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
AMINA BENDOUMA

DÉVELOPPEMENT D'UNE INFRASTRUCTURE DE GESTION DE CLÉS DE CRYPTAGE DANS LES RÉSEAUX AD HOC VÉHICULAIRES (VANET)

JUILLET 2017

CE MÉMOIRE A ÉTÉ ÉVALUÉ
PAR UN JURY COMPOSÉ DU :

Professeur Boucif Amar Bensaber, directeur de recherche
Département de mathématiques et d'informatique Université du Québec à Trois-Rivières.

Professeur Ismaïl Biskri, évaluateur
Département de Mathématiques et d'informatique Université du Québec à Trois-Rivières.

Professeur Mhamed Mesfioui, évaluateur
Département de Mathématiques et d'informatique Université du Québec à Trois-Rivières.

AUTHENTIFICATION DES RSU DANS LES VANET PAR AGRÉGATION EN UTILISANT UNE ZONE D'INTERACTION

Amina Bendouma

SOMMAIRE

Le réseau ad-hoc véhiculaire (VANET) est une innovation qui modifiera notre vision du trafic routier et qui améliorera la sécurité et l'efficacité du transport. VANET représente une cible pour les attaques, qui peuvent causer des pertes humaines et matérielles. Cela souligne la nécessité d'un système de sécurité robuste, qui doit sécuriser efficacement les communications entre les véhicules et le reste des entités du réseau, mais doit également garantir la disponibilité et la fluidité de la transmission.

Notre schéma de sécurité vise à assurer l'identification, l'authentification, la non-répudiation et l'intégrité de l'unité de bord de route (RSU) lors de la transmission des messages du (RSU) aux véhicules (R2V). Une agrégation d'identification sera réalisée par plusieurs RSU et sans l'intervention d'un tiers de confiance.

Notre algorithme assure d'abord l'identification des RSU par l'algorithme *Elliptic Curve Diffie-Hellman* (ECDH) où le véhicule vérifie que les deux RSU voisins ont le même secret partagé, ensuite, le véhicule procède à l'authentification du message préalablement signé, en utilisant l'*Elliptic Curve Digital Signature* (ECDSA). Pour les simulations nous avons utilisé l'environnement combiné OMNET ++, SUMO et VEINS, et nous avons intégré la bibliothèque Crypto++ afin d'atteindre les exigences de sécurité. Le modèle que nous avons proposé parachève une plus haute sécurité.

Mots-clés : réseau sans fil ; VANET ; Sécurité ; ECDSA.

RSU AUTHENTICATION BY AGGREGATION IN VANET USING AN INTERACTION ZONE

Amina Bendouma

ABSTRACT

Vehicular ad-hoc network (VANET) is an innovation that will change our vision of road traffic, it will improve the safety and the efficiently of transport. VANET represent a target for attacks that can cause human and material losses. This highlights the need for a robust security system, who must secure effectively communications between vehicles and the different network's entities, but also, it must guarantee availability and fluidity in the transmission.

Specifically, in transmission of messages from Road Side Unit (RSU) to vehicle (R2V), our security aims to ensure identification, authentication, non-repudiation and integrity for the RSU. An aggregation of identification will be achieved by multiples RSU and without asking for the intervention of a trusted third party.

In this paper, we proposed a security schema to firstly ensure identification for RSU by an Elliptic Curve Diffie-Hellman (ECDH) algorithm where the vehicle confirms that the two neighbours RSU have the same shared secret, then secondly the vehicle authenticates the message beforehand signing, using Elliptic Curve Digital Signature Algorithm (ECDSA). To simulate the vehicle scenario, we used the OMNET++, SUMO and VEINS combined environment, and we integrated on it the Crypto++ library to achieve the security requirement. Our proposed model ensures stronger security.

Keywords: Wireless network; VANET; Security; ECDSA.

REMERCIEMENTS

Je remercie mon directeur de recherche, le Professeur Boucif Amar Bensaber pour son aide et ses conseils dans la réalisation de ce travail.

Je remercie aussi mes évaluateurs Professeur Ismaïl Biskri et Professeur Mhamed Mesfioui.

Je remercie ma chère mère pour le soutien qu'elle m'a apporté et la confiance qu'elle a eue en moi ; c'est grâce à elle que j'ai pu réaliser mon but et concrétiser mon projet.

Je remercie également mon cher père et mon cher petit frère.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

Liste des tableaux du mémoire

Liste des tableaux de l'article

LISTE DES FIGURES

Liste des figures du mémoire

Liste des figures de l'article

LISTE DES ABRÉVIATIONS

CA: Central Authority

DOS: Denial Of service

DSRC: Dedicated Short Range Communication

GPS: Global Positioning System

MAC: Medium Access Control

ITS: Intelligent Transport System

MANET: Mobile Ad hoc Network

OBU: On Board Unit

RSU: Road Side Unit

SUMO: Simulation of Urban Mobility

TA: Trusted Authority

TPD: Tamper Proof Device

V2V: Vehicular-to-Vehicular

V2I: Vehicular-to-Infrastructure

VANET: Vehicular Ad hoc Network

WAVE: Wireless Access for the Vehicular Environment

INTRODUCTION

L'industrie automobile est constamment en évolution pour répondre aux exigences du transport. Son objectif est de toujours pousser les limites de la vitesse et du confort, aussi se heurte-elle à un problème majeur qui est la sécurité routière. Ces dernières années sont marquées par une importante augmentation d'accidents faisant des pertes humaines et des dégâts matériels considérables.

