UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À

L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES

PAR

AHCENE TENIOU

GESTION DES CERTIFICATS DANS L'INFONUAGE VÉHICULAIRE (VEHICULAR CLOUD NETWORKS)

-JUILLET 2017-

CE MÉMOIRE A ÉTÉ ÉVALUÉ PAR

UN JURY COMPOSÉ DE

- **Boucif Amar Bensaber,** directeur de recherche.

Professeur au département de Mathématiques et Informatique

Université du Québec à Trois-Rivières.

- **Mhamed Mesfioui,** évaluateur.

Professeur au département de Mathématiques et Informatique

Université du Québec à Trois-Rivières.

- **Ismail Biskri,** évaluateur.

Professeur au département de Mathématiques et Informatique

Université du Québec à Trois-Rivières.

À ma chère mère,
À mon père,
À mon frère,
À mes sœurs,
À tous ceux qui me sont chers...

Je dédie affectueusement ce modeste travail.

REMERCIEMENTS

Je tiens tout d'abord à exprimer mes sincères remerciements à mon directeur de recherche, le professeur Boucif AMAR BENSABER, pour son aide sans limite et ses précieux conseils, sans lesquels ce travail n'aurait pas vu le jour. Je ne le remercierai jamais assez de m'avoir surtout donné l'opportunité de faire mes premiers pas dans le champ de la recherche scientifique, notamment dans ce champ de recherche passionnant et promoteur : la sécurité des communications dans les réseaux véhiculaires.

Mes sincères remerciements vont particulièrement au professeur Mhamed MESFIOUI, un homme aux qualités extraordinaires. Qu'il trouve ici toute ma reconnaissance pour son aide qu'il m'avait fournie dès le premier jour de ma présence à l'université.

Je remercie également le professeur Ismaïl BISKRI d'avoir accepté d'évaluer ce travail, mes professeurs à l'UQTR qui m'ont permis d'acquérir plus de connaissances durant ma période d'études, ainsi que tous mes collègues du LAboratoire de Mathématiques et Informatique Appliquées (LAMIA).

Je remercie, par ailleurs, tous ceux qui, de près ou de loin, m'ont soutenu et encouragé pour réussir mes études.

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

VCN	Vehicular Cloud Network
ECQV	Elliptic Curve Qu-Vanstone
CA	Certificate Authority
RSU	Road Side Unit
STI	Systèmes de Transport Intelligents
VANET	Vehicular Ad-Hoc Networks
MANET	Mobile Ad-Hoc Networks
DSRC	Dedicated Short Range Communications
WAVE	Wireless Access in Vehicular environments
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1609.2	IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages-
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
OBU	On-Board-Unit
GHz	Gigahertz
ECIES	Elliptic Curve Integrated Encryption Scheme
QoS	Quality of Service
DoS	Denial of Service

AC	Autorité de certification
TPD	Tamper Proof Device
MAC	Message Authentication Code
PKI	Public Key Infrastructure
ICP	Infrastructure à clés publiques
CRL	Certification Revocation List
IBV	Identity-based Batch Verification scheme
ECPP	Efficient Conditional Privacy Preservation Protocol
LPP	Lightweight Privacy Preserving
SRAP	Scalable Robust Authentication Protocol
PASS	Efficient Pseudonymous Authentication Scheme with Strong Privacy Preserving
MAAC	Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks
MA	Master Authority
HMAC	Keyed-Hash Message Authentication Code
ECIES	Elliptic Curve Integrated Encryption Scheme
GPS	Global Positioning System

LISTE DES FIGURES

LISTE DES TABLEAUX

GESTION DES CERTIFICATS DANS L'INFONUAGE VÉHICULAIRES (VEHICULAR CLOUD NETWORKS)

Ahcene TENIOU

SOMMAIRE

Dans les réseaux d'infonuage véhiculaires (VCN), la gestion des certificats joue un rôle important dans les communications réseau. Tout nœud dans le réseau ne peut ainsi interagir avec les autres participants sans obtenir un certificat valide et approprié. Dans ce contexte, nous nous attèlerons ici à concevoir un mécanisme pour obtenir une distribution de certificats efficaces et dynamiques avec un coût réduit. Aussi, le présent mémoire propose un système de distribution de certificats implicites (ECQV) efficace et dynamique pour les réseaux d'infonuage véhiculaires, permettant aux véhicules de demander et d'obtenir des certificats implicites à travers une demande sécurisée à l'autorité de certification (CA basée sur le nuage), dans le but de signer les messages échangés avec les autres participants dans le réseau. Il n'en reste que la gestion des certificats soulève de nombreux problèmes telles que la façon d'établir des connexions sécurisées entre les différentes entités dans le réseau, la façon de protéger le système contre les véhicules malveillants et la révocation des certificats expirés des véhicules. C'est pourquoi une méthode simple et efficace de révocation est présentée dans le cadre de ce mémoire. Elle repose fondamentalement sur une technique sélective de distribution de messages de révocation, en vue de réduire le nombre de messages nécessaires pendant cette phase de révocation.

Dans ce travail, une analyse approfondie est effectuée pour démontrer comment le système proposé peut satisfaire efficacement les objectifs à atteindre. Le protocole proposé envisage une répartition uniforme des unités routières (RSUs) et une utilisation de la vitesse moyenne autorisée sur les routes dans les deux environnements urbain et autoroute afin d'évaluer les performances de notre système avec des simulations et dans toutes les circonstances. Le protocole fournit également une authentification préservant la vie privée, la non-répudiation et la confidentialité.

GESTION DES CERTIFICATS DANS l'INFONUAGE VÉHICULAIRES (VEHICULAR CLOUD NETWORKS)

Ahcene TENIOU

ABSTRACT

In Vehicular Cloud Networks (VCN), Certificate management plays an important role in network communications, any node in the network can't interact with other participants without obtaining the appropriate valid certificate. In this context, we are about to design an effective mechanism to achieve an efficient and dynamic certificate distribution with the most reduced cost possible. We propose ins this thesis, an efficient and dynamic ECQV implicit certificates distribution scheme for vehicular cloud networks, that enables vehicles to request and obtain implicit certificates upon a secure request to the Certificate authority (Cloud based-CA) to sign exchanged messages with other participants in the network. Dealing with certificate management raises many issues like how to make secure connections between different entities in the network, how to protect system from adversary vehicles and how to revoke expired certificates from vehicles. In this regard, a simple and efficient revocation method has been presented, which is basically based on selective revocation message delivery technique, to reduce the number of messages needed in revocation phase.

In this work, an extensive analysis is carried out to prove how the proposed scheme can efficiently fulfill the desired goals. The proposed protocol is considering a uniform distribution of roadside units and using the allowed average speed on roads in both urban and highway environments to evaluate the performance of our scheme with simulations and in all conditions. Our protocol provides authentication preserving privacy, non-repudiation and confidentiality.

CHAPITRE 1 INTRODUCTION GÉNÉRALE

Les systèmes de transport intelligents visent à fournir des applications et des services innovants liés à la gestion du trafic en vue de faciliter l'accès à l'information pour les différents utilisateurs du système. Plusieurs technologies ont été déployées pour maintenir et promouvoir les systèmes de transport intelligents (STI), notamment l'intégration des systèmes embarqués, le déploiement de la technologie de gestion de ressources informatiques dans le nuage conventionnel. Ce qui a permis de cultiver le concept du réseau d'infonuage véhiculaires (VCN), un concept développé à partir du réseau Ad Hoc véhiculaires (VANET), et qui est formé, d'une manière autonome, offrant ainsi une large gamme d'applications et de services à l'ensemble des participants dans les systèmes de transport intelligents.

Ces dernières années, les réseaux d'infonuage véhiculaires (VCN) sont devenus très populaires et continuent à croitre et à s'agrandir géographiquement, car ils permettent d'une part l'évolutivité en tant que propriété et d'autre part la gestion efficace du trafic, la sécurité routière et l'infodivertissement, en raison de leurs caractéristiques et applications spécifiques telles que la standardisation. En outre, ils fournissent également une clé importante pour atteindre une multitude d'objectifs actuels de transport tels que : la mobilité, la sécurité, le transport efficace et la base financière pour les nouvelles infrastructures routières, tout en réduisant aussi bien les menaces pour voyager en toute sécurité que les effets négatifs sur l'environnement. Cependant, en raison de la forte mobilité du trafic, le nuage véhiculaire est construit à la fois sur des ressources physiques, statiques et dynamiques. Il est confronté, par conséquent, à plusieurs défis inhérents, ce qui augmente la complexité de ses implémentations.

Pour faire face à ces défis, une bonne mise en place des réseaux d'infonuage est exigée. Elle reposera principalement sur le bon déploiement des réseaux véhiculaires sans fil et permettra aux véhicules d'être informés et à jour sur les conditions routières. En outre, au cours des communications entre les véhicules, ces réseaux diffusent plusieurs sortes de messages, comme des messages liés au trafic et qui contiennent une gamme d'informations très sensibles, telles que la position, la vitesse et la direction. Ainsi, un

adversaire malveillant peut, en l'absence de mesures de sécurité nécessaires, modifier le comportement des véhicules autour de lui, en signalant des fausses informations (pour tirer vraisemblablement des avantages personnels), engendrant ainsi des accidents. Un autre problème non moins important concerne la confidentialité d'un véhicule, puisqu'il n'est pas exclu qu'un adversaire puisse écouter des communications établies entre les différents nœuds dans le réseau. Les données échangées peuvent être ainsi interceptées et modifiées afin de dérouter les usagers et pire encore, de lancer une multitude d'attaques. Ce qui expose ainsi la vie privée à des situations malveillantes, voire dangereuses.

Pour résoudre ces problèmes, nous proposons, dans le cadre de notre mémoire, une étude d'un protocole de gestion efficace et dynamique des certificats de type ECQV (Elliptic Curve Qu-Vanstone) afin de protéger la vie privée des véhicules, par une authentification anonyme, efficace et dynamique.

Pour préserver la vie privée dans les réseaux véhiculaires sans fil, de nombreux mécanismes de gestion des certificats et de distribution des clés ont été proposés, au cours de ces dernières années. Ces mécanismes qui prennent en considération une meilleure authentification des données sont divisés en deux catégories principales : systèmes d'authentification basés sur des pseudonymes et les systèmes d'authentification basés sur la signature de groupe.

Dans ce mémoire, nous présentons quatre principales contributions visant à répondre à la problématique de l'authentification et de sa mise en œuvre dans notre modèle. Dans la première contribution, il sera question d'une introduction de notre système proposé, en l'occurrence la conception d'une approche de distribution efficace dynamique des certificats de type ECQV dans un environnement véhiculaire dans le nuage. Une autorité de certification est supposée être basée sur le nuage. Un véhicule demande dynamiquement un certificat via le RSU le plus proche. Une requête se propage dans le réseau proposé jusqu'à atteindre l'autorité de certification (Cloud based-CA). Par la suite, un certificat est renvoyé en toute sécurité. Le schéma de certificat implicite ECQV est utilisé pour la génération de certificats et la distribution des paires de clés.

La deuxième contribution présente, elle, une méthode légère et efficace de révocation de certificats expirés à la fin de la durée de vie du certificat de chaque véhicule. Cette méthode s'appuie sur une technique simple de distribution de messages de révocation sélective basée sur la trajectoire, la vitesse, la nature de la région, ainsi que sur d'autres paramètres. La pertinence de cette méthode s'explique par le fait qu'elle permet de réduire la bande passante consommée et de ne pas saturer les ressources physiques sans en altérer la disponibilité. La troisième contribution introduit, quant à elle, un processus de changement de certificats après la phase de révocation. Changement qui se fait, toutefois, aléatoirement dans un petit intervalle de temps. Ceci garantit ainsi un changement périodique des certificats, mais pas en temps constant. Ce qui empêche les véhicules malveillants de prédéfinir à l'avance le temps de changement du certificat de chaque véhicule.

Enfin, la quatrième contribution énonce une analyse approfondie afin de déduire comment le système proposé pourrait maitriser une distribution efficace et dynamique des certificats, ainsi que la façon dont il achève un processus d'authentification fiable avec une forte intégrité et confidentialité des messages pour tous les participants. Des exemples d'attaques et d'insuffisances de mécanisme qui y ont été mis en œuvre seront discutés dans cette partie. Une évaluation de la présente approche est effectuée en analysant les résultats de la simulation et surtout en les comparant avec d'autres approches déjà proposées dans les deux environnements de circulation, urbaine et autoroutière.

Le reste du mémoire est structuré comme suit : le deuxième chapitre présente les réseaux véhiculaires sans fil utilisent 802.11p en général, la notion du nuage véhiculaire et ses caractéristiques ainsi que les outils de cryptographie utilisés. Le troisième chapitre est un résumé de quelques travaux tirés de la littérature portant sur le problème d'authentification dans les réseaux véhiculaires sans fil, suivi d'un tableau récapitulatif. Le quatrième chapitre décrit nos principales contributions visant à répondre à la problématique de l'authentification et à sa mise en œuvre dans les réseaux d'infonuage véhiculaires, la gestion efficace des certificats et la distribution dynamique des clés avec une forte intégrité et confidentialité des messages échangés par tous les participants dans le réseau, sous forme d'un article scientifique. Les

résultats seront discutés dans le chapitre 5. Il y sera question notamment de l'apport des solutions proposées, ainsi que de leur pertinence dans la réduction des coûts dans le réseau par le processus d'authentification et de révocation sans en altérer la disponibilité. Quant au sixième chapitre, il présentera la conclusion de notre étude avec, en sus, quelques perspectives.

CHAPITRE 2 RÉSEAUX VÉHICULAIRES : GÉNÉRALITÉS ET CARACTÉRISTIQUES

2.1 Introduction

Les réseaux véhiculaires ad-hoc, plus connus dans la littérature sous la dénomination VANET (Vehicular Ad-hoc Networks), reprennent les mêmes principes architecturaux que les réseaux ad-hoc mobiles (MANET). Leur déploiement promeut l'émergence des systèmes de transports intelligents (STI) qui fournissent une large gamme d'applications et des services liés à la sécurité routière (p. ex. alerte accident, alerte ralentissement, conduite coopérative, messagerie instantanée inter-véhicules, musique et films en streaming et jeux de vidéo à temps réel inter-véhicules etc.) dont l'essor dans les VANETs est porté par l'accroissement du parc automobile et la nécessité dans le monde contemporain de maximiser la sécurité des biens et des personnes, tout en réduisant les menaces contre la sécurité routière et les effets nocifs sur l'environnement.

Pour mettre en œuvre ces applications, divers projets ont fleuri à travers le monde, plusieurs institutions et constructeurs d'automobiles ont mené des projets qui ont abouti à l'expérimentation de prototypes et de solutions variés. Avec les dernières avancées dans le domaine des technologies de communication, de calcul et de localisation, de nouveaux projets autour des applications des VANETs continuent de voir le jour.

Dans ce chapitre, nous présenterons plusieurs notions et définitions en liaison avec les réseaux VANETs et leur sécurité, y compris, l'architecture de ce type de réseaux, les modes de communications entre les différentes entités du réseau, les services issus de ces réseaux, la norme IEEE 1609.2-2016 (IEEE Standard for Wireless Access in Vehicular Environments—Security Service for Applications and Managment Messages), les mécanismes et les concepts de sécurité des réseaux VANETs et enfin les outils cryptographiques utilisés dans ce travail.

2.2 Architecture générale

Dans les réseaux véhiculaires sans fil, les trois principaux composants qui les constituent sont [1] :

- CA (Certificate Authority)

Cette entité représente l'autorité principale de certification qui contrôle l'ensemble du réseau, assure la gestion et la mise à jour de toutes les entités dans le réseau (RSU, véhicule), délivre des certificats et des pseudonymes de communication aux véhicules et établit également leurs identités.

- RSU (Road Side Unit)

Cette entité est installée au bord des routes. Elle sert à diffuser les différentes informations sur les conditions routières à l'ensemble de véhicules qui empruntent son passage. Elle est considérée comme un point de liaison entre l'autorité de certification et les véhicules ou un point d'accès au réseau.

- OBU (On-Board Unit)

Cette entité embarquée dans les véhicules représente l'ensemble des composants matériels et logiciels installé au bord des véhicules. Elle joue le rôle d'une interface qui interagit avec les autres entités dans le réseau. Elle permet également la localisation actuelle du véhicule, le calcul, le stockage, l'envoi et la réception des données échangées sur le réseau.

2.2.1 Modes de communication dans VANET

Dans les réseaux VANETs, on peut distinguer deux modes de communication, les communications véhicules à véhicules (V2V) et les communications véhicules à infrastructure (V2I) [2]. Comme illustré dans la Figure *2-1*.

- Mode de communication véhicule à véhicule (V2V)

Ce mode de communication fonctionne suivant une architecture décentralisée par le biais des unités embarquées au bord des véhicules (OBU). Ces véhicules pourront établir une communication entre eux si l'ensemble des participants est à la même

portée (même zone radio), ou bien par le biais d'un protocole multi-sauts qui prend en charge la transmission des messages échangés de bout en bout en exploitant les nœuds voisins comme des relais. Ce mode de communication est aussi efficace que rapide avec une faible latence pour transférer des informations liées aux conditions routières ou de l'infodivertissement. Reste cependant que la connectivité n'est pas toujours permanente.

- Mode de communication véhicule à infrastructure (V2I)

Ce mode de communication est établi entre les OBUs (On-Board Units) des véhicules et les RSUs (Road Side Units) installés au bord des routes. Il assure une meilleure utilisation des ressources partagées et les services fournis dans le réseau (ex. internet, météo, Info-divertissement etc.).

