SNR) pour le récepteur. Dans un réseau véhiculaire, le brouillage une fois réussi peut avoir des conséquences inévitables [62], [61].

– Attaque comportementale gourmande: C'est une attaque contre le fonctionnement de la couche MAC selon l'architecture du modèle OSI. Le nœud gourmand ne respecte pas la méthode d'accès au canal et essaie toujours de se connecter au réseau. L'objectif principal est d'interdire à d'autres nœuds d'utiliser le support et les services. Il essaie aussi de minimiser son temps d'attente pour un accès plus rapide au canal et de pénaliser les autres nœuds non compromis. Ces attaques provoquent des problèmes de surcharge et de collision sur le support de transmission, ce qui entraîne des retards dans les services des utilisateurs autorisés [63].

– Attaque Trou noir (Blackhole): C'est une attaque classique contre la disponibilité dans les réseaux Ad-hoc, elle existe aussi pour les réseaux véhiculaires. Dans l'attaque Blackhole, le nœud malveillant reçoit des paquets du réseau, mais il refuse de participer aux opérations de routage des données. Cela perturbe les tables de routage et empêche l'arrivée de données vitales aux destinataires [57], [64].

– Attaque du trou gris (Grayhole): Elle est considérée comme une variante d'attaque Blackhole. Elle consiste à supprimer uniquement les paquets de données de certaines applications surtout celles qui sont vulnérables à la perte de paquets [65].

– Attaque de gouffre (Sinkhole): Cette attaque consiste en ce que le nœud malveillant attire les nœuds voisins afin que leurs paquets le traversent, cela permet d'éliminer ou de modifier les paquets reçus avant de les retransmettre éventuellement. L'attaque Sinkhole peut être utilisée pour monter d'autres attaques comme Grayhole et Blackhole [66].

– Attaque trou de ver (Wormhole): C'est une attaque grave dans les réseaux véhiculaires, où deux nœuds malveillants ou plus créent un tunnel pour transmettre des paquets de données d'une extrémité "A" à l'autre extrémité "B" et ces paquets sont diffusés sur le réseau par "B". Ces paquets de données suggèrent aux nœuds voisins de "B", que "A" est leur voisin [67]. Cette attaque permet à deux ou plusieurs nœuds légitimes et non voisins d'échanger des paquets de contrôle entre eux pour créer des routes inexistantes [68].

– Attaque de malware: Étant donné l'existence de composants logiciels pour faire fonctionner l'OBU et le RSU, l'infiltration des malwares (logiciels malveillants) est possible dans le réseau véhiculaire lors de la mise à jour logicielle des unités OBU ou RSU [58], [64]. L'effet d'un malware est similaire à l'effet des virus et des vers dans un réseau informatique ordinaire, sauf que dans un réseau véhiculaire, la perturbation des fonctionnalités est toujours suivie de graves conséquences.

– Attaque de sabotage de diffusion: Dans ce type d'attaque, l'attaquant est un nœud légitime. Il tente de créer et d'injecter de faux messages d'alerte de sécurité dans le réseau. Cela peut cacher les vrais messages de sécurité aux utilisateurs légitimes, et peut également provoquer des accidents et affecter gravement la sécurité globale du réseau [57].

– Attaque de spam: Les messages de spam n'ont aucune utilité pour les utilisateurs. Dans un réseau véhiculaire qui est un environnement radio mobile, ce type d'attaque vise à consommer la bande passante et provoquer des collisions volontaires. L'absence d'une gestion centralisée du support de transmission, rend plus difficile le contrôle de telles attaques [58], [57].

2.2.2. Attaques contre l'authenticité:

– Attaque Sybil: Dans cette attaques un véhicule malveillant déclare être plusieurs véhicules en présentant plusieurs identités à la fois. Cette attaque est très dangereuse car un véhicule peut prétendre se trouver dans différentes positions en même temps, créant ainsi un chaos et d'énormes risques pour la sécurité du réseau véhiculaire [69].

– Attaque par falsification de position (GPS Spoofing): Dans les réseaux véhiculaires, une table de localisation avec les emplacements géographiques et les identités des véhicules est un élément critique qui est maintenu grâce au

satellite GPS [58]. L'attaquant utilise un simulateur de satellite GPS pour générer des signaux plus forts que ceux générés par le système satellite réel, et donc produire de fausses lectures dans le GPS pour tromper les véhicules en leur faisant croire qu'ils se trouvent à un endroit différent [64]. Cette attaque peut faciliter d'autres attaques telles que des attaques contre des applications qui utilisent la position du nœud comme méthode d'identification.

– Attaque d'usurpation d'identité de nœud: Chaque véhicule possède un identifiant réseau qui permet de le distinguer des autres nœuds dans le réseau [64]. Cet identifiant devient particulièrement important en cas de problème. Dans cette attaque, l'attaquant obtient une pièce d'identité valide et passe pour un autre véhicule légitime du réseau.

– Attaque par effet tunnel: Elle est presque similaire à l'attaque par trou de ver (Wormhole) [57]. Dans cette attaque, les attaquants utilisent le même réseau pour établir une connexion privée (tunnel), cette attaque relie deux parties distantes du réseau de véhicules en utilisant un canal de communication supplémentaire (tunnel) [70]. Ce qui permet aux victimes de deux parties éloignées du réseau de communiquer en tant que voisins.

2.2.3. Attaque contre la confidentialité et la vie privée:

– Attaque d'écoute clandestine: Dans les réseaux sans fil tels que les réseaux véhiculaires, l'écoute des médias est une attaque facile à réaliser. De plus, elle est passive et la victime n'est pas au courant de la collecte. L'attaque d'écoute est contre la confidentialité, elle est sans impact imminent sur le réseau [58]. Grâce à cette attaque, plusieurs types d'informations utiles peuvent être collectées, telles que des données de localisation qui peuvent être utilisées pour suivre les véhicules

– Attaque d'analyse du trafic: Dans un réseau véhiculaire, l'attaque d'analyse du trafic est une grave menace passive contre la confidentialité et la vie privée des utilisateurs. L'attaquant analyse les informations collectées après une phase d'écoute du réseau, il tente d'extraire le maximum d'informations utiles à ses propres fins [58].

– **Poursuite:** C'est la poursuite d'un véhicule pendant son trajet [71], [58].

– Ingénierie sociale: C'est savoir si un véhicule à un moment précis est dans un garage ou en circulation [71], [58].

2.2.4. Attaques contre l'intégrité:

– Attaque déguisée: Cette attaque est réalisé en utilisant la fabrication, l'altération et la relecture de messages. L'attaquant est caché à l'aide d'une identité valide (appelée masque), et il tente de former un trou noir ou de produire de faux messages qui semblent provenir d'un nœud authentique. Par exemple, un nœud malveillant peut se faire passer pour une ambulance pour demander à d'autres de prendre une voie prioritaire ou exiger des RSU à proximité de changer les feux de circulation au vert, et ainsi tromper les autres véhicules [70].

– Attaque de relecture: Il s'agit d'une attaque classique, elle consiste à rejouer (diffuser) un message déjà envoyé pour en profiter au moment de sa soumission. Par conséquent, l'attaquant l'injecte à nouveau dans les paquets réseau précédemment reçus. Cette attaque peut être utilisée afin que l'attaquant puisse manipuler l'emplacement et les tables de routage des nœuds. Contrairement à d'autres attaques, l'attaque de relecture peut être effectuée par des utilisateurs non légitimes [72].

– Informations fausses: Comme son nom l'indique, cette attaque est contre l'intégrité, elle consiste à modifier, supprimer, construire ou altérer des données existantes. Cela peut se produire en modifiant une partie spécifique du message à envoyer [70].

– Attaque d'illusion: C'est une application directe de l'attaque de fabrication de messages. Dans cette attaque l'attaquant qui est un nœud légitime trompe volontairement les capteurs de sa voiture pour produire des lectures de capteur erronées et donner des informations de trafic incorrectes [73]. Ainsi des messages d'avertissement de trafic incorrects sont diffusés aux voisins par le système du réseau.

Le masquage, la relecture, la falsification, la suppression, la fabrication, la modification et l'illusion de messages peuvent être considérés comme des attaques contre l'authenticité et l'identification.

2.2.5. Autres attaques:

– Attaque du timing: Cette attaque consiste à retarder la transmission de messages avec des exigences élevées sur le délai de propagation, lorsque des véhicules malveillants reçoivent un message, ils ne le transmettent pas

normalement, mais ajoutent des intervalles de temps au message d'origine pour créer un retard [74].

– **Attaque de l'homme au milieu:** Cette attaque peut être réalisée dans plusieurs contextes. Un véhicule malveillant est inséré entre le véhicule émetteur et le véhicule récepteur pour écouter les communications entre eux, faire semblant d'être chacun pour répondre à l'autre, et donc il peut contrôler la communication entre les deux victimes [64]. Dans la littérature, l'attaque de l'homme au milieu est utilisé pour violer les mécanismes d'authentification et /ou d'intégrité et de non-répudiation.

2.3. Travaux Connexes:

2.3.1. Les travaux connexes sur la préservation de la vie privée pour VANETs:

Schémas	Le model réseau	Les objectives	Les méthodes cryptographiques	Performance(+) et Limitation(-)
SECSPP [75] (2008) Cité 263 13/03/2020	VANET qui se compose de deux types d'entités: les véhicules mobiles et les dispositifs routiers.	Assurer la préservation conditionnelle de la vie privée sur la base d'un schéma d'établissement de clé légèrement authentifié.	– Cryptographie à clé publique basée sur l'ID [76]. – Signature aveugle [77]. – Chaîne de hachage unidirectionnelle [78].	+Coût de calcul réduit. +Temps de communication réduit. +pas de dépassements de mémoire. -Prise en compte limitée des exigences de routage. Comparé à: Schéma de *Yang et al.* [79]. Schéma de *He et al.* [80].
PASS [81] (2010) Cité 292 13/03/2020	VANET qui se compose d'une autorité de confiance (TA) de haut niveau, de quelques RSU stationnaires déployés au bord des routes et d'un grand nombre de véhicules équipés d'OBU se déplaçant sur la route.	Résoudre les problèmes d'authentification et de vie privée dans VANET.	– Chaînes de hachage [82]. – Appariements bilinéaires [83]. – L'algorithme de signature Schnorr [84].	+Faible charge de Révocation. +Faible charge de mise à jour du certificat. +Faible surcharge de l'authentification. -La vie privée de l'emplacement n'est pas considéré. Comparé avec: Schéma BP [85]. Schéma ECPP [86]. Schéma DCS [87]. Schéma Hybrid [88].
PACP [89] (2011) Cité 160 13/03/2020	VANET avec une autorité de certification allégée qui comprend les	Résoudre les problèmes d'authentification et de vie privée dans	– Cartographie bilinéaire [90]. – PKI basée sur le crypto système à courbe elliptique	+Analyse de latence du protocole. +Comparaison des temps de recherche pour la révocation.

	véhicules, les RSU et le réseau de communication.	VANET tels que la faible latence de génération de pseudonymes, la grande évolutivité et la révocation facile.	(ECC) [91]. – Cryptage basé sur l'identité [83]. – Signature BLS [92].	-Les modèles de mobilité ne sont pas pris en compte. Comparé avec: Schémas basés sur RSA[47]. Schéma ECPP [86].
PCS [93]. (2012) Cité 393 13/03/2020	VANET qui se compose d'un grand nombre de véhicules et d'une collection de spots sociaux.	Facilitez les véhicules pour atteindre une localisation de haut niveau.	– Technologie d'authentification de la préservation de la vie privée conditionnelle [94]. – La courte signature Boneh-Boyen [95].	+Taille du jeu d'anonymat. +Gain de confidentialité de la position. +La faisabilité est prouvée en utilisant des techniques de théorie des jeux. -Analyse limitée avec le modèle de menace. Pas de comparaison avec d'autres schémas.
DIKE [96] (2012) Cité 164 13/03/2020	VANET avec un service basé sur la localisation (LBS) qui comprend un fournisseur de services (SP), certaines unités RSU déployées et un grand nombre d'utilisateurs de véhicules.	Soutenir l'authentification et la préservation de la vie privée et permettre aux utilisateurs de véhicules à mettre à jour de manière autonome la clé de session.	– Technique d'appariement [97]. – Authentification PPA avec la vérification double d'enregistrement [97].	+Un bon délai de mise à jour des clés. +Ratio de mise à jour clé très acceptable. -Nécessitent des opérations cryptographiques coûteuses Comparé uniquement avec des schémas traditionnels de distribution des clés.
PPBMA [98] (2013) Cité 37 13/03/2020	VANET qui se compose de trois entités: l'autorité de confiance supérieure (TA), RSUs et OBUs.	Soutenir une conservation de la vie privée des messages diffusés.	– Chaînes de hachage à deux niveaux [99]. – AP-Kerberos [100]. – Méthode de signature publique / privée [101].	+Délai moyen de la couche liaison. +Délai moyen de la transmission des paquets de données. -La confidentialité de l'emplacement n'est pas prise en compte. Comparé avec: Schéma ECDSA [102]. Schéma TSVC [103]. Schéma TESLA [104].
VSPN [40] (2014) Cité 157 13/03/2020	VANET qui se compose d'unités embarquées (OBU)	Guider les véhicules vers les destinations souhaitées de manière	– Carte bilinéaire [106]. – schéma de ré-chiffrement du proxy [107],	+Coût de calcul réduit. +Réduction du temps de déplacement +Analyse de la complexité temporelle

	installées sur les véhicules, d'unités routières (RSU) le long des routes et d'une autorité de confiance (TA).	distribuée et soutenir la préservation de la vie privée des conducteurs.	[108].	-Analyse limitée avec le modèle de menace Comparé avec: Schéma IBV[109].
Rabich et al. [110]. (2015) Cité 23 13/03/2020	VANET avec une autorité centralisée (TP), les RSU et un grand nombre de véhicules.	Protéger la vie privée des intérêts des autres véhicules qui n'ont pas le même intérêt.	– Le cryptage Homomorphique [111]. – Cryptage basé sur les attributs [112], qui utilise la méthode cartographie d'appariement bilinéaire.	+Coût de calcul réduit. +Temps de communication réduit. -Analyse limitée avec le modèle de menace. -Les modèles de mobilité ne sont pas pris en compte. -La confidentialité de l'emplacement n'est pas prise en compte. Aucune comparaison avec d'autres schémas.
MixGroup [113]. (2016) Cité 77 13/03/2020	VANET qui se compose d'un certain nombre de véhicules, des RSUs et d'un centre de données Intelligent Transportation System (ITS) et de globale Social Spots et de individuel Social Spots.	Exploiter les opportunités de réunion pour changer le pseudonyme et améliorez la préservation de la confidentialité de l'emplacement.	– La courte signature Boneh-Boyen [95] [114]. – Algorithme RSA [105]. – Mécanisme de pseudonyme [113]. – Signature de groupe [113]. – Identité temporelle en groupe [113].	+Entropie globale du pseudonyme du VSN entier. +Entropie pseudonyme attendue et réelle d'un véhicule cible. +Analyse avec le modèle de menace. -De nombreuses hypothèses nécessaires pour comprendre la mise en œuvre. Comparé avec: schéma Mix-zone [115] PCS [93]

Tableau 2.1. Travaux connexes sur la préservation de la vie privée pour VANETs

2.3.1.1. Schéma SECSPP [75]:

Il s'agit d'un schéma d'établissement de clés légèrement authentifié avec préservation de la vie privée proposée pour sécuriser les communications entre les véhicules mobiles et l'infrastructure routière dans un VANET appelé SECSPP. Ce système proposé permet non seulement l'authentification des infrastructures de véhicule à véhicule et de véhicule à bord de route et

l'établissement des clés pour la communication entre les membres, mais aussi intègre des techniques de signature aveugle dans le système en permettant aux véhicules mobiles d'interagir de manière anonyme avec les services de l'infrastructure routière. Ce schéma est également efficace dans sa mise en œuvre sur les véhicules mobiles par rapport à d'autres propositions connexes.

2.3.1.2. Schéma PASS [81]:

Il s'agit d'un schéma d'authentification pseudonyme efficace avec une forte protection de la vie privée, pour les communications véhiculaires. Contrairement aux schémas d'authentification pseudonymes traditionnels, la taille de la liste de révocation de certificats (CRL) dans PASS est linéaire avec le nombre de véhicules révoqués et indépendante du nombre de certificats pseudonymes détenus par les véhicules révoqués. PASS prend en charge le service de certificats distribués assisté par l'unité routière (RSU) qui permet aux véhicules de mettre à jour les certificats sur la route, mais où la surcharge de service est presque indépendante du nombre de certificats mis à jour. De plus, PASS assure une forte protection de la vie privée des véhicules afin que les adversaires ne puissent tracer aucun véhicule, même si toutes les RSU ont été compromises. Des simulations approfondies démontrent que PASS surpasse les programmes précédemment signalés en termes de coût de révocation et de surcharge de mise à jour des certificats.

2.3.1.3. Schéma PACP [89]:

Il s'agit d'un système de préservation de la vie privée, appelé vie privée conditionnelle basée sur l'authentification pseudonyme (PACP), ce qui permet aux véhicules d'un réseau VANET d'utiliser des pseudonymes à la place de leur véritable identité pour obtenir une intimité dont la fiabilité est prouvée. Dans ce schéma, les véhicules interagissent avec les unités routières pour les aider à générer des pseudonymes pour la communication anonyme. Dans sa configuration, les pseudonymes ne sont connus que par les véhicules. De plus, ce schéma fournit un mécanisme de révocation efficace qui permet d'identifier et de révoquer les véhicules du réseau si nécessaire. Ainsi, il fournit une vie privée conditionnelle aux véhicules du système, c'est-à-dire que les véhicules seront anonymes dans le réseau jusqu'à ce qu'ils soient révoqués.

2.3.1.4. Schéma PCS [93]:

Il s'agit d'une stratégie efficace de changement de pseudonyme aux points sociaux (PCS) présentée pour atteindre la confidentialité de l'emplacement probable. En particulier, il présente d'abord les espaces sociaux où plusieurs véhicules peuvent se rassembler, en prenant une taille anonyme d'un ensemble comme mesure de la vie privée de l'emplacement, il développe ensuite deux modèles analytiques d'anonymat pour enquêter quantitativement sur la vie privée de l'emplacement qui est obtenue par la stratégie PCS. De plus, il utilise des techniques de théorie des jeux pour prouver la faisabilité de la stratégie PCS dans la pratique. Des évaluations approfondies des performances sont menées pour démontrer qu'une meilleure confidentialité de l'emplacement peut être obtenue lorsqu'un véhicule change ses pseudonymes à certains endroits hautement sociaux et que la stratégie PCS proposée peut aider les véhicules à changer intelligemment leurs pseudonymes au bon moment et au bon endroit.

2.3.1.5. Schéma DIKE [96]:

Il s'agit d'un schéma de gestion de clés dynamiques préservant la vie privée appelé DIKE. Il proposé d'assurer la protection de la vie privée d'un utilisateur de véhicule tout en améliorant l'efficacité de la mise à jour des services basés sur la localisation (LBS) dans les réseaux VANETs. Plus précisément, dans le schéma DIKE proposé, il introduit d'abord une technique d'authentification préservant la vie privée qui fournit non seulement l'authentification anonyme de l'utilisateur du véhicule mais permet également la détection de double enregistrement. Il présente ensuite des procédures efficaces de mise à jour des clés de session LBS. Les évaluations des performances via des simulations approfondies démontrent l'efficience et l'efficacité du schéma DIKE proposé en termes de délai de mise à jour discret et de ratio de mise à jour rapide.

2.3.1.6. Schéma PPBMA [98]:

Il s'agit d'un schéma d'authentification de messages diffusés préservant la confidentialité (PPBMA), qui, au lieu d'effectuer une vérification asymétrique, utilise la fonctionnalité MAC (Message Authentication Code) et les opérations HASH pour authentifier les messages. De plus, il utilise une

chaîne de hachage de clé à deux niveaux, ce qui permet d'éviter les pertes de messages. Les résultats de la simulation montrent que PPBMA a des performances supérieures en termes de taux de perte de paquets et de latence de livraison des messages par rapport aux solutions existantes. En raison de cet avantage, il peut prendre en charge les messages d'urgence et de routine, tandis que les solutions existantes ne peuvent prendre en charge que les messages de routine.