L'intégration d'un réseau Ad-hoc dans les véhicules leur permet de communiquer entre eux. Ceci semble être le début d'une nouvelle ère technologique prometteuse, pouvant remédier à l'insécurité sur les routes, minimiser les risques et les accidents, alerter rapidement la police et les ambulances pour sauver des vies et améliorer le trafic routier et le confort des conducteurs et des passagers.

Tous les réseaux informatiques sont victimes d'attaques régulières de plus en plus sophistiquées, le réseau Ad-Hoc de véhicules (VANET) n'en fait pas l'exception. Il est la cible d'un bon nombre de hackeurs qui exploitent les vulnérabilités de la sécurité. Il est donc impératif d'intégrer un système de sécurité aux réseaux VANET pour assurer un ensemble d'options sécuritaires telles que l'authentification, l'identification, la non répudiation, l'intégrité et la confidentialité, tout en gardant la disponibilité et la fluidité de transmission dans le réseau véhiculaire.

Tout comme les véhicules, les unités de bord de route (RSU) peuvent être aussi corrompues. Nous nous sommes consacrés dans notre étude à assurer une agrégation d'authentification des RSU, en utilisant l'algorithme d'échange de clés Diffie-Hellman basé sur les courbes elliptiques (ECDH) et l'algorithme de signature numérique basé sur les courbes elliptiques (ECDSA). Nous avons éliminé l'autorité de confiance (CA) pour réduire l'impact négatif qui en découle, tels que le temps et les moyens de stockage dédiés aux listes de révocation et à leur vérification. Ceci dans le but d'alléger la communication et de diminuer le nombre de saut et la transition des données, et ainsi, libérer les ressources matérielles et assurer la décentralisation du réseau.

Notre mémoire se divise en quatre parties : I) Architecture des réseaux VANET, II) État de l'art, III) Article scientifique, IV) Résultats et discussion V) Conclusion générale.

CHAPITRE 1

PRÉLIMINAIRE

1.1 Architecture des réseaux VANET

Le réseau VANET est une sous-catégorie du réseau Ad-Hoc mobile (MANET)[1], où les nœuds sont remplacés par des véhicules pouvant communiquer entre eux grâce à l'unité de bord (OBU) et avec d'autres entités du réseau telles que l'unité de bord de route (RSU).

Ce chapitre se devise en deux parties distinctes, dans la première nous traitons l'architecture du réseau VANET, dans la seconde nous introduisons les bases de la sécurité des réseaux.

1.1.1 Les entités de communication

Les réseaux véhiculaires se composent de plusieurs entités qui communiquent entre elles via des ondes radio. Ces entités ainsi que leurs fonctions sont décrites et détaillées dans ce chapitre.

Figure 1 : Vue globale des entités de communication

1.1.1.1 RSU

L'RSU (*Road Side Unit*) est une infrastructure située à proximité des routes. Elle joue le rôle de routeur qui fournit une connectivité entre OBU-OBU (V2V) ou entre un OBU et une autre infrastructure (RSU, CA etc...) (V2I). Ses principales fonctions sont [2] l'élargissement de la portée de communication, la procuration de la connectivité à l'OBU et aux autres entités et l'exécution des applications de sécurité.

Figure 2 : Unité de bord de route RSU « Road Side Unit »

1.1.1.2 OBU

L'OBU (*On-Board-Unit*) est un dispositif sans fil, embarqué sur les véhicules intelligents. Il permet la transmission des informations entre voitures ou entre une voiture et une autre infrastructure grâce aux communications dédiées à courte portée (DSRC). Il est relié à une ou plusieurs unités d'application « AU ». L'OBU se base sur la technologie radio IEEE 802.11p pour l'envoi des données de sécurité à courte portée. Il assure entre autre l'accès radio sans fil, le routage géographique ad hoc, le transfert fiable et sécurisé des données, ainsi que le support de la mobilité IP[3]. Ses principaux constituants sont [4, 5] :

- Le CPU (*Central Processing Unit*) Unité centrale de calcul qui implémente les applications et les protocoles de commutation.
- L'EDR (*Event Data Recorder*) : enregistreur de données et d'évènements, il enregistre l'ensemble des messages émis/reçus, les événements qui ont eu lieu ainsi que les itinéraires le long du voyage.
- L'émetteur-transmetteur sans fil (*wireless transceiver*) qui assure la transmission sans fil des données.

- Le GPS : (*Global Positioning System*) récepteur de système de positionnement global donnant la direction et la vitesse des nœuds ainsi que leurs positionnements.
- Antenne multidirectionnelle pour accéder aux canaux sans fil.
- L'ELP (*Electronic License Plate*) : plaque d'immatriculation électronique qui représente et diffuse l'identité du véhicule.
- Interface entrée/sortie pour que le conducteur puisse interagir avec.
- Autres radars et capteurs pour la détection du statut du véhicule et son environnement dont la consommation de carburant, la détection des conditions météorologiques et les obstacles de la route.