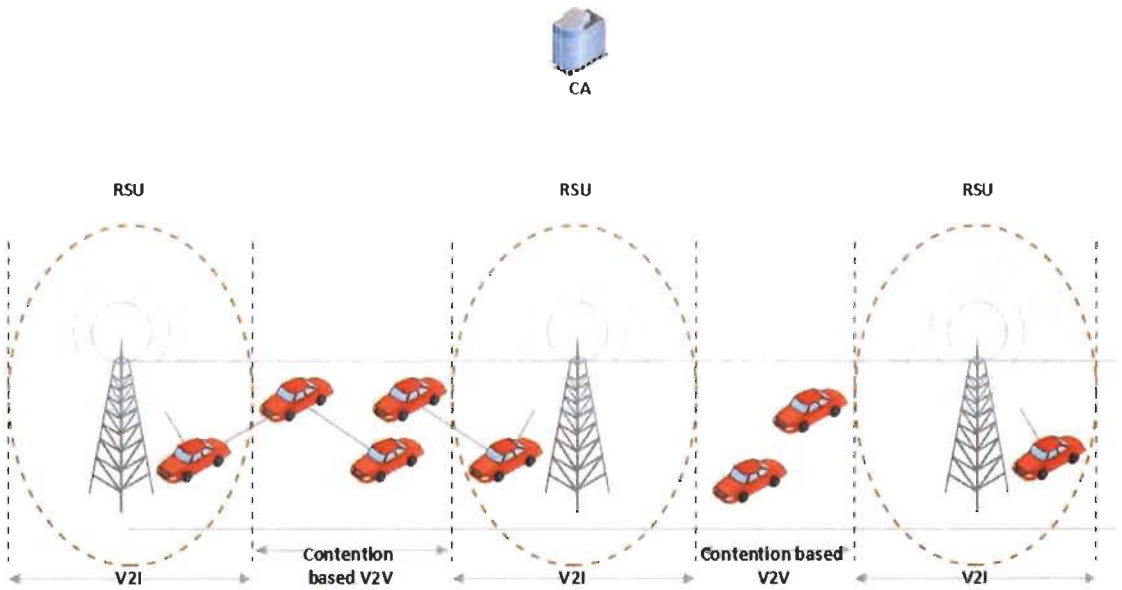

Figure 2-1 Modèle des réseaux VANETs et leur mode de communication

2.2.2 Caractéristiques des VANETs

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des réseaux ad hoc mobiles. Ces caractéristiques doivent être prises en compte lors de la conception des protocoles pour les VANETs.

Dans cette partie, nous présentons quelques propriétés et contraintes concernant ce type de réseau :

a) Capacité et autonomie d'énergie

La disposition d'une capacité suffisante d'énergie constitue l'une des principales caractéristiques des réseaux VANETs. Elle peut alimenter les différents équipements électroniques d'un véhicule [3]. Ce qui n'est pas le cas pour les réseaux MANET. Les nœuds sont donc censés avoir une grande capacité de traitement et de stockage des données.

b) Topologie et connectivité

Les réseaux VANETs sont caractérisés par une connectivité éphémère et relativement faible. Cela est dû à la haute mobilité des véhicules (nœuds) dans le réseau, à leurs déplacements imprédictibles et à leurs réactions face à des obstacles, ce qui rend ainsi les durées de communications entre les nœuds très réduites. En outre, un véhicule peut rejoindre ou quitter un groupe de véhicules en un temps très court, ce qui nous mène ainsi à avoir une topologie très dynamique de plusieurs groupes séparés [3]. Ceci conduit à une topologie très dynamique et fréquemment réorganisée.

c) Modèle de mobilité

Le modèle de mobilité dans les réseaux VANET est lié à la diversité environnementale et les infrastructures routières [4]. Cependant, le mode de mobilité des réseaux VANETs est affecté par la vitesse des véhicules, leurs déplacements aléatoires, le comportement des conducteurs et leurs réactions face à des obstacles ou à des situations différentes et complexes. (ex. les heures de pointe, les accidents, etc.) [5].

d) Technologies de communications

Pour la mise en place des différents modes d'échange de données entre les entités dans les VANETs, une norme de la famille IEEE 802.11 a été adoptée. Elle porte l'indice 802.11p. Cette extension du standard concerne les communications de services entre les véhicules et l'infrastructure ou entre véhicules, dans la bande 5,9 GHz dédiée à cet usage. Sa couche physique est basée sur la norme IEEE 802.11a

[6]. Elle définit essentiellement les services de sécurité et le format des messages échangés pour soutenir et satisfaire au premier lieu les exigences américaines des STIs.

e) Sécurité contre les menaces

En raison de l'importante des informations échangées via les communications véhiculaires dans les VANETs, le processus de sécurisation des canaux de communication est devenu crucial et un prérequis primordial pour le déploiement de ce type de réseaux [7].

2.3 La sécurité dans les réseaux VANETs

2.3.1 Introduction

La sécurité des réseaux véhiculaires est un enjeu majeur dont il faut se saisir pour garantir la plus large adaptation possible de ces réseaux. À cause de l'importance et la grande quantité des informations échangées, le nombre énorme d'utilisateurs, la topologie dynamique et la connectivité intermittente, les messages liés à la sécurité peuvent être falsifiés par des entités malveillantes afin de causer des accidents et mettre la vie des personnes en péril. Pour assurer donc un bon déploiement de ces réseaux, il convient de mettre en œuvre des mécanismes de sécurité appropriés afin d'éviter ce type d'attaques.

Dans cette section, nous aborderons en particulier les exigences et défis liés à la sécurité et les différents mécanismes de sécurité qui y sont en vigueur et qui peuvent y être utilisés afin de bien sécuriser les informations échangées à travers ces réseaux. Nous présenterons aussi une brève description sur l'utilité des certificats implicites, en citant leurs avantages par rapport aux certificats explicites, ainsi le standard WAVE/DSRC IEEE 1609 axé sur la sécurité, soit : le IEEE 1609.2

2.3.2 Exigences et défis de sécurité

Nous discuterons dans cette section également des principales exigences et autres défis qui se posent à la sécurité dans les réseaux véhiculaires. Ces questions importantes sont abordées pour être prises en compte dans la conception des protocoles de sécurité

et des algorithmes cryptographiques, ainsi que dans leur mise en œuvre dans les VANETs. À ce titre, nous pouvons en citer :

a. L'authenticité

Ce concept de sécurité permet aux entités du réseau de s'assurer de la bonne identité des entités avec lesquelles elles communiquent. L'authenticité permet aux différentes entités du réseau de se fier aux données et messages diffusés. Elle est la seule exigence qui permet la coopération entre les différents participants ; leur identification permet ainsi d'assurer le bon contrôle de l'authenticité des messages échangés [8]. Il convient de préciser ici qu'il existe deux types d'authentification : une authentification des messages qui permet d'en retracer la source et une authentification des entités qui permet, elle, d'identifier les nœuds du réseau [9].

b. La non-répudiation

Ce concept de sécurité permet de démontrer et localiser avec certitude l'origine des données. Grâce à ce principe, chaque entité diffusant un message sur le réseau ne peut le nier ou se rétracter de l'avoir émis. Ainsi, la non-répudiation permet d'identifier les entités malveillantes qui tentent de commettre des actes illégaux, ce qui permet d'écarter toute possibilité pour qu'un attaquant injecte des données erronées sans qu'elles ne soient immédiatement identifiées. Le concept de non-répudiation est essentiel dans les transactions commerciales en lignes et financières, ainsi que dans les opérations électroniques de facturation. Dans le contexte des VANETs, la signature numérique est utilisée pour garantir la non-répudiation des messages concernant les applications de sécurité et de gestion du trafic [10].

c. La confidentialité

Ce concept de sécurité permet de garantir la non-divulgation des données transmises dans le réseau à des parties non autorisées. Seules les parties habilitées peuvent y accéder à travers le réseau [10]. La confidentialité consiste ainsi à préserver les informations vitales liées aux véhicules par l'application des algorithmes de cryptographie asymétrique et symétrique, ce qui empêche les entités malveillantes de suivre et d'écouter les messages concernant un véhicule ciblé dans le réseau. Le standard IEEE 1609.2 utilise le chiffrement *Advanced Standard in CCM mode* (AES-

CCM) [11] comme algorithme de cryptographie symétrique. Reste que la faille majeure dans ce type de cryptographie réside dans cette difficulté rencontrée lors de l'établissement d'un canal sécurisé pour la distribution de la clé privée. Par ailleurs, le standard IEEE 1609.2 utilise la cryptographie asymétrique pour l'échange de la clé secrète grâce à l'algorithme de chiffrement *Elliptic Curve Integrated Encryption Scheme* (ECIES) [12]. Chaque véhicule dans ce mode de cryptographie détient une paire de clés publique et privée. La clé privée n'est connue que du véhicule émetteur, tandis que la clé publique est partagée avec toutes les autres entités du réseau.

d. L'intégrité

Ce concept de sécurité permet d'assurer que les messages diffusés ne seront pas modifiés ou altérés volontairement ou accidentellement entre la phase d'émission et de réception par des entités non autorisées (malveillantes). Cet objectif de sécurité vise ainsi à doter les destinataires d'un pouvoir permettant de détecter les manipulations de données effectuées durant leur transmission par les entités malveillantes et rejeter les paquets correspondants. L'intégrité peut être réalisée principalement par l'utilisation des fonctions de hachage et de la cryptographie sur des champs spécifiques des paquets. Cependant, dans les réseaux sans fil, se pose toujours la contrainte de l'intégrité qui n'est pas toujours forcément liée au terme de manipulation. En effet, bien des altérations sont le fait des conditions de propagation radio.

e. La disponibilité

Ce concept de sécurité permet de garantir que toute entité autorisée puisse accéder aux ressources du réseau en tout temps avec une qualité de service (QoS) adéquate [10]. En effet, tous les participants dans le réseau doivent avoir un accès effectif et rapide aux différents services de la gestion du trafic, aux applications de sécurité et de confort sollicités. Pour atteindre un bon niveau de disponibilité, il est indispensable d'installer du matériel et mettre en œuvre des protocoles de sécurité de hautes performances. Cependant, ce concept est principalement menacé par les attaques de type dénis de services (DoS) et trou noir (Black Hole), qui sont des attaques très difficiles à prévoir et à contrôler [8]. Ainsi, il est certainement bien plus difficile d'atteindre cet objectif que les autres ; le but étant juste de réduire des effets de ce type d'attaques.

2.3.3 Mécanismes de base de la sécurité

Après avoir expliqué les différentes exigences et autres défis de sécurité dans les réseaux VANET, nous aborderons dans cette section les mécanismes appropriés et les techniques cryptographiques existantes qui peuvent apporter des solutions aux problèmes liés à l'authentification, l'intégrité et la non-répudiation.

a. Cryptographie

La cryptographie est une discipline qui désigne l'ensemble des techniques permettant de chiffrer les données transmises en employant souvent des clés secrètes. Elle consiste, comme son nom l'indique, à crypter le contenu des messages échangés à l'aide des algorithmes de chiffrement par les entités expéditrices afin de les rendre incompréhensibles. Pour décrypter ensuite ces messages cryptés, les entités destinataires appliquent le processus de déchiffrement à l'aide des algorithmes de déchiffrement afin de reconstruire les messages originaux. Il convient de noter que, dans cette discipline, nous distinguons deux types de cryptographie :

- Cryptographie symétrique : où il y a une seule clé secrète partagée entre l'expéditeur et le destinataire pour le processus du chiffrement et déchiffrement des messages.
- Cryptographie asymétrique (Cryptographie à clé secrète) : elle repose sur le principe de diffuser la clé publique entre l'expéditeur et le destinataire et, en même temps, garder la clé privée secrète qui permet de coder et décoder les messages échangés.

b. Hachage

Le hachage consiste à déterminer une information de taille fixe et réduite appelée « l'empreinte ou le condensé » à partir d'une chaine de données fournie en entrée, ayant différentes tailles plus longues [5]. Les fonctions de hachage les plus utilisées sont celles à sens unique. Ce genre de fonction irréversible fournit l'empreinte à partir de ladite chaine. La particularité de cette fonction est qu'il est très facile de calculer l'empreinte d'une chaine donnée, mais il est difficile, voire impossible, de retrouver ou déduire la chaine initiale à partir de l'empreinte [13].

c. Signature numérique

La signature numérique est un mécanisme permettant de garantir l'intégrité et la non-répudiation d'un message et d'en authentifier l'expéditeur. En pratique, le concept de la signature numérique s'appuie sur la cryptographie asymétrique, en faisant un appel aux fonctions de hachage et à la clé privée du signataire (l'expéditeur). Le message est signé avec la clé privée de l'expéditeur, tandis que le destinataire vérifiera l'intégrité et l'authenticité du message en utilisant la clé publique correspondante à l'expéditeur. Pour ce faire, il est recommandé de réunir les conditions suivantes : authenticité, infalsifiabilité, non-réutilisabilité, irrévocabilité.

Ainsi, le récepteur d'un message pourra s'assurer que l'émetteur a bien utilisé sa clé privée pour signer le message. L'hypothèse de base avec les certificats fait que les véhicules doivent être capables de vérifier les certificats, car ce genre de documents peut attester l'authenticité de la paire de clés publique/privée

d. Certificats numériques

Afin de renforcer le concept de signature numérique, il y a lieu de combiner ce dernier avec un certificat numérique délivré par un tiers de confiance appelé l'autorité de certification (AC). Il est à noter ici que les certificats sont des structures de données décrivant des identités numériques et permettant de prouver l'identité du propriétaire d'une clé publique. Grâce à la cryptographie asymétrique, le certificat atteste de l'authenticité de la paire de clés publique/privée et permet l'identification des véhicules de façon unique. Nous distinguons ici deux types de certificats [5] :

- **Certificat à long terme**

Ce certificat est délivré par l'autorité de certification (AC), il contient des informations indiquant l'identité du véhicule et son propriétaire, les caractéristiques des équipements du véhicule (p. ex. le modèle du TPD). Il est utilisé principalement pour le renouvèlement des certificats à court terme et l'établissement de communications sécurisées avec les autres entités dans le réseau.

- **Certificat à court terme**

Ce certificat a une durée de vie très courte (d'environ une minute [14]), il est léger par rapport aux certificats à long terme, car il ne contient pas l'identification réelle du conducteur. À cet effet, ce certificat utilise un pseudonyme permettant d'identifier le véhicule d'une façon unique.

Il faut souligner que chaque véhicule possède un seul certificat à long terme et plusieurs certificats à court terme. Ainsi, toutes les clés privées correspondant aux clés publiques sont stockées dans un dispositif inviolable dénommé TPD (Tamper-Proof Device). Le TPD doit avoir donc une grande capacité de stockage afin que les véhicules puissent communiquer de manière sécurisée même en l'absence de connectivité avec l'AC pour des périodes très longues [5].

e. MAC (Message Authentication Code)

Le MAC est un mécanisme qui assure et renforce principalement l'authentification des messages échangés. Son rôle est d'accompagner les messages durant leur phase de transmission dans le but d'assurer l'intégrité de ces derniers, en permettant de vérifier s'ils n'ont subi aucune modification. L'implémentation de ce mécanisme est basée sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage.

f. TPD (Tamper-Proof Device)

TPD est un autre dispositif composé de matériels et logiciels, contenant plusieurs capteurs de hautes performances permettant de déduire d'une manière automatique les informations stockées après chaque manipulation du matériel [15]. Il permet aussi le stockage en toute sécurité des données liées à la confidentialité du véhicule (Certificats, Pseudonymes privés). Ce dispositif se préoccupe ainsi de la signature de tous les messages envoyés par le véhicule [8]. Reste cependant qu'il coûte très cher.

2.3.4 Certificats implicites

Comme les certificats conventionnels ou explicites, les certificats implicites sont composés de trois parties [16] : des données d'identification, une clé publique et une signature numérique qui lie la clé publique aux données d'identification de l'utilisateur et vérifie si cette liaison est acceptée par l'autorité de certification (AC). Dans un

certificat conventionnel, la clé publique et la signature numérique sont des éléments de données distincts. Mais dans les certificats implicites, elles sont fortement reliées, permettant ainsi au destinataire d'extraire et de vérifier la clé publique de l'autre partie à partir de la partie signature. Cela réduit considérablement la bande passante requise, car il n'est pas nécessaire de transmettre à la fois le certificat et la clé de vérification. Ce genre de certificats sont plus rapides que les certificats explicites et elles sont de petites tailles.

Le schéma des certificats implicites de type *Elliptic Curve Qu-Vanstone* (ECQV) utilisé dans la présente étude est conçu principalement pour les environnements d'applications où les ressources telles que la bande passante, la capacité de traitement et le stockage sont limitées. En plus de ses atouts de flexibilité et de rapidité, ce schéma présente de grands avantages fonctionnels par rapport aux certificats ordinaires, mais dont le coût de traitement et de stockage reste toutefois très réduit.

2.3.5 Standard de sécurité : IEEE 1609.2

Le standard IEEE 1609.2 [17] décrit l'aspect de la sécurité dans les VANETs. Il définit le format des messages signés et chiffrés pour le système DSRC/WAVE, ainsi que celui des certificats. Le standard spécifie les méthodes à suivre pour sécuriser les messages de gestion et d'application. Il décrit aussi les procédures qu'un véhicule doit accomplir afin d'assurer les exigences de sécurité décrites dans les sections précédentes telles que l'authenticité, la confidentialité, l'intégrité, et la non-répudiation. Le format des messages dans ce standard diffère selon le service déployé. À titre exemple, le message contenant un certificat à long terme est à la fois signé et chiffré contrairement à celui d'alerte qui est seulement émargé. Le IEEE 1609.2 protège ainsi les messages et les véhicules contre les différentes attaques connues dans les VANETs comme l'écoute clandestine, l'usurpation d'identité, l'altération, ou le rejeu de message.