2.3.1.7. Schéma VSPN [40]:

Il s'agit d'un système de navigation qui utilise les informations routières en ligne collectées par un réseau ad hoc de véhicules (VANET) pour guider les conducteurs vers les destinations souhaitées en temps réel et de manière répartie. Le schéma proposé a l'avantage d'utiliser les conditions routières en temps réel pour calculer un meilleur itinéraire et en même temps, la source d'information peut être correctement authentifiée. Pour protéger la vie privée des chauffeurs, la requête (destination) et le chauffeur qui l'émet sont garantis d'être non liés à aucune partie, y compris l'autorité de confiance. Il utilise l'idée des identifiants anonymes pour atteindre cet objectif. Ainsi que l'authentification et la préservation de la vie privée, ce système remplit toutes les autres exigences de sécurité nécessaires. En utilisant les vraies cartes de New York et de Californie, *T. W. Chim et al.* ont menés une étude de simulation sur leur schéma montrant qu'il est efficace en termes de retard de traitement et en fournissant des itinéraires de temps de déplacement beaucoup plus courts.

2.3.1.8. Schéma de *Rabich et al.* [110]:

Il s'agit d'un système de conversation efficace entre les chauffeurs qui préserve une telle vie privée. Il utilise la technique de chiffrement basé sur les attributs (ABE) pour la vérification anonyme d'intérêt commun et la technique de chiffrement Homomorphique pour la vérification DOI anonyme. De plus, *Rabich et al.* a proposé un mécanisme de recherche efficace pour permettre aux véhicules de vérifier s'ils ont des intérêts communs avec un faible coût de calcul et de communication. Pour sécuriser la conversation, un protocole d'accord de clés est utilisé pour permettre aux chauffeurs qui ont le même intérêt et le même DOI d'établir une clé secrète partagée. Leurs évaluations

approfondies démontrent que leur système peut réussir à préserver la vie privée des conducteurs avec une faible communication et une surcharge de calcul.

2.3.1.9. Schéma MixGroup [113]:

Il s'agit d'un schéma de protection de la vie privée, appelé MixGroup, qui est capable d'exploiter efficacement les rares occasions de réunion pour le changement de pseudonyme. En intégrant le mécanisme de signature de groupe, MixGroup construit des régions étendues pour le changement de pseudonyme, dans lesquelles les véhicules sont autorisés à échanger successivement leurs pseudonymes. En conséquence, pour l'adversaire qui suit, l'incertitude du mélange des pseudonymes est agrandie de manière cumulative, et donc la préservation de la vie privée de l'emplacement est considérablement améliorée. Nous réalisons des simulations pour vérifier les performances de MixGroup. Les résultats indiquent que MixGroup surpasse considérablement les schémas existants. De plus, MixGroup est capable d'atteindre des performances favorables même dans des conditions de faible trafic.

2.3.2. Les travaux connexes sur l'authentification pour IoV:

Schème	Le model réseau	Les objectifs	Les méthodes cryptographiques	Performance(+) et Limitation(-)
PPDAS [116] (2017) Cité 49 15/03/2020	IoV qui se compose de TA, RSU stationnaires et certains véhicules équipés de TPM (module de plateforme de confiance) et OBU circulant sur la route.	Améliorer la sécurité et la vie privée des communications V2V dans les systèmes de transport intelligents.	– Cartes bilinéaires [83]. – TPM et technologie de calcul fiable [116]. – Évaluation de la réputation des nœuds en IoV [116].	+Améliore la sécurité. +Améliore la protection de la vie privée. +Évite le problème de clés escroquées. -Ajout de retard dans la circulation à haute densité. Comparé avec: Schéma CLAKA [117]. Schéma VGKM [118]. Schéma PPAS [119]. Schéma VAAS [120].
P^3 [121] (2017) Cité 59 15/03/2020	IoV qui se compose de trois couches: couche de nuage (Cloud), couche de	Fournit une communication sécurisée et la préservation de la vie privée des véhicules.	– La courte signature Boneh-Boyen [95]. – Certificat de pseudonyme [113]. – Horodatages.	+Améliore la vie privée de l'emplacement. +Temps de communication Réduit. -Les situations avec des véhicules épars ne sont pas prises en compte.

	brouillard (Fog) et couche d'utilisateur.			Comparés avec: Schéma de gestion des pseudonymes [122].
CLSS [123] (2018) Cité 5 15/03/2020	IoV qui se compose principalement de TCC(Centre de contrôle des transports), TBA(autorité du suivi de trace), véhicules et RSU.	fournit une authentification mutuelle anonyme conditionnelle et la préservation de la vie privée.	– Fonctions de hachage unidirectionnelles [78]. – Cartographie bilinéaire [90]. – PKI basée sur le crypto système à courbe elliptique (ECC) [91].	+Coût de calcul réduit. +Atteint une efficacité plus élevée. -Délai de communication élevé. Comparé avec: Schéma HHC [124]. Schéma HTH [125]. Schéma THSW [126]. Schéma CCL [127].
Sharma, N et al. [128] (2018) Cité 1 15/03/2020	IoV qui se compose de Cloud, de RSUs placées à une distance égale le long de la route et de véhicules.	Assure une communication sécurisée entre deux nœuds en IoV et s'assure également qu'aucun nœud malveillant n'est en mesure de pénétrer le système.	– Certificat de pseudonyme [113]. – Technique d'appariement [97]. – Signature de groupe [113].	+Améliore la vie privée des utilisateurs. +Tient des registres des certificats. +Communication sécurisée. -Pas réalisable pour un système à grande échelle. Pas de comparaison avec d'autres schémas.
Cloud-basé RFID [129] (2019) Cité 4 15/03/2020	IoV composé d'étiquettes RFID, de lecteurs et d'un Cloud semi-fiable	Assure une préservation efficace de la vie privée dans le système IoV et empêche le suivi malveillant des attaquants extérieurs.	– Fonctions de hachage [129]. – PRNG [129]. – Exponentiation modulaire [129]. –Flag [129].	+Coût de calcul réduit. +Récupération rapide des informations. +Temps de communication réduits. -La confidentialité de l'emplacement n'est pas prise en compte. -Un temps limité pour les authentifications. Comparé avec: Schéma *Xie et al.* [130]. Schéma *Sarah et al.* [131]. Schéma *Xiao et al.* [132].
WEI HU et al. [133] (2019) Cité 9 15/03/2020	IoV basé sur le Blockchain, qui intègre les OBU et les RSU dans la plate-forme Cloud du Blockchain,	Assure la sécurité de la communication des nœuds dans l'Internet des véhicules et améliore l'efficacité et la vitesse de la communication	– Algorithme BCA-TG [133]. – Méthodes Blockchain [134]. – La séquence temporelle [133].	+Décentralisation. +Tolérance aux pannes. +Évolutivité. -L'entrée / sortie simultanée de plus de 10 nœuds n'est pas prise en charge. Comparé avec: Schéma de *Dorri et al.*

	formant un réseau systématique .	et de la réalisation de consensus entre les nœuds.		[135].

Tableau 2.2. Travaux connexes sur l'authentification pour IoV

2.3.2.1. Schéma PPDAS [116]:

Ce schéma se concentre sur la sécurité et la préservation de la vie privée. Il s'agit d'un schéma d'authentification double pour l'IoV selon ses différents scénarios. Tout d'abord, l'OBU génère automatiquement une identité anonyme et une clé de chiffrement temporaire pour ouvrir une session d'authentification. Deuxièmement, la légitimité et l'anonymat de l'identité réelle du véhicule peut être vérifiée par l'autorité de confiance (TA). Après cela, la réputation du véhicule est évaluée en fonction de son historique de comportement interactif et enfin la clé de session pour V2V peut être établie. Il y a trois avantages majeurs, y compris la préservation de la vie privée et l'amélioration de la sécurité sans une charge de gestion des clés dans des conditions de délai acceptable, l'introduction de l'évaluation de la confiance dans le protocole d'authentification, ainsi que la prise en compte des attributs de comportement du véhicule dans la nouvelle méthode d'évaluation de la réputation. De plus, l'utilisation de la logique Burrows–Abadi–Needham (BAN) prouve l'exactitude de ce schéma.

2.3.2.2. Schéma (P^3) [121]:

La gestion des pseudonymes dans ce schéma est déplacée vers des Fogs spécialisés au bord du réseau appelés pseudonymes Fogs, qui sont composés d'infrastructures routières et déployés à proximité des véhicules. Le programme P^3 présente les avantages suivants:

1. Changement de pseudonyme contextuel.
2. Distribution rapide des pseudonymes.
3. Réduction des charges de gestion des pseudonymes.

De plus, une architecture hiérarchique pour le schéma P^3 est introduite dans F-IoV. Grâce à l'architecture, un jeu de changement de pseudonyme sensible au contexte et des protocoles de communication de gestion des pseudonymes sécurisés sont proposés. L'analyse de sécurité montre que le

schéma P^3 assure une communication sécurisée et la préservation de la vie privée des véhicules. Les résultats numériques indiquent que le schéma P^3 améliore efficacement la vie privée de l'emplacement et réduit les frais de communication pour les véhicules.

2.3.2.3. Schéma CLSS [123]:

Ce schéma se concentre sur la communication sécurisée entre les véhicules et les unités routières. Premièrement *Liu, J et al.* proposent un nouveau schéma de signature courte sans certificat (CLSS) et prouvent son imprévisibilité dans le modèle Oracle aléatoire. Ensuite, en combinant CLSS et une stratégie de gestion régionale. Ils conçoivent un schéma d'authentification rapide mutuelle anonyme efficace pour l'IoV. De plus, l'analyse quantitative des performances montre que le schéma proposé atteint une efficacité plus élevée en termes d'interaction entre les véhicules et les unités routières par rapport aux autres schémas existants.

2.3.2.4. Schéma de *Sharma et al.* [128]:

Il s'agit d'un schéma d'authentification V2I mutuel pour les véhicules se connectant au système IoV. Lorsqu'un véhicule est sur la route et à portée d'une station de base, il est authentifié par la station de base. Le schéma est appelé authentification mutuelle car le véhicule lui-même effectue également une authentification sur la station de base pour s'assurer qu'il ne s'agit pas d'une fausse entité.

2.3.2.5. Schéma Cloud-basé RFID [129]:

Il s'agit d'un protocole d'authentification mutuelle basé sur le Cloud visant à assurer une protection efficace de la vie privée dans le système IoV, qui permet aux gens de voyager efficacement et intelligemment tout en protégeant leur vie privée contre la divulgation. De plus, le fait que l'anonymat du tag soit mis en œuvre protège non seulement les données de vie privée des propriétaires, mais empêche également le suivi malveillant des attaquants extérieurs. Quant au schéma proposé, la preuve basée sur la logique BAN indique qu'il s'agit d'une sécurité logique.

2.3.2.6. Schéma de *WEI HU et al.* [133]:

Ce schéma utilise une architecture d'IoV basée sur la Blockchain, l'algorithme de consensus byzantin basé sur la séquence temporelle et le

protocole de bavardage (Gossip Protocol) pour compléter la communication des informations et l'authentification par consensus, ce qui non seulement garantit la sécurité de la communication et améliore l'efficacité du consensus des nœuds, mais améliore également la tolérance au pannes de l'algorithme. Les résultats expérimentaux montrent que l'algorithme a dépassé la méthode d'authentification traditionnelle en matière de sécurité de l'information et d'efficacité de consensus de l'IoV.

Chapitre III

Un schéma d'authentification sécurisé pour l'IoV

Chapitre III

Un schéma d'authentification sécurisé pour l'IoV

Dans ce chapitre, nous introduisons les différentes notions et connaissances de base concernant les méthodes cryptographiques que nous avons étudiées afin de réaliser ce travail. Ensuite, nous présentons une explication détaillée de notre schéma d'authentification proposé avec ses différentes phases.

3.1. Préliminaires:

3.1.1. Le crypto-system des courbes elliptiques (ECC):

3.1.1.1. Définition:

Une courbe elliptique est l'ensemble des points qui satisfont une équation mathématique spécifique [136]. L'équation d'une courbe elliptique ressemble à ceci:

$$y^2 = x^3 + ax + b. \quad (1)$$

Où le discriminant de $x^3 + ax + b$ soit non nul.

$$\Delta = -(4a^3 + 27b^2) \neq 0. \quad (2)$$

En plus en rajout pour cette courbe un point qui tend vers l'infini noté O.

3.1.1.2 Théorème:

Pour un ECC, nous nous intéressons à une forme restreinte de courbe elliptique qui est définie sur un champ fini. Un intérêt particulier pour la cryptographie est ce que l'on appelle le groupe elliptique modulo p, où p est un nombre premier [136]. Ceci est défini comme suit:

- Choisir deux entiers non négatifs a et b, inférieurs à p qui satisfont:

$$4a^3 + 27\, b^2 \pmod p \neq 0. \quad (3)$$

- Puis former le groupe elliptique E_p (a, b) modulo p dont les éléments (x, y) sont des paires d'entiers non négatifs inférieurs à p satisfaisant:

$$y^2 \equiv x^3 + ax + b \pmod p. \quad (4)$$

Avec le point O qui tend vers l'infini.

Le problème du logarithme discret de la courbe elliptique **(ECDLP)** peut être énoncé comme suit:

- Fixer un point P premier et une courbe elliptique tel que:

$$Q = xP. \quad (5)$$

Où xP représente le point P sur la courbe elliptique ajouté à lui-même x fois.

- Ensuite, le problème du logarithme discret de la courbe elliptique consiste à déterminer x étant donné P et Q. Il est relativement facile de calculer Q étant donné x et P, mais il est très difficile de déterminer x étant donné Q et P [136].

3.1.1.3. Chiffrement /Déchiffrement ECC:

Ils ya plusieurs approches de chiffrement / déchiffrement qui utilisent des courbes elliptiques. La première tâche de ce système consiste à coder le message en clair m à envoyer en tant que point x-y noté P_m. C'est le point P_m qui sera chiffré sous forme de cipher texte et ensuite déchiffré. Notez que nous ne pouvons pas simplement coder le message en tant que coordonnée x ou y d'un point, car ces coordonnées ne sont pas toutes dans le groupe E_p (a, b). Tout comme avec le système d'échange de clés, un système de cryptage/décryptage nécessite comme paramètres un point G et un groupe elliptique E_p (a, b). Alice sélectionne une clé privée n_A et génère une clé publique P_A pour crypter et envoyer un message P_m à Bob.

$$P_A = n_A * xG. \quad (6)$$

Puis Alice choisit un entier positif aléatoire x et produit le cipher texte C_m composé de la paire de points:

$$C_m = \{xG, P_m + xP_B\} \quad (7)$$

Notez qu'Alice a utilisé la clé publique de Bob P_B pour déchiffrer le cipher texte. Donc Bob multiplie le premier point de la paire par sa clé secrète n_B et soustrait le résultat du deuxième point:

$$P_m + xP_B - n_B(xG) = P_m + x(n_BG) - n_B(xG) = P_m \quad (8)$$

Alice a masqué le message P_m en y ajoutant xP_B. Personne sauf Alice ne connaît la valeur de x, donc même si P_B est une clé publique, personne ne peut supprimer le masque xP_B. Cependant, Alice inclut également un indice qui

aide à supprimer le masque si l'on connaît la clé privée n_B. Pour qu'un attaquant récupère le message, il devrait calculer x étant donné G et xG, ce qui est difficile.

3.1.2. Fonction de hachage unidirectionnelle:

3.1.2.1. Définition:

Une fonction de hachage à sens unique est un algorithme qui prend un message de longueur variable en entrée et produit une chaîne de longueur fixe en tant que sortie appelée code de hachage ou simplement hachage du message d'entrée [137]. Une fonction de hachage unidirectionnelle robuste est généralement sensée satisfaire certaines exigences: la résistance à la collision, la résistance à l'image réciproque et l'image réciproque seconde [138].

3.1.2.2. SHA 256 (Secure Hash Algorithm 256):

SHA256 est une fonction de hachage de cryptographie utilisée dans la création de certificats numériques ainsi que dans l'intégrité des données. SHA256 est développé par N.I.S.T (l'Institut National des Normes et de la Technologie) [139]. L'algorithme SHA256 prend en entrée un message de longueur arbitraire inférieure à 2^{64} bits et produit en sortie un résumé de message de 256 bits à l'entrée [140].

3.1.2.3. L'algorithme de SHA 256:

D'une façon générale, l'algorithme SHA256 passe par 7 étapes. Chaque sortie d'une étape devient l'entrée de l'étape qui vient juste après. Ces étapes sont:

- ***Étape 1:*** *Ajout des bits de remplissage*

Le message est rempli de façon à ce que sa longueur soit congrue à 448 modulos 512. Ce remplissage est un seul bit ajouté à la fin du message, suivi par autant de zéros que nécessaire pour que la longueur des bits soit égale à 448 modulos 512 [141].

- ***Étape 2:*** *Ajout de longueur*

Une représentation 64 bits de la longueur du message est ajoutée au résultat. Cette étape consiste à rendre la longueur du message un multiple exact de 512 bits [141].

- ***Étape 3:*** *Analyser le message*

Le message complété est analysé en N blocs de messages de 512 bits, $M^{(1)}$, $M^{(2)}$, ..., $M^{(N)}$, en ajoutant un bloc de 64 bits [141].

- Étape 4: *initialiser la valeur de hachage*

La valeur de hachage initial, $H^{(0)}$ est définie, composée de huit mots de 32 bits, sous une forme hexadécimale [141].

- Étape 5: *préparer le calendrier du message*

SHA256 utilise un calendrier de messages de soixante-quatre mots de 32 bits. Les mots du calendrier du message sont étiquetés W_0, W_1,..., W_{63} [142].

$$W_t = \begin{cases} M_t^{(t)} & 0 \leq t \leq 15 \\ \sigma_1^{(256)}(W_{i-2}) + W_{i-7} + \sigma_0^{(256)}(W_{i-15}) + W_{i-16} & 16 \leq t \leq 63 \end{cases}$$

Où:

$\sigma_1^{(256)}(W_{i-2}) = ((W_{i-2})\ \text{ROTR}\ 17) \oplus ((W_{i-2})\ \text{ROTR}\ 19) \oplus ((W_{i-2})\ \text{SHR}\ 10)$

$\sigma_0^{(256)}(W_{i-15}) = ((W_{i-15})\ \text{ROTR}\ 7) \oplus ((W_{i-15})\ \text{ROTR}\ 18) \oplus ((W_{i-15})\ \text{SHR}\ 3)$

- Étape 6: *initialiser les huit variables de travail a, b, c, d, e, f, g et h avec la* $(i\text{-}1)^{ème}$ *valeur de hachage*

For t=0 to 63:

{

$T_1 = h + \sum_1^{(256)}(e) + Ch(e,f,g) + K_1^{(256)} + W_t$

$T_2 = \sum_0^{(256)}(a) + Maj(a,b,c)$

$H = G$

$G = F$

$F = E$

$E = d + T_1$

$D = C$

$C = B$

$B = A$

$A = T_1 + T_2$

}

Où:

$\sum_1^{(256)}(\boldsymbol{e})$ = *(e ROTR 6)* $\oplus$ *(e ROTR 11)* $\oplus$ *(e ROTR 25)*

$\sum_0^{(256)}(\boldsymbol{a})$ = *(e ROTR 2)* $\oplus$ *(e ROTR 13)* $\oplus$ *(e ROTR 22)*

Ch (e, f, g) = $(e \wedge f) \oplus (\sim e \wedge g)$

Maj (a, b, c) = $(a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$

- Étape 7: *sortie*

Après avoir répété les étapes 1 à 4 au total N fois, la fonction de hachage résultante est: $H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$

3.1.3. La Blockchain:

3.1.3.1. Définition:

La Blockchain est l'une des technologies les plus prometteuses de l'avenir. Elle remplace effectivement le système de transactions actuel. L'idée de la Blockchain a été lancée par un chercheur avec un pseudonyme "Satoshi Nakamoto" qui a appliqué cette technologie pour mettre en œuvre la crypto-monnaie Bitcoin [143]. Cette technologie est décentralisée d'où elle utilise un grand registre public distribué dans lequel les blocs sont chiffrés et enchaînés ensemble dans un ordre chronologique. Diverses fonctionnalités de la Blockchain comme les contacts intelligents, les algorithmes des consensus et le concept du grand registre public peuvent être utilisés indépendamment et appliqués dans différents secteurs [144], [145].