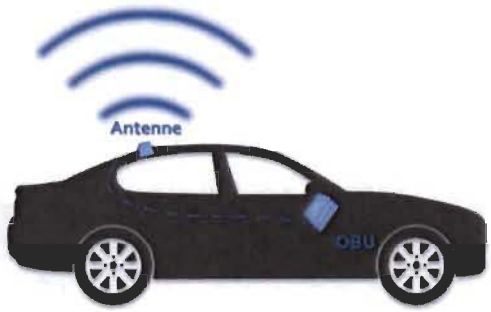

Figure 3 : Unité de bords OBU « On-Board Unit »

1.1.1.3 AU

L'unité d'application est une entité logique, intégrée dans les dispositifs physiques qui composent le réseau VANET. Elle se divise en deux branches principales, celles qui assurent la sécurité et celles qui assurent le confort des passagers[2] tel qu'illustré dans le schéma ci-dessous :

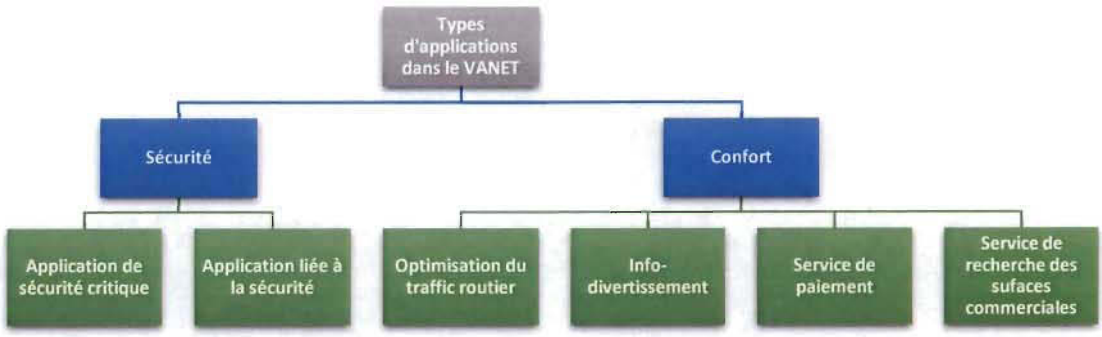

Figure 4 : Types d'applications dans le VANET

1.1.1.4 TPD

TPD (*Tamper Proof Device*) ou TRD (*Tamper Resistant Device*) est un dispositif physique anti-sabotage, son accès est limité aux personnes autorisées. Il possède sa propre batterie et sa propre horloge interne qui peut être resynchronisée de façon sécurisée, empêchant ainsi les attaqueurs de le compromettre. Son rôle est de fournir une entrée sécurisée pour le système de communication, de stocker les différentes clés de chiffrement et les informations sensibles, d'assurer leur confidentialité et leur protection et de signer les messages sortants.

Le TPD est équipé de capteurs qui déclenchent la destruction automatique des données lors de tentative de vol ou de manipulation non autorisée du matériel [6].

1.1.1.5 Capteurs

Les capteurs sont des dispositifs physiques installés sur chaque véhicule. Ils permettent la mesure et la collecte d'informations concernant l'état du véhicule ainsi que celui de son environnement. Ces capteurs ouvrent des possibilités plus larges pour les applications des réseaux véhiculaires[7].

1.1.2 Domaines et types de communication

Différents domaines et types de communication existent dans les réseaux VANET[2]. Ils sont résumés dans l'illustration ci-dessous :

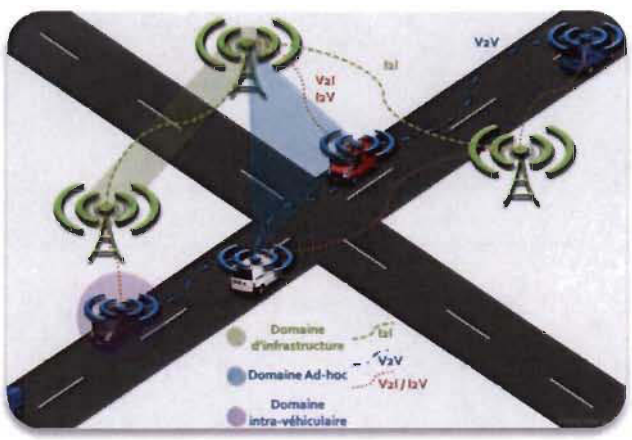

Figure 5 : Domaines et types de communication

1.1.2.1 Domaine intra-véhiculaire

Il s'agit du réseau entre l'OBU, l'AU, les capteurs et d'autres dispositifs montés sur la même voiture et qui communiquent entre eux avec ou sans fil.

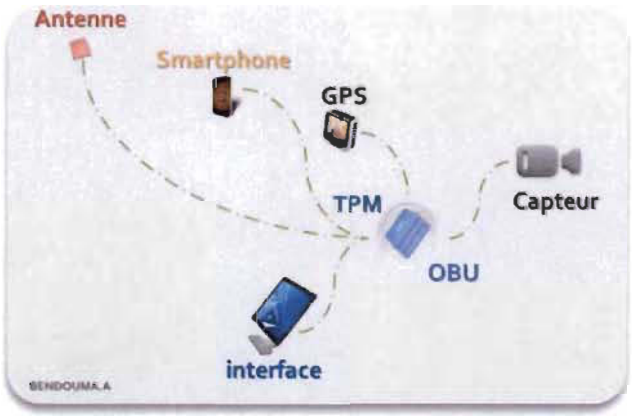

Figure 6 : Domaine intra-véhiculaire

1.1.2.2 Domaine Ad-Hoc (V2V, V2I)

La communication inter-véhiculaire (V2V) est une communication établie entre deux véhicules plus précisément d'OBU à OBU.

Figure 7 : V2V

La communication V2I est une communication établie entre un véhicule et un RSU (Infrastructure) ou l'inverse I2V.

Figure 8 : V2I / I2V

Lorsque deux véhicules sont proches une liaison directe est établie entre leurs OBU et les informations sont envoyées en un seul saut. Dans le cas où les voitures sont distantes l'une de l'autre, les informations envoyées passent du premier OBU vers une succession de RSU jusqu'à atteindre le deuxième OBU (V2I, I2I, I2V).