2.3.6 Conclusion

Dans ce chapitre, nous avons abordé le problème de la sécurité dans les VANETs au sens général. Afin de comprendre comment sécuriser ce genre de réseau, nous en avons présenté les principaux concepts, leurs différents modes de communication et leurs caractéristiques. Ensuite, nous avons entamé l'aspect de sécurité dans ces réseaux, en abordant et énumérant les différentes exigences et autres défis de sécurité permettant d'assurer les services de sécurité conventionnels, particulièrement les plus employés dans les applications véhiculaires : l'authenticité, la non-répudiation, la confidentialité, l'intégrité et la disponibilité. Nous avons conclu en présentant une vue d'ensemble sur les mécanismes appropriés et les techniques cryptographiques existantes qui peuvent apporter des solutions aux problèmes liés à la sécurité dans les réseaux VANETs, les certificats implicites et enfin une brève description du standard IEEE 1609.2.

Bien que la sécurité dans les réseaux VANETs ait attiré déjà beaucoup d'attention et suscité autant de travaux au cours de ces dernières années, elle reste toutefois l'un des principaux sujets controversés dans les applications des systèmes de transport intelligents. En effet, face aux menaces et attaques externes, le déploiement des techniques cryptographiques comme la signature numérique avec certificat demeure indispensable pour assurer l'authenticité des données échangées et préserver la vie privée des véhicules. Notre mission est de créer donc de nouvelles techniques de sécurité afin d'assurer cette authenticité dans les réseaux véhiculaires sans fil et de mieux renforcer les solutions existantes.

Dans le chapitre suivant, nous allons présenter l'état de l'art à travers quelques travaux existant dans la littérature liée au problème d'authentification et de gestion des certificats.

CHAPITRE 3 REVUE DE LITTÉRATURE

3.1 Introduction

Le bon fonctionnement des applications déployées dans les réseaux véhiculaires sans fil et adoptées par les systèmes de transport intelligents (STI) passe par le développement de mécanismes de sécurité appropriés assurant en particulier l'authentification et l'autorisation des entités communicantes. En l'absence de mesures de sécurité nécessaires, les messages échangés peuvent être une source de menaces pour ces entités. Seules les entités dont la légitimité est démontrée peuvent donc avoir accès aux ressources et aux services du réseau. Au cours de ces dernières années, diverses solutions ont été proposées afin de sécuriser d'une manière efficace les messages échangés et conserver l'identité des utilisateurs du réseau.

Dans le présent chapitre, nous résumons quelques travaux récents qui ont surtout porté sur le problème de l'authenticité et son apport dans la préservation de la vie privée des véhicules.

Nous avons notamment choisi de résumer des travaux qui sont en liaison explicite avec la gestion efficace des certificats et la gestion des pseudo-identités de certificats. Même si elles utilisent différentes techniques, ces gestions ont toutes le même objectif de sécurité, à savoir, la gestion de l'authenticité en préservant la vie privée des véhicules dans les réseaux VANETs.

3.2 Protocoles d'authentification dans les réseaux VANETs

Dans le cadre des efforts de recherche déployés précédemment, plusieurs protocoles et systèmes de gestion de certificats ont été proposés en vue d'assurer la sécurité et la préservation de la vie privée dans l'environnement VANET. Ces systèmes peuvent être divisés en deux catégories principales : les systèmes d'authentification basés sur l'identité et les systèmes d'identification basés sur la signature de groupe.

Dans [18] [19], les auteurs utilisent un dispositif dénommé le *Tamper Proof Device* (TPD). Il est employé comme un support de stockage pour la clé publique de l'autorité de certification (AC). Dans cette approche, un nœud envoie à un autre le hash de la clé globale. S'il est identique au hash généré à partir de la clé stockée dans le TPD, la communication est établie entre ces deux nœuds. Cette approche repose ainsi sur l'utilisation du TPD qui reste, néanmoins, un dispositif coûteux et peu fiable.

Dans une autre optique, Aslem et Zou [20] tentent d'ignorer le TPD considéré comme un dispositif irréaliste. Ils utilisent en échange un dispositif embarqué et chargé avec des cartes prépayées contenant les clés d'authentification. Chaque carte contient une identification et un certificat. Au cours de l'initialisation, les informations de l'utilisateur seront conservées auprès du fournisseur des cartes et non pas stockées dans ce périphérique. Ainsi, lorsqu'un utilisateur entre dans une zone de service, il effectue le paiement de service à l'aide de ce dispositif de paiement embarqué à bord. Les messages sont chiffrés par la clé publique du fournisseur, dissimilant ainsi le certificat et les services demandés aux écoutes. L'utilisateur reçoit un pseudonyme valide pour une petite période et valable pour une zone précise. C'est presque le même comportement utilisé par le TPD.

Dans [21], Zhang a supposé que le véhicule s'authentifie en générant des clés publiques/privées par lui-même. Lorsqu'il entre dans la zone de communication d'un RSU, il lance un processus d'authentification mutuelle avec le RSU. L'algorithme Diffie-Hellman est utilisé pour échanger les clés symétriques. Le RSU et les autres véhicules dans le périmètre de couverture du RSU reçoivent un message crypté et un code d'authentification de message en anglais : *Message Authentication Code* (MAC). Le MAC généré est basé sur le message de la clé symétrique partagée avec le RSU. Ce dernier peut valider le MAC car il est le seul propriétaire de la clé symétrique. S'il le valide, il enverra un message authentifié aux autres véhicules. Pour éviter l'échec du RSU, la communication V2V sera effectuée en remplaçant V2I. L'infrastructure de clé publique, en anglais : *Public Key Infrastructure* (PKI) est utilisé pour générer et distribuer des clés. Idem pour le TPD qui est utilisé pour le stockage des clés. Cette approche garantit certes la confidentialité, mais sans entrer en communication avec l'autorité de certification pour s'assurer que le véhicule est légitime. En outre, dans

cette étude, l'auteur traite chaque RSU comme un réseau distinct et aucune coopération ni communication n'est établie avec les autres RSU dans le réseau. Cela obligera les véhicules de répéter le processus d'authentification chaque fois qu'ils entrent dans la zone de couverture et de communication de chaque RSU. Le résultat est évident, les frais généraux de calcul connaitront une augmentation fulgurante dans le réseau.

Comme nous l'avons mentionné précédemment, les systèmes d'authentification peuvent être divisés en deux catégories. La première est basée sur les pseudonymes avec l'utilisation de certificats anonymes basés, eux aussi, sur une infrastructure à clé publique (ICP), en anglais : *public Key Infrastructure* (PKI). Le système est capable de vérifier les messages signés par des clés privées anonymes associées. Ces certificats anonymes sont générés pour préserver l'identité réelle d'un véhicule. Ils sont utilisés pour établir des communications avec d'autres entités dans le réseau. Dans une étude similaire, Raya et Hubaux [22] proposent un système qui repose sur la distribution de milliers de certificats de clés privées associées. Pour ce faire, ils supposent que les véhicules sont équipés d'un dispositif inviolable TPD (Tamper-Proof Device). Il est utilisé comme un outil de stockage des clés et de certificats pour préserver l'intimité des véhicules et améliorer la sécurité. Chaque véhicule est censé stocker un grand nombre de certificats pseudonymes avec des pseudo-identités. Il sélectionne ensuite d'une manière aléatoire la clé privée à partir de ce groupe de certificats pseudonymes disponibles pour signer un message. De plus, un vérificateur peut contrôler la signature avec l'aide d'un certificat anonyme associé. En outre, l'autorité de certification distribue des certificats et conserve le mappage des identités réelles de ces certificats. Le système présenté ainsi par ces auteurs semble fort intéressant. Ils estiment qu'il remplit la vie privée conditionnelle en profitant des clés privées associées et répond aux problèmes de sécurité. Reste cependant que ce système présente plusieurs lacunes. Tout d'abord, en raison de la haute mobilité du réseau et de la présence de milliers de certificats par véhicule et lorsque le certificat d'un véhicule est révoqué, les listes de révocation de certificats, en anglais *Certificate revocation lists* (CRL) augmentent rapidement, prenant ainsi un espace de stockage remarquable pour emmagasiner toutes les CRL dans le réseau. Ce qui nécessite beaucoup de temps pour vérifier toutes les CRL avant de déclencher le processus CRL réel. Il en résulte ainsi une saturation de

la capacité de stockage. D'autre part, le CA doit révoquer tous les certificats détenus par un véhicule après un certain temps. Cela augmente non seulement les frais généraux du réseau, mais aussi une consommation supplémentaire de la bande passante, de sorte que tous ces inconvénients peuvent entraîner une inondation du réseau.

Une solution a été proposée pour résoudre les problèmes rencontrés dans [22]. Ainsi, les auteurs dans [23] ont étudié comment distribuer efficacement les CRLs par le biais des communications véhicule-véhicule (V2V). Cependant, en raison de la grande mobilité des nœuds due à leurs vitesses élevées, la bande passante limitée, la topologie dynamique et la connectivité intermittente, il est difficile de distribuer un grand CRL à tous les véhicules en temps opportun. Pour diminuer la taille du CRL, Bellur [24] suggère de segmenter un pays en plusieurs régions géographiques et d'attribuer des certificats spécifiques à chaque région avec une période de validité précise.

Sun et al. [25] proposent, dans une autre contribution, un schéma d'authentification de pseudonymes efficaces avec une forte protection de la vie privée nommé PASS (Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation). Dans ce schéma, le mécanisme repose sur l'utilisation des certificats pseudonymes appartenant au même propriétaire. Il est basé sur la technologie de la chaine hash à sens unique pour réduire la taille des CRLs. Notons ici que la taille CRL dans PASS est linéaire avec le nombre de véhicules révoqués et interconnectés avec le nombre de certificats pseudonymes détenus par les véhicules révoqués. Les auteurs de la contribution utilisent également la technique de signature par procuration (Proxy signing technique) comme une solution pour la mise à jour des certificats. Ceci implique une réduction considérable du coût de révocation et les frais généraux de la mise à jour des certificats.

Les auteurs dans [26] utilisent un schéma de vérification par un lot basé sur l'identité des véhicules, en anglais *Identity-based Batch Verification scheme* (IBV). Dans leurs propositions, IBV est utilisé pour générer des certificats de pseudo-identité aléatoires et des clés privées associées. La confidentialité conditionnelle est obtenue dans la mesure où l'autorité de confiance (AC) peut récupérer l'identité réelle d'un véhicule à

partir de la signature numérique des messages. Le (AC) peut effectuer plusieurs signatures de message à la fois. Les auteurs estiment que leur proposition est une solution efficace pour la confidentialité conditionnelle. En tirant avantage des pseudo-identités, elle répond ainsi aux exigences de sécurité. Cependant elle reste moins efficace par rapport à la technique de la cryptographie symétrique. Pis encore, le système proposé est exposé aux attaques DoS.

Dans [27], Guo et autres proposent un protocole d'authentification LPP (Lightweight Privacy Preserving) pour préserver la vie privée, avec une traçabilité de l'autorité d'authentification en utilisant des courbes elliptiques basées sur le hachage caméléon. Il est à noter ici que la principale caractéristique des algorithmes de signature de caméléon est non-interactive. Cela signifie que la signature est générée sans interagir avec le destinataire prévu. Ce protocole proposé qui exploite les clés publiques dynamiques générées pour améliorer la sécurité et l'efficacité des communications VANET, se compose de trois phases : la phase d'enregistrement, la phase d'authentification mutuelle et la phase de suivi CA. La version améliorée proposée évite l'utilisation des clés publiques fixes. En outre, et par rapport aux schémas existants, le LPP peut obtenir une authentification mutuelle et anonyme pour deux modes de communication V2V et V2I avec un coût de calcul beaucoup plus faible. Les auteurs estiment, de ce fait, que leur protocole LPP garantit l'authentification mutuelle et anonyme pour les communications V2V et V2I, la non-traçabilité du véhicule, la capacité de suivi d'autorité avec un faible coût et une grande efficacité de calcul. Si, de l'avis de ces concepteurs, le protocole LPP est très approprié pour un environnement véhiculaire avec une utilisation efficace des courbes elliptiques basées sur le hachage caméléon, il n'en demeure pas moins qu'ils ne proposent aucune méthode de révocation des certificats actuels ou une approche de modification régulière des certificats ou des pseudonymes, pour assurer l'anonymat et prévenir le suivi illégal.

La deuxième catégorie des systèmes d'authentification est basée sur la signature de groupe, elle consiste à former des groupes composés de véhicules, puis à en dissimuler les membres pour protéger leur identité réelle et préserver ainsi leur vie privée. Dans l'un de leurs travaux précédents, Hao and al. [28] ont introduit, dans le contexte de la

gestion des clés distribuées, un système de gestion de clés avec authentification de message coopératif dans le réseau VANET. Les auteurs établissent une technique de communication de groupe entre les véhicules, en tablant sur le fait que chaque véhicule dans le réseau devrait périodiquement envoyer sa position au RSU le plus proche. Bien que cette technique réduise le coût de calcul et les frais généraux, elle entraine toutefois de vrais problèmes concernant le leader de groupe et les véhicules qui se joignent et quittent le groupe.

Une autre étude non moins importante est celle proposée par Lin et autres [29]. Ces auteurs proposent un système nommé GSIS introduisant un nouveau protocole de sécurité et de préservation de la vie privée pour les réseaux VANETs, en intégrant les techniques de signature de groupe et de signature basée sur l'identité. La caractéristique principale de la signature du groupe est qu'elle est signée par le membre principal du groupe et vérifiée par la clé publique du groupe [30]. La signature basée sur l'identité [31] est utilisée par les RSUs, pour valider et autoriser chaque message qu'ils produisent. Par conséquent, les frais généraux de signature peuvent être sensiblement réduits. Il convient de noter ici que l'un des paramètres importants est la taille réduite du CRL des signatures de groupe, car elle croît linéairement avec le nombre de véhicules révoqués. Néanmoins, l'inconvénient réside dans le fait que le coût de calcul est trop élevé, car chaque opération de vérification du CRL effectue deux calculs d'appariement. Comme dans le système de clé de groupe, ce protocole est proposé pour impliquer l'obtention de la non-traçabilité entre les signatures des messages et leurs signataires. Tous les véhicules signent avec leur clé secrète et la clé publique du groupe se charge de la vérification des signatures. L'anonymat est ainsi garanti aux véhicules, puisque l'on vérifie tout le temps si le véhicule fait partie du groupe et s'il ne relève aucune information privée. Cependant, la révocation des membres de GSIS n'est pas efficace. Plus le nombre de véhicules révoqués augmente, Plus la taille de la liste de révocation augmente elle aussi, ce qui entraine ainsi l'augmentation des coûts de la vérification des messages de sécurité.

Dans [32], Lu et al ont introduit un protocole de préservation de la vie privée conditionnelle, en anglais : *Efficient Conditional Privacy Preservation Protocol* (ECPP). Dans ce protocole, les véhicules s'authentifient auprès des RSUs du réseau et

ces derniers leur envoient par la suite des certificats anonymes. Après avoir reçu ces messages qui contiennent des paires de clés publiques/privées anonymes, l'utilisateur peut générer anonymement des messages de sécurité et les signer avec sa clé privée.

Ce dispositif proposé est considéré comme le premier protocole ayant pour but de soutenir les véhicules légitimes qui actualisent fréquemment des certificats pseudonymes de courte durée à partir d'un RSU. Étant donné que chaque RSU vérifie si l'identité du véhicule se trouve sur la liste de révocation ou non, les véhicules n'ont pas besoin ainsi de conserver la liste de révocation, ce qui signifie que l'augmentation des coûts causés par l'opération de vérification des messages de sécurité dans la phase de révocation dans le protocole GSIS est supprimée. En outre, comme ECPP est basé sur la technique de génération de clés anonymes à court terme à la volée entre un OBU et un RSU, en anglais (On-the-Fly Short-Time Anonymous Key Generation), il peut donc intervenir pour pouvoir améliorer l'efficacité en termes de stockage de clés anonymes minimisé à chaque OBU, de vérification rapide et d'efficacité de suivi pour préserver la vie privée conditionnelle. Cependant, le protocole a une latence RSU élevée, nécessitant ainsi beaucoup de temps pour rechercher des nœuds révoqués.

Un autre protocole d'authentification appelé SRAP [30] a été développé par Zhang et les autres. Il est robuste et évolutif et contient également des étapes similaires à [32]. Ainsi dans le cadre de ce protocole, seuls les véhicules dans la zone de couverture des RSUs seront reliés si certains RSUs sont brisés. Chaque RSU maintient un groupe généré à la volée dans sa gamme de communication, dans laquelle les véhicules peuvent anonymement générer des messages V2V et vérifier les messages V2V anonymes provenant d'autres véhicules. De plus, les véhicules générant de faux messages peuvent être signalés par un tiers. En raison des groupes contrôlés indépendamment, ce protocole est remarquablement plus évolutif. Cependant, la faille principale réside dans le temps élevé enregistré durant le processus de renouvellement des clés.