3.1.3.2. La Structure de la Blockchain:

Considérons un système de N utilisateurs à travers un réseau partageant des informations et réalisant des échanges d'actifs. Au lieu de s'appuyer sur un intermédiaire parmi eux, ils s'accordent sur un protocole appelé algorithme de consensus, qui permet d'établir une confiance mutuelle et permet la validation des transactions de pair à pair. Ainsi, les éléments constitutifs d'un système basé sur la Blockchain incluent les participants du réseau, et un protocole de consensus, comme la preuve de travail, les hachages cryptographiques et les signatures numériques. Les participants du réseau peuvent être des individus, des organisations ou des institutions partageant une copie du grand livre contenant leurs transactions valides dans un ordre séquentiel. Le registre est composé d'une séquence de blocs, reliés entre eux par leurs valeurs de hachage

dans l'ordre chronologique pour maintenir l'intégrité et l'actualité des données. Chaque bloc se compose d'un ensemble de transactions signées numériquement par le propriétaire et vérifiées par le reste des participants avant d'être ajoutées au bloc [146].

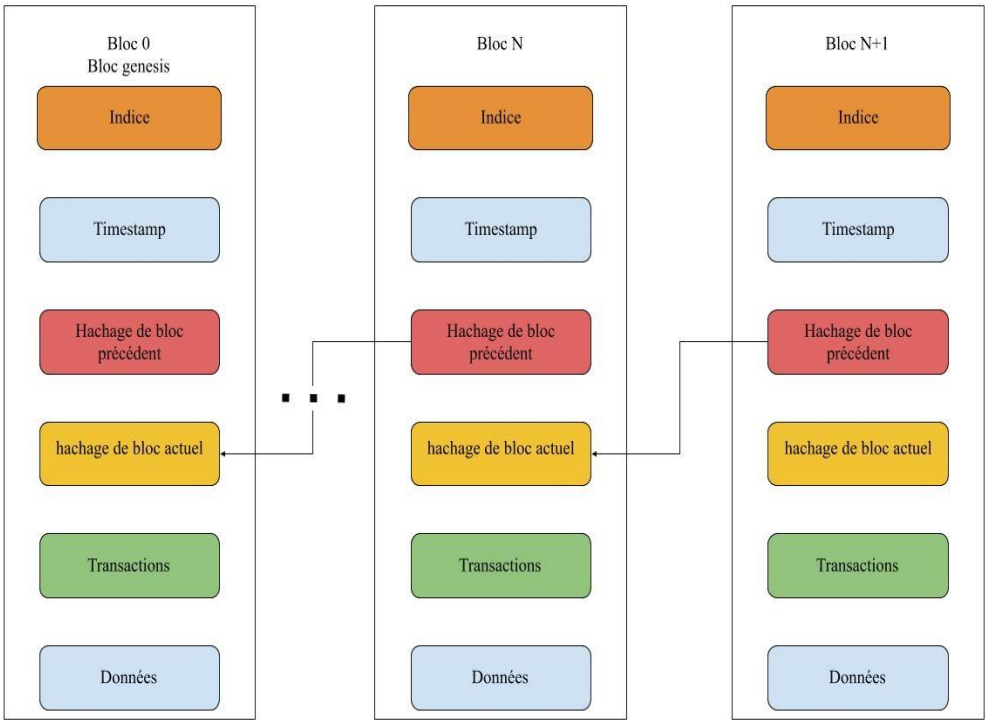

Figure 3.1. Structure d'une Blockchain [147].

3.1.3.3. Application de la Blockchain pour l'IoV:

L'application de la Blockchain libère non seulement le potentiel de nombreuses applications intelligentes, mais change également l'avenir des recherches orientées vers l'internet des véhicules. De nos jours, la Blockchain est la partie essentielle des voitures connectées ou IoV pour gérer la gestion des véhicules, stocker les données dans la durée de vie de la voiture, les exécutions de transactions autonomes, l'efficacité de la gestion des prestataires de services. L'IoV est basé sur l'extension d'un réseau ad hoc qui peut améliorer l'efficacité du trafic [148]. L'IoV est un sous-domaine de l'IoT et leurs caractéristiques sont presque les mêmes, mais la plupart du temps, l'IoT fonctionne en position statique et l'IoV fonctionne sur le mobile. Il est déployé sur les réseaux des capteurs sans fil ouverts qui augmentent la complexité lors des calculs et les traitements des données en raison de l'évolution rapide de la topologie du réseau due à la mobilité. Simultanément, cela augmente les

problèmes de sécurité et de confidentialité tels que les attaques de logiciels malveillants, le piratage d'informations confidentielles ainsi que la falsification de données. La Blockchain est une technologie appropriée pour les applications décentralisées avec des fonctionnalités d'accord réparties, en particulier dans le cas d'un trafic composite où les nœuds mobiles ou les véhicules ne peuvent pas configurer une connexion appropriée en raison d'un manque de confiance les uns envers les autres [46]. Sous le bouclier de protection de la technologie Blockchain, les pirates ne peuvent pas pénétrer ce bouclier grâce à l'utilisation de la fonction de chiffrement. De plus, cette fonctionnalité permet de conserver la réplication des données de comptes par plusieurs fournisseurs de services. D'autre part, la confidentialité des véhicules est un autre défi dans le réseau IoV qui comprend les coordonnées de localisation ainsi que les identités. La Blockchain aide à maintenir le niveau de sécurité et masque les informations des véhicules voisins [149].

3.1.3.4. Algorithme de consensus:

Un algorithme de consensus peut être défini comme le mécanisme par lequel un réseau Blockchain parvient à mettre un accord. Les blocs publics sont construits comme des systèmes distribués et, puisqu'ils ne dépendent pas d'une autorité centrale, les nœuds distribués doivent se mettre d'accord sur la validité des transactions en utilisant un algorithme de consensus [150]. Il y a beaucoup d'algorithmes de consensus, mais en raison des exigences élevées en temps réel et de l'absence de jeton requis, l'algorithme PBFT avec un nombre relativement fixe de nœuds participant au processus de consensus est plus adapté à notre schéma.

L'algorithme de tolérance aux pannes byzantine pratique PBFT est le premier à pouvoir tolérer les défauts "byzantins", proposé par Miguel Castro et Barbara Liskov en 1999 [151]. Cet algorithme fournit des propriétés de fiabilité et de robustesse dans un environnement synchrone et nécessite (N=3f +1) réplique pour tolérer des failles byzantines simultanées. L'algorithme PBFT peut être appliqué efficacement dans presque tous les domaines de l'IoT, y compris l'Internet des véhicules [152].

3.2. Schéma d'authentification pour l'IoV:

3.2.1. Le modèle architecture:

Le scénario envisagé se compose principalement des entités suivantes qui participent activement au provisionnement de la solution d'authentification et d'échange de clés conçu dans le schéma considéré basé sur Blockchain et ECC.

- **Unité côté route (RSU):** Dans les IoV, les RSU sont les nœuds responsables des communications. Ils fournissent des véhicules par les différents services et relaient les différentes informations du trafic entre les autres nœuds. Dans le scénario envisagé, les RSU fournissent des services aux utilisateurs légitimes et aident les véhicules à communiquer avec l'infrastructure IoV.
- **Unité embarquée (OBU):** Les OBU sont les unités et les capteurs montés sur les véhicules pour les aider à faire différentes interactions entre eux (V2V), avec les RSU (V2I) et avec l'environnement / la route (V2R). Ils sont fournis par des entités de communication, de calcul et de stockage. Dans le contexte actuel, les OBU sont référés à des véhicules / utilisateurs qui doivent être enregistrés et authentifiés pour accéder aux services fournis.
- **Autorité de confiance (TA):** La TA est une autorité centrale de confiance qui est responsable de l'enregistrement d'autres nœuds tels que les OBU, les RSU et les BM. C'est aussi le lieu d'initialisation et de publication des paramètres publics pour les fonctions cryptographiques utilisées.
- **Autorité de certification (CA):** Il s'agit d'une entité autorisée enregistrée auprès de la TA, qui prend en charge la mise à jour des certifications dans chaque zone de Fog. Elle peut être un parking, un RSU spécial, une station de service ou un drone dédié.
- **Gestionnaire de la Blockchain (BM):** Le BM est essentiellement responsable de la gestion du réseau Blockchain dans une zone de Fog particulière. Il s'agit d'une entité autorisée, enregistrée auprès de la TA, qui aide les OBU à s'authentifier et à établir une connexion de confiance avec l'infrastructure du Fog.

- **Gestionnaire d'authentification (AM):** Les AM aident à écrire les résultats de l'authentification dans le grand registre public. Les AMs et les BMs sont associés l'un à l'autre pour former un consortium Blockchain et s'appuient sur la tolérance aux pannes byzantines pratiques (PBFT) pour former et établir un consensus.
- **Zone de Fog:** Elle est composée de différents centres de données du Fog véhiculaire chargés de fournir des services aux utilisateurs ciblés. De plus, chaque zone peut encapsuler une ou plusieurs unités RSU, une ou plusieurs entités CA et un seul gestionnaire Blockchain (BM) associé à un gestionnaire d'authentification (AM).

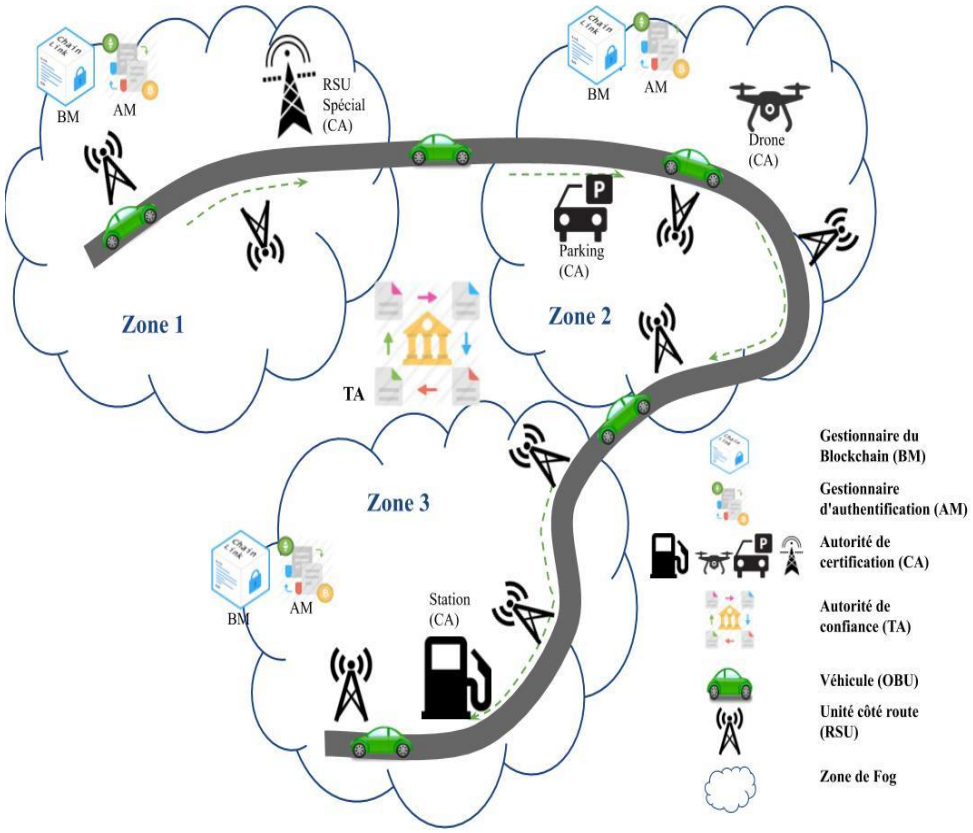

Figure 3.2. Le modèle architecture basé sur le Fog et la Blockchain.

Symbole	Notation
E	Courbe elliptique
P	Point de base de E
n	Un grand nombre premier
PK_X	Clé publique de X
SK_X	Clé secret de X
(•)	Opération multiplicative ECC

SHA265 ( )	Fonction de hachage
ID_X	Identifiant de X
TW_X	Fenêtre de temps généré par X
To_i	Un jeton
h	Un hachage
$CPK_X(M)$	Chiffre le message M avec la clé publique de X
Cert	Un certificat
$\oplus$	Opération XOR
S	Une signature
rn_i	Un nombre aléatoire ∈ Z*p
N_i	Un nombre construit de rni
$AuthTok_X$	Un jeton d'authentification généré par X
SK_{ij}	Une clé de session
CDKf()	Fonction de dérivation de clé
$Vote_{req}$	Un jeton de demande de vote
B_i	Indice du bloc i
Bloc	Contenue du bloc
AM_P	Identifiant de l'AM marqué président
SignK (*B*)	Signé B avec la clé K
$Vote_{res}$	Un jeton de la réponse du vote
Acc_{req}	Un jeton de demande d'accès au service Fog
Maj_{req}	Un jeton de demande de mise à jour de certificat

Tableau 3.1. Les notations utilisées dans notre schéma.

3.2.2. Le modèle system:

Nous pouvons représenter le processus d'échange de clés et d'authentification sur lequel repose notre schéma à travers cinq phases: **Initialisation**, **Enregistrement**, **Authentification mutuelle et échange de clés**, **Consensus** et **Mise à jour du certificat**. Les cinq phases sont décrites en détail ci-dessous:

A. Phase I: *Phase d'initialisation du système*

Lors de l'initialisation, le TA prépare l'environnement pour les phases à venir du schéma proposé en générant différents paramètres publics. Cette phase est élaborée en trois grandes étapes comme suit:

- *Étape 1:* TA génère la courbe elliptique E et fixe ses paramètres publics n et P; un grand nombre premier et le point de base de cette courbe.

- *Étape 2:* TA calcule ses clés publiques et secrètes comme (SK_{TA} & PK_{TA}), où il génère une clé secrète comme: $SK_{TA} \in Z^*_p$ et une clé public comme: $PK_{TA} = SK_{TA} \bullet P$.

- *Étape 3:* Au final, TA définit une fonction unidirectionnelle *SHA265* ( ) fonction de hachage à utiliser pour vérifier l'intégrité lors de la phase III.

Ensuite, les paramètres < *E*, *P*, *n*, *SHA265* ( ), PK_{TA} > sont publiés publiquement.

B. Phase II: *Phase d'enregistrement*

Lors de l'enregistrement, les OBU et RSU sont enregistrés à proximité de TA. Leurs identités respectives (ID_{OBUi} et ID_{RSUk}) sont gardées anonymes et ne sont jamais échangées sans être chiffrées, comme indiqué ci-dessous:

OBU *i* / RSU *k*	TA
- Sélectionne ID_{OBUi} - Générer une fenêtre de temps: TW_{OBUi} - Générer une clé secrète aléatoire: $SK^0_{OBUi} \in Z^*_p$ - Calculer sa clé publique: $PK^0_{OBUi} = SK^0_{OBUi} \bullet P$ - Calculer: $To_0 = \{ID_{OBUi} \| TW_{OBUi} \| PK^0_{OBUi}\}$ - Calculer: $h_0 = SHA256\ (To_0)$ - Calculer: $CPK_{TA}\ (To_0)$	
$\xrightarrow{<CPK_{TA}(To_0),\ h_0,\ TW_{OBUi}>}$	
	- Déchiffrer $CPK_{TA}\ (To_0)$ en utilisant SK_{TA} - Calculer: $h_0' = SHA256\ (To_0)$ - Si $h_0' = h_0$ alors continuer sinon demande au OBU_i de réessayer l'envoie - Extraire ID_{OBUi} et TW_{OBUi} à partir de To_0 - Valider TW_{OBUi} - Vérifier la disponibilité de l'ID_{OBUi} dans son Blockchain - Attribuer un identifiant unique ID_{OBUi} pour l'OBU_i - Générer une clé secrète aléatoire: $SK_{OBUi} \in Z^*_p$ - Calculer sa clé publique: $PK_{OBUi} = SK_{OBUi} \bullet P$ - Calculer: $To_1 = < PK_{OBUi}, SK_{OBUi} >$ - Générer une fenêtre de temps: TW_{TA} - Calculer: $h_1 = SHA256\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$ - stocker: $Cert = SHA256\ (SK_{OBUi} \| ID_{OBUi}) \oplus SHA256\ (SK_{TA} \| ID_{OBUi})$ - Calculer: $CPK_{OBUi}\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$
$\xleftarrow{< CPK^0_{OBUi}\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA}), h_1, TW_{TA} > \text{ sur un canal sécurisé}}$	
- Déchiffrer $CPK^0_{OBUi}\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$ en utilisant SK^0_{OBUi} - Valider TW_{TA} - Calculer: $h_1' = SHA256\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$	

- Si $h_1' = h_1$ alors continuer sinon demande au TA de réessayer l'envoie - Sauvegarder PK_{OBUi}, SK_{OBUi}, et $S = SHA256\ (SK_{TA} \| ID_{OBUi})$

Algorithme 3.1. Phase II: Phase d'enregistrement.

- ***Étape 1:*** OBU_i choisit son identité ID_{OBUi} et génère TW_{OBUi} sa fenêtre de temps en même temps. La fenêtre de temps sera utilisée dans la validation des messages transmis entre lui et TA pour s'assurer qu'ils ne sont pas retardés ou transmis dans le futur. Ensuite, il génère une clé privé initiale SK^0_{OBUi} et calcule sa clé publique PK^0_{OBUi}.

- ***Étape 2:*** Ensuite, l'OBU crée un jeton temporaire composé de la fenêtre de temps, de son identité et de sa clé publique initiale $To_0 = \{ID_{OBUi} \| TW_{OBUi} \| PK^0_{OBUi}\}$, suivi de son hachage en utilisant SHA256 () la fonction de hachage, puis utilise la clé publique de TA PK_{TA} pour le crypter. Le jeton chiffré $CPK_{TA}(To_0)$ et son hachage $h_0 = SHA256(To_0)$ sont ensuite envoyés au TA.

- ***Étape 3:*** Lors de la réception du message $<CPK_{TA}(To_0), h_0, TW_{OBUi}>$, le TA le déchiffre à l'aide de sa clé secrète SK_{TA}, calcule ensuite $h_0' = SHA256(To_0)$ pour le comparer avec h_0 s'ils sont égaux, il passe aux étapes suivantes, sinon demande à OBU_i de renvoyer le message. Puis le TA extrait les valeurs ID_{OBUi}, TW_{OBUi} et PK^0_{OBUi}. Ensuite, valide le jeton en vérifiant sa fenêtre de temps. Si TW_{OBUi} ne dépasse pas la période autorisée, alors le TA passe aux étapes suivantes, sinon la transmission est interrompue et coupe la connexion. Ensuite, TA vérifie dans sa Blockchain si ID_{OBUi} est disponible ou non. S'il est déjà disponible, TA demande à l'$i^{ème}$ OBU pour choisir une nouvelle identité et refaire les étapes ci-dessus.

- ***Étape 4:*** Ensuite, TA déduit une clé secrète et calcule sa clé publique $To_1 =< PK_{OBUi}, SK_{OBUi} >$ pour l'OBU et une signature $SHA256\ (SK_{TA} \| ID_{OBUi})$ et une fenêtre de temps TW_{TA}, les chiffrer à l'aide de la clé publique initiale de l'OBU PK^0_{OBUi} puis calcule son hachage $h_1 = SHA256\ (To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$ et transmet $CPK^0_{OBUi}(To_1, SHA256\ (SK_{TA} \| ID_{OBUi}), TW_{TA})$ et h_1 sur un canal sécurisé. De plus, la TA calcule et stocke également la valeur $Cert = SHA256\ (SK_{OBUi} \| ID_{OBUi}) \oplus SHA256\ (SK_{TA} \| ID_{OBUi})$ dans son registre distribué et transmet $S = SHA256\ (SK_{TA} \| ID_{OBUi})$ au OBU_i.

- *Étape 5:* L'*i*^{ème} OBU déchiffre le message à l'aide de sa clé secrète initiale SK^0_{OBUi}, valide la fenêtre de temps TW_{TA}, puis calcule h_1' = *SHA256* (To_1, *SHA256* (SK_{TA} || ID_{OBUi}), TW_{TA}) et le compare à h_1 s'ils sont égaux, son intégrité est valide et l'OBU stocke les valeurs PK_{OBUi} , SK_{OBUi} et S = *SHA256* (SK_{TA} || ID_{OBUi}) dans son référentiel sinon, il demande au TA de réessayer d'envoyer le dernier message transmis.