1.1.2.3 Domaine d'infrastructure (I2I)

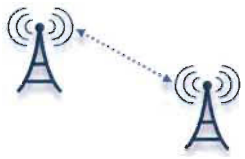

Figure 9 : I2I

C'est le réseau établi entre le RSU et un autre RSU ou avec d'autres infrastructures afin d'élargir la portée de communication.

1.1.3 Normes de communication

Le réseau VANET intègre plusieurs technologies de réseau Ad-Hoc comme le WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee, etc… Ceci pour rendre la communication facile, précise, efficace et simple entre les entités dotées de mobilité dynamique.

1.1.3.1 DSRC

DSRC (*Dedicated Short Range Communications*) est une communication sans fil (radio), spécialement conçue pour les systèmes de transport intelligents (ITS). C'est une allocation de 75MHz de la bande des 5.9GHz (de 5.85 à 5.925GHz) du spectre électromagnétique. Elle a une portée de 300m jusqu'à 1Km. Elle vise à fournir un transfert de données élevé de débit de 27Mbps avec une faible latence de communication dans les petites zones et avec une vitesse de déplacement de voitures atteignant les 200KmH [8, 9].

Les 75Mhz sont divisés en sept canaux de 10Mhz afin de fournir des services sans causer des interférences :

- Le canal 178 est appelé *control channel* (CCH), réservé aux communications de sécurité,
- Les canaux 172 et 184 appelés *service channel* (SCH), réservés aux applications de sécurité, quant aux autres (174, 176, 180, 182) ils sont réservés à des utilisations sécuritaires et non sécuritaires.

La catégorisation des canaux est illustrée dans la figure ci-dessous [10].

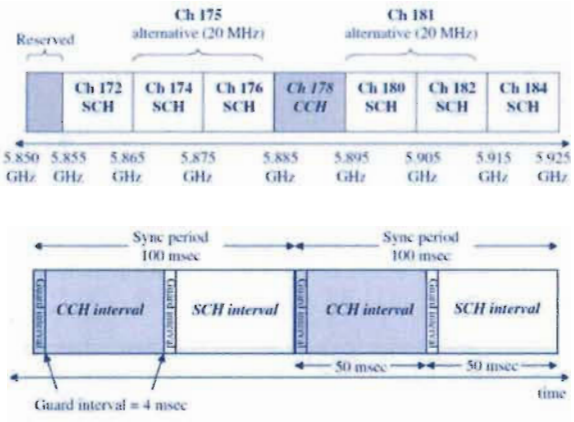

Figure 10 : Les canaux de la bande DSRC

Différentes normes de DSRC sont utilisées selon les pays :

- Aux USA allouées par FCC « Commission Fédérale des Communications » en 1999,
- En Europe allouées par ETSI « Institut européen des normes de télécommunication » en 2008,
- D'autre normes en Corée du sud et au Japon.

1.1.4 Architecture des couches du réseau VANET

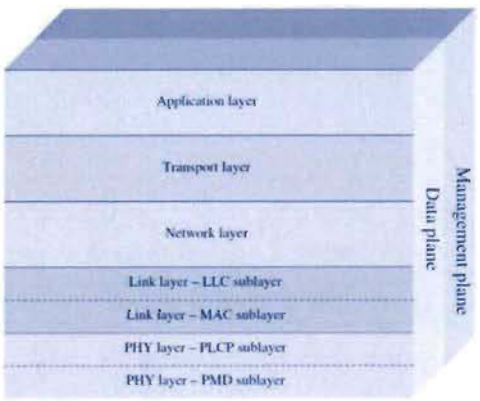

Figure 11 : OSI

L'*Open Systems Interconnection* (OSI), est une référence d'architecture contenant cinq couches qui séparent et décomposent le système pour favoriser l'extensibilité, la conception structurée et l'évolution technique[10].

– La couche PHY (Physical) est divisée en deux sous-couches :

- PMD (Physical Medium Dependent),
- PLCP (Physical Layer Convergence Procedure).

– La couche (*Data Link*) est aussi divisée en deux sous-couches :
  - MAC (Medium Access Control) ;
  - LLC (Logical Link Control).
– La couche Réseau,
– La couche Transport,
– La couche Application.

L'OSI est aussi divisé en deux couches verticales :

– La couche « Plans de données » représente les différents acteurs d'un réseau. Ils sont initiés par des applications et soutiennent directement la communication des données d'un utilisateur à un autre.
– La couche « Plans de gestion » est l'ensemble des actions entreprises pour gérer et entretenir le réseau. Ces actions comprennent les diagnostics, la synchronisation, la découverte et l'association de dispositifs voisins.

1.1.4.1 IEEE 1609 WAVE / IEEE 802.11p

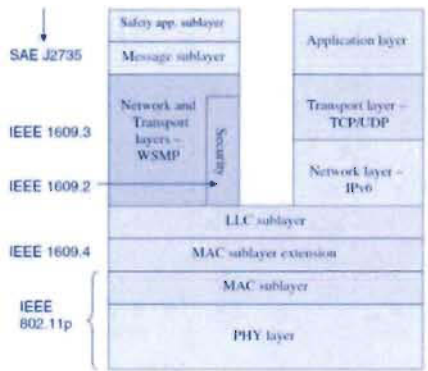

Figure 12 : Architecture de la norme IEEE 1609 WAVE

La norme IEEE 1609 WAVE (*Wireless Access in Vehicular Environments*) ou IEEE 802.11p est normalisée par l'*IEEE Standards Association,* où la norme populaire du réseau local sans fil (LAN) IEEE 802.11 a été modifiée et ajustée afin de prendre en charge les communications sur le spectrum du DSRC. En d'autres termes, la norme WAVE est constituée de l'ensemble des protocoles réservés aux communications établies sur la bande DSRC[10]. Ces protocoles sont regroupés comme suit :

1.1.4.1.1 La norme IEEE 1609-1

Faisant partie de la couche d'application, elle définit un gestionnaire de ressources RM (*Resource Manager*) qui permet à plusieurs applications exécutées par les RSU de communiquer avec les OBU des véhicules.