Dans [33], JH Kim et JS Song ont proposé une méthode de pré-authentification basée sur le protocole SRAP (The Scalable Robust Authentication protocol) [30]. La méthode proposée a pour but de réduire les retards dans le processus de

renouvellement des clés SRAP. Lorsqu'un véhicule finit de s'authentifier auprès d'un RSU, il n'aura pas besoin d'envoyer une autre demande pour obtenir une nouvelle clé secrète. Il faut noter également que cette méthode utilise un algorithme de chiffrement de clé symétrique, ce qui fait que le calcul des frais généraux est beaucoup moins élevé que dans le protocole SRAP. Reste à régler toutefois le problème de la mobilité et la densité dans le réseau pour optimiser la taille des paquets diffusée et l'intervalle de temps entre l'expédition et la réception. Cela va réduire beaucoup mieux les frais de communications et rendre le protocole plus efficace.

Dans [34], les auteurs proposent un protocole de sécurité basé sur le changement périodique des pseudonymes. Ils proposent deux approches. Dans la première, chaque véhicule lance le processus de changement de pseudonyme auprès de l'autorité de certification, après un temps donné. Dans la seconde approche, chaque véhicule lance le processus de changement de pseudonyme et le génère par lui-même, après un temps donné. Le protocole proposé est ainsi basé sur la répartition équidistante entre les unités routières et l'utilisation de la vitesse moyenne autorisée sur la route, et ce, pour évaluer la durée de vie des pseudonymes de communication. Les auteurs ont évalué la bande passante utilisée en fixant la vitesse des véhicules à la moyenne dans chaque approche. L'étude révèle que la deuxième approche (génération des pseudonymes par véhicule) présente plus de résultats positifs en termes de pourcentage de véhicules ayant changé de pseudonymes de communication par rapport à la première approche. Les vitesses utilisées, dans le cadre de ce protocole, sont des vitesses moyennes théoriques dédiées à l'expérimentation.

Dans un travail distinct, Wasef et Shen [35] ont construit un protocole de distribution de certificats pour les VANETs nommé MAAC (Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks). Ils ont introduit une architecture à quatre niveaux, composée de Master CA (MA), CA, RSU et OBU. La différence principale entre l'architecture VANET classique et le protocole présenté est que ce dernier introduit une nouvelle entité (MA) dans son architecture réseau représentant le niveau le plus élevé dans la hiérarchie du système. Les auteurs adoptent l'infrastructure à clé publique (PKI) et la liste de révocation de certificats (CRL) pour sécuriser d'une manière fiable l'ensemble du réseau. Dans tout le système PKI, il performe les

opérations de génération et de diffusion des clés PKI entre les différents niveaux du réseau. De plus, la phase d'authentification d'un message reçu est effectuée en vérifiant que le certificat de l'expéditeur n'est pas inclus dans la liste CRL en cours et en contrôlant en même temps l'authenticité du certificat et la signature de l'expéditeur. Dans cette étude, le processus de vérification de révocation utilise un code d'authentification de message de hachage avec les clés HMAC (a keyed-hash message authentication code), où la clé utilisée pour calculer le HMAC n'est partagée que par des nœuds non révoqués. Le protocole MAAC utilise une nouvelle technique probabiliste de distribution de clés, ce qui permet aux nœuds non révoqués de mettre à jour d'une manière sécurisée leur clé secrète. Toutefois, il utilise deux CRLs pour les RSU et les OBU respectivement et le GPS (Global Positioning System) pour localiser les véhicules. Il en résulte ainsi une inondation du réseau avec des informations inutiles.

Dans un autre travail, Wasef et al. [36] ont mené une étude afin de comprendre la relation entre la densité des RSUs dans la ville de New York et le nombre de certificats qu'un véhicule doit mettre à jour. Leurs résultats concluent qu'il est inefficace et difficile pour un RSU de transmettre des centaines de certificats aux véhicules, tout en leur fournissant des services de divertissement en même temps, en raison de la bande passante du canal sans fil limitée. En outre, l'expéditeur du certificat devrait avoir une capacité de calcul énorme et assez forte pour qu'il puisse générer des centaines de milliers de certificats à tous les demandeurs dans un petit intervalle de temps. Ce qui n'est pas sans épuiser l'ensemble du service et réduire des performances de l'expéditeur des certificats.

Dans [37], Salem et les autres proposent un protocole léger et dynamique de distribution des clés PKI, lequel élimine la nécessité de stocker un grand nombre de clés dans le TPD. Ils utilisent l'infrastructure à clés publiques (PKI) pour la distribution des clés générées. Dans leur protocole, ils introduisent une nouvelle entité dans la hiérarchie VANET, soit un gestionnaire RSU, qui permet de stocker les emplacements des RSUs, transmettre les messages entre le CA et les RSUs et surveiller les RSUs qui transmettent des demandes de clés pour chaque véhicule jusqu'à ce que la clé expire. Le dispositif proposé est censé avoir toutes les informations des RSUs sous son

autorité. Un CA basé sur le nuage a été déployé, ce qui rend les gestionnaires RSU libres de communiquer avec ce nuage sans avoir une limitation d'un serveur ou d'une région non autorisée. Le protocole réduit considérablement le rôle du TPD, en déployant une méthode dynamique de distribution de clés. En outre, dans la phase de révocation, si la clé d'un véhicule est demandée pour la révocation, un message sera envoyé uniquement aux véhicules ayant une probabilité de communication avec le véhicule concerné. Dans les précédentes recherches, les messages de révocation auraient pu être envoyés à des véhicules qui n'auraient jamais une probabilité de communiquer avec le véhicule révoqué ce qui ne fait que consommé les ressources réseau. Le protocole proposé réduit considérablement les coûts de révocation et améliore l'utilisation du réseau par rapport aux travaux connexes. En outre, la solution actuelle pourrait être améliorée en éliminant la chaîne des gestionnaires RSU et en déployant un gestionnaire RSU basé sur le nuage, ce qui rendra les RSUs libres de communiquer avec ce nuage sans avoir une limitation d'un serveur. Il y a lieu d'étudier ensuite l'impact de cette solution et ses retombées sur la phase de révocation, notamment la façon dont elle va agir sur le nombre de messages de révocation.

Nous choisissons de résumer notre état de l'art sous une forme d'un tableau récapitulatif (Tableau 3.1) qui résume les caractéristiques techniques, les avantages et les inconvénients de chaque approche.

Tableau 3 1. Matrice de revue de la littérature

Approche	Caractéristiques	Catégorie	Référence
TPD based approach	Utilise TPD comme un dispositif de stockage des clés distribuées. TPD est cher et non fiable. Aucune méthode de révocation n'a été proposée.	Système d'authentification basé sur l'identité	[18] [19]
Distributed Certificate and application architecture for VANETs	Utilise des périphériques embarqués chargés avec des cartes prépayées contenant des certificats. Pas besoin de TPD. Certificats temporaires sont utilisés dans une zone géographique spécifique pendant une période de temps particulier. Procédure de révocation de certificat simplifiée.	Système d'authentification basé sur l'identité	[20]
On achieving Secure Message Authentication for Vehicular Communications	Méthode d'auto authentification avec un générateur de clé publiques/privé. Processus d'authentification mutuelle est déclenché lorsque le véhicule entre dans la zone de communication de RSU. TPD est utilisé pour le stockage des certificats PKI. Confidentialité est assurée à l'aide d'un message chiffré et d'un code d'authentification de message (MAC). MAC utilise la clé symétrique, validée par RSU. Aucune coopération ou communication avec les autres RSUs. Chaque zone de couverture d'un RSU est considérée comme un réseau distinct, et le processus d'authentification se répète chaque fois un véhicule entre dans cette zone.	Système d'authentification basé sur l'identité	[21]

Tableau Matrice de revue de la littérature .1 3 *(suite)*

Approche	Caractéristiques	Catégorie	Référence
The security of Vehicular Ad hoc Networks	Répartition de milliers de certificats associés. Utilise des certificats anonymes associés pour vérifier la signature des messages échangés. Utilise TPD comme outil de stockage de clés et de certificats. CA distribue des certificats et continue de mapper les identités réelles de ces certificats. Les listes de révocation de certificats augmentent rapidement, ce qui implique une inondation du réseau. Aucune méthode de révocation n'a été proposée.	Système d'authentification basé sur l'identité	[22]
An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preserving for Vehicular Communication (PASS)	Prise en charge des services de certificats distribués assistés par les voies routières. Génération de pseudo-identités de certificats pseudonymes appartenant au même propriétaire par le biais de la technologie de fonction de hachage unidirectionnelle. Révocation des certificats non valides en libérant seulement deux graines de hachage contrairement, les systèmes traditionnels. La taille du CRL est linéaire avec le nombre de véhicules révoqués et liés au nombre de certificats pseudonymes. La technique de signature de proxy est utilisée comme solution pour améliorer la mise à jour des certificats. PASS proposé comme une solution aux problèmes rencontrés en [22]	Système d'authentification basé sur l'identité	[25]

Tableau Matrice de revue de la littérature .1 3 *(suite)*

Approche	Caractéristiques	Catégorie	Référence
An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks	*Identity-based Batch Verification scheme* (IBV) est utilisé pour générer des certificats de pseudo-identité aléatoires et des clés privées associées. Vérification de plusieurs signatures de message à la fois. La confidentialité conditionnelle est obtenue par IBV en permettant à l'autorité de confiance (*Trusted Authority*) de récupérer l'identité réelle d'un véhicule à partir de la signature numérique des messages. Moins efficace en le comparant avec la cryptographie symétrique.	Système d'authentification basé sur l'identité	[26]
Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communication (LPP)	Utilise la méthode *Curve-based Chameleon Hash Method* L'algorithme de signature de Chameleon n'est pas interactif. La signature du message peut être générée sans interagir avec le récepteur prévu. L'authentification mutuelle et anonyme est obtenue pour les deux modes V2V et V2R. Assure la non-mobilité du véhicule, la capacité de suivi de l'autorité et une efficacité de calcul.	Système d'authentification basé sur l'identité	[27]
A Distributed Key Management Framework with Cooperative Message Authentication in VANET	Communication de groupe utilisée entre les véhicules. Soulève des problèmes techniques sérieux et importants concernant le meneur du groupe et les véhicules qui rejoignent et sortent du groupe.	Système d'authentification basé sur la signature du groupe	[28]

Tableau Matrice de revue de la littérature .1 3 *(suite)*

Approche	Caractéristiques	Catégorie	Référenc
The case for dynamic key distribution for PKI-based VANETs	Pas besoin d'un grand nombre de clés. Utilise PKI-standard pour la distribution de clés. Présente *RSU-manager* comme nouvelle entité dans l'architecture, entre le CA et les RSUs. RSU-managers sauvegarde les emplacements des RSUs, transmet les messages au CA et conserve la trace des RSU actuelles qui demandent des clés. L'autorité de certification basée sur Cloud a été déployée. Message de révocation envoyé uniquement aux véhicules qui ont une probabilité de communication avec le véhicule révoqué. La solution pourrait être améliorée en déployant un RUS-manager basé sur le Cloud remplaçant la chaîne des gestionnaires RSU.	Système d'authentification basé sur l'identité	[37]
A Secure and Privacy-Preserving Protocol for Vehicular Communications (GSIS)	Le message est vérifié par la clé publique et signé par la clé privée du membre principal du groupe. Les frais généraux de la signature sont considérablement réduits en utilisant GSIS. Les CRL augmentent linéairement avec le nombre de véhicules. Plus le nombre de véhicules révoqués augmente, plus la taille de la liste de révocation augmente. La révocation des membres GSIS n'est pas efficace en raison du coût de calcul élevé. Aucune méthode de révocation n'a été proposée.	Système d'authentification basé sur la signature du groupe	[29]

Tableau Matrice de revue de la littérature .1 3 *(suite)*

Approche	Caractéristiques	Catégorie	Référence
Efficient Conditional Privacy Preserving Protocol for Secure Vehicular Communications (ECPP)	Basé sur la génération de clés anonymes à court terme à la volée entre un OBU et un RSU (*on-the-fly short-time anonymous key generation*). Capable d'améliorer l'efficacité en termes de stockage de clés anonymes minimisé à chaque OBU. Effectue une vérification rapide sur les messages de sécurité Fournit un mécanisme efficace de suivi de la vie privée conditionnelle. Chaque RSU vérifie par lui-même si l'ID du véhicule est sur la liste de révocation ou non. Les véhicules ne doivent pas conserver la liste de révocation Considéré comme le premier protocole qui a soutenu la technique d'actualisation fréquente des certificats pseudonymes de courte durée des véhicules auprès des RSUs. Supprime le problème de surcharge de GSIS. Caractériser par une latence élevée au niveau des RSUs et ça nécessite beaucoup de temps pour rechercher des nœuds révoqués.	Système d'authentification basé sur l'identité	[32]
A Scalable Robust Authentication Protocol (SRAP)	Contient les mêmes étapes et les caractéristiques proposées dans 25. Les véhicules peuvent anonymement générer des messages V2V, vérifier le message V2V anonyme des véhicules, et les véhicules générant des faux messages peuvent être tracés. Plus évolutif grâce aux groupes contrôlés indépendamment. Trop long pendant le processus de renouvellement des clés.	Système d'authentification basé sur la signature du groupe	[30]

Tableau Matrice de revue de la littérature .1 3 *(suite)*

Approche	**Caractéristiques**	**Catégorie**	**Référence**
A Pre-Authentication Method for Secure Communications in Vehicular Ad hoc Networks	Proposée comme une solution aux problèmes rencontrés dans 26. Les retards ont été réduits dans le processus de renouvellement des clés SRAP. Pas besoin d'envoyer des nouveaux messages pour obtenir une nouvelle clé secrète après l'authentification du véhicule. Réduit considérablement les frais généraux de calcul par rapport au SRAP. Prévoie d'optimiser la taille et l'intervalle de diffusion des paquets pour rendre le protocole plus efficace.	Système d'authentification basé sur l'identité	[33]
MAAC: Message Authentication Acceleration Protocol for Vehicular Ad hoc Networks	Architecture à quatre niveaux utilisés, qui contient Master-CA, CA, RSU et OBU. Transmets-les CRL entre tous les niveaux. Utilisé deux CRL pour RSU et OBU respectivement. Supporte des informations inutiles, qui ont inondé le réseau	Système d'authentification basé sur l'identité	[35]
An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks	Examine la relation entre la densité RSU à New York et le nombre de certificats mis à jour. Tâche difficile pour les RSUs de transmettre des certificats aux véhicules autour de lui en leur fournissant en même temps un service de diffusion d'infodivertissant. Nécessite une forte puissance de calcul pour générer tous les besoins dans un délai très court.	Système d'authentification basé sur l'identité	**[36]**

3.3 Conclusion

Dans ce troisième chapitre, nous avons présenté les différentes œuvres et approches proposées qui sont intrinsèquement liées au problème d'authentification dans les réseaux VANET. Il est évident que la plupart des études et travaux réalisés jusque-là n'ont pas réussi à offrir un protocole fiable et fonctionnel dans toutes les situations. Aucune approche n'a pu, en effet, atteindre un niveau de sécurité élevé avec des résultats garantis. Une distribution des certificats légers dans un environnement très contraignant avec des changements périodiques aléatoires satisfaisant les exigences requises pour une autorité de certification et de confiance, une révocation efficace des CRLs, une gestion efficace des groupes de véhicules tout en minimisant les coûts de calcul et l'utilisation du stockage sont autant de défis auxquels nous sommes confrontés.

Dans le présent travail, la nouveauté consiste à concevoir un nouveau mécanisme de distribution efficace et dynamique des certificats dans un nuage véhiculaire en déployant le schéma ECQV (Elliptic Curve Qu-Vanstone) pour un mode de communication sûr et fiable entre toutes les entités du réseau et en toutes circonstances. L'approche et les mécanismes de sécurité déployés avec des résultats de simulations sont présentés sous forme d'article scientifique dans le chapitre suivant. Nous avons soumis notre proposition d'article au SECURITY and PRIVACY journal, John Wiley & Sons 2017.

CHAPITRE 4 EFFICIENT AND DYNAMIC ECQV IMPLICIT CERTIFICATES DISTRIBUTION SCHEME FOR VEHICULAR CLOUD NETWORKS

Soumis au journal SECURITY and PRIVACY, John Wiley & Sons 2017
Numéro papier: SPY-2017-0013

ORIGINAL ARTICLE
Security and Privacy - Wiley Online Library

Efficient and Dynamic ECQV Implicit Certificates Distribution Scheme for Vehicular Cloud Networks

Ahcene Teniou[1*] | Boucif Amar Bensaber[2*]

[1] LAboratoire de Mathématiques et Informatique Appliquées (LAMIA), Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières, 3351 Bd des Forges, C.P 500, G9A 5H7, Trois-Rivières, QC, Canada
Ahcene.Teniou@uqtr.ca

[2] LAboratoire de Mathématiques et Informatique Appliquées (LAMIA), Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières, 3351 Bd des Forges, C.P 500, G9A 5H7, Trois-Rivières, QC, Canada
Boucif.Amar.Bensaber@uqtr.ca

Correspondence
Boucif Amar Bensaber
Local 3079, Pavillon Ringuet, Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières, 3351 Bd des Forges, C.P 500, G9A 5H7, Trois-Rivières, QC, Canada
Tel: +1 819 376 5011 poste 3807
Email: Boucif.Amar.Bensaber@uqtr.ca

Present address
[1] LAboratoire de Mathématiques et Informatique Appliquées (LAMIA), Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières, 3351 Bd des Forges, C.P 500, G9A 5H7, Trois-Rivières, QC, Canada

Funding information
Natural Sciences and Engineering Research Council of Canada (NSERC), Grant/Award Number: RGPIN 23972-2013.