C. Phase III: *Phase d'authentification mutuelle et d'échange de clés*

Dans cette phase, les OBU échangent des clés et s'authentifient mutuellement auprès des BM et, à la fin, ils partagent une clé de session pour une connexion ultérieure. Les étapes qui décrivent cette phase sont répertoriées ci-dessous:

- *Étape 1:* Initialement, l'*i*^{ème} OBU génère un nombre aléatoire rn1 et calcule N_1 en effectuant des opérations multiplicatives ECC ($rn_1 \bullet P \bullet SK_{OBUi}$). Puis, il génère une fenêtre de temps TW_{OBUi}.

- *Étape 2:* L'OBU utilise la fonction de hachage *SHA256* ( ), concaténation et opérations XOR pour calculer la valeur du jeton To_{OBUi} = *SHA256* (SK_{OBUi} || ID_{OBUi}) $\oplus$ *S*; comme il est indiqué dans l'algorithme 3.2. Construit ensuite un jeton d'authentification comme suit:

$$AuthTok_{OBUi} = \text{SHA256}\ (N_1 \,||\, ID_{OBUi} \,||\, TW_{OBUi} \,||\, To_{OBUi}\ ).$$

Ensuite chiffrer $AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi} à l'aide de la clé publique PK_{BMj} du BM_j come suit:

$$CPK_{BMj}\,(AuthTok_{OBUi},\ rn_1,\ ID_{OBUi},\ TW_{OBUi}).$$

Enfin, les valeurs < CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}), TW_{OBUi} > sont transmises à la *j*^{ème} BM pour une analyse ultérieure.

OBU *i*	BM *j*
- Sélectionner un nombre aléatoire: $rn_1 \in Z^*_p$ - Générer une fenêtre de temps: TW_{OBUi} - Calculer: $N_1 = rn_1 \bullet P \bullet SK_{OBUi}$ - Calculer: To_{OBUi} = *SHA256* (SK_{OBUi} || ID_{OBUi}) $\oplus$ *S* - Calculer: $AuthTok_{OBUi}$ = *SHA256* (N_1 || ID_{OBUi} || TW_{OBUi} || To_{OBUi}) - Calculer: CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi})	
< CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}), TW_{OBUi} > →	
	- Déchiffrer CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi},

	TW_{OBUi}) en utilisant SK_{BMj} - Valider la fenêtre de temps: TW_{OBUi} - Chercher la valeur *Cert* correspondante à ID_{OBUi} dans la *Blockchain* - Calculer: $AuthTok^*_{OBUi}$ = SHA256 ($rn_1 \bullet PK_{OBUi}$ || ID_{OBUi} || TW_{OBUi} || *Cert*) - Vérifier si: $AuthTok^*_{OBUi} = AuthTok_{OBUi}$ - S'ils sont égales, OBU est marqué authentique; sinon rompre la connexion. - Sélectionner un nombre aléatoire: $rn_2 \in Z^*_p$ - Calculer: $N_2 = rn_2 \bullet P \bullet SK_{BMj}$ - Générer une fenêtre de temps: TW_{BMj} - Calculer: $AuthTok_{BMj} = SHA256$ (N_2 || TW_{BMj} || *Cert*) - Calculer: $SK_{ij} = CDKf$ (ID_{OBUi} || *Cert* || TW_{OBUi} || TW_{BMj}) - Calculer: CPK_{OBUi} ($AuthTok_{BMj}$, rn_2, TW_{BMj})
	< CPK_{OBU} ($AuthTok_{BMj}$, rn_2, TW_{BMj}), TW_{BMj} >
- Déchiffrer CPK_{OBU} ($AuthTok_{BMj}$, rn_2, TW_{BMj}) en utilisant SK_{OBUi} - Valider la fenêtre de temps: TW_{BMj} - Calculer: $AuthTok^*_{BMj} = SHA256$ ($rn_2 \bullet PK_{BMj}$ || TW_{BMj} || To_{OBUi}) - Vérifier si: $AuthTok^*_{BMj} = AuthTok_{BMj}$ - S'ils sont égales, BM est marqué authentique; sinon rompre la connexion. - Calculer: $SK_{ij} = CDKf$ (ID_{OBUi} || To_{OBUi} || TW_{OBUi} || TW_{BMj})	

Algorithme 3.2. Phase III: Phase d'authentification mutuelle et d'échange de clés.

- ***Étape 3:*** Lorsque le BM_j reçoit ces valeurs, il décrypte d'abord CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}) à l'aide de sa clé privée SK_{BMj}, puis il valide la fenêtre de temps TW_{OBUi}. Si la validation est réussie, le BM recherchera donc la valeur *Cert* correspondante à la valeur de ID_{OBUi} dans la liste des OBU enregistrée sur la Blockchain. À l'aide de ces valeurs, BM calcule un jeton d'authentification pour valider la véracité de $AuthTok_{OBUi}$ comme suit:

$$AuthTok^*_{OBUi} = SHA256 ((rn_1 \bullet PK_{OBUi}) \| ID_{OBUi} \| TW_{OBUi} \| Cert)$$

Si les valeurs de $AuthTok_{OBUi}$ et $AuthTok^*_{OBUi}$ correspondent alors le BM valide le $i^{ème}$ OBU et le marque comme authentique, sinon il interrompt la connexion.

- *Étape 4:* Dans cette étape, BM*j* choisit son nombre aléatoire rn_2 pour calculer $N_2 = rn_2 \bullet P \bullet SK_{BMj}$, puis génère sa fenêtre de temps TW_{BMj}, et enfin il calcule son $AuthTok_{BMj}$ comme suit:

$$AuthTok_{BMj} = SHA256\ (N_2 \,||\, TW_{BMj} \,||\, Cert)$$

Ensuite chiffrer $AuthTok_{BMj}$, rn_2, TW_{BMj} à l'aide de la clé publique PK_{OBUi} d'OBU_i comme suit:

$$CPK_{OBU}\,(AuthTok_{BMj},\ rn_2,\ TW_{BMj})$$

De plus, il calcul une clé symétrique, en utilisant la fonction de dérivation de clé de session *CryptDeriveKey* (*CDKf*), pour l'utiliser comme clé de session qui garantira la sécurité sans réauthentification pour les prochaines sessions de communication entre ces deux nœuds:

$$SK_{ij} = CDKf\ (\ ID_{OBUi} \,||\, Cert \,||\, TW_{OBUi} \,||\, TW_{BMj})$$

Enfin, il relaie les valeurs < $CPK_{OBUi}\,(AuthTok_{BMj},\ rn_2,\ TW_{BMj})$, TW_{BMj} > à l'$i^{ème}$ OBU.

- *Étape 5:* A la réception des valeurs < $CPK_{OBUi}\,(AuthTok_{BMj},\ rn_2,\ TW_{BMj})$, TW_{BMj} >, l'OBU décrypte $CPK_{OBUi}\,(AuthTok_{BMj},\ rn_2,\ TW_{BMj})$ à l'aide de sa clé privée SK_{OBUi}, et vérifie si la fenêtre de temps est valide puis continue.

- *Étape 6:* l'OBU collecte les données relatives au BMj et calcule $AuthTok^*_{BMj}$ pour valider l'authenticité du BM comme suit:

$$AuthTok^*_{BMj} = SHA256\ ((rn_2 \bullet PK_{BMj}) \,||\, TW_{BMj} \,||\, To_{OBUi}\ )$$

Ensuite il compare $AuthTok^*_{BMj}$ et $AuthTok_{BMj}$. S'ils sont égaux, cela confirme l'authenticité du $j^{ème}$ BM; et cela implique que les deux parties ont effectué une authentification mutuelle et sont prêtes à transmettre des données différentes entre elles.

- *Étape 7:* Au final, l'OBU_i est capable de calculer la clé symétrique pour l'utiliser comme clé de session et de la stocker pour d'autres communications:

$$SK_{ij} = CDKf(\ ID_{OBUi} \,||\, To_{OBUi} \,||\, TW_{OBUi} \,||\, TW_{BMj}\ )$$

D. Phase IV: *Phase de consensus*

Dans le schéma proposé, les résultats de l'authentification sont transférés à la Blockchain. Nous considérons donc un algorithme de consensus PBFT pour former le grand registre public. On suppose qu'il y a *k* nombre d'AM avec la possibilité d'écrire un bloc dans le grand registre. Au début du consensus, l'un des AM joue le rôle d'un président nommé "**Speaker**" chargé de lancer le processus de consensus; tandis que les autres agissent en tant que membres du congrès nommés "**Congressmen**" qui participent au mécanisme de vote lancé par le président. Pour gagner du temps et éviter de sélectionner de nombreux présidents, nous donnons à un AM sélectionné la possibilité de diriger plusieurs cycles du consensus mais nous lui refusons de participer au vote, les étapes ci-dessous décrivent en détail le processus de consensus:

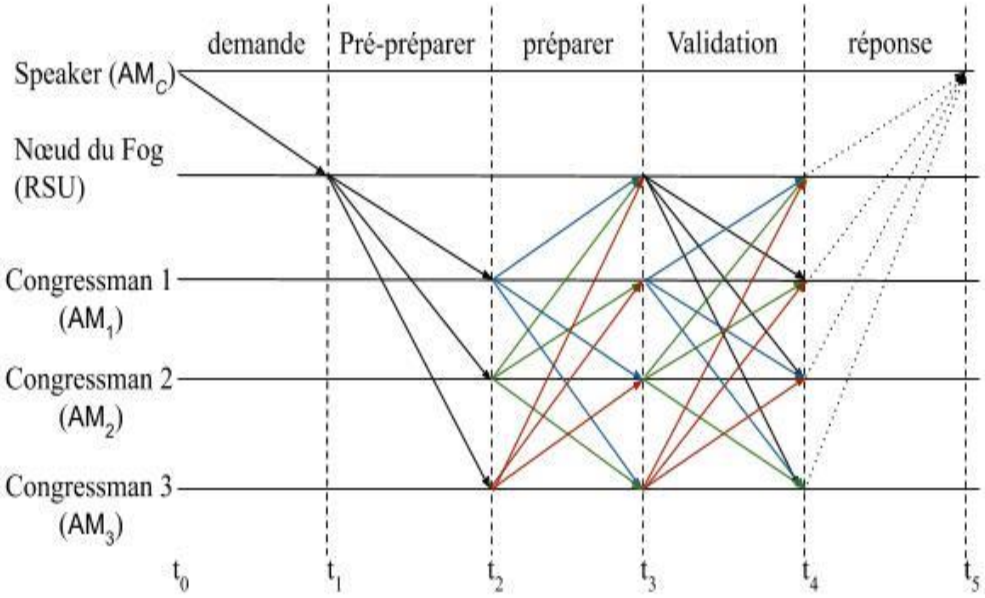

Figure 3.3. Phase IV: La phase de consensus basée sur l'algorithme pratique de tolérance aux pannes byzantine (PBFT).

- *Étape 1:* Sélectionner le président *P* en utilisant l'évaluation suivante: $P = (B_i \bmod k) + 1$ où B_i fait référence à l'indice du bloc actuel.

- *Étape 2:* Après l'authentification réussie et l'échange de clés entre l'OBU_i et le BM_j, le $j^{ème}$ BM partage les résultats d'authentification avec tous les AM.

- *Étape 3:* Lors de la réception des résultats d'authentification diffusés, les AM stockent les résultats après les avoir reçus; puis les transfèrent dans le grand registre public.

- *Étape 4:* Le processus de vote commence juste après la création du bloc qui contient les résultats de l'authentification après le temps nécessaire *t* pour générer un bloc. Au premier tour, le Président envoie une requête < $Vote_{req}$, B_i, AM_P, *bloc*, $Sign_{AMP}$ (*block*) > via un nœud Fog (RSU) aux membres du congrès leur demandant de commencer à voter. Ici, la variable $Vote_{req}$ désigne la demande du président aux autres membres du congrès pour lancer le vote, la variable B_i désigne l'index du bloc créé, la variable AM_P désigne l'identifiant du président marqué AM, la variable *bloc* désigne le contenu du bloc créé et enfin la variable $Sign_{AMP}$ (*block*) désigne la signature du bloc créé avec la clé AM_P.

- *Étape 5:* La demande est transmise sous forme de message *Pré-Préparer* aux membres du congrès via le nœud Fog. Une réponse est envoyée par les répliques correctes sous la forme d'un message *Préparer* à tous les autres membres.

- *Étape 6:* Les membres du congrès se mettent d'accord sur la demande du président une fois qu'ils ont reçu 2f messages *Préparer* des autres membres et le *Pré-Préparer* associé. Par conséquent, ils envoient à tous les autres membres un message *Validation*.

- *Étape 7:* Après avoir reçu $2f + 1$ *Validation* associées, le $k^{ème}$ AM partage son vote en utilisant < $Vote_{res}$, B_i, AM_k, *bloc*, $Sign_{AMk}$ (*bloc*) > où la variable $Vote_{res}$ désigne la réponse du $k^{ème}$ AM, la variable AM_k désigne l'identifiant de le $k^{ème}$ AM, *bloc* désigne le contenu du bloc créé, la variable $Sign_{AMk}$ (*bloc*) désigne la signature du bloc créé avec la clé AM_k.

- *Étape 8:* Après avoir terminé le vote, le bloc contenant les résultats d'authentification est ajouté au grand registre immédiatement après que l'AM président a reçu la réponse des membres du congrès.

E. Phase V: *mise à jour des certificats*

Cette phase particulière offre aux véhicules deux scenarios le premier est la possibilité de passer d'une zone de Fog à une autre de manière transparente sans avoir à se ré-authentifier, et le second de demander au CA de mettre à jour son certificat.

Dans le premier scénario, l'$i^{ème}$ OBU envoie une demande d'accès Acc_{req} composé d'une fenêtre de temps TW_{OBUi}, un jeton crypté CTok = CPK_{BMj*} (ID_{OBUi}, TW_{OBUi}) et h=SHA265 (ID_{OBUi}, TW_{OBUi}) au nouveau BM_{j*} via le nouveau RSU_{j*}. Une fois que le nouveau BM_{j*}, reçoit la demande d'accès Acc_{req} = < CTok, TW_{OBUi}, h> et extrait les valeurs CTok, TW_{OBUi} et h, il déchiffre le jeton CTok en utilisant sa clé secrète $SK_{BM\ j*}$ pour déduire ID_{OBUi} et TW_{OBUi}, il valide la fenêtre de temps TW_{OBUi}. Ensuite il vérifie l'intégrité du message en calculant h' = SHA265 (ID_{OBUi}, TW_{OBUi}) et le compare à h, une fois qu'ils sont tous les deux valides, il cherche la valeur *Cert* correspondante à ID_{OBUi} dans sa base de données locale. Si elle n'est pas trouvée, il la vérifie dans le grand registre public. S'il trouve une correspondance, cela indique que l'authentification a été effectuée dans le passé. BM_{j*} vérifie ensuite la liste de révocation, si la valeur *Cert* n'est pas trouvé, il est établi que l'$i^{ème}$ OBU est valide et BM_{j*} informe directement le RSU_{j*} pour répondre à la demande de service du OBUi sans qu'il soit nécessaire de ré-authentifier. Dans le cas contraire, il informe le RSU_{j*} de refuser de fournir des services à ce véhicule. Pendant tout le processus, si un véhicule est déclaré illégal au TA, TA accédera au grand registre public, découvrira son identité et informera tous les BM que la clé publique du véhicule illégal est invalide et l'ajoutera à la liste de révocation.

Pour le deuxième scenario on fait les mêmes étapes que le premier scenario. Lorsque l'$i^{ème}$ OBU entre dans la zone du CA, il envoie une demande de mise à jour de son certificat Maj_{req} au CA_j. Cette requête est formé d'une fenêtre de temps TW_{OBUi}, d'un jeton chiffré CTok = CPK_{CAj} (ID_{OBUi}, TW_{OBUi}) et d'un hachage h = SHA265 (ID_{OBUi}, TW_{OBUi}). Une fois que CA_j reçoit la demande Maj_{req} = < CTok, TW_{OBUi}, h> et extrait les valeurs CTok, TW_{OBUi} et h, il déchiffre le jeton CTok en utilisant sa clé secrète $SK_{CA\ j}$ pour en déduire ID_{OBUi} et TW_{OBUi}, il valide la fenêtre de temps TW_{OBUi}, ensuite vérifie l'intégrité du message en calculant h' = SHA265 (ID_{OBUi}, TW_{OBUi}) et le compare à h, une fois qu'ils sont tous les deux valides, il cherche la valeur *Cert* correspondante à ID_{OBUi} dans le grand registre public. S'il trouve une correspondance cela indique que ce véhicule est authentique, et donc procède à la mise à jour de son certificat. Il génère une nouvelle paire de clés publiques

secrètes To^{*} =< PK^{*}_{OBUi}, SK^{*}_{OBUi} > pour l'OBU_i et une fenêtre de temps TW_{CAj}, crypte tous ces valeur à l'aide de l'ancienne clé publique de l'$i^{ème}$ OBU PK_{OBUi} puis calcule le hachage h_1= *SHA256* (To^{*}, TW_{CAj}). De plus, la CA calcule et remplace l'ancienne valeur de *Cert* correspondante à ID_{OBUi} par la nouvelle valeur *Cert* = *SHA256* (SK^{*}_{OBUi} || ID_{OBUi}) ⊕ *SHA256* (SK_{CAj} || ID_{OBUi}) dans le registre public et transmet CPK_{OBUi} (To^{*}, TW_{CAj}), TW_{CAj}, h_1 et *S* = *SHA256* (SK_{CAj} || ID_{OBUi}) au OBU_i et enfin il génère une nouvelle clé de session SK_{ij}. Le $i^{ème}$ OBU déchiffre donc le message à l'aide de son ancienne clé secrète SK_{OBUi}, valide la fenêtre du temps TW_{CAj}, puis calcule h_1' = *SHA256* (To^{*}, TW_{CAj}) et le compare à h_1 s'ils sont égaux, son intégrité est valide et l'OBU stocke les nouvelle valeurs PK^{*}_{OBUi} , SK^{*}_{OBUi} et *S* = *SHA256* (SK_{CAj} || ID_{OBUi}) dans son référentiel et génère sa nouvelle clé de session SK_{ij}.

Chapitre IV

Implémentation, analyse et évaluation des performances

Chapitre IV

Implémentation, analyse et évaluation des performances

Dans ce chapitre, nous présentons le détail de l'implémentation du schéma d'authentification et les résultats fournis après la simulation. Ensuite, nous effectuons une analyse des objectifs de sécurité atteints et étudions la capacité d'affronter les attaques potentielles contre ces objectifs. Au final, nous fournissons une analyse détaillée sur les performances de notre schéma.

4.1. Implémentation:

4.1.1. L'outil AVISPA:

4.1.1.1. Définition:

AVISPA (Validation automatisée des protocoles et applications de sécurité Internet) est un outil open source pour l'analyse et la vérification automatisées des protocoles et des applications sensibles à la sécurité. Il fournit un langage formel modulaire et expressif pour spécifier les protocoles et leurs propriétés de sécurité, et intègre différents back-end qui mettent en œuvre une variété de techniques d'analyse automatique [153].

4.1.1.2. Architecture de l'outil AVISPA:

Afin de valider tout protocole de sécurité conçu, AVISPA a besoin que l'entrée soit en langage de spécification de protocole de haut niveau (HLPSL). La structure de HLPSL permet de décrire les protocoles de sécurité avec les exigences et objectifs de sécurité prévus. Le HLPSL définit les protocoles en termes de différentes fonctions telles que les rôles de base qui représentent le rôle de chaque participant, des transitions qui représentent le comportement de chaque participant en fonction de son état, des rôles de composition qui représentent des scénarios des rôles de base, et un rôle de niveau supérieur nommé environnement pour initier les variables d'environnement et instancier des sessions pour les rôles. Chaque rôle est indépendant des autres, obtenant des informations initiales par paramètres, communiquant avec les autres rôles par canaux [153].

De plus, AVISPA s'appuie sur le support de quatre back-end différents pour valider tout protocole de sécurité conçu [153]. Ces back-end sont:

- Vérificateur de modèle On-the-Fly (OFMC): utilisé pour la détection rapide des attaques et pour prouver l'exactitude du protocole.
- Chercheur d'attaque basée sur CL (CL-AtSe): utilisé pour trouver des attaques sur les protocoles.
- Vérificateur de modèle basé sur SAT (SATMC): utilisé pour découvrir les attaques sur les protocoles et prouver que le protocole satisfait ses exigences de sécurité.
- Analyseur de protocole basé sur l'arborescence des automates (TA4SP): utilisé pour conclure que les propriétés de confidentialité sont sûres pour l'état initial donné.