1.1.4.1.2 La norme IEEE 1609-2

Cette norme aborde les questions de sécurisation des messages WAVE contre l'espionnage, l'usurpation d'identité, et d'autres attaques. Les composants de l'infrastructure de sécurité IEEE 1609.2 sont basés sur les normes de la cryptographie à clé publique. Elle prend également en charge la cryptographie à courbe elliptique (ECC), les formats de certificats du WAVE et les méthodes de chiffrement hybrides. Ceci, afin de fournir des services sécurisés pour les communications WAVE (authenticité, confidentialité, intégrité, non-répudiation).

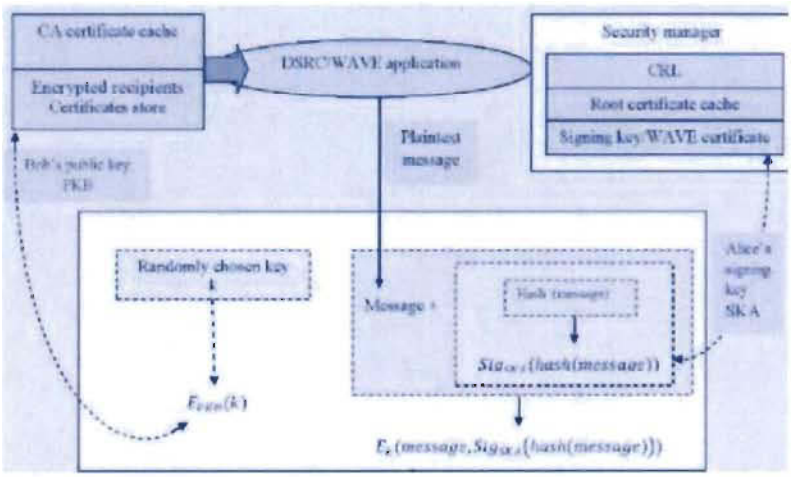

Figure 13 : les services de sécurité de la norme IEEE 1609.2

1.1.4.1.3 La norme IEEE 1609-3

Elle spécifie les services du réseau pour les communications incluant les protocoles qui couvrent la mise en place et la gestion des connexions WAVE. Elle définit aussi le *WAVE Short Message* (WSM) et le protocole d'échange associé *WAVE Short Message Protocol* (WSMP).

1.1.4.1.4 La norme IEEE 1609-4 pour la couche MAC

Le DSRC ne peut disposer que d'un seul canal à la fois. Pour utiliser des canaux multiples (172, 174, 176, 180, 182, 184), il est nécessaire de commuter dynamiquement de l'un à l'autre. Ce mécanisme requiert une organisation et une coordination distribuée des canaux dans le réseau, de sorte que les émetteurs et les récepteurs soient sur le même canal en même temps. Ces opérations de contrôle de commutation sont incluses dans la norme IEEE 1609-4.

1.1.5 Caractéristiques des réseaux VANET

Des caractéristiques essentielles doivent être assurées pour architecturer les réseaux VANET. Parmi celles-ci, nous citons[4, 11-15] :

1.1.5.1 Haute mobilité des nœuds

Une des caractéristiques du réseau VANET est que ses nœuds se déplacent à grande vitesse et d'une façon aléatoire. Cette contrainte de mobilité influence négativement la communication entre les nœuds. Les problèmes de connectivité qui en découlent rendent le traçage des nœuds difficile et ouvrent des failles dans la sécurité. Néanmoins le déplacement des voitures est régi par la morphologie et le code de la route. Ces paramètres facilitent la prédiction des trajectoires et les positions des véhicules.

1.1.5.2 Conduite sécurisée et confortable

Diverses applications ont été conçues pour le réseau VANET. Celles-ci visent à assurer :

- La sécurité routière aux conducteurs (alerter police et ambulance lors d'accidents) ;
- L'amélioration du trafic routier (informations météorologiques, embouteillages) ;
- Le confort des conducteurs et des passagers en leur donnant accès à différentes informations (internet, vidéos et jeux de distraction pour les enfants).

1.1.5.3 Pas de contrainte d'énergie

Les entités et les dispositifs intra-véhiculaires (OBU, GPS, TPD, etc...) disposent de capacités énergétiques suffisantes et continuelles qu'elles tirent du système d'alimentation des véhicules, levant ainsi la contrainte d'énergie.

1.1.5.4 Haute capacité de calcul

Un des points forts des réseaux VANET est la haute capacité de calcul qui peut améliorer la connectivité et accélérer le traitement des données, grâce aux différents dispositifs et capteurs ainsi que les composants électroniques installés dans les véhicules.

1.1.5.5 Dynamisme de la topologie

La topologie des réseaux VANET est très variable à cause la mobilité et la vitesse variable des nœuds. Cette topologie dépend de la connexion et déconnection établie entre les nœuds, et qui elle-même, dépend de deux facteurs distincts, la portée de connexion sans fil et le nombre de véhicules formant le réseau.