ABSTARCT: In this paper, we introduce an efficient and dynamic ECQV implicit certificates distribution scheme for vehicular cloud networks. We are concerned about how to achieve efficiently and dynamically certificates distribution with a reduced cost. We design an efficient mechanism that reduces the communication cost and the computational overhead for more safety and robustness of intelligent transportation systems. Our proposal enables vehicles to request and obtain implicit certificates upon a secure request, which can be used for further signing exchanged messages. Due to the restricted nature of these certificates, a simple and efficient revocation method has been presented. It's literally based on selective revocation message delivery technique that reduces the number of messages needed for revocation phase and solves a bunch of drawbacks of existing solutions. An extensive analysis is performed to demonstrate how the proposed scheme can dynamically carry out an effective certificates distribution. We further discuss and evaluate simulation results to demonstrate the merits gained by the proposed protocol.

KEYWORDS
Vehicular Cloud Networks (VCN), *ECQV implicit certificates*, security, privacy, authentication, revocation.

Abbreviations: ECQV: Elliptic Curve Qu-Vanstone

* Equally contributing authors.

1 | INTRODUCTION

Vehicular Cloud Networks (VCN) that became highly popular in recent years, continue to grow and enlarge geographically since they promise scalability as a property, and due to their specific features and applications such as standardization, efficient traffic management, road safety and infotainment. Several technologies have been deployed to maintain and promote Intelligent Transportation Systems (ITS). ITS aim to provide innovative applications and services related to traffic management and access to information for different users of the system. The intention to use embedded resources in intelligent transportation systems, as well as the modern-day technology of management of computing resources in the conventional cloud, allowed cultivating the concept of Vehicular Cloud (VC). Developed from Vehicular Ad Hoc Networks (VANETs), it can be trained autonomously and offers a wide range of applications and services that can benefit the entire transportation systems as well as drivers, passengers and pedestrians. It also provides an important key to achieving many of today's transportation objectives: mobility, safety, efficient transportation and providing a financial base for new highway infrastructure, while reducing threats to travel safety and security as well as the negative effects to the environments which in turn can benefit air quality and reduction of greenhouse gases. However, due the high mobility of traffic, the vehicular cloud is built on both static and dynamic physical resources. As a result, it encounters several inherent challenges, which increases the complexity of its implementation.

Besides that, traditional Vehicle Ad Hoc Network (VANET) consists of network entities, including On-Board Units (OBU), Road Side Units (RSU) and a Certificate Authority (CA). These entities communicate with each other in two different modes: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). According to the IEEE 1609 standard, the communication technology used is Dedicated Short Range Communication (DSRC) [1]. In the context of road safety applications, either a car manufacturer or government authority plays the role of the CA and it is responsible for key generation and distribution. The RSUs are responsible for linking and delivering messages between vehicles and the CA. RSUs are installed in standalone towers and organized according to the network topology. Vehicles are equipped with wireless communication devices (OBUs), which are required to broadcast traffic messages, to receive and to validate them [2]. These messages contain a range of sensitive information, such as vehicle's position, direction, time, speed and traffic events. Thus, this information allows drivers to better know the traffic conditions. However, attackers can report false information such as signaling traffic congestion to gain unfair advantage or they can even cause accidents, making the security of this vital information a critical problem in VANET.

Another important issue in VANET is the privacy of a vehicle; an attacker can listen to the communication established between different moving nodes. So, the data exchanged can be intercepted, traced and altered, in order to track down and to follow the targeted nodes and in the worst cases launch a variety of attacks. Therefore, their privacy could be in trouble, so any sensitive information that belongs to them, such as their identity, electronic license plate, current position must be kept private all the time. As a result, the authenticity of the information would be very important since malicious information may result in loss of life and property. Besides non-repudiation, confidentiality, privacy and authentication are the desired security attributes. The best possible solution is to use digital certificates tied to a user by a trusted third party. These certificates can then be used to sign the information. Most of the existing solutions use some kind of certificates, with a central certificate issuing (Trusted Authority). To protect the privacy, the architecture can be extended to use many temporary certificates (pseudonyms) instead of one permanent certificate. The pseudonyms can be stored in a bulk (Temper Proof Device TPD) [3]. Numerous mechanisms for pseudonyms change have been proposed in the recent years. They can be divided into two main categories: The first category is group signature-based schemes [4] and the second category is pseudonym-based schemes [5,6]. These authentication schemes mostly implement key public infrastructure (PKI) by employing digital signatures to authenticate messages but this approach may lead to significant delay [7]. These schemes address most security and privacy issues in VANET but each has its own limitations,

which makes the protection of vehicle's privacy and identity by anonymous authentication, a fundamental issue [8], however its deployment is slightly difficult, due to the high mobility of the network. The challenge is to authenticate a legitimate user without compromising privacy and in case a malicious activity is detected, the system should be able to track a user down [9]. In most pseudonym authentication-based schemes, a centralized certification authority (CA) based solutions issues a bunch of signed certificates as anonymous pseudonyms, to assign a new vehicle in the network. However, this approach present several challenges, which may be difficult to address during the initial deployment stages of VANET. According to standard IEEE 1609.2, the interval between two messages sent by a vehicle is 100-300 Ms for a communication range of 300 m. The OBU of a vehicle is equipped with a 400 MHz processor which requires approximately 20ms to verify a signature [11]. If the density of vehicles is small, then that will not present any problem in the certificate verification phase, but if the density of vehicles increases, this can lead to significant delays though, due to the time taken by the certification verification phase and therefore, cause significant overhead in the network. Thus, the main concern is how to deal with the limitations of memory and bandwidth to get the best performances from these approaches.

In the case of revocation, the two main issues we are facing are the limited bandwidth of wireless channel and the size of the certificate revocation list. Therefore, the more CRL (Certificate Revocation List) size increases, the more transmission delay gets longer and that might cause significant overhead on the OBUs. First, the major problem of the group signature-based schemes in the revocation phase is that the group managers have complete knowledge of the group members, which allow them to track down the members, so the selection of group managers is also a critical issue. Moreover, if the groups are dynamic then group managers can leave the group at any time and newly selected group manager have all the information about the leaved members. The other disadvantage of this approach is the required time to perform pairing calculations between the signature and the identity of the vehicle. This may cause the calculation overhead if the number of vehicle increases. Second, the major problem of the Pseudonym-based authentication schemes in the revocation phase is the overhead on RSUs. With the limited resources in the proposed architectures so far, it is not possible for an RSU to carry out multi tasks at the same time, such as sending thousands of pseudonym certificates to the vehicles while providing them other entertainment services and revocation of the expired certificates. In addition to this, there is an evidence in VANET that vehicles store in their tamperproof device several encryption keys that are renewed during the visit of a certification authority (CA).

In this paper, to address both the security and performance challenges in Vehicular Cloud, we propose an efficient and dynamic distribution of certificates in VANET-Cloud environment using Elliptic Curve Qu-Vanstone (ECQV) implicit certificates, which are smaller than other comparable certificates and highly recommended in very constrained environments, where not a lot of memory and bandwidth is available. A vehicle dynamically requests a certificate from its nearest RSU. A query is propagated via the proposed network infrastructure to reach a Cloud based-CA and then a certificate is returned safely. Our contribution of this work are as follows:

- The security aspect of this scheme has been enhanced by adding a cloud-based entity (Cloud based-RSU-Manager) that is located between the Cloud-based CA and RSUs, eliminating at the same time the chain of RSU-Manager [12]. This means a reduction in the number of transmitted packets in the certificates request stage. In addition, the calculation time will also be reduced.

- We conduct in this study an extensive analysis using this reliable authentication scheme with a strong message integrity and privacy for all participants; it is very difficult for an attacker to get the real identity of a vehicle in the network. A key revocation mechanism to reduce the number of messages required in the revocation phase is proposed in Section 3.

- An extensive analysis of the proposed protocol under various attack scenarios is presented. Various works have been proposed to secure communication between vehicles, but most of them present various inherent disadvantages,

such as the cost of communication, the cost of storage and the cost of calculation. So, these disadvantages motivated us to work on securing communication between vehicles with the least storage cost and the least possible cost of calculation.

In this regard, our system performs an authentication process efficiently and at a reduced cost. The evaluation of the safety performance of the proposed scheme is examined by network simulations. In the end, a critical and in-depth analysis will be carried out to deduce how the proposed scheme can master an efficient and dynamic distribution of certificates.

The remainder of the paper is organized as follows: Section II presents the state of the art. Section III discusses the system model including the network model, the proposed protocol and the method for managing certificates revocation. Section IV provides an analysis of the characteristics of the proposed protocol under various attack scenarios mentioned in the literature. In section V, performance of our protocol is measured through network simulations and compared to a protocol in the literature, while Section VI concludes the work done in this paper.

2 | STATE OF THE ART

Effective management of keys distribution is a cornerstone in the design of security algorithms. Considerable efforts have been done in this field over the past years. Several protocols and certificate management systems have been proposed that consider security and privacy in VANET environment. These systems or schemes can be divided into two main categories: pseudonymous authentication based schemes and group signature based schemes.

As a part of previous research efforts, Hubaux and al. [13,14] used the TPD as a storage medium for the CA public key. In this approach, one node sends to another the hash of the global key. If it is identical to the hash generated from the key stored in the TPD, communication is established between these two nodes. This approach is based on TPD, which is an expensive and unreliable device.

In [15], Aslem and Zou attempted to ignore the TPD as an unrealistic device and they used an embedded device loaded with prepaid cards containing the keys. The cards contain identification and a certificate. During initialization, user's information will be retained with the provider and not stored in the device. When a user enters in a service area, he makes the service payment using an on-board payment device. The message is encrypted by the provider's public key, hiding the device certificate and the services requested from the listening. The user receives a valid nickname for a given period or zone. This is almost the behavior using the TPD.

In [16], Zhang assumed that a vehicle registers itself with a public/private key generator. When it enters to the communication area of an RSU, it triggers a process of mutual authentication with this latter. The Diffie-Hellman algorithm is used to exchange a symmetric key. The RSU and other vehicles in the range receive an encrypted message and a Message Authentication Code (MAC). The MAC generated is based on the symmetric key message shared with the RSU. Only the RSU can validate the MAC, because it is the only another owner of the symmetric key. If the RSU validates the MAC, it sends a valid message to vehicles. To avoid RSU failure, V2V communication will be performed by replacing V2I communication. PKI is used for keys generation and the TPD is also deployed for key storage. This approach ensures confidentiality, but without communication with the certification authority to ensure that, the vehicle is legitimate. In addition, it treats each RSU as a separate network with no cooperation or communication with other RSUs in the network. This will allow the vehicle to repeat this authentication process each time it enters in the communication range of an RSU.

As we mentioned before, the first category of certificate management systems is pseudonyms-based schemes. They use certificates based on an anonymous Public Key Infrastructure (PKI) to verify messages signed by associated

anonymous private keys. These anonymous certificates are generated to preserve the real identity of a vehicle and used to establish communications with other nodes in the network.

In a previous work, Raya and Hubaux [6] proposed a system that relies on the distribution of thousands of associated private key certificates. They use the tamper proof device as a storage tool of keys and certificates, to preserve privacy of vehicles and enhance security. Each vehicle is supposed to store a large set of pseudonymous certificates, with pseudo identities and randomly selects the private key from a large pool of available pseudonymous certificates, for signing a message. Each vehicle may verify the received message's signature with the help of an associated anonymous certificate. Moreover, certificate authority distributes certificates and keeps the mapping of the actual identities to these certificates. The system presented by the authors seems interesting, they believe it fulfils conditional privacy by taking advantage of associated private keys and addresses the safety issues. However, it has several shortcomings. First, due to the high mobility of network and the presence of thousands of certificates per vehicle, when a vehicle's certificate is revoked, certificate revocation lists grow quickly and that means it takes a remarkable storage space to store all CRLs in the network and consequently takes long time to check all the CRLs before triggering the real CRL process. The obvious result is storage capacity drain. On the other hand, CA needs to revoke all the certificates held by a vehicle after a given time. That not only increases overhead within the network but also consumes more bandwidth, so all these flops can lead to network's flooding. Above all that, they did not prove their scheme with simulations.

In [18], a solution was proposed to resolve problems found in [6], it investigates how to distribute the CRL efficiently by vehicle-to-vehicle communication. However, due to the limited bandwidth of wireless communication and the high-speed mobility of vehicles, it is difficult to distribute a large CRL to all vehicles in a timely fashion.

To decrease the CRL size, Bellur [17] suggests to segment a country into a number of geographic regions and assign each region-specific certificates with validity period to a vehicle.

In another effort, Sun and al. [18] proposed a scheme that significantly reduces the revocation cost, and the certificate updating overhead, named PASS (Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation). It uses pseudonymous certificates belonging to the same owner based on one-way hash-chain technology, to reduce the size of CRL. The CRL size in PASS is linear with the number of revoked vehicles, and irrelated to the number of pseudonymous certificates held by the revoked vehicles. They also use the proxy signing technique as a solution, to improve the certificate's update.

In [19]. Zhang and al used an Identity-based Batch Verification (IBV) scheme. They used the TPD to generate random pseudo-identity certificates and associated private keys. This scheme is less efficient when comparing with symmetric cryptography and it is also subject to DoS (Denial-of-Service) attacks.

In [20], the authors propose a privacy-preserving authentication protocol with authority traceability using elliptic curve-based chameleon hashing, Called LPP. Chameleon signature algorithms are non-interactive, that means the signature can be generated without interacting with the intended receiver. However, it requires the same public key. This improved version avoids using the fixed public keys. Compared to existing schemes, LPP protocol can achieve mutual authentication for both V2V and V2I traffics, with much lower computational cost. Consequently, the authors think that their protocol ensures both mutual and anonymous authentication, authority tracking capability and high computational efficiency. Although, their protocol is highly suitable in a realistic vehicular environment, the use of the elliptic curve-based chameleon hashing looks effective. However, they did not propose any revocation method for present certifications, to change them regularly and to ensure anonymity and prevent illegal tracking.

In [21], authors propose a security protocol based on periodic change of pseudonyms. They propose two approaches. In the first one, each vehicle initiates the pseudonym change process nearby the certification authority, after a specified time. However, in the second approach, each vehicle initiates the pseudonym change process, by itself and generates it after a time t. Based on equidistant distribution of RSUs and the use of the average permitted speed on the roads,

the proposed protocol evaluates the lifetime of communication's pseudonyms. They evaluated the bandwidth used by setting the vehicle speed to the mean in each approach. Their results revealed that the second approach gives better results in terms of pseudonyms change rate and bandwidth consumption, compared to the first one. It Ensures anonymity and prevent illegal tracking by changing pseudonyms of at least two vehicles simultaneously. Nevertheless, speeds used in this study are theoretical average speeds, whereas, in reality vehicles move on roads at variable speeds and even unauthorized speeds.

In [12] Ahmed H.Salem and al proposed a lightweight dynamic key protocol, that eliminates the need to store a large amount of keys. They used the PKI standard for key distribution, and introduced an RSU manager into the standard VANET hierarchy. The RSU manager stores RSU locations, transmits CA messages to a specific RSU, keeps track of current RSUs that requested keys for each vehicle until the key expires. It is assumed to have all RSUs' informations under its authority. A Cloud based CA has been deployed, this makes RSU managers free to communicate with such cloud without having a limitation on an unauthorized server or region. The protocol remarkably reduces the role of TPD from being the main carrier and protector of the keys into carrying a key until the end of its lifetime. If a vehicle's key is requested for revocation, the revocation message will be sent only to vehicles that have a probability of communication with the revoked vehicle. In previous efforts, revocation message could have been sent either to vehicles in all the network, or to vehicles that would never have a probability to communicate with the revoked vehicle. This can overwhelm the network resources.

On the other hand, the main concept of group signature based schemes is to form a group consisting of vehicles, then hide the members of the group to protect their real identity for the preservation of privacy.

In [22], Hao and al. introduced distributed key management by reducing overhead calculation costs. Authors used group communication between vehicles. The vehicle is expected to periodically return its location to the RSU. Although, this technique looks effective but it can lead to serious issues, concerning the group leader and vehicles joining and leaving the group.

Lin and al. have proposed a system called GSIS [7]. In this system, authors proposed a scheme based on group signature, preserving confidentiality and authentication. The main character of the group signature scheme is that the message is signed by the main member's private key of the group and verified by the group's public key [23]. However, signature's overhead can be significantly reduced using this method. One of the most important things we should ensure, is the small size of group signatures' CRL, because it grows linearly with the number of vehicles revoked. The main disadvantage of this scheme is the high calculation cost, because each CRL check operation performs two matching calculations. Such as the group key system, it may involve obtaining the untraceability between the signatures of the messages and their signatories. All vehicles signed with their secret key and their signs are checked with the public key of the group. Since the verification only checks if the vehicle is part of the group, and does not find any private information, anonymity is guaranteed to the vehicle. However, revocation of GSIS members is not effective. As the number of vehicles revoked increases, the size of the revocation list also increases. This may increase the overhead on security messages verification phase.