Les back-end permettent de valider la sécurité du mécanisme proposé par rapport aux objectifs de sécurité ciblés et fournissent à l'utilisateur une trace détaillée en cas de violation [153].

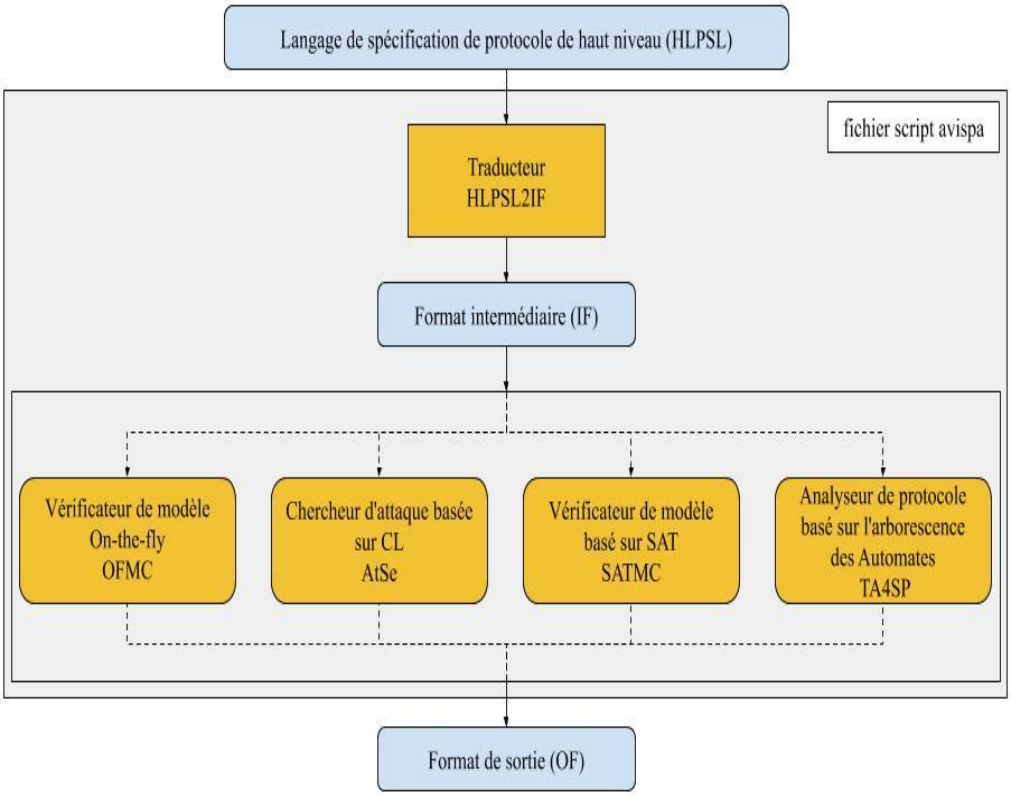

Figure 4.1. Architecture de l'outil AVISPA v.1.1 [153].

4.1.2. Code et exécution:

Afin de valider le schéma proposé, la phase d'authentification de notre système a été codée en HLPSL et soumise à AVISPA pour vérifier sa sécurité contre les différentes attaques de sécurité. Notre code se compose de 4 agents: OBU, BM, CPU et BC, deux rôles de base : rôle "role_OBU" joué par l'agent OBU et rôle "role_BM" joué par l'agent BM, un rôle de composition: rôle "session", un rôle "environnement", deux rôles supplémentaire: rôle "role_BC" joué par l'agent BC et rôle "role_CPU" joué par l'agent CPU, et une partie pour spécifie les objectifs de sécurité du processus.

4.1.2.1. Code:

Le rôle "role_OBU" se compose de 3 parties. Premièrement les paramètres qui sont des informations reçues de l'environnement. Ces paramètres sont: son identifiant, sa clé publique, les identifiants et les clés publiques des agents qui va communiquer avec, les fonctions nécessaires (**SHA256** pour calculer les hachages, **Mult** pour l'opération multiplicative ECC (•) et **CDKf** pour la dérivation des clés de session) et des canaux de communication (**SND** et **RCV** pour communiquer avec BM, et **CHECKcpu** et **VALIDcpu** pour communiquer avec CPU pour tester et valider le jeton d'authentification de BM). Deuxièmement les variables locales qui sont: **State** (son état), **TWobu** et **TWbm** (des fenêtres de temps), **To** (sa signature), **AuthTbm**, **AuthTobu** et **CERTbm** (les jetons d'authentification) et **SKij** (la clé de session). Troisièmement les transitions. L'OBU a trois transitions: la première transition est pour initialiser les variables et calculer le jeton d'authentification d'OBU qui vont être ensuite transmis au BM, la deuxième transition montre qu'après la réception du jeton d'authentification de BM, l'OBU le transmet au CPU pour le valider et la troisième transition montre qu'après la validation du jeton d'authentification de BM, l'OBU procède au calcul de la clé de session SKij.

```
role role_OBU(OBU:agent,BM:agent,CPU:agent,
              P:nat,
              PKobu:public_key,PKbm:public_key,PKcpu:public_key,
              CDKf,SHA256,Mult:hash_func,
              SND,RCV,CHECKcpu,VALIDcpu:channel(dy))
played_by OBU
def=
    local
        State:nat,
        TWobu:text,Rn1:text,N1:message,AuthTobu:message,
        TWbm:text,Rn2:text,AuthTbm:message,
        To:message,SKij:message,CERTbm:message
    init
        State := 0
    transition
     1. State=0 /\ RCV(start) =|>
      State':=2
      /\ TWobu':=new()
      /\ Rn1':=new()
      /\ N1' := Mult(Rn1'.Mult(P.inv(PKobu)))
      /\ To' := SHA256(inv(PKobu).OBU)
      /\ AuthTobu':=SHA256(TWobu'.N1'.OBU.To')
      /\ secret({AuthTobu'.Rn1'},sec_1,{OBU,BM})
      /\ SND({AuthTobu'.OBU.Rn1'.TWobu'}_PKbm.TWobu')

     2. State=2 /\ RCV({AuthTbm'.Rn2'.TWbm'}_PKobu.TWbm') =|>
      State':=4
      /\ CERTbm':=AuthTbm
      /\ secret({CERTbm'.To},sec_6,{CPU,OBU})
      /\ CHECKcpu({CERTbm'.Rn2'.TWbm'.To}_PKcpu)

     3. State=4 /\ VALIDcpu({CERTbm}_PKobu) =|>
      State':=6
      /\ request(OBU,CPU,auth_2,CERTbm)
      /\ SKij':=CDKf(OBU.To.TWobu.TWbm)
end role
```

Figure 4.2. Rôle "role_OBU".

Le rôle "role_BM" contient aussi 3 parties tout comme le rôle "role_OBU". Premièrement les paramètres qui sont des informations reçues de l'environnement. Ces paramètres sont: son identifiant et sa clé publique, les identifiants et les clés publiques des agents qui va communiquer avec, les fonctions nécessaires (**SHA256** pour calculer les hachages, **Mult** pour l'opération multiplicative ECC (•) et **CDKf** pour la dérivation des clés de session), des canaux de communication (**SND** et **RCV** pour communiquer avec BM, et **CHECK** et **VALID** pour communiquer avec BC pour tester et valider le jeton d'authentification du OBU). Deuxièmement les variables locales qui sont **State** (son état), **TWobu** et **TWbm** (des fenêtres de temps), **Cert** (signature du OBU obtenue du BC), **AuthTbm**, **AuthTobu** et **CERTobu** (les jetons d'authentification) et **SKij** (la clé de session). Troisièmement les transitions. Le BM a deux transitions: la première montre qu'après la réception du jeton d'authentification de l'OBU, le BM le transmet au BC pour le valider. La deuxième montre qu'après la validation du jeton

d'authentification du OBU, le BM initialise les variables et calcule son jeton d'authentification et les transmis au OBU ensuite il procède au calcul de la clé de session SKij.

```
role role_BM(OBU:agent,BM:agent,BC:agent,
             P:nat,
             PKbm:public_key,PKobu:public_key,PKbc:public_key,
             CDKf,SHA256,Mult:hash_func,
             SND,RCV,CHECK,VALID:channel(dy))
played_by BM
def=
    local
        State:nat,
        TWobu:text,Rn1:text,AuthTobu:message,
        TWbm:text,Rn2:text,N2:message,AuthTbm:message,
        CERTobu:message,IDobu:message,Cert:message,
        SKij:message
    init
        State := 1
    transition
     1. State=1 /\ RCV({AuthTobu'.OBU.Rn1'.TWobu'}_PKbm.TWobu') =|>
      State':=3
      /\ IDobu':=OBU
      /\ CERTobu':= AuthTobu
      /\ secret({CERTobu'.IDobu'.TWobu.Rn1},sec_3,{BC,BM})
      /\ CHECK({CERTobu'.IDobu'.TWobu.Rn1}_PKbc)
     2. State=3 /\ VALID({CERTobu.Cert'}_PKbm) =|>
      State':=5
      /\ request(BM,BC,auth_1,CERTobu)
      /\ TWbm':=new()
      /\ Rn2':=new()
      /\ N2' := Mult(Rn2'.Mult(P.inv(PKbm)))
      /\ AuthTbm':=SHA256(N2'.TWbm'.Cert)
      /\ secret({AuthTbm'.Rn2'},sec_2,{OBU,BM})
      /\ SND({AuthTbm'.Rn2'.TWbm'}_PKobu.TWbm')
      /\ SKij':=CDKf(IDobu.Cert.TWobu.TWbm')
end role
```

Figure 4.3. Rôle "role_BM".

Les rôles "role_CPU" et "role_BC" ne sont que des rôles créés pour simuler respectivement l'unité de calcul de l'OBU et la Blockchain vu que HLPSL est limité en termes de manipulation de données (les calculs et les comparaisons). Donc le rôle "role_CPU" est conçu pour simuler la comparaison et la validation du jeton d'authentification. Il calcule le jeton $AuthTok^{*}_{BMj}$, ensuite l'envoie à OBU pour qu'il puisse déterminer la validité de $AuthTok_{BMj}$ reçu. Même chose pour "role_BC" qui est conçu pour simuler l'accès à la Blockchain pour comparer et valider le jeton d'authentification. Il

calculer le jeton $AuthTok^{*}_{OBUi}$, ensuite l'envoie au BM pour qu'il puisse déterminer la validité de $AuthTok_{OBUi}$ reçu.

```
role role_CPU(OBU:agent,CPU:agent,
              P:nat,
              PKbm:public_key,PKobu:public_key,PKcpu:public_key,
              SHA256,Mult:hash_func,
              CHECKcpu,VALIDcpu:channel(dy))
played_by CPU
def=
    local
        State:nat,TWbm:text,Rn2:text,IDobu:message,To:message,CERTbm:message
    init
        State := 0
    transition
     1. State=0 /\ CHECKcpu({CERTbm'.Rn2'.TWbm'.To'}_PKcpu) =|>
      State':=1
      /\ CERTbm':=SHA256(Mult(Rn2'.Mult(P.inv(PKbm))).TWbm.To)
      /\ secret({CERTbm'},sec_5,{CPU,OBU})
      /\ VALIDcpu({CERTbm'}_PKobu)
      /\ witness(CPU,OBU,auth_2,CERTbm')
end role
```

Figure 4.4. Rôle "role_CPU".

```
role role_BC(BM:agent,BC:agent,
             P:nat,
             PKbm:public_key,PKobu:public_key,PKbc:public_key,
             SHA256,Mult:hash_func,
             CHECK,VALID:channel(dy))
played_by BC
def=
    local
        State:nat,TWobu:text,Rn1:text,IDobu:message,
        Cert:message,CERTobu:message
    init
        State := 0
    transition
     1. State=0 /\ CHECK({CERTobu'.IDobu'.TWobu'.Rn1'}_PKbc) =|>
      State':=1
      /\ Cert':= SHA256(inv(PKobu).IDobu)
      /\ CERTobu':=SHA256(TWobu'.Mult(Rn1'.Mult(P.inv(PKobu))).IDobu.Cert')
      /\ secret({CERTobu'.Cert'},sec_4,{BC,BM})
      /\ VALID({CERTobu'.Cert'}_PKbm)
      /\ witness(BC,BM,auth_1,CERTobu')
end role
```

Figure 4.5. Rôle "role_BC".

Le rôle "session" est le rôle qui décrit le scénario à considérer lors du lancement du processus d'authentification. Il contient 3 parties:

Premièrement les paramètres qui sont des informations reçues de l'environnement, ces paramètres sont: les agents participant au processus, les clés publiques des agents, les fonctions utilisées lors du processus. Deuxièmement la déclaration des canaux de communication. Troisièmement la composition, c'est la partie où on fait appel aux autres rôles, chacun avec ses propres paramètres, pour les combinés afin d'assurer le bon fonctionnement du processus.

```
119 role session(OBU:agent,BM:agent,BC:agent,CPU:agent,
120              P:nat,
121              PKbm:public_key,PKobu:public_key,PKbc:public_key,PKcpu:public_key,
122              CDKf,SHA256,Mult:hash_func)
123 def=
124     local
125         CHECK4,VALID4,CHECK3,VALID3,CHECK2,VALID2,CHECK1,VALID1,
126         SND2,RCV2,SND1,RCV1:channel(dy)
127 
128     composition
129      role_BC(BM,BC,P,PKbm,PKobu,PKbc,SHA256,Mult,CHECK2,VALID2)
130      /\ role_BM(BM,OBU,BC,P,PKbm,PKobu,PKbc,CDKf,SHA256,Mult,SND2,RCV2,CHECK1,VALID1)
131      /\ role_OBU(OBU,BM,CPU,P,PKobu,PKbm,PKcpu,CDKf,SHA256,Mult,SND1,RCV1,CHECK3,VALID3)
132      /\ role_CPU(OBU,CPU,P,PKbm,PKobu,PKcpu,SHA256,Mult,CHECK4,VALID4)
133 
134 end role
```

Figure 4.6. Rôle "session".

Le rôle "environment" contient 3 parties. La première est l'instanciation de toutes les variables globales comme les identifiants et les clés publiques des agents, les fonctions utilisées et les prédicats. La deuxième partie est la spécification des connaissances de l'intrus. La troisième parties est l'instanciation du rôle "session" en passant les variables globales comme paramètres.

```
role environment()
def=
    const
        p:nat,
        pkbc,pki,pkbm,pkobu,pkcpu:public_key,
        obu,bm,bc,cpu:agent,
        hash_0,cdfk,sha256,mult:hash_func,
        sec_1,sec_2,sec_3,sec_4,sec_5,sec_6,auth_1,auth_2:protocol_id

    intruder_knowledge = {obu,bm,pkobu,pkbm,pki,inv(pki),sha256,mult}

    composition
     session1(obu,bm,bc,cpu,p,pkbm,pkobu,pkbc,pkcpu,cdfk,sha256,mult)
end role

%%%%%%%%%%%% Les exigences %%%%%%%%%%%%
goal
        secrecy_of sec_1
        secrecy_of sec_2
        secrecy_of sec_3
        secrecy_of sec_4
        secrecy_of sec_5
        secrecy_of sec_6
        authentication_on auth_1
        authentication_on auth_2
end goal
environment()
```

Figure 4.7. Rôle "environment" et les objectifs.

Partie objectif est la partie où on spécifie des exigences de confidentialité et d'authenticité sur les différents prédicats qui vont être utilisé ensuite pour assurer la confidentialité et l'authenticité de certains messages transmis entre les agents.

4.1.2.2 Exécution et simulation:

L'exécution du processus d'authentification est spécifiée dans les transitions des rôles, chaque rôle possède une description détaillée de ce qu'il a à faire dans un certain état du processus. Selon les transitions on peut décomposer notre processus en 5 phases.

Phase 1: On commence par l'OBU lorsqu'on lance le processus, L'OBU change son état pour passer à la prochaine transition, génère ses propres variables et calcule son jeton d'authentification **AuthTobu** et il les envoie au BM, tout en ajoutant une condition de confidentialité sur le message pour qu'il soit secret entre lui et BM, c.-à-d. si un autre nœud parvient à intercepter ce message et extraire son contenu, AVISPA déclare que le processus n'est pas sûr et nous montre les traces des potentielles attaques.

Phase 2: Une fois que le BM reçoit le message, il change son état pour passer à la prochaine transition, valide **TWobu**. Ensuite il commence le processus de

validation du jeton **AuthTobu**, il stocke l'identifiant de l'OBU dans la variable **IDobu** et **AuthTobu** dans la variable **CERTobu** et il les envoie au BC avec les variables envoyées de la part de l'OBU pour recalculer la nouvelle valeur de **CERTobu** et la comparer avec l'ancienne valeur. L'instruction qui assure cette comparaison est la condition d'authenticité ajoutée sur le jeton **CERTobu** dans la prochaine transition, impose que le BM doit recevoir la même valeur du jeton qu'il a envoyé, c.-à-d. **CERTobu** reçue doit être égale à **CERTobu** envoyée. Et il ajoute une condition de confidentialité sur le message pour qu'il soit secret entre lui et BC.

Lorsque BC reçoit le message, il passe vers un état final. Il récupère la signature **Cert** de OBU en se basant sur son **IDobu**, reconstruit le jeton **CERTobu** et il les renvoie à BM, tout en ajoutant une condition de confidentialité et une condition d'authenticité espérant que la valeur qu'il a envoyée soit égale à la valeur qu'il a reçue.

Phase 3: Si le BM parvient à recevoir le message envoyé par BC cela signifie que **CERTobu** est valide et donc l'OBU est marqué authentique. Il passe vers un état final c.-à-d il n'y a aucune transition pour BM dans le future. Il génère ses propres variables et calcule son jeton d'authentification **AuthTbm** et il les envoie à OBU, tout en ajoutant une condition de confidentialité sur le message pour qu'il soit secret entre lui et OBU. Enfin il génère une clé de session **SKij** pour les communications futures.

Phase 4: Une fois que l'OBU reçoit le message, il change son état pour passer à la prochaine transition, valide **TWbm**. Ensuite il commence le processus de validation du jeton **AuthTbm**, il le stocke dans la variable **CERTbm** et il l'envoie au CPU avec les variables envoyées de la part du BM pour recalculer la nouvelle valeur de **CERTbm** et la comparer avec l'ancienne valeur. L'instruction qui assure cette comparaison est la condition d'authenticité ajoutée sur le jeton **CERTbm** dans la prochaine transition, c.-à-d. **CERTbm** reçue doit être égale à **CERTbm** envoyée. Et il ajoute une condition de confidentialité sur le message pour qu'il soit secret entre lui et CPU.

Lorsque CPU reçoit le message, il passe vers un état final. Il reconstruit le jeton **CERTbm** et il le renvoie à OBU, tout en ajoutant une condition de

confidentialité et une condition d'authenticité espérant que la valeur qu'il a envoyée soit égale à la valeur qu'il a reçue.

Phase 5: Si l'OBU parvient à recevoir le message envoyé par CPU cela signifie que **CERTbm** est valide et donc le BM est marqué authentique. Il passe vers un état final c.-à-d Il n'y a aucune transition pour OBU dans le future. Il génère une clé de session **SKij** pour les communications futures.