1.1.5.6 Variabilité de la densité

La variabilité de la densité du réseau est reliée à la densité du trafic routier. Le réseau est habituellement dense dans les zones urbaines, pouvant être saturé en cas d'embouteillage, et faiblement dense dans les zones rurales.

1.1.6 Limites et challenges des réseaux VANET

Le réseau VANET est en cours de développement. Il est actuellement le sujet de plusieurs recherches et études qui visent à résoudre ses limites et ses challenges[10, 16, 17], nous citons ici les plus importants.

1.1.6.1 Affaiblissement du signal

L'environnement a un impact sur la propagation du signal. Plusieurs obstacles comme les tunnels et les immeubles peuvent influencer la qualité du signal et l'empêcher d'atteindre ses cibles.

1.1.6.2 Congestion et priorisation des paquets

Les congestions de canaux sont fréquentes surtout dans les environnements très denses. Ceci a un impact sur le délai de transmission des messages en allongeant le temps de latence. Les données de type urgent sont priorisées dans ces cas-là.

1.1.6.3 Connectivité

La grande mobilité et le changement rapide de la topologie causent de fréquentes fragmentations dans le réseau, cependant, le temps de la connexion doit être maintenu et allongé. Ceci peut être réalisé par l'augmentation de la puissance de transmission et l'utilisation de protocoles ayant un bon délai de traitement.

1.1.6.4 Sécurité et anonymat

La réception d'informations qui prouvent l'identité d'une source expéditrice est un point essentiel pour le destinateur. Toutefois, ces informations peuvent violer la vie privée de l'expéditeur. Garder un bon équilibre entre la sécurité et l'anonymat est un des challenges majeurs du réseau VANET.

1.1.7 Conclusion

Les réseaux VANET sont une technologie prometteuse pour la mise en œuvre des systèmes de transports intelligents. Ces réseaux sont vulnérables à plusieurs attaques pouvant causer des pertes non seulement financières mais aussi humaines. Le déploiement des réseaux VANET dans la vraie vie est lié à leur sécurité. Il faut donc prévoir des algorithmes et des protocoles hautement sécurisés. Nous aborderons les grandes lignes de la sécurité dans la partie qui suit.

1.2 Sécurité des réseaux VANET

Le réseau VANET comme tous les réseaux et les systèmes informatiques, n'est pas immunisé contre les exploits. Dans cette partie, nous commencerons par décrire les profils des attaquants et les différentes attaques qui peuvent être réalisées à l'encontre du réseau VANET. Nous résumerons les exigences de la sécurité dans les réseaux VANET et nous finirons par introduire les notions de base en sécurité ainsi que les techniques de cryptographie utilisées dans le modèle de sécurité proposé.

1.2.1 Profils d'attaquants

1.2.1.1 Actif ou passif

L'attaquant passif ne fait qu'espionner ou écouter clandestinement sur le canal sans fil du réseau. L'attaquant actif quant à lui passe à l'action en altérant les messages qui circulent dans le réseau[2].

1.2.1.2 Interne ou externe

Un attaquant externe est un nœud non authentifié, ses accès sont limités. Il s'agit d'un intrus au réseau. Un attaquant interne est par contre un membre authentifié qui possède une clé publique ainsi que d'autres privilèges, ce qui lui donne la possibilité de causer plus de dommage dans le réseau qu'un attaquant externe[2].

1.2.1.3 Malicieux ou rationnel

Un attaquant rationnel œuvre pour des fins personnelles ce qui rend ses attaques plus prévisibles que celles du malicieux pour qui le but de nuire aux autres membres du réseau n'est pas pour assouvir des besoins personnels mais seulement pour le plaisir de créer un disfonctionnement[5, 18].

1.2.1.4 Indépendant et collaboratif

Les attaqueurs peuvent agir indépendamment ou en collaboration en coordonnant leurs actions, dans le but de rendre l'attaque plus puissante[2].

1.2.1.5 Local et étendu

Un attaquant peut avoir une portée d'action limitée due à la portée limitée des OBU et des RSU qu'il contrôle. Toute fois si les OBU et les RSU sont éparpillés dans le réseau les attaques vont être plus étendues[2].

1.2.2 Les types d'attaques

Les réseaux VANET peuvent être victimes de plusieurs attaques de différentes natures. Nous les classons ici selon leur cible [19] :

1.2.2.1 Attaques contre les messages

1.2.2.1.1 Attaque sur la cohérence de l'information

L'attaque sur la cohérence de l'information (*Bogus information attacks*) s'agit d'une transmission de fausses informations aux autres véhicules pour les inciter à changer de comportement ou pour causer des accidents[17].

1.2.2.1.2 Trou noir

Le trou noir (*Black Hole*) est une attaque formée lorsqu'un nœud refuse de participer au réseau, ou lorsqu'un nœud déjà formé est supprimé. Le nœud attaquant commence par inciter les nœuds à lui transmettre les messages en donnant l'illusion d'avoir le chemin le plus court vers le nœud destinataire ou vers le paquet qu'il veut intercepter. Une fois qu'il les a collectés il les supprime ou il supprime le nœud. Cela conduit à un échec de transmission et à la création d'un trou sur le réseau[20].

1.2.2.1.3 Attaque de l'homme du milieu

On parle d'attaque de l'homme du milieu (*Man in the Middle Attack MiM*) lorsqu'un nœud malveillant écoute la communication établie entre deux autres véhicules. Il prétend être chacun d'entre eux pour répondre à l'autre et il leur injecte de fausses informations[17].