In [24], Lu and al. introduces a Conditional Privacy Preservation Protocol (ECPP). In this protocol, an RSU authenticates vehicles and issues anonymous certificates. After receiving an anonymous certificate that contains private anonymous public key pairs, the user establishes security messages signed with their private key. It was considered as the first protocol to support legitimate vehicles updating short-time pseudonymous certificates from the RSUs frequently. Since each RSU verifies whether the vehicle"s identity is on the revocation list or not, vehicles do not have to maintain the revocation list and this means that the GSIS overhead check is deleted. This protocol is based on the on-the-fly short-time anonymous key generation between an OBU and RSU. It has been identified to be able to improve efficiency, in terms of the minimized anonymous key storage at each OBU, fast verification and efficient conditional

privacy tracking mechanism. However, it has high RSU latency, and it takes longer time to search for revoked nodes.

A scalable Robust Authentication Protocol (SRAP) [25] developed by Wu and other also contains similar steps as [24]. However, it is more robust and more scalable. In other words, only vehicles in the coverage area of RSUs will be linked up, if some RSUs are broken. Thus, each RSU maintains an on-the-fly-generated group within its communication range, in which vehicles can anonymously generate V2V messages, and verify anonymous V2V messages from other vehicles. Moreover, a third party can trace vehicles generating false/bogus messages. Due to the independently controlled groups, this protocol is remarkably more scalable. However, the main lack in this protocol is the high time taken during the keys renewal process.

In [9], JH kim and JS Song proposed a pre-authentication method based on the Scalable Robust Authentication Protocol (SRAP). The purpose of their proposed method is to reduce delays in the renewal process of SRAP's keys. So, after a vehicle has been authenticated by the RSU, it does not need to send packets to obtain a new secret key. In addition, since this method uses a symmetric key encryption algorithm, computational overhead is much less than SRAP's computational overhead. The problem of mobility and density in the network has yet to be solved to optimize the size of the packets and the broadcast interval; this will reduce communications costs much more efficiently and make the protocol more efficient.

In [26], Wasef and Shen introduced a certified distribution protocol for VANETs. They used a four-tier architecture, consisting of CA Master or MA (Master Authority), CA, RSU and OBU. The difference between the classic VANET architecture and the presented protocol is that the last one adds a new entity (MA) to its network architecture, which is the highest level in the hierarchy of the system. Authors use PKI standard and broadcast CRLs between all levels. They use two CRLs for the RSUs and OBUs respectively and the GPS to locate vehicles. The obvious result is flooding the network with unnecessary information.

In another separate work, Wasef and al. [27] conducted a study to get understand the relationship between the RSU density in New York city, and the number of the certificates that a vehicle has to update once. Their results conclude that it is inefficient and difficult for an RSU to transmit hundreds of certificates for each passing by vehicle while providing infotainment dissemination service at the same time, due to the limited wireless channel bandwidth. Furthermore, the certificate issuer should have quite strong computation power to generate hundreds of thousands of certificates to all the requesters in a short time. Subsequently, it will aggravate the service burden and even bring down the certificate issuer.

It is evident that most studies done so far and current approaches have not been able to offer a reliable and functional protocol in all situations. Distribution of lightweight certificates in very constrained environment with random periodic changes, fulfilling necessary requirement for a trusted certification authority, efficient CRL revocation, efficient group management, minimizing the computation overhead and the storage use, are the main issues we are facing, in our way to make a real contribution of previous works.

In this paper, an efficient and dynamic certificates distribution in vehicular cloud using ECQV scheme is presented to provide a safe and reliable communication between all entities in the network and in all circumstances. Besides, we are about to improve the solution presented in [12], by eliminating the chain of RSU managers and deploying a Cloud based-RSU manager, this will make the RSUs free to communicate with such cloud without having a limitation of a server and see how this solution could affect the number of revocation messages.

3 | SYSTEM MODEL

In this section, we discuss the network model. We present assumptions and overall idea, cryptographic tools and the proposed scheme.

3.1 | Network model

The network model of our system is illustrated in figure 1. It consists of two administrative domains that contain four entities, namely Cloud based Certification Authority (Cloud based-CA), Cloud based Roadside Units Manager (Cloud based-RSU-Manager), Road Side Units (RSUs) and vehicles. A description of each of entity is presented below.

A.Cloud based-CA

It is the superior entity that ensures the full control of the entire network in its geographical area. It is the authority responsible for issuing digital certificates to vehicles, and maintaining the revocations list. It is supposed to have enough storage space for different tasks, sufficient computing power, reliable and rarely compromised.

B.Cloud based-RSU-Manager

It is the intermediate entity between Cloud based-CA and RSUs. It is responsible for a group of RSUs, that belongs to the same administrative domain in the network, knowing that each domain represents a suitable geographical area. It also sends messages or queries from Cloud based-CA to an RSU and vice versa, and saves the location of each RSU in the network. It insures the tracking down process of the current RSUs that requested keys for each vehicle until those keys expires.

C.Road Side Units

RSUs are installed along the route, they disseminate the various road conditions information to the set of vehicles passing by. They are considered as a bridge between the certification authority and the vehicles. Also, they have an internal medium storage for the purpose of storing conditions of the vehicles that pass through them as long as their life certificates have not expired.

D.Vehicles

Each vehicle has a unique authentication key (IDV) composed of a chassis number and an electronic license plate. Only the cloud based-CA and the vehicle itself know the IDV. This IDV is issued and installed in a vehicle's OBU by a vehicle registration authority such as Quebec Automobile Insurance Corporation (SAAQ) or Department of Motor Vehicles in many US states and other Canadian provinces. OBUs are installed on vehicles and they are responsible for communication with RSUs or other OBUs. This IDV is considered as a long-term digital certificate that uniquely authenticates a vehicle. Therefore, the main role of vehicles is to broadcast safety messages containing traffic information or local emergencies.

In our proposal, we assume that the route is safe; it means that we mainly process the authentication and integrity of messages. Our main task is to generate the pair keys that is used for encryption and decryption of exchanged messages between the vehicle and other entities in the network. We use Elliptic Curve Qu-Vanstone implicit certificates scheme (ECQV), in which we will generate two keys that are, public and private keys.

3.2 | Assumptions and overall idea

In our protocol, following assumptions have been taken in consideration:

1. Vehicles are supposed to communicate, interact and share information between one another after requesting their

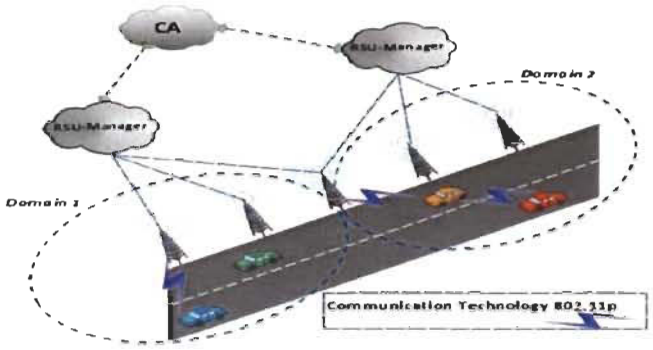

FIGURE 1 Network Model.

own certificates.

2. RSUs have an intern storage space to store the state of the vehicles passing by.
3. Cloud based-RSU-Manager is responsible for a group of RSUs to cover the whole network as shown in Figure 1. Locating RUSs and securing exchanged messages in its area of responsibility.
4. Any kind of sinister among Cloud based-CA, Cloud based-RSU-Manager and RSUs has not been considered.
5. All participants keep their private keys safe.
6. All parties' clocks are synchronized.

3.3 | Cryptographic tools

The main cryptosystem that has been used in our proposed study is the Elliptic Curve Qu-Vanstone implicit certificate scheme (ECQV), for certificates and keys pair generation. It should be noted that only Cloud based-CA needs to use this cryptosystem to generate certificates and keys pair for vehicles in the network, while the rest of entities including Cloud based-CA use ECQV Self-Signed certificate Generation Scheme, to generate their own keys pair. Following are the details about the ECQV cryptosystem that is used in our protocol.

•Elliptic Curve Qu-Vanstone Implicit Certificate Scheme is particularly well suited for very constrained application environments, where resources such as bandwidth, computing power and storage are limited.

•ECQV provided a more efficient alternative to traditional certificates. Each of the various cryptographic ingredients of the ECQV scheme has a range of security levels. The aim is to implement certificates with small sizes in order not to increase the calculation costs. Essentially, each extra bit of certificate doubles the amount of computation and compromise security.

3.4 | Proposed Scheme

This section explains the working of our proposed protocol. First, a user (vehicle) registers nearby the certificate authority (Cloud-based CA) to get a valid Certificate. Certificates get renewed after, at a random time following the actual certificate's lifetime is being expired. After the expiration, a new process must be triggered by the Cloud based-CA,

it is called revocation (Figure 3). It involves a trigger-based system for vehicles in need for a new certificate. It should be noted that for each vehicle in our system, its certificate is renewed at a random time within an interval of time. Thus, we ensure that certificates are renewed periodically and not after a constant time. Applying this technique, malicious nodes cannot predefine the exact time of certificates changes for each vehicle. Following are the steps involved in our protocol and that are also shown in Figure 2.

3.4.1 | *System Initialization*

System is initialized by Cloud based-CA. In this step, Cloud based-CA establishes the elliptic curve domain parameters, a hash function, the certificate encoding format and all parties have selected a random number generator.

1) Cloud based-CA establishes a set of Elliptic Curve (EC) domain parameters for its use with ECQV: *q,a,b,G,n and h* in the finite field *(Fp)* (Table 1).

2) Cloud based-CA selects an approved hash function *H* with desired security level *s*.

3) Cloud based-CA and a vehicle, each choose and initialize an approved random number generator *(G)* that offers *s-bit* security.

4) Cloud based-CA obtains a *EC* pair; public key *Pk (CA)* , private key *Sk(CA)* associated with the *EC* domain parameters established in step 1 for use during certificate generation. The certificate requester (Vehicle) and other participants obtain in an authentic manner, the elliptic curve domain parameters, the hash function, and Cloud based-CA's public key *Pk(CA)*. All participants shall have assurance of:

- The validity of the EC domain parameters.

- The validity of Cloud based-CA's public key *Pk(CA)*.

- The possession of the private key, *Sk(CA)* by CA.

5) All the involved parties download these parameters form Cloud based-CA. Other participants generate their private and public keys using the same implicit certificate scheme (ECQV), which is shown in Table 1.

6) Define ΔT(Certificate's lifetime) and T (Time to change the actual certificate).

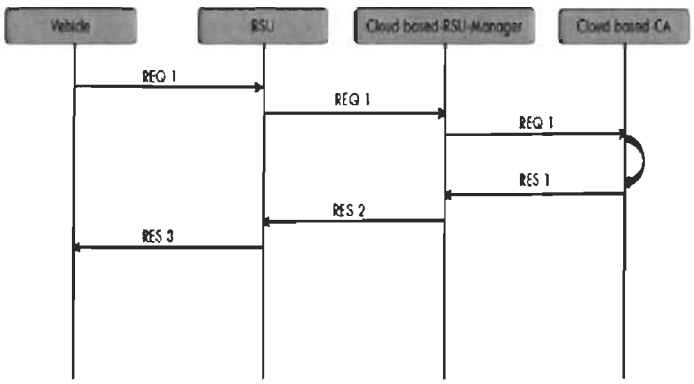

FIGURE 2 Working of proposed protocol.

TABLE 1 NOTATIONS.

Notations	Explanations
V	Vehicle
IDV	Vehicle's ID
IDA	Conductor's ID
Pk(CA)/Sk(CA)	CA's public/private key
Pk(RSU_M)/Sk(RSUM)	RSU_M's public/private key
Pk(RSU)/Sk(RSU)	RSU's public/private key
Pkv/Skv	Vehicle's public/private key
Evac	Shared secret key
ΔT	Certificate's lifetime (min)
T	Time to change certificate (sec)
S	Vehicle's speed (Km/h)
r	Radius of circular area where the vehicle is most probably in (m)
N	Number of RSU's in the whole network
N1,N2,N3,N4	Nonces (arbitrary Numbers)
a,b	Elliptic Curve coefficients
q	Field Size
n	Order of G

3.4.2 | *Requesting a new certificate*

The process of requesting a new certificate is detailed below:

1. *Vehicle to RSU communication*
   During the communication with RSU, vehicle (V) generates through its own identity (IDV) temporary public/private ECQV key pair, (Pk(V), Sk(V)) and sends this information along with IDV (identity of Vehicle (V)), IDA (Conductor identity) and a time-stamp to the nearest RSU in the network. This information is needed to be sent securely via some secure channel as it is already mentioned in our assumptions. The message must be securely sent by the private key of the vehicle, and the public key of the nearest RSU.
   Step1: Vehicle ⇒ RSU:
   Pk(RSU)[Sk(V)[IDA ‖ IDV ‖ (P,a,b,G,n,h) ‖ N1]] ***(REQ 1)***

2. *RSU to Cloud based-RSU_Manager communication*
   Once the RSU receives the message, it verifies its integrity and authenticity, by verifying its digital signature. If the received message is well verified, then, it adds its nonce, and double-encrypts the set mentioned in the previous step (step1), with the ECQV private key of RSU (sk(RSU)) and ECQV public key of Cloud based-RSU_Manager. Then, it sends the request to its superior where it belongs.

Step2: RSU ⇒ Cloud based-RSU_Manager:

Pk(RSU_M)[Sk(RSU)[IDA || IDV || (P,a,b,G,n,h) || N1 || N2]] ***(REQ 2)***

3. *Cloud based-RSU_Manager to Cloud based-CA communication*

Before Cloud based-RSU_Manager establishes a communication with its superior, it verifies the authenticity and integrity of the received message by verifying RSU's signature. If the message is correctly verified, the Cloud based-RSU-Manager add its nonce N3, and encrypts the previous set with ECQV secret key of Cloud based-RSU-Manager (SK(RSU_M)) and ECQV public key of Cloud based-CA (PK(CA)), respectively.

Step3: Cloud based-RSU_Manager ⇒ Cloud based-CA:

Pk(CA)[Sk(RSU_M)[IDA || IDV || (P,a,b,G,n,h) || N1 || N2|| N3] ***(REQ3)***

4. *Generation of pair key*

Before the generation of vehicle's pair key, authentication authority (Cloud based-CA) carries out a couple of verification process. The first one is verifying the integrity and authenticity of the received message. If the message's signature is OK, then it moves on to the second verification. It checks whether the vehicle is on the blacklist or if a recent revocation request has been recently lunched.

Upon getting verification that the message came from a legal vehicle (V), Cloud based-CA shall use the process described below, to generate a certificate and private key contribution data in response to a certificate request from vehicle (V). It is assumed that Cloud based-CA has received the request in an authenticate manner, and has decided to issue a certificate.

Step 4: Qv= e*Pv

Where Pv is the private key, Qv is the public key and e= H'n (Certv): it's an integer modulo n.

NB: H is the hash function used in ECQV Scheme.

5. *Sending off the generated pair key*

After generating the pair of keys, the Cloud based-CA unicasts it to the vehicle via a secure channel, until it reaches its destination. It adds its nonce N4, and encrypts the set (IDA, IDV, d(V), q(V), N1, N2, N3, N4) with the shared secret key (Evac), the ECQV private key of Cloud based-CA and the ECQV public key of Cloud based_RSUManager, respectively.

Step 5: Cloud based-CA ⇒ Cloud based-RSU_Manager:

Sk (CA)[Pk(RSU_M)[Evac[IDA || IDV || Q(V)|| P(V)|| N1 || N2|| N3 || N4]]] ***(RES1)***

6. *forwarding the pair key*

After that, Cloud based-RSU-Manager verifies the signature of the received message. If it is OK, it sends it to RSUs under its authorities after adding it nonce N5 and encrypting it with the ECQV public key of RSU and the private key of Cloud based_RSUManager, respectively.

Step 6: Cloud based-RSU_Manager ⇒ RSU:

Sk(RSU_M)[Pk(RSU)[Evac[IDA || IDV || Q(V) || P(V) || N1|| N2 || N3 || N4 || N5]] ***(RES2)***

7. *Broadcasting the pair key*

After receiving the encrypted message by Evac, the RSU broadcasts it into its area after adding its nonce N6. The only vehicle that can decrypt the sent-message is the one that sends the request for obtaining a pair key. Because, it is the only entity that can decrypt the message using the shared secret key, between the vehicle and the certification

authority.

Step 7: RSU ⇒ Vehicle

[Evac[IDA || IDV || Q(V) || P(V) || N1 || N2 || N3 || N4 || N5 || N6]] *(RES3)*

3.4.3 | *Revocation*

The process of invalidating the certificate is called revocation. It occurs when a certificate needs to be invalidated before the expiration date of the certificate. Revocation informs a user attempting to validate a public key that the private key associated with the public key is no longer valid and warns other vehicles from dealing with the revoked-certificate vehicle. Our solution for this problem is literally inspired by the solution proposed by authors in [12] with specific changes in the architecture of course to see how the proposed system effects on the revocation phase.

As shown in the Figure 3, The revocation process starts from the certification authority. When it receives a request to revoke a specific vehicle's certificate for some reasons. It checks its validity (lifetime). If the certificate's lifetime is not yet expired, Cloud based-CA triggers the real revocation process and sends a revocation message to the Cloud based-RSU-Manager. This latter checks by itself if the vehicle is still registered and sends the message to all RSUs situated in a circular area with radius (r) where the vehicle is most probably in. Finally, each RSU forwards the message to all vehicles in its area to warn them from dealing with this vehicle.