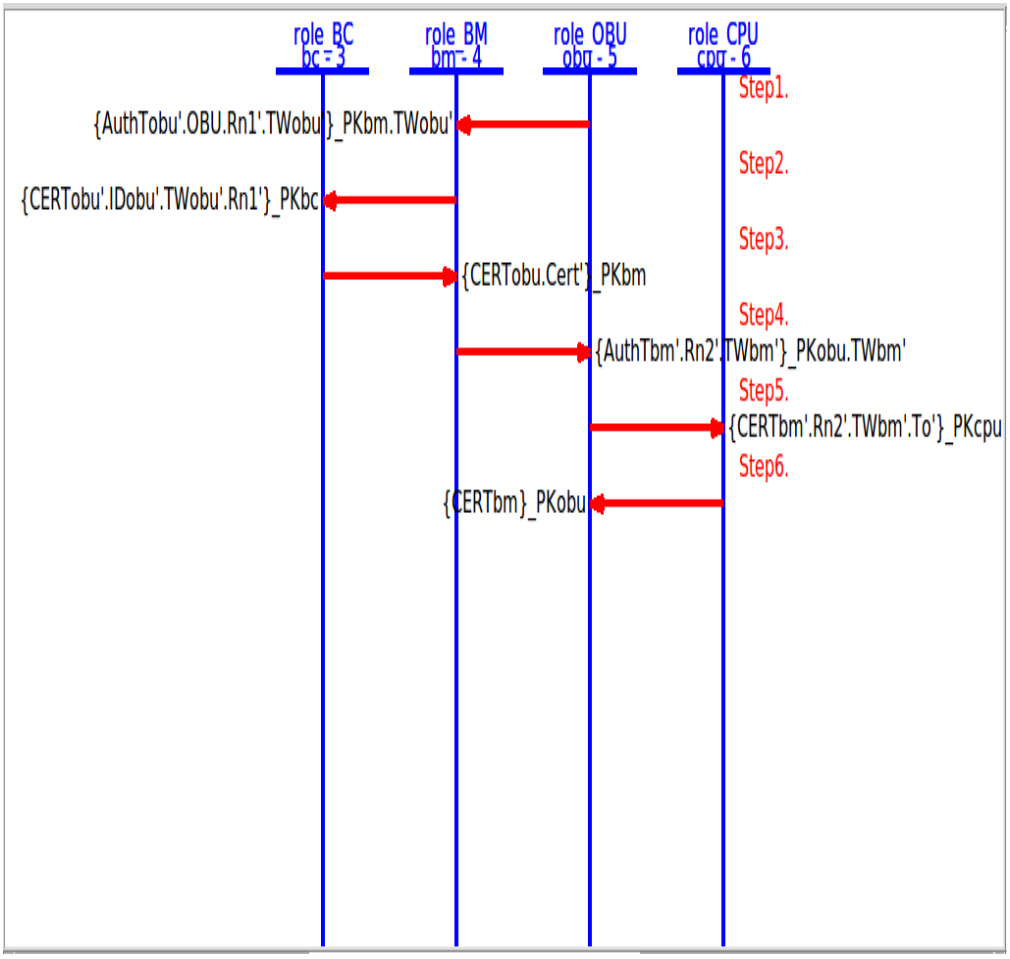

Figure 4.8. Simulation du processus d'authentification sur AVISPA.

4.1.3. Résultats:

Après avoir exécuté le code sur AVISPA, les résultats associés, représentés sur la figure 4.9, montrent clairement que le mécanisme d'authentification proposé est sûr pour les back-end OFMC et CL-AtSe. Ce qui signifie que tout les objectifs de sécurité spécifiés dans notre code sont valider par AVISPA, et donc notre schéma assure la confidentialité et l'intégrité des messages transmit dans le réseau, et assure l'authentification mutuelle entre le nœud OBU et le nœud BM.

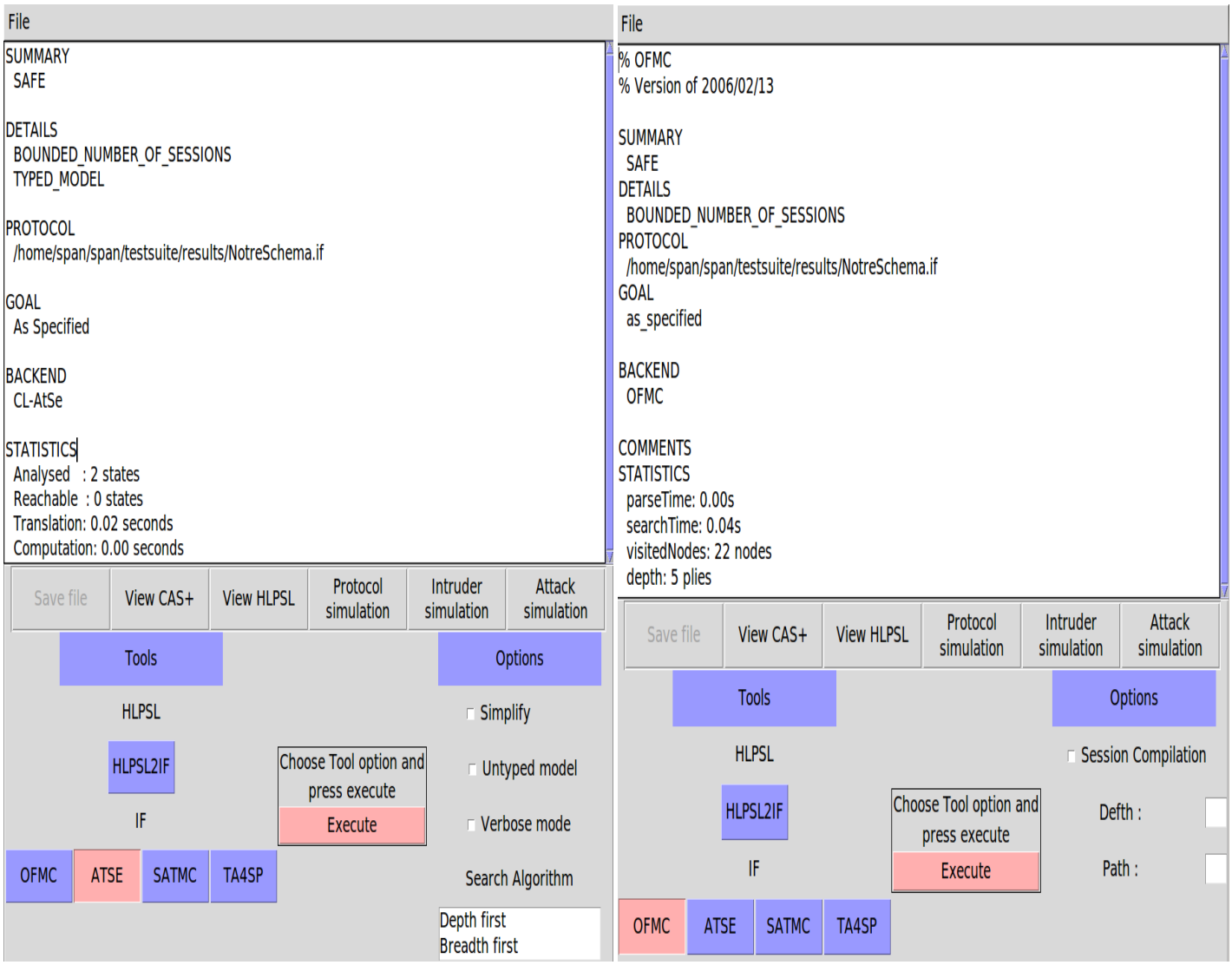

Figure 4.9. Évaluation du mécanisme d'authentification sur AVISPA.

4.2. Analyse de Sécurité:

4.2.1. Les objectifs de sécurité atteints:

4.2.1.1. Confidentialité:

Premièrement, en phase d'initialisation, selon le problème **ECDLP**, étant donné la clé publique de TA $PK_{TA} = SK_{TA} \bullet P$, il est difficile pour les attaquants de calculer la clé privée de TA. De la même manière, SK_{BMj} et SK_{OBUi} sont également difficiles à calculer. C'est la base de ce qui suit. Deuxièmement, pendant tout le processus d'exécution de notre système, les informations privées transmises sont toujours cryptées. Dans la phase d'enregistrement, les identités réelles des RSU et OBU sont cryptées par la clé publique de TA. Personne, sauf TA qui possède la clé privée correspondante, ne peut décrypter ces messages. À propos du message CPK^{0}_{OBUi} (To_1, *SHA256* (SK_{TA} || ID_{OBUi}), TW_{TA}), retourné par le TA, les OBU/RSU inscrits peuvent

l'obtenir hors ligne pour une sécurité plus élevée. Parce qu'ils n'ont besoin d'être enregistrés qu'une seule fois, à moins que leurs clés privées ne soient compromises. En phase d'authentification, le texte chiffré CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}) peut être déchiffré pour obtenir les informations uniquement par le BM ayant la clé secrète SK_{BM}. De plus, seules les personnes autorisées par la loi peuvent accéder au registre public comme les BM, AM, CA et TA. En phase de mise à jour des certificats, lorsque le message transmis Acc_{req} = < CPK_{BMj*} (ID_{OBUi}, TW_{OBUi}), h = SHA265 (ID_{OBUi}, TW_{OBUi}), TW_{OBUi} > est intercepté par un adversaire, celui-ci ne peut obtenir que la fenêtre de temps TW_{OBUi} inutile et la valeur h. Par conséquent, le schéma proposé garantit la confidentialité des informations clés tout au long de ses phases.

4.2.1.2. Intégrité:

Pour atteindre l'intégrité, il faut s'assurer qu'aucun adversaire ne peut altérer les messages transmis et que les messages altérés puissent être découverts. Premièrement, selon **CDHP** (le problème computationnel de Diffie-Hellman), si on leur donne une clé publique PK_x, il est difficile pour les attaquants de calculer la clé secrète SK_x. Deuxièmement, à chaque échange de message, les nœuds effectuent un test d'intégrité basé sur la fonction d'hachage SHA256. Dans la phase d'enregistrement, les identités réelles des BM et des OBU sont cryptées par la clé publique PK_{TA} de TA et accompagnées par un hash h. Un adversaire ne possédant pas la clé privée SK_{TA} pour décrypter les messages envoyés au TA et ne pouvant pas inversé le résultat de h, ne pourra ni lire ni falsifier les messages échangés. Lorsque le message CPK^0_{OBUi} (To_1, *SHA256* (SK_{TA} || ID_{OBUi}), TW_{TA}) est renvoyé par TA, les OBU inscrits peuvent l'obtenir hors ligne, afin d'assurer qu'aucun adversaire n'ait la possibilité de l'altérer. En phase d'authentification, si le texte chiffré CPK_{BMj} ($AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}) est altéré, le BM ne sera pas en mesure de calculer les informations correctes de $AuthTok_{OBUi}$, et donc la validation de l'intégrité échouera. C'est ainsi que le message falsifié peut être découvert. En phase de mise à jour des certificats, lorsque le message transmis Acc_{req} = < CPK_{BMj*} (ID_{OBUi}, TW_{OBUi}), h = SHA265 (ID_{OBUi}, TW_{OBUi}), TW_{OBUi} > est altéré par un adversaire, la valeur de h' sera différente de h reçu et la validation

de l'intégrité échouera, et donc le BM ne permettra pas à cet utilisateur d'accéder aux services du Fog. Le véhicule aura juste besoin de renvoyer une nouvelle demande d'accès.

4.2.1.3. Authenticité:

Selon la phase d'authentification il est garanti que tout les messages sont générés par des utilisateurs légitimes ayant un certificat, où le BM identifie l'OBU via le jeton $AuthTok^*_{OBU,}$ construit via le certificat *Cert* extrait du public ledger correspondant à l'identité ID_{OBU} du OBU et l'OBU identifie le BM via un le jeton $AuthTok^*_{BM}$ calculé comme suit: $AuthTok^*_{BMj}$ = SHA256 ($rn_2 \bullet PK_{BMj} \| TW_{BMj} \| To_{OBUi}$) où ce jeton est validé si et seulement si $rn_2 \bullet PK_{BMj}$ = N2, parce que $N2 = rn_2 \bullet P \bullet SK_{BMj}$ ne peut être généré que par le BM. Donc l'authentification mutuelle est assurée.

4.2.1.4. Vie privée et Anonymat:

Pour atteindre l'anonymat, il doit garantir qu'aucun adversaire ne puisse extraire de véritables identités lorsque notre système est déployé. Premièrement, comme mentionné ci-dessus, notre système peut garantir la confidentialité des messages transmis. Aucune véritable identité ne peut être obtenue par un adversaire car elle est toujours cachée dans les messages cryptés. Deuxièmement, dans la phase d'authentification, un véhicule au lieu d'envoyer sa véritable identité, il crée un jeton To_{OBUi} basé sur SHA256 ( ) et l'utilise comme sa signature, et décide quand il expire. Notre système accorde la responsabilité de préserver la vie privée aux utilisateurs eux-mêmes, ce qui est un avantage. Si un véhicule veut changer sa signature, il doit juste être ré-authentifié. De plus, les vraies identités sont inscrites dans le registre public, mais seules les entités autorisées par la loi peuvent y accéder. Il est donc difficile pour un adversaire d'obtenir la véritable identité des véhicules, et la signature d'un véhicule peut être modifiée régulièrement. Ainsi l'anonymat du mécanisme est garanti.

4.2.1.5. Traçabilité et Non-répudiation:

Le premier responsable qui assure la traçabilité est le TA. Lorsque quelqu'un découvre qu'un véhicule se comporte mal, il le signale au TA qui vérifiera le registre public pour connaître son identité réelle et révoquera sa clé publique. Ainsi, la traçabilité peut être garantie. Pendant ce temps, la véritable

identité du véhicule illégal est révélée et marquée dans le registre public comme une menace, ce qui signifie qu'il ne pourra pas nier ses mauvais comportements. En conséquence, l'objectif de non-répudiation est atteint.

4.2.1.6. Non-interactivité:

Chaque fois qu'un véhicule accède au service du Fog, il n'envoie qu'un seul jeton qui est la demande d'authentification à un BM dans le cas de phase d'authentification ou la demande d'accès au service et la demande de mise à jour de certificat à un CA dans le cas de phase de mise à jour des certificats, et n'a pas besoin de transmettre des messages supplémentaires c.-à-d. il n'y a aucun jeton qui dépend d'un autre. Donc, notre schéma n'est pas interactif.

4.2.2. Résistance aux attaques potentielles:

4.2.2.1. Résistance aux attaques de relecture:

Grâce à la fonction d'hachage SHA256 et les fenêtres de temps TW générées à chaque fois que nous transmettons un message entre les nœuds, notre système a acquis la résistance contre les attaques de relecture. Chaque fois que les nœuds reçoivent un message, ils extraient la fenêtre de temps attachée au message et la comparent avec celui chiffrée dans le message, et aussi calculent la valeur d'hachage du message reçu et la comparent avec la valeur d'hachage attachée aux messages. Si les valeurs ne correspondent pas, ils découvriront que ce message n'est pas récent ou a été modifié et ils le signaleront au TA.

4.2.2.2. Résistance aux attaques d'homme au milieu:

Grâce aux fenêtres de temps TW, la fonction d'hachage SHA256 et les jetons d'authentification *AuthTok*, cette attaque devient inoffensive. Quand un attaquant intercepte une communication, il ne serait pas en mesure de passer pour un véhicule légitime, parce qu'il ne peut ni génère ni valider des jetons d'authentification, et il ne pourrait ni altérer ni retarder les messages échangés à cause de la fonction d'hachage qui contrôle l'intégrité des messages et les fenêtres de temps qui contrôlent la fraîcheur des messages.

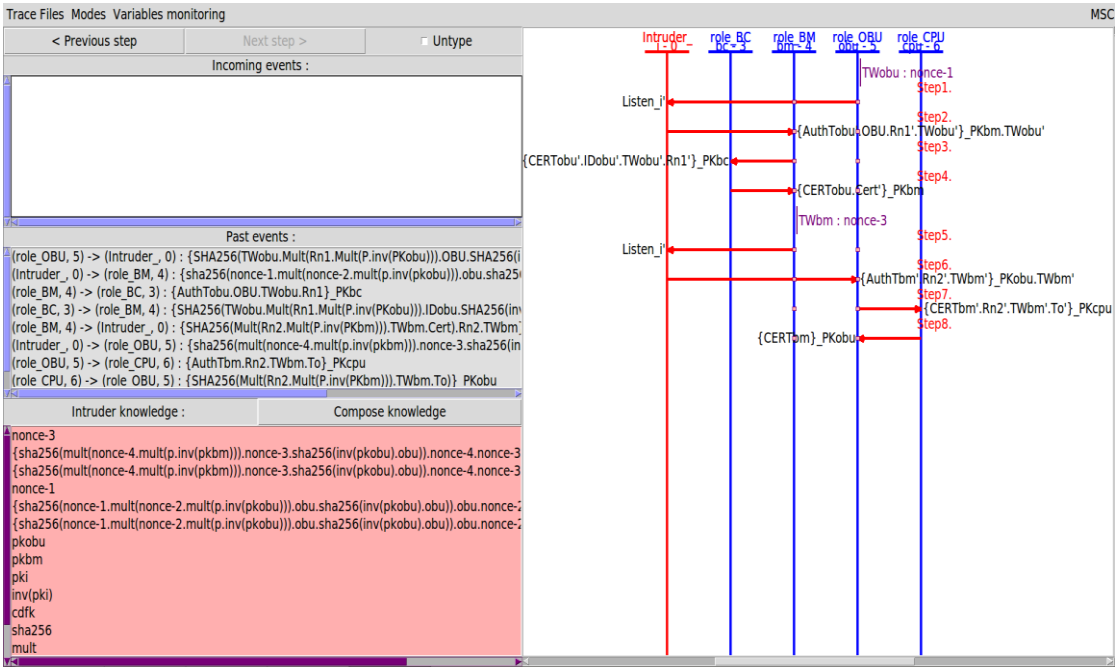

Figure 4.10. Simulation de l'attaque homme au milieu sur AVISPA.

Nous avons simulés cette attaque sur notre schéma a l'aide de l'outil AVISPA pour prouver sa résistance voir figure 4.10. En supposant que l'adversaire ait la possibilité d'écouter sur tous les messages échangés pour voir ce qu'il peut extraire comme informations et après avoir lancé l'attaque, nous avons observé que les seules informations que l'adversaire pouvait extraire sont les fenêtres de temps **TWobu**=nonce-1 et **TWbm**=nonce-3 et les messages chiffrés comme l'indique la figure 4.11. Même si nous lui permettons de connaître les fonctions utilisées pour construire les jetons, il ne peut toujours pas décrypter ou extraire le contenue des messages parce que ces fonctions sont inversibles. Même s'il veut construire des jetons compromis, ils seront refusés car il ne pourra pas prouver son authenticité.

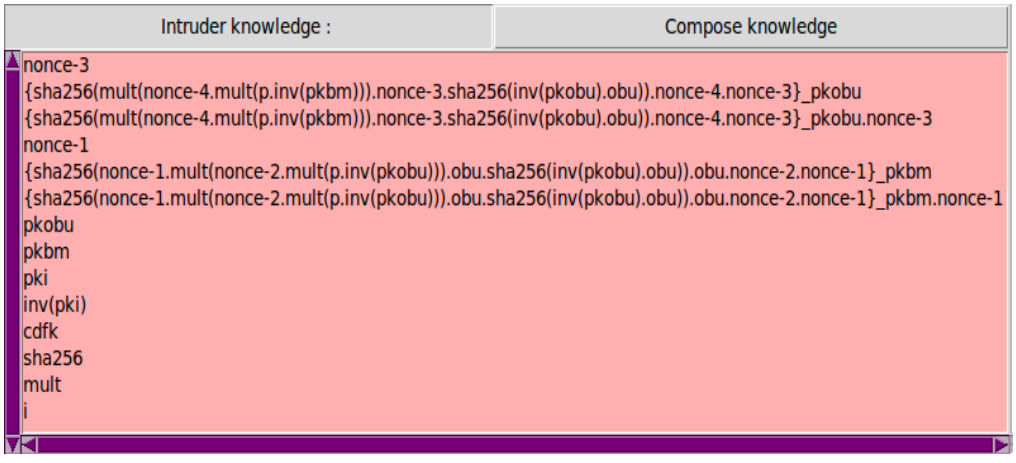

Figure 4.11. Connaissances de l'intrus + informations extraites.

4.2.2.3. Résistance aux attaques d'usurpation d'identité:

Cette attaque se base sur le vol des identités des véhicules ce qui est impossible dans notre schéma, car les identités des nœuds ne sont jamais transmises en claire. Seuls les nœuds TA, BM, AM et CA ont accès au registre public et ainsi la liste des identités des véhicules. Donc les identités des véhicules légitimes sont protégées de l'attaquant dans notre schéma.

4.2.2.4. Résistance aux attaques d'analyse du trafic:

Dans cette attaque l'attaquant analyse les informations collectées après une phase d'écoute du réseau, il tente d'extraire le maximum d'informations utiles à ses propres fins, et tant que les données utiles ne sont jamais échangées en claire dans notre schéma, la collecte des données utiles est impossible tant que l'attaquant est incapable de déduire les clés secrètes SK_x comme l'indique la figure 4.11.

4.2.2.5. Résistance aux attaques de déguise:

Dans cette attaque, l'attaquant caché à l'aide d'une identité valide (appelée masque) cherche à générer des faux messages. Cette attaque est impossible car même si l'attaquant réussit à acquérir l'identité d'un véhicule légitime, il est impossible pour lui de s'authentifier auprès du BM, car l'authentification d'un nœud ne requiert pas seulement l'identité du véhicule, mais aussi la signature $S = SHA256\ (SK_{TA} \parallel ID_{OBUi})$ du TA qui a enregistré ce véhicule.