1.2.2.1.4 Usurpation d'identité

L'usurpation d'identité (*Masquerading / spoofing*) a lieu lorsqu'un attaquant prétend être quelqu'un d'autre en usurpant l'identité d'un véhicule légitime. Cela lui permet

de recevoir les messages de la victime et de bénéficier de l'ensemble de ses privilèges [10, 17].

1.2.2.1.5 Attaque par rejeu

L'attaque par rejeu (*Replay attack*) a lieu lorsque l'entité malveillante utilise des paquets interceptés ou déjà reçus et les réinjecte à nouveau dans le réseau. Par exemple un attaquant peut utiliser d'anciens messages indiquant sa position, il les réinjecte dans le réseau pour empêcher les autorités d'identifier le véhicule lors d'un accident ou pour se faire passer pour un autre véhicule[17, 21].

1.2.2.1.6 Déni de Service

L'attaque DOS (*Denie of Service*) est définie comme étant le résultat d'une action qui empêche toute partie d'un réseau de fonctionner correctement ou en temps opportun. Son but est de rendre les services inaccessibles par les utilisateurs légitimes.

L'attaque DOS est d'abord malveillante car l'attaquant œuvre dans un but malveillant, elle est aussi perturbatrice vu qu'elle peut dégrader ou perturber les capacités du réseau ou ses services et elle est aussi réalisée à distance.

Elle peut être faite de plusieurs façons. Soit en brouillant le canal sans fil, en inondant le réseau de requêtes afin d'épuiser les ressources et de ralentir les services, ou en multipliant les attaques par différents nœuds malveillants (*DDoS attaque*).

Les attaques DOS sont classées selon P.G. Neumann en trois types basés sur la source de l'attaque :

- L'attaque se fait à distance sans aucune pénétration dans le réseau.
- L'attaquant exploite une certaine vulnérabilité pour pénétrer le réseau, puis accroit l'utilisation de ressources.
- L'attaquant pénètre dans de nombreux ordinateurs pour lancer une attaque DOS contre le réseau cible. Cette attaque est appelée DOS distribué (DDOS)[22].

1.2.2.1.7 Attaque temporelle

L'attaque temporelle (*Timing attack*), consiste à manipuler le contenu d'un message en lui rajoutant un Δ_t à son délai de transmission. Elle retarde ainsi la transmission

des données, pour que les paquets n'arrivent pas à temps aux véhicules destinataires[13].

D'autres attaques contre les messages peuvent exister telles que l'attaque d'illusion, d'analyse du trafic ou d'altération du trafic en transit.

1.2.2.2 Attaque contre les véhicules

1.2.2.2.1 Véhicule caché

En cas d'accident, le véhicule le mieux positionné est supposé diffuser le message d'alerte. Dans l'attaque de véhicule caché (*Hidden vehicle attack*) l'entité malveillante prétend être à la meilleure position pour émettre le message d'alerte en fournissant une fausse localisation[23].

1.2.2.2.2 Attaque par message indésirable

L'attaquant envoie aux conducteurs des messages nuisibles ou sans utilité tels que les *malwares* et les *spams*, dans le but d'augmenter le temps de latence et la consommation de la bande passante. Cette attaque est plus difficile à contrôler lors de l'absence d'une infrastructure de base et d'une administration centralisée[17].

1.2.2.2.3 Système de localisation mondial

L'attaquant peut altérer les informations des appareils GPS (*Global Positioning System*) placés sur les véhicules, faisant ainsi croire aux conducteurs qu'ils sont dans un endroit différent de là où ils sont réellement. Cette modification de données est possible grâce aux simulateurs de satellites GPS qui produisent des signaux plus forts que ceux générés par le véritable satellite[21].

1.2.2.2.4 Attaque de Tunnel

Dans cette attaque l'entité malveillante exploite la faille des signaux GPS qui faiblissent, voire même disparaissent lors d'un tunnel. L'attaquant exploite cette perte temporaire d'informations et injecte à son tour de fausses informations sur l'OBU du véhicule cible influençant ainsi son comportement avant qu'il ne reçoive une authentique mise à jour de sa réelle position [18].

1.2.2.2.5 Attaque trou de ver

L'attaque trou de ver (*Wormhole attack*) consiste à enregistrer les paquets à un endroit dans le réseau puis les réacheminer à un autre nœud complice dans le réseau par le biais d'un tunnel[23].

1.2.2.2.6 Écoute clandestine

L'attaque d'écoute clandestine (*Eavesdropping*) est l'une des attaques les plus importantes dans les réseaux VANET qui affecte la confidentialité des données. L'attaquant écoute illégitimement sur le canal de transmission et espionne les communications entre les nœuds. Il collecte ainsi les informations échangées afin d'utiliser ces données confidentielles pour son propre profit [13, 24].

1.2.2.2.7 Attaque Sybil

Dans cette attaque le nœud malveillant se présente comme étant plusieurs et distinctes entités, soit simultanément ou en des temps différents. Il peut ainsi envoyer plusieurs messages véhiculant de fausses informations grâces aux différentes identités créées. Il peut aussi présumer être en différentes positions en même temps ou essayer de convaincre un autre nœud de lui déléguer des tâches vu qu'il donne l'illusion d'être plusieurs nœuds à la fois. Cette attaque affecte les performances du réseau car les nombreux nœuds créés (ou les sybils) consomment la bande passante et endommagent la topologie du réseau [13, 18].

1.2.2.2.8 Altération des dispositifs embarqués

Parfois, il est plus facile de modifier et bipasser les câblages des capteurs ou le temps réel de l'horloge, plutôt que de modifier l'implémentation des codes[17].C'est ce qu'on appelle altération des dispositifs embarqués (*On-board tampering*).