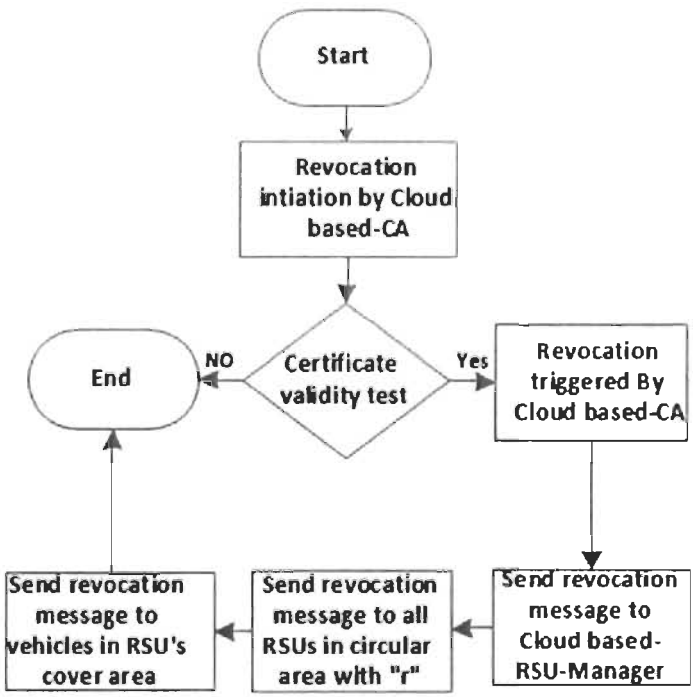

FIGURE 3 Certificate revocation flowchart.

The summary of our protocol is as follows:

ALGORITHM
Repeat for each vehicle.
Define Δ T
New Certificate (V)
Trigger the countdown time Δ T
if $T = 0$
Lunch Revocation
Generate a random number $0<\sigma<60$
Trigger the timer T
if $T = \sigma$
Request a new Certificate (V)
Endif
Endif
Until End of simulation

4 | ANALYSIS OF SECURITY

4.1 | Introduction

Vehicular cloud as most of mobile systems are susceptible to a plenty of security threats. In this section, security characteristics and resistance to various attacks of our proposed protocol are qualitatively highlighted using some scenarios, as a proof of fulfilling vehicular cloud's requirements to be secure. Furthermore, it should provide privacy preserving authentication, message integrity, conditional anonymity, availability, non-repudiation, certificate revocation and being effective in real-time systems. In the following subsections, we analyze our proposed protocol through various attack scenarios including man-in-the-middle, Sybil and replay attacks that are briefly summarized below.

- Man-in-the-middle attack
  It is a security attack towards precise nodes, where the attacker sits in the middle of the two-communicating vehicles and launch this attack. In this type of attacks, the attacker controls all the communication between the sender and the receiver. However, communicating vehicles assume that they are directly communicating with each other [28]. The attacker listens to communication between the vehicles and injects false or modified generated message, pretending to be an authorized member of the communication.
- Sybil attack
  In this case, an attacker pretends to be another member or multiple numbers in the network, by faking his ID. It sends multiple wrong messages to alternative nodes on the road, to enforce them to go away the road for its own advantages [29].
- Replay attack
  In this attack, an attacker replays the transmission of earlier information to take advantage of the situation of the message at the time of sending [30]. Furthermore, a secure system must provide some services such as non-repudiation where a sender/receiver cannot possibly deny sending/receiving a specific message.

4.2 | Analysis

Scenario 1: messaging system is semantically confidential.

Proof: All the communication in our protocol is protected and confidential, so any sent message must reach an intended receiver securely following these steps:

- Vehicle (V) sends a key request to RSU with (IDV || N1) as shown in step1.
- RSU forwards the key request until it receives a key back.
- If an attacker captures the message sent by Cloud based-CA in step 5, then, it will not be able to decrypt it, as it does not own the shared secret key (Evac). Using this technique and generalized it between any two entities in our protocol, we eliminate the vulnerability of the man-in-the-middle attack.

Scenario 2: Communication between all the participants is highly secure.

Proof: All communications in our protocol are encrypted using the Elliptic Curve Qu-Vanstone implicit certificate (ECQV). According to this scheme, given an element G and the value cG, it is computationally infeasible for an attacker to compute the secret key c. Therefore, the communication is secure.

Scenario 3: Impersonate an initiator or even a Road Side Unit by replying them via the message sent in step 5.

Proof: The proposed protocol requires the vehicle identity (IDV) to request the keys pair and then receives it encrypted using the shared Secret key (Evac). Since Evac is not known except for the vehicle and CA, this will eliminate the vulnerability against non-repudiation and Sybil attacks by following these steps:

- Vehicle (V) sends a new key request, no one can send it on behalf of (V) as no entity other than (V) and the CA knows the IDV (non-repudiation).
- Supposed, under any case, an attacker (A) gets to know the vehicle's identity (IDV) and sends a key request to the RSU. The message reply containing the keys pair will be encrypted with the Evac, which is the mainly shared secret key between the vehicle and the CA. Therefore, the generated keys are going to be useless for the attacker (A), since it cannot decrypt the received message.
- On the other hand, if an attacker (A) pretends to be the CA and sends the keys pair to (V): a case that will not happen, since the Evac is required to message's decryption (Masquerade).

Scenario 4: An attacker tries to replay the message in Step 1.

Proof: In every single step in our proposed solution, we have used nonce. Therefore, a replay could not happen since, each message containing the keys pair requested from a vehicle (V) must be sent with nonce to the RSU and then, to the Cloud based-RSU-Manager with another nonce and finally to the Cloud based-CA with a different nonce. The following steps show how our protocol can abort any tentative of a replay attack:

- Vehicle (V) sends a key request message with its nonce to the nearest RSU. Supposing that an attacker (A) intercepts the vehicle's message. A will resend the message after a moment to the RSU, on behalf of vehicle (V).
- Only vehicle (V) can decrypt the reply message containing the requested keys pair. However, it realizes from the nonce that the message is an old one, so it will ignore it and it requests another pair of keys.

5 | PERFORMANCE EVALUATION

Performance of the proposed protocol is measured through network simulations using Omnet++. To demonstrate the efficiency of our protocol, the forgoing analysis will consider vehicle mobility using two different models, urban and highway environments.

First, considering a vehicle moving in a city with average speed limits, and frequently changing directions. The Manhattan Grid model is adopted to represent the urban model. Second, considering a vehicle moving in a highway, which is most probably in fixed direction, with high limited speed.

In our simulations, we are interested 1/-in proportion of vehicles that obtain a new certificate, 2/-the proportion of vehicles that update (renew) their certificate and 3/-the effect of speed on certificate update rate in both mobility models, because these parameters are directly linked to the lifetime of certificates. The attention will now turn to the revocation phase; the focus is set to shift to the effect of vehicles density on revocation, in other words, trying to figure out how the fact of increasing the number of vehicles in a fixed area will affect the number of messages needed for revocation. Finally, we focused on the packet lost proportion versus number of vehicles, trying to investigate the effect of changing vehicles' number and how this will also affect the packet delivery ratio.

5.1 | Simulation parameters

We performed our experiments in both mobility models, urban and highway environments. For simulations, we ran our tests five times for each environment and then we calculated the average of simulation results. We used OMNET ++ 5.0 [31] with SUMO-0.25.0 [32] and Veins 4.4 [33].

TABLE 2 SIMULATION PARAMETERS.

Parameter	Value
Map of Manhattan	2.5 km x 2.5 km
Map of highway	15 km
Simulation time	1000 s
Certificate's lifetime	300 s
Urban max vehicle speed	14 m/s
Highway max vehicle speed	30 m/s
Number of vehicles	100; 200; 300; 400
MAC Protocol	IEEE 802.11p
Packet Size	1024 bytes
Bit rate	18 Mbps
RSUs distribution	Uniform
Range	1000 m

5.2 | Results

1. Proportion of vehicles that obtain a new certificate.
   The simulation results in figure 4 show the rate of vehicles that obtain a new certificate, in both urban and highway environment. In urban mode, the proportion of vehicles that require certificates and obtain them successfully starts at close to 60% and increases eventually with the Increase of vehicles' number, until it reaches the threshold of 91%, which is literally a high rate. In highway mode, the proportion of vehicles begins at 43% and increases slightly to 67%. The rate's increase in the second mode is slightly lower than the rate's increase in the first mode. This is directly related to the packet loss ratio, which is more significant for the highway environment, by dint of the high speed of vehicles.

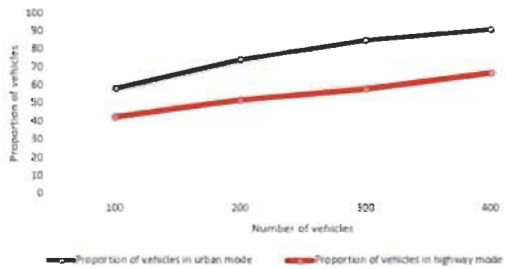

FIGURE 4 Proportion of vehicles that obtain a new certificate.

2. Proportion of vehicles that update (renew) their certificates.
   The simulation results in figure 5 show that the proportion of vehicles that update their certificates (Certificates renewal process after revocation phase) in urban area is about 18%, with a simulation of 100 vehicles. It gradually increases to reach 52% when the number of vehicles is 400. In highway area, the proportion of vehicles that update their certificates starts little over 10% for 50 vehicles and increases slightly until it reaches 15% for 100 vehicles. After that, it increases sharply until the threshold of 37 for 400 vehicles.

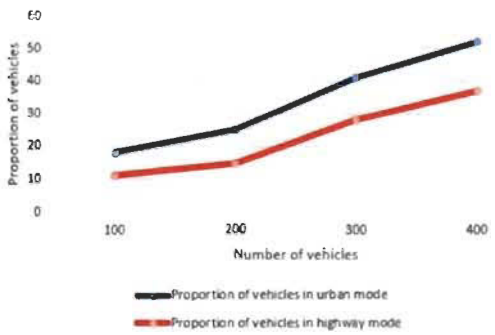

FIGURE 5 Proportion of vehicles that update their certificate.

These results show that the rate of certificates update is more significant in urban area compared to the highway

area; here we can observe an average rate of change of 34% between 100 and 400 vehicles in urban area. For highway, an average ratio of change is just 26%. This demonstrates that the certificates update process is much more effective in urban area compared to highway and that phenomena is strongly related both to the speed and the density of vehicles and not to the revocation phase. This means that the more vehicles are on the road, the more certificates' update phase is ensured.

3. Effect of speed on certificate update ratio.
   For this experiment, the number of vehicles in a precise area is fixed to identify the effect of speed on the certificate's update phase. Figure 6 illustrates the simulation results. We can see here that, at a speed of about 50 km/h, the ratio of certificates updated is around 35% and decreases sharply by increasing proportionally the speed of vehicles until it reaches 8.8% when the speed reaches the threshold of 110 km/h. The obvious conclusion from this experiment, the more the speed increases, the more the number certificates updates decreases.

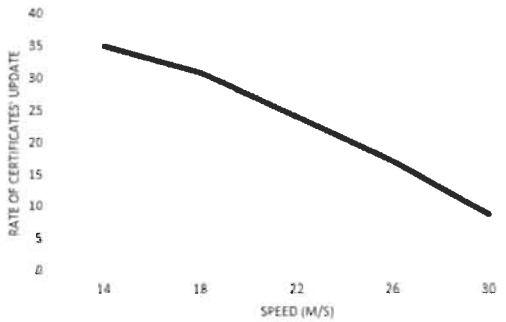

FIGURE 6 Effect of speed on certificate update rate.

4. Effect of density on revocation.

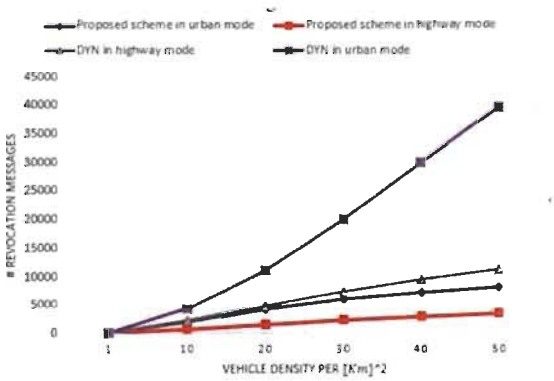

FIGURE 7 Effect of density on revocation.

For this experiment, we made a comparison with the method proposed in [12]. This scheme was used during simulation for comparison and we named it "DYN" (Dynamic). The simulation results in figure 7 show that in our proposed protocol with 10 vehicles, the percentage of messages needed for revocation is less than 0.05% for urban environment and around 0.02% for highway environment (of the total number of broadcasting messages). Now, for 50 vehicles, the results reveal that the percentage of messages required in our protocol is about 1/5 in urban environment and around 1/12 in highway environment compared to the total of messages required in [12].
Here, we can perceive that, it is much easy and effective for our proposed protocol to precise the position of the targeted node with high accuracy, contrary to the method proposed in [12] where the number of messages is too much high especially in urban mode. That means, sending the fewest messages possible into the circular area with radius (r) where the vehicle is most probably in. We can also notice that the revocation process is much more effective in highway environment, when a vehicle is traveling on a very long road, at a fixed speed and without changing directions.

5. Packet lost ratio by vehicles
Simulation results in figure 8 show that the Packet Lost Ratio (PLR) in the urban environment is around 10% with a simulation of 100 vehicles. It increases depending on the increased number of vehicles until it is nearly 29% for 400 vehicles. While in highway environment, the rate starts slightly above 18% and increases to over 40% for 400 vehicles. The PLR is principally related to the number of vehicles and the traffic environment. Rates increase in highway environment due to high vehicles' speed. Furthermore, we can notice from our experiment, that the PLR is considerably low. It is also linked somehow to the lifetime of certificates, which is 5 minutes, so the proportion of vehicles, which their certificates are revoked and updated, is low regardless the traffic environment.

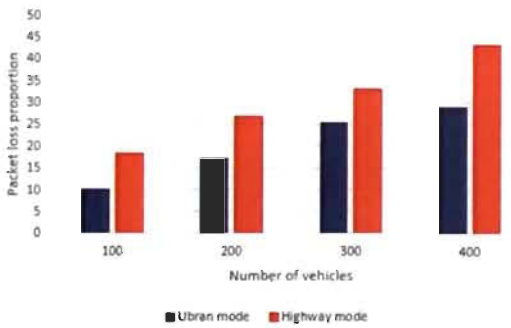

FIGURE 8 Packet lost ratio by vehicles.

6 | CONCLSUION

In this paper, an efficient dynamic ECQV certificates distribution scheme for vehicular cloud was proposed and thoroughly evaluated through network simulation. The CA is assumed to be cloud-based and the RSU managers as well, for better latency and more flexibility to cover the whole owned administrative domain, including better control of RSUs under responsibility and securing the passing by messages. ECQV implicit certificate scheme is used for generation

of certificates and encryption keys, which are well suited for very constrained environments. Previous studies could have sent revocation messages to vehicles that would have a very weak probability to communicate with, which in turn increases the overhead and decreases tragically the network's performance. Our protocol not only satisfies the security and privacy requirements in vehicular cloud environment, but also significantly reduces the revocation cost and the certificate updating overhead by supporting a selective revocation message delivery technique based on trajectory, speed, region nature and other parameters. In future work, we intend to study other techniques for nodes location issue under the context of the proposed protocol, with a fast disseminating revocation information for both expired certificates and misbehaving vehicles to enhance the proposed revocation technique.

ACKNOWLEDGEMENTS

This work was completed with the support of the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

1. IEEE Standard for Wireless Access in Vehicular Environments, Security Services for Applications and Management Messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1-240, 2016.

2. J. P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles, *IEEE Security and Privacy*, vol 2, pp. 49-55, 2004.

3. T. L. Willke, P. Tientrakool, and N. F. Maxemchuk. A survey of inter-vehicle communication protocols and their applications. *IEEE Communications Surveys and Tutorials*, vol 11, 2009.

4. B. Parno and A. Perrig. Challenges in securing vehicular networks. *in Workshop on hot topics in networks (HotNets-IV)*,pp. 1-6, 2005.

5. M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: a survey," IEEE Communications Surveys and Tutorials, vol. 10, 2008.

6. M. Raya and J. P. Hubaux. The security of vehicular ad hoc networks. Presented at *the Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, USA, 2005.

7. X. Lin, X. Sun, P. H. Ho, and X. Shen. GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on vehicular technology*, vol. 56, pp. 3442-3456, 2007.

8. H. C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, et al.. Flooding-resilient broadcast authentication for vanets. In *Proceedings of the 17th annual international conference on Mobile computing and networking*, pp. 193-204, 2011.

9. J. Kim and J. Song. A pre-authentication method for secure communications in vehicular ad hoc networks. In *Wireless Communications, Networking and Mobile Computing (WiCOM)*, 8th International Conference, pp. 1-6, 2012.

10. Y. J. Li. An overview of the DSRC/WAVE technology. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp. 544-558, 2010.

11. M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing*, vol. 98, pp. 685-708, Springer Vienna, 2016.

12. A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr. The case for dynamic key distribution for PKI-based VANETS. *International Journal of Computer Networks and Communications (IJCNC)*, vol. 6, 2016.

13. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, et al.. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, vol. 46, 2008.

14. S. Capkun and J. P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM*

2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, pp. 1917-1928, 2005.

15. B. Aslam and C. Zou. Distributed certificate and application architecture for VANETs. Presented at *the Proceedings of the 28th IEEE conference on Military communications*, Boston, Massachusetts, USA, 2009.

16. C. Zhang. PhD Thesis: On Achieving Secure Message Authentication for Vehicular Communications. University of Waterloo, Ontario, Canada, 2010.