4.2.2.6. Résistance aux attaques de DDoS:

Vu que notre schéma est basé sur plusieurs nœuds dépendants, sur la technologie de la Blockchain et le calcul du Fog, il est considéré comme un système distribué même si un nœud tombe en panne, les autres nœuds ne seront pas affectés.

4.3. Évaluation des performances:

Dans cette section, nous évaluons les performances de notre système. Nous avons évalué les coûts de calcul et les coûts de communication sur toutes les phases du système. Nous avons implémentés les méthodes cryptographiques utilisées dans notre système en C++ sous Visual Studio 2019 en utilisant la bibliothèque Crypto++ (voir les figures 4.12, 4.13 et 4.14) pour calculer leurs temps de calcul (voir le tableau 4.2).

```cpp
int main(int argc, char* argv[])
{
    auto start = chrono::steady_clock::now();
    using namespace CryptoPP;
    typedef DL_GroupParameters_EC<ECP> GroupParameters;
    typedef DL_GroupParameters_EC<ECP>::Element Element;

    AutoSeededRandomPool prng;
    GroupParameters group;
    group.Initialize(ASN1::secp256r1());

    // private key
    Integer x(prng, Integer::One(), group.GetMaxExponent());

    std::cout << "Private exponent:" << std::endl;
    std::cout << "  " << std::hex << x << std::endl;

    // public key
    Element y = group.ExponentiateBase(x);

    //std::cout << "Public element:" << std::endl;
    //std::cout << "  " << std::hex << y.x << std::endl;
    //std::cout << "  " << std::hex << y.y << std::endl;

    // element addition
    Element u = group.GetCurve().Add(y, ECP::Point(2, 3));

    std::cout << "Add:" << std::endl;
    std::cout << "  " << std::hex << u.x << std::endl;
    std::cout << "  " << std::hex << u.y << std::endl;
    auto end = chrono::steady_clock::now();

    auto startm = chrono::steady_clock::now();
    // scalar multiplication
    Element v = group.GetCurve().ScalarMultiply(u, Integer::Two());

    std::cout << "Mult:" << std::endl;
    std::cout << "  " << std::hex << v.x << std::endl;
    std::cout << "  " << std::hex << v.y << std::endl;
    auto endm = chrono::steady_clock::now();
    cout << "Temps d'initialization en milliseconds : "
        << chrono::ceil<chrono::milliseconds>(end - start).count()
        << " ms" << endl;
    cout << "Temps de operation multiplicative Ecc en milliseconds : "
        << chrono::ceil<chrono::milliseconds>(endm - startm).count()
        << " ms" << endl;
    return 0;
}
```

Figure 4.12. Les opérations ECC.

```cpp
int main(int argc, char* argv[])
{
    typedef std::chrono::duration<float> fms;

    using namespace CryptoPP;
auto start = chrono::steady_clock::now();
    SHA256 hash;
    std::cout << "Name: " << hash.AlgorithmName() << std::endl;
    std::cout << "Digest size: " << hash.DigestSize() << std::endl;
    std::cout << "Block size: " << hash.BlockSize() << std::endl;
    auto end = chrono::steady_clock::now();
    cout << "Elapsed time in millisecondes : "
        << chrono::round<chrono::milliseconds>(end - start).count()
         << endl;

    return 0;
}
```

Figure 4.13. Fonction de hachage SHA256.

```
14  int main(int argc, char* argv[])
15  {
16      using namespace CryptoPP;
17      auto start = std::chrono::steady_clock::now();
18
19      byte password[] = "password";
20      size_t plen = strlen((const char*)password);
21
22      byte salt[] = "salt";
23      size_t slen = strlen((const char*)salt);
24
25      byte info1[] = "CKDF key derivation";
26      size_t ilen1 = strlen((const char*)info1);
27
28      byte info2[] = "CKDF iv derivation";
29      size_t ilen2 = strlen((const char*)info2);
30
31      byte key[AES::DEFAULT_KEYLENGTH];
32      byte iv[AES::BLOCKSIZE];
33
34      HKDF<SHA256> ckdf;
35
36      ckdf.DeriveKey(key, sizeof(key), password, plen, salt, slen, info1, ilen1);
37      ckdf.DeriveKey(iv, sizeof(iv), password, plen, salt, slen, info2, ilen2);
38
39      std::cout << "Key: ";
40      StringSource(key, sizeof(key), true, new HexEncoder(new FileSink(std::cout)));
41      std::cout << std::endl;
42
43      std::cout << "IV: ";
44      StringSource(iv, sizeof(iv), true, new HexEncoder(new FileSink(std::cout)));
45      std::cout << std::endl;
46
47      CBC_Mode<AES>::Encryption enc;
48      enc.SetKeyWithIV(key, sizeof(key), iv, sizeof(iv));
49      auto end = std::chrono::steady_clock::now();
50      std::cout << "Temps d'execution de CDKf en milliseconds : "
51          << std::chrono::ceil<std::chrono::milliseconds>(end - start).count()
52          << " ms" << std::endl;
53      // Use AES/CBC encryptor
54
55      return 0;
56  }
```

Figure 4.14. Fonction de dérivation de clé.

Dispositif	Configuration
Processeur	Processeur Intel (R) Core (TM) i5-3470 @ 3,20 GHz jusqu'à 3,60 GHz
RAM	8.00 Go
Système d'exploitation	Windows 7 Professional version 64-bit

Tableau 4.1. Configuration matérielles et logicielles.

Méthodes cryptographiques	Temps de calcul en milliseconde
ECC initialisation	10.916 ms
Génération des clés publiques et privées ECC	16.592 ms
Opération multiplicative ECC	5.627 ms
Fonction de hachage SHA256	1.297 ms
Fonction de dérivation de clé CDKf	2.856 ms

Tableau 4.2. Temps de calcul des méthodes cryptographiques.

4.3.1. Coût des calculs:

Tout d'abord, les opérations de base de la phase d'enregistrement sont: les fonctions de hachage, les opérations XOR, les opérations de concaténation, les opérations multiplicatives ECC et les comparaisons. Par rapport aux autres fonctions et opérations, les opérations XOR, concaténations et comparaisons sont négligeables. Pour les fonctions de hachage et les opérations multiplicatives ECC, le temps moyen mesuré via la bibliothèque chrono du C++ est respectivement de 1.297 ms et 5.627 ms. Au total, cette phase exécute 5 fonctions de hachage SHA256 et 2 opérations multiplicatives ECC (•). Donc le temps total d'enregistrement d'un véhicule T_{Eng} est:

$$T_{Eng} = 5 * (1.297) + 2 * (5.627) \approx 17.739 \text{ ms}$$

Ensuite, les opérations de base de la phase d'authentification sont les mêmes que la phase d'enregistrement plus la fonction de dérivation de clé. Le temps de calcul de la fonction de dérivation de clé *CDKf* est de 2.856 ms. Au total, cette phase exécute 5 fonctions de hachage SHA256, 6 opérations multiplicatives ECC (•) et 2 fonctions de dérivation de clé *CDKf*. Ainsi, le temps total T_{Auth} pour authentifie un véhicule est:

$$T_{Auth} = 5 * (1.297) + 6 * (5.627) + 2 * (2.856) \approx 45.959 \text{ ms}$$

Enfin, les opérations de base de la phase de mise à jour de certificat sont les mêmes que la phase d'authentification. Au total, cette phase exécute 8 fonctions de hachage SHA256, 2 opérations multiplicatives ECC (•) et 2 fonctions de dérivation de clé *CDKf*. Alors le temps total T_{Maj} pour mettre à jour un certificat est:

$$T_{Maj} = 8 * (1.297) + 2 * (5.627) + 2 * (2.856) \approx 27.342 \text{ ms}$$

4.3.2. Coût des communications:

Le coût des communications est basé sur le nombre de jetons transmis entre les nœuds pendant les phases d'enregistrement, d'authentification et de mise à jour de certificat. Pour le schéma proposé, les jetons suivants < To_0, h_0, TW_{OBUi}, To_1, S, h_1, TW_{TA} > ont été transmis entre les deux nœuds OBU et TA pendant la phase d'enregistrement, ce qui donne un total de 7 jetons dans cette phase. Les jetons suivants < $AuthTok_{OBUi}$, rn_1, ID_{OBUi}, TW_{OBUi}, $AuthTok_{BMj}$, rn_2, TW_{BMj} > ont été transmis entre les deux nœuds OBU et BM pendant le processus d'authentification, ce qui donne un total de 7 jetons dans cette phase.

Et enfin, les jetons suivants < 2 CTok, 2 TW_{OBUi}, 2 h, To^{*}, TW_{CAj}, h_1, S > ont été transmis entre les deux nœuds OBU et CA pendant la phase de mise à jour de certificat, ce qui donne un total de 10 jetons dans cette phase. Donc le coût total des communications CTCo pour toutes les phases est:

$$CTCo = 7 + 7 + 10 = 24 \text{ jetons}$$

4.3.3. Comparaison avec d'autre schéma:

Conformément aux objectifs de sécurité évalués précédemment, la comparaison relative avec deux systèmes existants basés sur la Blockchain a été détaillée dans le tableau 4.3. Après avoir comparé notre schéma avec les schémas *WEI HU et al.* [133] et BLA [150], il est évident que notre schéma prévoit un nombre plus élevé de caractéristiques de sécurité.

Caractéristiques	[133]	[150]	Notre schéma
Confidentialité	✗	✓	✓
Intégrité	✗	✓	✓
Authentification mutuel	✓	✗	✓
Vie privé et anonymat	✗	✓	✓
Traçabilité et Non-répudiation	✓	✓	✓
Transmission sécurisé	✓	✗	✓
Échange de clés	✓	✗	✓
Non-interactivité	✗	✓	✓
Résistance aux attaques DDoS	✓	✓	✓
Résistance aux attaques de relecture	✓	✗	✓
Résistance aux attaques de l'homme au milieu	✗	✗	✓
Résistance aux attaques d'usurpation d'identité	✓	✓	✓
Résistance aux attaques d'analyse du trafic	✗	✓	✓
Résistance aux attaques de déguise	✓	✗	✓

Tableau 4.3. Comparaison des caractéristiques de sécurité fournies par notre schéma avec le schéma [133] et [150].

Travaux futurs

Avec les résultats obtenus, notre contribution a permis de progresser significativement dans la sécurisation des réseaux IoV. Cependant, comme ces réseaux sont basés sur la prestation de services nécessaires pour fournir divers divertissements et assurer une conduite en toute sécurité, tout fournisseur de services compromis pourrait mettre en danger la vie et la sécurité personnelle des conducteurs en divulguant leurs informations privées ou en leur fournissant des informations erronées. Par conséquent, la conception d'un mécanisme de prestation de services aux véhicules plus sûr et efficace est également une future orientation de recherche. Aussi, une autre direction de recherche future est la conception des mécanismes qui assurent la disponibilité et augmentent la tolérance aux pannes de ces systèmes. Cette recherche est vraiment importante car elle augmente la sécurité et les performances de ces systèmes et garantit une expérience fluide pour les utilisateurs.

Conclusion générale

Notre étude nous a conduits à la réalisation d'un schéma d'authentification mutuel basé sur la Blockchain et ECC pour un réseau IoV basé sur le Cloud et le calcul du Fog. Ce qui aide les véhicules à accéder en toute transparence à des services fournis par le Fog, tout en considérons les objectifs de sécurité suivants: la confidentialité des informations personnelles, l'intégrité des messages échangés, une authentification mutuelle sécurisée, la préservation de la vie privé, de l'anonymat des individus, la traçabilité et la non-répudiation. L'intégration de la technologie Blockchain a non seulement efficacement défendue notre système contre de nombreuses attaques malicieuses, mais a également réduit le temps d'authentification des utilisateurs en éliminant les communications entre les BM dans le processus d'authentification grâce à des registres publics. L'utilisation des méthodes cryptographique ECC ont efficacement augmentées le niveau de sécurité des d'informations échangées lors de l'exécution des différentes phases du système. Les caractéristiques de sécurité de notre système sont démontrées

par une analyse de sécurité évaluées par le biais d'une simulation sous l'outil AVISPA. Ses performances ont été réalisées en implémentant et en calculant le temps d'exécution des différentes fonctions et méthodes cryptographiques en C++ sous visuel studio 2019.

Références

[1] Yang, F., Wang, S., Li, J., Liu, Z., & Sun, Q. (2014). An overview of internet of vehicles. *China communications*, *11*(10), 1-15.

[2] Saini, M., Alelaiwi, A., & Saddik, A. E. (2015). How close are we to realizing a pragmatic VANET solution? A meta-survey. *ACM Computing Surveys (CSUR)*, *48*(2), 1-40.

[3] Hasan, S. F., Ding, X., Siddique, N. H., & Chakraborty, S. (2010). Measuring disruption in vehicular communications. *IEEE Transactions on Vehicular Technology*, *60*(1), 148-159.

[4] Aslam, B., Wang, P., & Zou, C. C. (2013). Extension of internet access to VANET via satellite receive–only terminals. *International Journal of Ad Hoc and Ubiquitous Computing*, *14*(3), 172-190.

[5] Toutouh, J., & Alba, E. (2016). Light commodity devices for building vehicular ad hoc networks: An experimental study. *Ad Hoc Networks*, *37*, 499-511.

[6] Bitam, S., Mellouk, A., & Zeadally, S. (2015). VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks. *IEEE Wireless Communications*, *22*(1), 96-102.

[7] Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, *11*(8), 745303.

[8] Barbaresso, J., Cordahi, G., Garcia, D., Hill, C., Jendzejec, A., Wright, K., & Hamilton, B. A. (2014). *USDOT's Intelligent Transportation Systems (ITS) ITS strategic plan, 2015-2019* (No. FHWA-JPO-14-145). United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office. Disponible en ligne: https://rosap.ntl.bts.gov/view/dot/3506 (Consulté le: 18/05/2020).

[9] World Health Organization. (2015). *Global status report on road safety 2015*. World Health Organization.

[10] Dahdah, S., & McMahon, K. (2008). The true cost of road crashes: valuing life and the cost of a serious injury. *International Road Assessment Programme, World Bank Global Road Safety Facility*. Disponible en ligne: https://www.alternatewars.com/BBOW/ABM/Value_Injury.pdf (Consulté le: 18/05/2020).

[11] EEA. (2015). European environment–state and outlook 2015: assessment of global megatrends. Disponible en ligne: https://www.eea.europa.eu/soer/2015/global/action-download-pdf (Consulté le: 18/05/2020).

[12] McKinsey, A. C., Moh, D., Weig, F., Zerlin, B., & Hein, A. P. (2012). Mobility of the future, opportunities for automotive OEMs. Disponible en ligne: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/automotive%20and%20assembly/pdfs/mobility_of_the_future_brochure.ashx (Consulté le: 18/05/2020).

[13] Mohr, D., Müller, N., Krieg, A., Gao, P., Kaas, H. W., Krieger, A., & Hensley, R. (2013). The road to 2020 and beyond: What's driving the global automotive industry. *McKinsey Co Automot Assembly Latest Think*, *28*(3), 2014. Disponible en ligne: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Automotive%20and%20Assembly/PDFs/McK_The_road_to_2020_and_beyond.ashx (Consulté le:18/05/2020).

[14] Walport, M. (2014). *The Internet of Things: Making the most of the second digital revolution, A report by the UK government chief scientific adviser*. Technical Report, 2014. Disponible en ligne: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf (Consulté le: 18/05/2020).

[15] Statista, I. H. S. (2018). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Consulté 17/05/2020).

[16] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access*, *4*, 5356-5373.

[17] Wellens, M., Westphal, B., & Mahonen, P. (2007, April). Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios. In *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring* (pp. 1167-1171). IEEE.

[18] Yao, Y., Rao, L., Liu, X., & Zhou, X. (2013, April). Delay analysis and study of IEEE 802.11 p based DSRC safety communication in a highway environment. In *2013 Proceedings IEEE INFOCOM* (pp. 1591-1599). IEEE.

[19] Huang, J., Qian, F., Gerber, A., Mao, Z. M., Sen, S., & Spatscheck, O. (2012, June). A close examination of performance and power characteristics of 4G LTE networks. In *Proceedings of the 10th international conference on Mobile systems, applications, and services* (pp. 225-238).

[20] Hossain, E., Chow, G., Leung, V. C., McLeod, R. D., Mišić, J., Wong, V. W., & Yang, O. (2010). Vehicular telematics over heterogeneous wireless networks: A survey. *Computer Communications*, *33*(7), 775-793.

[21] Alam, K. M., Saini, M., & El Saddik, A. (2015). Toward social internet of vehicles: Concept, architecture, and applications. *IEEE access*, *3*, 343-357.

[22] Kowshik, H., Caveney, D., & Kumar, P. R. (2011). Provable systemwide safety in intelligent intersections. *IEEE transactions on vehicular technology*, *60*(3), 804-818.

[23] Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE communications surveys & tutorials*, *10*(3), 74-88.

[24] Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials*, *13*(4), 584-616.

[25] Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1-14. Disponible en ligne: https://link.springer.com/article/10.1007%2Fs10708-013-9516-8 (Consulté le:18/05/2020).

[26] Mitton, N., Papavassiliou, S., Puliafito, A., & Trivedi, K. S. (2012). Combining Cloud and sensors in a smart city environment. Disponible en ligne: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/1687-1499-2012-247 (Consulté le:18/05/2020).

[27] Campolo, C., Iera, A., Molinaro, A., Paratore, S. Y., & Ruggeri, G. (2012, November). SMaRTCaR: An integrated smartphone-based platform to support traffic management applications. In *2012 first international workshop on vehicular traffic management for smart cities (VTM)* (pp. 1-6). IEEE.

[28] Singh, K. D., Rawat, P., & Bonnin, J. M. (2014). Cognitive radio for vehicular ad hoc networks (CR-VANETs): approaches and challenges. *EURASIP journal on wireless communications and networking*, *2014*(1), 49. Disponible en ligne: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/1687-1499-2014-49 (Consulté le:18/05/2020).

[29] Wazid, M., Das, A. K., Kumar, N., & Vasilakos, A. V. (2019). Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer Systems*, *91*, 475-492.

[30] Huang, B., Liu, W., Wang, T., Li, X., Song, H., & Liu, A. (2019). Deployment optimization of data centers in vehicular networks. *IEEE Access*, *7*, 20644-20663.

[31] Yao, Y., Chang, X., Mišić, J., & Mišić, V. (2018). Reliable and secure vehicular fog service provision. *IEEE Internet of Things Journal*, *6*(1), 734-743.

[32] Asuquo, P., Cruickshank, H., Morley, J., Ogah, C. P. A., Lei, A., Hathal, W., ... & Sun, Z. (2018). Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. *IEEE Internet of Things Journal*, *5*(6), 4778-4802.

[33] Wazid, M., Bagga, P., Das, A. K., Shetty, S., Rodrigues, J. J., & Park, Y. H. (2019). AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment. *IEEE Internet of Things Journal*, *6*(5), 8804-8817.

[34] Zheng, K., Zhang, L., Xiang, W., & Wang, W. (2016). Architecture of Heterogeneous Vehicular Networks. In *Heterogeneous Vehicular Networks* (pp. 9-24). Springer, Cham.

[35] Tönjes, R., Barnaghi, P., Ali, M., Mileo, A., Hauswirth, M., Ganz, F., ... & Puiu, D. (2014, June). Real time iot stream processing and large-scale data analytics for smart city applications. In *poster session, European Conference on Networks and Communications*. sn. Disponible en ligne: https://pdfs.semanticscholar.org/85d9/3961c45712af1f3441649d6ddb2ea1c3288d.pdf (Consulté le: 18/05/2020).

[36] Zhao, Q., Zhu, Y., Chen, C., Zhu, H., & Li, B. (2013). When 3G meets VANET: 3G-assisted data delivery in VANETs. *IEEE Sensors Journal*, *13*(10), 3575-3584.

[37] Kathiriya, H., Kathiriya, N., & Bavarva, A. (2013). Review on V2R Communication in VANET. *ICIAME Feb2013*. Disponible en ligne: https://www.researchgate.net/profile/Arjav_Bavarva/publication/256204807_Review_on_V2R_Communication_in_VANET/links/02e7e522059b5686c2000000.pdf (Consulté le:18/05/2020).

[38] Cooperation, M. O. S. T. (2004). MOST media oriented system transport—multimedia and control networking technology. *MOST Specification Rev*, *2*, 2-2. Disponible en ligne: https://ir.nctu.edu.tw/bitstream/11536/80678/1/254801.pdf (Consulté le: 18/05/2020).

[39] Zhang, J., Ma, X., & Wu, T. (2014). Performance modeling and analysis of emergency message propagation in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, *14*(3), 366-379.

[40] Chim, T. W., Yiu, S. M., Hui, L. C., & Li, V. O. (2012). VSPN: VANET-based secure and privacy-preserving navigation. *IEEE Transactions on Computers*, *63*(2), 510-524.

[41] Li, Z., Liu, C., & Chigan, C. (2012). VehicleView: A universal system for vehicle performance monitoring and analysis based on VANETs. *IEEE Wireless Communications*, *19*(5), 90-96.

[42] Chang, T. W., & Chen, J. L. (2010). Remote vehicular system management functions and information structure. In *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications* (pp. 310-330). IGI Global.

[43] Al-Sultan, S., Al-Bayatti, A. H., & Zedan, H. (2013). Context-aware driver behavior detection system in intelligent transportation systems. *IEEE transactions on vehicular technology*, *62*(9), 4264-4275.

[44] Sou, S. I., & Tonguz, O. K. (2011). Enhancing VANET connectivity through roadside units on highways. *IEEE transactions on vehicular technology*, *60*(8), 3586-3602.

[45] Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., ... & Hu, B. (2018). Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, *21*(2), 1314-1345.

[46] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications*, *7*, 7-20.

[47] Raya, M., Papadimitratos, P., & Hubaux, J. P. (2006). Securing vehicular communications. *IEEE wireless communications*, *13*(5), 8-15.

[48] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., ... & Xiong, Y. (2015, October). Security and Privacy in the Internet of Vehicles. In *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)* (pp. 116-121). IEEE

[49] La, V. H., & Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey.

[50] Garg, T., Kagalwalla, N., Churi, P., Pawar, A., & Deshmukh, S. (2020). A survey on security and privacy issues in IoV. International Journal of Electrical & Computer Engineering (2088-8708), 10(5).

[51] Dak, A. Y., Yahya, S., & Kassim, M. (2012). A literature survey on security challenges in VANETs. *International Journal of Computer Theory and Engineering*, *4*(6), 1007. Disponible en ligne: https://pdfs.semanticscholar.org/8e95/74001b3100812e9681fe1be459fd34dda6d3.pdf (Consulté le: 18/05/2020).

[52] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., & Park, Y. (2020). Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. IEEE Access, 8, 54314-54344.

[53] Quyoom, A., Mir, A. A., & Sarwar, A. (2020). Security Attacks and Challenges of VANETs: A Literature Survey. Journal of Multimedia Information System, 7(1), 45-54.

[54] Masood, A., Lakew, D. S., & Cho, S. (2020). Security and Privacy Challenges in Connected Vehicular Cloud Computing. IEEE Communications Surveys & Tutorials.

[55] Biswas, S., Md. Mahbubul Haque, & Misic, J. V. (2010). Privacy and Anonymity in VANETs: A Contemporary Study. *Ad Hoc & Sensor Wireless Networks*, *10*(2-3), 177-192.

[56] Li, K., Lau, W. F., Au, M. H., Ho, I. W. H., & Wang, Y. (2020). Efficient Message Authentication with Revocation Transparency Using Blockchain for Vehicular Networks. Computers & Electrical Engineering, 86, 106721.

[57] Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. *Telecommunication Systems*, *50*(4), 217-241.

[58] Dhamgaye, A., & Chavhan, N. (2013). Survey on security challenges in VANET 1.

[59] RoselinMary, S., Maheshwari, M., & Thamaraiselvan, M. (2013, February). Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). In *2013 international conference on information communication and embedded systems (ICICES)* (pp. 237-240). IEEE.

[60] Buttyan, L., & Hubaux, J. P. (2007). *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press.

[61] Tilal, M., & Minhas, R. (2010). *Effects of Jamming on IEEE 802.11 p Systems* (Doctoral dissertation, MS Thesis, Chalmers Univ. of Technology, Gothenburg, Sweden).

[62] Hamieh, A., Ben-Othman, J., & Mokdad, L. (2009, November). Detection of radio interference attacks in VANET. In *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference* (pp. 1-5). IEEE.

[63] Hamieh, A., Ben-Othman, J., Gueroui, A., & Naït-Abdesselam, F. (2009, June). Detecting greedy behaviors by linear regression in wireless ad hoc networks. In *2009 IEEE International Conference on Communications* (pp. 1-6). IEEE.

[64] Al-Kahtani, M. S. (2012, December). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In *2012 6th International Conference on Signal Processing and Communication Systems* (pp. 1-9). IEEE.

[65] Nogueira, M., Silva, H., Santos, A., & Pujolle, G. (2012). A security management architecture for supporting routing services on WANETs. *IEEE Transactions on Network and Service Management*, *9*(2), 156-168.

[66] Karpijoki, V. (2000). Security in ad hoc networks. In *Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland*. Disponible en ligne: https://www.scss.tcd.ie/~htewari/papers/netsec00_manet_sec.pdf (Consulté le:18/05/2020).

[67] Sumra, I. A., Ahmad, I., & Hasbullah, H. (2011, April). Classes of attacks in VANET. In *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)* (pp. 1-5). IEEE.

[68] Safi, S. M., Movaghar, A., & Mohammadizadeh, M. (2009, October). A novel approach for avoiding wormhole attacks in VANET. In *2009 Second International Workshop on Computer Science and Engineering* (Vol. 2, pp. 160-165). IEEE.

[69] Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.

[70] Rawat, A., Sharma, S., & Sushil, R. (2012). VANET: Security attacks and its possible solutions. *Journal of Information and Operations Management*, *3*(1), 301. Disponible en ligne: http://www.academia.edu/download/31082026/VANET_SECURITY_ATTACKS_AND_ITS_POSSIBLE_SOLUTIONS.pdf (Consulté le: 18/05/2020).

[71] Kaushik, S. S. (2013). Review of different approaches for privacy scheme in VANETs. *International Journal of Advances in Engineering & Technology*, *5*(2), 356. Disponible en ligne: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.384.4874&rep=rep1&type=pdf (Consulté le:18/05/2020).

[72] Parno, B., & Perrig, A. (2005, November). Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)* (pp. 1-6). Disponible en ligne: http://conferences.sigcomm.org/hotnets/2005/papers/parno.pdf (Consulté le:18/05/2020).

[73] Zhang, J. (2011, March). A survey on trust management for vanets. In *2011 IEEE International Conference on Advanced Information Networking and Applications* (pp. 105-112). IEEE.

[74] Sumra, I. A., Ab Manan, J. L., & Hasbullah, H. (2011, July). Timing attack in vehicular network. In *Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), Corfu Island, Greece* (pp. 151-155). Disponible en ligne: http://www.academia.edu/download/5644633/computers-24.pdf (Consulté le: 18/05/2020).

[75] Li, C. T., Hwang, M. S., & Chu, Y. P. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy

preserving for vehicular ad hoc networks. *Computer Communications*, *31*(12), 2803-2814.

76] Maurer, U. M., & Yacobi, Y. (1996). A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, *9*(3), 305-316.

[77] Hwang, M. S., Lee, C. C., & Lai, Y. C. (2002). Traceability on low-computation partially blind signatures for electronic cash. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, *85*(5), 1181-1182.

[78] Lin, C. W., Tsai, C. S., & Hwang, M. S. (2006). A new strong-password authentication scheme using one-way hash functions. *Journal of Computer and Systems Sciences International*, *45*(4), 623-626.

[79] Yang, C. C., Tang, Y. L., Wang, R. C., & Yang, H. W. (2005). A secure and efficient authentication protocol for anonymous channel in wireless communications. *Applied Mathematics and Computation*, *169*(2), 1431-1439.

[80] Q. He, D. Wu, P. Khosla, The quest for personal control over mobilelocation privacy, IEEE Communications Magazine 42 (5) (2004) 130–136.

[81] Sun, Y., Lu, R., Lin, X., Shen, X., & Su, J. (2010). An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, *59*(7), 3589-3603.

[82] Bellare, M., & Rogaway, P. (2005). Introduction to modern cryptography. *Ucsd Cse*, *207*, 207. Disponible en ligne: http://almuhammadi.com/sultan/crypto_books/BR.2005.pdf (Consulté en ligne: 18/05/2020).

[83] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Springer, Berlin, Heidelberg.

[84] Schnorr, C. P. (1991). Efficient signature generation by smart cards. *Journal of cryptology*, *4*(3), 161-174.

[85] Raya, M., & Hubaux, J. P. (2005, November). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (pp. 11-21). Disponible en ligne: https://dl.acm.org/doi/pdf/10.1145/1102219.1102223 (Consulté le: 18/05/2020).

[86] Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008, April). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications (pp. 1229-1237). IEEE.

[87] Wasef, A., Jiang, Y., & Shen, X. (2009). DCS: an efficient distributed-certificate-service scheme for vehicular networks. *IEEE Transactions on Vehicular Technology*, *59*(2), 533-549.

[88] Calandriello, G., Papadimitratos, P., Hubaux, J. P., & Lioy, A. (2007, September). Efficient and robust pseudonymous authentication in VANET. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks* (pp. 19-28).

[89] Huang, D., Misra, S., Verma, M., & Xue, G. (2011). PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *12*(3), 736-746.

[90] Blake, I. F., Murty, V. K., & Xu, G. (2006). Refinements of Miller's algorithm for computing the Weil/Tate pairing. *J. Algorithms*, *58*(2), 134-149. Disponible en ligne: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.1179&rep=rep1&type=pdf (Consulté le: 18/05/2020).

[91] Blake, I. F., Seroussi, G., & Smart, N. P. (Eds.). (2005). *Advances in elliptic curve cryptography* (Vol. 317). Cambridge University Press. Disponible en ligne: https://www.cambridge.org/core/books/advances-in-elliptic-curve-cryptography/136CF5172D2342471E9F5AF5AAFB2744 (Consulté le: 18/05/2020).

[92] Boneh, D., Lynn, B., & Shacham, H. (2004). Short signatures from the Weil pairing. *Journal of cryptology*, *17*(4), 297-319.

[93] Lu, R., Lin, X., Luan, T. H., Liang, X., & Shen, X. (2011). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE transactions on vehicular technology*, *61*(1), 86-96.

[94] Lu, R., Lin, X., & Shen, X. (2010, March). Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9). IEEE.

[95] Boneh, D., & Boyen, X. (2008). Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of cryptology*, *21*(2), 149-177.

[96] Lu, R., Lin, X., Liang, X., & Shen, X. (2011). A dynamic privacy-preserving key management scheme for location-based services in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *13*(1), 127-139.

[97] Boneh, D., & Shacham, H. (2004, October). Group signatures with verifier-local revocation. In *Proceedings of the 11th ACM conference on Computer and communications security* (pp. 168-177).

[98] Ying, B., Makrakis, D., & Mouftah, H. T. (2013). Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Applications*, *36*(5), 1352-1364.

[99] Huan, Q., Avramopoulos, I. C., Kobayashi, H., & Liu, B. (2005, May). Secure data forwarding in wireless ad hoc networks. In *IEEE International Conference on Communications, 2005. ICC 2005. 2005* (Vol. 5, pp. 3525-3531). IEEE.

[100] Moustafa, H., Bourdon, G., & Gourhant, Y. (2005, September). AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks* (pp. 79-80).

[101] Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE*, *99*(7), 1162-1182.

[102] Bendouma, A., & Bensaber, B. A. (2017, May). RSU authentication by aggregation in VANET using an interaction zone. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[103] Lin, X., Sun, X., Wang, X., Zhang, C., Ho, P. H., & Shen, X. (2008). TSVC: Timed efficient and secure vehicular communications with privacy preserving. *IEEE Transactions on Wireless Communications*, *7*(12), 4987-4998.

[104] Perrig, A., Song, D., Canetti, R., Tygar, J. D., & Briscoe, B. (2005). Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction. *Request For Comments*, *4082*. Disponible en ligne: http://www.hjp.at/doc/rfc/rfc4082.html (Consulté le: 18/05/2020).

[105] Zhou, X., & Tang, X. (2011, August). Research and implementation of RSA algorithm for encryption and decryption. In *Proceedings of 2011 6th International Forum on Strategic Technology* (Vol. 2, pp. 1118-1121). IEEE.

[106] Menezes, A. (2009). An introduction to pairing-based cryptography. *Recent trends in cryptography*, *477*, 47-65.

[107] Ateniese, G., Fu, K., Green, M., & Hohenberger, S. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, *9*(1), 1-30.

[108] Green, M., & Ateniese, G. (2007, June). Identity-based proxy re-encryption. In *International Conference on Applied Cryptography and Network Security* (pp. 288-306). Springer, Berlin, Heidelberg.

[109] Zhang, C., Lu, R., Lin, X., Ho, P. H., & Shen, X. (2008, April). An efficient identity-based batch verification scheme for vehicular sensor networks. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications* (pp. 246-250). IEEE.

[110] Rabieh, K., Mahmoud, M., Siraj, A., & Misic, J. (2015, December). Efficient privacy-preserving chatting scheme with degree of interest verification for vehicular social networks. In *2015 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

[111] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).

[112] Cheung, L., & Newport, C. (2007, October). Provably secure ciphertext policy ABE. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 456-465).

[113] Yu, R., Kang, J., Huang, X., Xie, S., Zhang, Y., & Gjessing, S. (2015). MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Transactions on Dependable and Secure Computing*, *13*(1), 93-105.

[114] Guo, J., Baugh, J. P., & Wang, S. (2007, May). A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments* (pp. 103-108). IEEE.

[115] Guo, N., Ma, L., & Gao, T. (2018). Independent mix zone for location privacy in vehicular networks. *IEEE Access*, *6*, 16842-16850.

[116] Liu, Y., Wang, Y., & Chang, G. (2017). Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. *IEEE Transactions on Intelligent Transportation Systems*, *18*(10), 2740-2749.

[117] Song, J., He, C., Zhang, L., Tang, S., & Zhang, H. (2014). Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs. *China Communications*, *11*(9), 93-103.

[118] Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2015). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(4), 1015-1028.

[119] Zhu, H., Liu, T., Wei, G., & Li, H. (2013). PPAS: privacy protection authentication scheme for VANET. *Cluster computing*, *16*(4), 873-886.

[120] Zhu, H., Pan, W., Liu, B., & Li, H. (2012, September). A lightweight anonymous authentication scheme for VANET based on bilinear pairing. In *2012 Fourth International Conference on Intelligent Networking and Collaborative Systems* (pp. 222-228). IEEE.

[121] Kang, J., Yu, R., Huang, X., & Zhang, Y. (2017). Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2627-2637.

[122] Park, Y., Sur, C., & Rhee, K. H. (2016). Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. *Journal of Ambient Intelligence and Humanized Computing*, *7*(5), 661-671.

[123] Liu, J., Li, Q., Sun, R., Du, X., & Guizani, M. (2018, May). An efficient anonymous authentication scheme for internet of vehicles. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[124] He, D., Huang, B., & Chen, J. (2013). New certificateless short signature scheme. *IET Information Security*, *7*(2), 113-117.

[125] Hung, Y. H., Tseng, Y. M., & Huang, S. S. (2016). A revocable certificateless short signature scheme and its authentication application. *Informatica*, *27*(3), 549-572.

[126] Tso, R., Huang, X., & Susilo, W. (2012). Strongly secure certificateless short signatures. *Journal of Systems and Software*, *85*(6), 1409-1417.

[127] Chen, Y. C., Horng, G., & Liu, C. L. (2013). Strong non-repudiation based on certificateless short signatures. *IET Information Security*, *7*(3), 253-263.

[128] Sharma, N., Chauhan, N., & Chand, N. (2018, December). Security challenges in Internet of Vehicles (IoV) environment. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 203-207). IEEE.

[129] Fan, K., Jiang, W., Luo, Q., Li, H., & Yang, Y. (2019). Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV. *Journal of the Franklin Institute*.

[130] W. Xie , L. Xie , C. Zhang , Q. Zhang , C. Tang , Cloud-based RFID authentication, in: Proceedings of the IEEE International Conference on RFID, 2013, pp. 168–175.

[131] S. Abughazalah , K. Markantonakis , K. Mayes , Secure improved cloud-based RFID authentication protocol, in: Proceedings of the Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, 2015, pp. 47–164.

[132] H. Xiao , A. Alshehri , B. Christianson , A cloud-based RFID authentication protocol with insecure communication channels, in: Proceedings of the IEEE Trustcom/BigDataSE/ISPA, 2017, pp. 332–339.

[133] Wang, X., Zeng, P., Patterson, N., Jiang, F., & Doss, R. (2019). An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE access*, *7*, 45061-45072.

[134] Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, *98*, 461-466.

[135] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, *55*(12), 119-125.

[136] Dahab, R., & López, J. (2000). An overview of elliptic curve cryptography. *Institute of Computing State University of Campinas Brazil, Brazil*.

[137] Gauravaram, P. (2007). *Cryptographic hash functions: cryptanalysis, design and applications* (Doctoral dissertation, Queensland University of Technology).

[138] Handschuh, H., & Gilbert, H. (2002). Evaluation Report Security Level of Cryptography–SHA-256. *Journal of Women s Health*. Disponible en ligne: http://www.academia.edu/download/52011803/1045_IPA-SHA256.pdf (Consulté le: 18/05/2020).

[139] Kasgar, A. K., Agrawal, J., & Shahu, S. (2012). New modified 256-bit MD 5 Algorithm with SHA Compression Function. *International Journal of Computer Applications*, *42*(12). Disponible en ligne: https://pdfs.semanticscholar.org/8a11/b01015cf6387f404e2ea6590b84ce841e635.pdf (Consulté le: 18/05/2020).

[140] NIST, S. H. S. (2002). FIPS Pub. 180-2. Disponible en ligne: http://everyspec.com/NIST/NIST-FIPS/download.php?spec=FIPS_PUB_180-2(AUG_2002).003221.pdf (Consulté le: 18/05/2020).

[141] Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018, March). A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In *Journal of Physics: Conference Series* (Vol. 978, No. 1, p. 012116). IOP Publishing.

[142] Roshdy, R., Fouad, M., & Aboul-Dahab, M. (2013). Design and Implementation a new Security Hash Algorithm based on MD5 and SHA-256. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(1), 29-36. Disponible en ligne: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.429.902&rep=rep1&type=pdf (Consulté le: 18/05/2020).

[143] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.(2008). [En ligne]. Évalué: https://bitcoin.org/bitcoin.pdf

[144] Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983-994.

[145] Samaniego, M., & Deters, R. (2016, December). Hosting virtual iot resources on edge-hosts with blockchain. In *2016 IEEE International Conference on Computer and Information Technology (CIT)* (pp. 116-119). IEEE.

[146] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18-21.

[147] Qi, Z., Zhang, Y., Wang, Y., Wang, J., & Wu, Y. (2018, August). A Cascade Structure for Blockchain. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)* (pp. 252-253). IEEE.

[148] Qiu, T., Liu, X., Li, K., Hu, Q., Sangaiah, A. K., & Chen, N. (2018). Community-aware data propagation with small world feature for internet of vehicles. *IEEE Communications Magazine*, *56*(1), 86-91.

[149] Ferrag, M. A., Maglaras, L., & Janicke, H. (2019). Blockchain and its role in the internet of things. In *Strategic Innovative Marketing and Tourism* (pp. 1029-1038). Springer, Cham.

[150] Yao, Y., Chang, X., Mišić, J., Mišić, V. B., & Li, L. (2019). BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. *IEEE Internet of Things Journal*, *6*(2), 3775-3784.

[151] Castro, M., & Liskov, B. (1999, February). Practical Byzantine fault tolerance. In *OSDI* (Vol. 99, No. 1999, pp. 173-186).

[152] Kaur, K., Garg, S., Kaddoum, G., Gagnon, F., & Ahmed, S. H. (2019, May). Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1-6). IEEE.

[153] Tutorial, H. L. P. S. L. (2005). A Beginner's Guide to Modelling and Analysing Internet Security Protocols. *The AVISPA Project*. Disponible En ligne: http://www.avispa-project.org/package/user-manual.pdf (Consulté le: 18/05/2020).

[154] Malhi, A. K., Batra, S., & Pannu, H. S. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. Computers & Security, 89, 101664.