17. B. Bellur. Certificate assignment strategies for a PKI-based security architecture in a vehicular network. In *Global Telecommunications Conference, 2008*. IEEE GLOBECOM, pp. 1-6, 2008.

18. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 3589-3603, 2010.

19. C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. in *The 27th Conference on Computer Communications*, INFOCOM 2008. IEEE, pp. 246-250, 2008.

20. S. Guo, D. Zeng, and Y. Xiang. Chameleon hashing for secure and privacy-preserving vehicular communications. *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 2794-2803, 2014.

21. A. Adigun, B. A. Bensaber, and I. Biskri. Protocol of change pseudonyms for VANETs. In *Local Computer Networks Workshops (LCN Workshops),IEEE 38th Conference*, Sydney, Australia, pp. 162-167, 2013.

22. Y. Hao, Y. Cheng, C. Zhou, and W. Song. A distributed key management framework with cooperative message authentication in VANETs. *IEEE Journal on selected areas in communications*, vol. 29, pp. 616-629, 2011.

23. D. Chaum and E. Van Heyst. Group signatures. In *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 257-265,1991.

24. R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In *INFOCOM 2008. The 27th Conference on Computer Communications*. IEEE, pp. 1229-1237,2008.

25. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer. A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions on vehicular Technology*, vol. 59, pp. 1606-1617, 2010.

26. A. Wasef and X. Shen. MAAC Message authentication Acceleration Protocol for Vehicular Ad Hoc Networks. *Proceedings of Global Telecommunication Conference*, pp. 1-6, Honolulu, HI, USA, November 30-December 4 2009.

27. A. Wasef, Y. Jiang, and X. Shen. DCS: an efficient distributed-certificate-service scheme for vehicular networks. *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 533-549, 2010.

28. G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, et al.. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys and tutorials*, vol. 13, pp. 584-616, 2011.

29. S. Park, B. Aslam, D. Turgut, and C. C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *Military Communications Conference, 2009*. MILCOM 2009. IEEE, pp. 1-7, 2009.

30. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, et al.. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium*, pp. 447-462, 2010.

31. http://www.omnetpp.org/ visited 20/06/2017.

32. http://sumo.sourceforge.net/ visited 20/06/2017.

32. http://veins.car2x.org/ visited 20/06/2017.

CHAPITRE 5 ANALYSE ET DISCUSSION DES RÉSULTATS

5.1 Environnement de simulation

Dans ce chapitre, nous résumons les différentes expérimentations et tests réalisés à travers des simulations afin de mesurer l'efficacité et évaluer les performances de notre protocole. Nous avons réalisé nos simulations avec le simulateur réseau OMNET+ + 5.0 [38] et le simulateur de trafic routier SUMO-0.25.0 [39]. Notons ici qu'OMNET++ est un simulateur qui est largement utilisé pour la simulation des protocoles et des applications de sécurité dans les réseaux sans fil. Le choix de ce simulateur est dû aux nombreux avantages qu'il offre par rapport aux autres simulateurs y compris l'interface utilisateur riche qui facilite la visualisation et la manipulation de cet outil. Il faut rappeler que, dans le cadre de notre étude, nous avons intégré aussi un Framework open source dénommé Veins-4.4 [40], qui fédère SUMO et OMNET++ et ce, dans le but d'avoir des résultats de simulation significatifs proches de la réalité.

5.2 Discussion des résultats

Afin de démontrer l'efficacité de notre protocole proposé, nous l'avons simulé dans les deux environnements urbain et autoroutier. Premièrement, nous avons étudié et calculé le pourcentage de véhicules qui ont obtenu un nouveau certificat (voir Figure 4 dans l'article). Les résultats montrent que le nombre de véhicules qui demandent et obtiennent avec succès un certificat dans un environnement urbain augmente proportionnellement avec le nombre de véhicules, jusqu'à atteindre le seuil de 91 %, ce qui est excessivement élevé. Par contre, en mode autoroutier, la proportion de véhicules qui obtiennent un certificat augmente légèrement et atteint le taux de 67 %. En effet, le nombre de véhicules qui ont obtenu un nouveau certificat est élevé dans les deux environnements. Comme nous avons pu le remarquer, le taux d'augmentation en deuxième mode est légèrement inférieur par rapport au premier mode. Ceci est directement lié au taux de perte de paquets qui est essentiellement plus important dans l'environnement autoroutier à cause de la vitesse élevée des véhicules. Dans une

deuxième étape, nous avons évalué la proportion de véhicules qui mettent à jour leurs certificats (processus de renouvellement de certificats après la phase de révocation) (voir Figure 5 dans l'article). En mode urbain, le taux commence à 18 %, avec une simulation de 100 véhicules, il augmente progressivement jusqu'à atteindre le seuil de 52 % lorsque le nombre de véhicules atteint les 400. En mode autoroutier, la proportion de véhicules qui mettent à jour leurs certificats commence avec un léger pourcentage de 10 % pour 100 véhicules et augmente jusqu'à à atteindre le seuil de 37 pour 400 véhicules. Ces résultats montrent ainsi que le taux de mise à jour des certificats est plus important dans l'environnement urbain par rapport à l'environnement autoroutier. Ce qui donne un taux de variation moyen de 34 % entre 100 et 400 véhicules en mode urbain et seulement de 26 % pour l'environnement autoroutier. Cela démontre que le processus de mise à jour des certificats est beaucoup plus efficace en mode urbain qu'en mode autoroutier, et que ce phénomène est fortement lié à la densité des véhicules, à la vitesse des véhicules et à la durée de vie limitée des certificats. Les véhicules changent leurs certificats expirés périodiquement à des moments aléatoires, ce qui empêche les véhicules malveillants de prévoir les changements de certificats par chaque véhicule. Cela garantit l'anonymat et la vie privée des véhicules.

Troisièmement, nous avons expérimenté l'effet de la vitesse sur la phase de mise à jour des certificats. Pour ce faire, nous avons fixé le nombre de véhicules dans les deux environnements et inspecté ensuite l'effet de la vitesse sur cette phase (voir la Figure 6 dans l'article). Les résultats de la simulation montrent que la proportion des véhicules qui mettent à jour leurs certificats diminue fortement au fur et à mesure que la vitesse des véhicules augmente. Il en résulte ainsi que plus la vitesse augmente, plus le taux de mise à jour des certificats numériques diminue.

Quatrièment, nous nous sommes intéressés à l'effet de la densité des véhicules dans la phase de la révocation (voir Figure 7 dans l'article). Pour cette expérience, nous avons fait une comparaison avec la méthode proposée par [37] et nous l'avons nommée DYN (DYNAMIQUE). Les résultats de la simulation montrent que dans notre protocole proposé avec 10 véhicules, le pourcentage de messages nécessaires à la révocation est inférieur à 0,05 % du nombre total requis par DYN pour l'environnement urbain et d'environ 0,02 % pour celui de l'autoroute par rapport au nombre total des messages

diffusés par DYN. Pour 50 véhicules, les résultats révèlent que le pourcentage de messages nécessaires à la révocation totale dans notre protocole est d'environ 1/5 du nombre de messages requis par DYN dans l'environnement urbain et de 8 % dans l'environnement autoroutier. Pour récapituler, Nous estimons que le protocole proposé est avantageux dans la mesure où il est très facile et efficace de préciser la position exacte du nœud ciblé avec une forte exactitude. Cela signifie également qu'il est permis d'expédier un minimum possible de messages dans une zone circulaire de rayon (r) où se trouve probablement le véhicule. Par conséquent, plus le nombre de véhicules augmente, plus le nombre de messages requis pour la révocation est réduit par rapport à DYN. De plus, nous pouvons constater que le processus de révocation est beaucoup plus efficace dans l'environnement autoroutier, notamment lorsqu'un véhicule se déplace pendant un long trajet à une vitesse fixe et sans changement de direction.

Enfin, nous avons aussi évalué les pourcentages de perte de paquets (voir Figure 8 dans l'article), car il s'agit là d'un paramètre qui représente une contrainte majeure dans les réseaux VANET. Les résultats montrent, à ce sujet, que le taux de perte de paquets est principalement lié au nombre de véhicules et à l'environnement de circulation. Les taux augmentent sensiblement dans l'environnement autoroutier en raison de la vitesse élevée des véhicules. En outre, nous avons constaté, lors de notre expérience, que le taux de perte de paquets est considérablement faible. Ce taux est également lié en quelque sorte à la durée de vie des certificats qui est de 5 minutes, de sorte que la proportion de véhicules, dont les certificats sont révoqués et mis à jour, est quand même faible, quel que soit le mode de trafic.

CHAPITRE 6 CONCLUSION GÉNÉRALE ET PERSPECTIVE

Les systèmes de transport intelligents sont nés d'une union des technologies de l'information et de la communication avec les réseaux véhiculaires qui assurent la mobilité des personnes et des biens, la réduction des dégâts en cas de collision et la limitation des émissions de gaz à effet de serre. Ces systèmes ont pour but de fournir de manière pratique aux voyageurs un accès instantané aux informations sur l'état des routes, en leur permettant d'échanger entre eux des infodivertissants visant à rendre leurs voyages aussi agréables que conviviaux. Une meilleure compréhension générale des STI pourrait donc faciliter l'implémentation des systèmes et des services actuellement en cours de développement. Un bon fonctionnement de ces systèmes reposera sur les réseaux véhiculaires sans fil. Ce qui fait qu'il existe un intérêt grandissant pour ce genre de réseaux, quand bien même les travaux dans ce domaine en particulier dans le champ de la sécurité restent encore relativement modestes. C'est en partie ce qui nous a encouragés à aborder ce champ d'étude.

Le travail réalisé dans le cadre de notre mémoire vise à proposer une solution de sécurité globale pour ces réseaux, en intégrant la notion de nuage pour donner plus d'élasticité et d'évolutivité à notre protocole d'authentification et de gestion de certificats. Ainsi, nous avons proposé un système de gestion et de distribution des certificats ECQV pour les réseaux véhiculaires dans le nuage. L'autorité de certification et les gestionnaires RSU sont supposés être basés sur le nuage, et ce, pour une meilleure latence, pour plus de contrôle et pour plus de souplesse afin de couvrir l'ensemble du domaine administratif détenu. S'ensuivent un meilleur contrôle des unités de routes qui sont disposées d'une manière uniforme et une sécurisation du passage de messages entre les différentes unités dans le réseau.

Un schéma de certificats implicites ECQV est utilisé pour la génération de certificats et les paires de clés qui conviennent bien aux environnements très contraignants. Après une analyse de sécurité du protocole, il en ressort que le dispositif répond non seulement aux exigences de sécurité suivantes : l'authentification, la non-répudiation, la gestion de la vie privée et l'intégrité, mais aussi à réduire considérablement le coût

de révocation et le surcoût de la mise à jour des certificats en soutenant une technique de distribution des messages de révocation sélective basée sur des paramètres, comme la trajectoire, la vitesse, la nature de la région et d'autres.

Dans nos futurs projets, nous avons l'intention d'étudier davantage de techniques afin d'améliorer la révocation proposée, notamment le problème de localisation des nœuds sans pour autant saturer l'ensemble du réseau avec des informations inutiles et catalyser le processus en le rendant plus efficace. Ainsi, nous allons contribuer à la mise en œuvre d'une méthode de révocation coopérative entre les autorités civiles et l'autorité de certification pour mieux détecter les véhicules malveillants, révéler leur identité et les mettre ainsi à la disposition des autorités civiles.

REFERENCES

[1] H. Hartenstein and K. Laberteaux, *VANET vehicular applications and inter-networking technologies* vol. 1: John Wiley & Sons, 2009, ISBN: 978-0-470-74056-9

[2] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks," *NEW2AN,* vol. 9, pp. 291-300, 2009.

[3] M. Jerbi, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain: Routage et GeoCast basés sur les intersections," Evry-Val d'Essonne, 2008.

[4] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "Vehicular mobility simulation for vanets,"" in *40th IEEE Annual Simulation Symposium (ANSS'07), Norfolk, USA*, 2007.

[5] N. CHAIB, "La sécurité des communications dans les réseaux VANET," Université de Batna 2, 2011.

[6] A. Khan, S. Sadhu, and M. Yeleswarapu, "A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks," *Project Report, Department of Computer Science, University of Californai, Santa Barbara,* pp. 1-8, 2009.

[7] S. N. Pathak and U. Shrawankar, "Secured communication in real time vanet," in *Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference on*, 2009, pp. 1151-1155.

[8] K. Moghraoui, "Gestion de l'anonymat des communications dans les réseaux véhiculaires Ad hoc sans fil (VANETs)," Université du Québec à Trois-Rivières, 2015.

[9] A. Adigun, "Gestion de l'anonymat et de la traçabilité dans les réseaux véhiculaires sans fil," Université du Québec à Trois-Rivières, Mémoire de maitrise, 2014.

[10] Christian TCHEPNDA, "Authentication dans les Réseaux Véhiculaires Opérés", Thèse de Doctorat, École Nationale Supérieure des Télécommunications, Spécialité: informatique et Réseaux, 18 décembre 2008, Paris- France.

[11] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*: Springer Science & Business Media, 2013, Hardcover ISBN: 978-3-540-42580-9.

[12] V. G. Martínez, L. H. Encinas, and C. S. Ávila, " A Survey of the Elliptic Curve Integrated Encryption Scheme. Journal of Computer Science and Engineering. *ratio,* vol. 80, pp. 160-223, 2010.

[13] A. Yger and J. Weil, "Mathématiques appliquées L3," *Cours complet avec 500 tests et exercices corrigés*". Pearson *Education, Ed,* 2009, ISBN-13: 978-2744073526.

[14] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, 2009, pp. 106-115.

[15] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in *ITS Telecommunications (ITST), 2011 11th International Conference from 25 to 25 Aug* 2011, pp. 613-618, ISBN: 978-1-61284-668-2.

[16] https://www.certicom.com/.

[17] "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013),* pp. 1-240, 2016, Electronic ISBN: 978-1-5044-0767-0.

[18] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, *et al.*, "Secure vehicular communication systems: design and architecture" *IEEE Communications Magazine,* vol. 46, no. 11, pp. 100-109, DOI: 10.1109/MCOM.2008.4689252

[19] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks" in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE.* 3. 1917 - 1928 vol. 3. 10.1109/INFCOM.2005.1498470.

[20] Baber Aslam and Cliff Zou. 2009. Distributed certificate and application architecture for VANETs. In *Proceedings of the 28th IEEE conference on Military communications* (MILCOM'09). IEEE Press, Piscataway, NJ, USA, 30-36, ISBN: 978-1-4244-5238-5.

[21] C. Zhang, "PhD Thesis: On Achieving Secure Message Authentication for Vehicular Communications," *University of Waterloo, Ontario, Canada,* 2010.

[22] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks" presented at the Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA, 2005, ISBN: 1-59593-227-5 .

[23] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET," in *Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking (VANET '08).* ACM New York, USA, 2008, pp. 88-89, ISBN: 978-1-60558-191-0

[24] B. Bellur, "Certificate assignment strategies for a PKI-based security architecture in a vehicular network" in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. New Orleans, USA, IEEE* 2008, pp. 1-6, doi: 10.1109/GLOCOM.2008.ECP.355, ISBN: 978-1-4244-2324-8.

[25] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications" in *IEEE Transactions on Vehicular Technology,* vol. 59, pp. 3589-3603, Sep 2010, ISBN: 978-1-4244-6402-9.

[26] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, Atlanta,GA, USA 2008, pp. 246-250, ISBN: 978-1-4244-2026-1.

[27] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications" *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, pp. 2794-2803, 2014, ISBN: 978-1-4673-0436-8.

[28] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs" *IEEE Journal on selected areas in communications,* vol. 29, pp. 616-629, 2011, DOI=http://dx.doi.org/10.1109/JSAC.2011.110311.

[29] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications" *IEEE Transactions on vehicular technology,* vol. 56, pp. 3442-3456, 2007, ISBN: 978-1-319-01351-0.

[30] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications" *IEEE Transactions on vehicular Technology,* vol. 59, pp. 1606-1617, 2010.

[31] A. Shamir, "Identity-based cryptosystems and signature schemes" in Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, pp.47-53, ISBN:0-387-15658-5

[32] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications" in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, Phoenix, Arizona, USA, pp. 1229-1237, ISBN: 978-1-4244-2025-4.

[33] J. Kim and J. Song, "A pre-authentication method for secure communications in vehicular ad hoc networks," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference in* Shanghai, China 2012, pp. 1-6, ISBN: 978-1-61284-684-2

[34] A. Adigun, B. A. Bensaber, and I. Biskri, "Protocol of change pseudonyms for VANETs" in *Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference, Sydney, Australia*, 2013, pp. 162-167, ISBN: 978-1-4799-0538-6.

[35] A. Wasef and X. Shen, "MAAC: message authentication acceleration protocol for vehicular ad hoc networks," presented at the Proceedings of the 28th IEEE conference on Global telecommunications, Honolulu, Hawaii, USA, 2009, ISBN: 978-1-4244-4147-1.

[36] A. Wasef, Y. Jiang, and X. Shen, "DCS: an efficient distributed-certificate-service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology,* vol. 59, pp. 533-549, 2010.

[37] A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, "The case for dynamic key distribution for PKI-based VANETS" *International Journal of Computer Networks & Communications (IJCNC)* vol. 6, No.1, pp. 61-78, 2016.

[38] http://www.omnetpp.org/, visited 20/06/2017.

[39] http://sumo.sourceforge.net/, visited 20/06/2017

[40] http://veins.car2x.org/, visited 20/06/2017.