1.2.3 Exigences de la sécurité

L'importance de la sécurité dans le réseau VANET est majeure pour les communications V2I et V2V. Elle repose essentiellement sur les paramètres critiques suivants[21] :

1.2.3.1 Authentification et identification

L'authentification garantie que l'expéditeur d'un message a bien été identifié. Elle permet de déterminer le niveau d'autorisation d'une entité et d'empêcher les attaques Sybil en attribuant une identité spécifique à chaque véhicule[5]. Le principe de confiance est l'une des exigences des applications de sécurité. En effet, l'authentification permet de s'assurer qu'un message a été reçu d'un nœud légitime. Sans l'authentification les nœuds malicieux peuvent injecter au réseau des messages contenant de fausses informations, ils créent ainsi la confusion. A l'inverse, avec l'authentification les nœuds vont simplement supprimer les messages provenant des entités malicieuses non authentifiées[2]. En pratique, l'authentification peut être assurée par la vérification de la signature du message en considérant que la relation entre l'identité et la signature a été préalablement vérifiée par le processus de l'identification ou ce qu'on appelle aussi ID-Authentification[25].

1.2.3.2 Non répudiation

La non répudiation permet d'empêcher les expéditeurs de nier d'être à l'origine de la création d'un message. Cette propriété est importante lors d'un accident ou d'une injection de fausses informations car certaines applications de sécurité nécessitent le retracement des messages envoyés et la reconstitution d'une partie de l'historique des échanges de données établis entre les nœuds [4, 26].

1.2.3.3 Intégrité

L'intégrité garantie que les données qui ont été sauvegardées ou celles échangées entre un expéditeur et un destinataire sont protégées de toute altération perte ou destruction causée par un tiers malveillant. L'intégrité est souvent assurée par la signature numérique qui inclut le processus de hachage [27, 28].

1.2.3.4 Confidentialité

La confidentialité assure que les données qui transitent sur le réseau ne sont pas interceptées illégalement par des tiers malveillants. Aussi l'accès au contenu des messages ou à des informations confidentielles tels le nom et le matricule du véhicule est strictement restreint aux nœuds autorisés[27, 28]. Cette propriété est

assurée par différentes méthodes de cryptographie. L'expéditeur du message le crypte avec la clé publique du destinataire qui lui le décrypte avec sa clé privée.

1.2.3.5 Disponibilité

La disponibilité signifie que chaque nœud peut envoyer l'information en tout temps. Elle garantit que les messages arrivent aux destinataires et que le réseau reste disponible même en cas d'attaque. C'est une des exigences de sécurité les plus importante car les réseaux VANET sont souvent cibles des attaques DoS. Elle est aussi difficile à assurer à cause de la haute mobilité des nœuds[18, 29].

1.2.3.6 Anonymat ou vie privée

La sécurité doit veiller à ce que les informations sensibles des conducteurs ne soient pas divulguées à de tierces personnes. Cependant, en cas d'attaque ou de problème majeur les autorités de confiance doivent être en mesure de tracer les messages et de connaître l'identité réelle et la position de l'entité malveillante[30].

1.2.3.7 Contrôle d'accès

Déterminer les droits et les privilèges de chaque nœud permet de protéger l'accès aux informations, qui lui doit être contrôlé en tout temps. Cette propriété permet d'assurer la fiabilité et la sécurité du système. Elle vérifie que les ressources sont disponibles seulement pour les entités légitimes et selon les privilèges qui lui sont associés[5].

1.2.3.8 Contrainte de temps

Les messages doivent arriver aux conducteurs à temps, puisque plusieurs applications liées à la sécurité en dépendent. Cette contrainte de temps doit être maintenue même si les véhicules roulent à grandes vitesses. Citons pour exemple les informations météorologiques ou les messages d'avertissement ou pour la prévention d'un accident ne doivent pas arriver en retard pour que le conducteur puisse anticiper[2, 30].

1.2.4 Notion de base en sécurité

1.2.4.1 Certification

1.2.4.1.1 Certificats numériques

C'est une structure de données (fichier électronique) qui permet de relier une clé publique à son possesseur afin de garantir l'authenticité des entités et de délivrer les clés d'une façon sécurisée. Un certificat est validé, signé et émis par un tiers de confiance appelé autorité de certification[31]. Il se compose de [32]:

- Numéro de série du certificat,
- Durée de validité,
- Nom de l'entité qui possède la clé publique,
- Clé publique qui est liée à l'entité,
- Algorithme de chiffrement,
- Le nom de la CA qui l'a publié,
- Restrictions d'utilisation de la clé publique.

1.2.4.1.2 Autorités de confiance CA / TTP

CA (*certificate authority*) ou TTP (*Trusted third party*) est une infrastructure centrale qui joue le rôle d'un tiers de confiance afin de signer et de délivrer les certificats. La CA peut être une agence gouvernementale ou une organisation certifiée par le gouvernement qui certifie et signe son propre certificat. Elle est aussi responsable de la révocation des certificats émis au cas où ces derniers sont compromis[10].

1.2.4.1.3 Liste des révocations

C'est une liste qui contient les certificats révoqués comme ceux qui ont expiré ou ne sont plus fiables. Cette liste est signée afin de prouver son authenticité. Il existe deux types de CRL (*Certificate Revocation List*), la CRL directe qui ne contient que les certificats révoqués d'un seul émetteur et la CRL indirecte qui contient la liste des certificats révoqués de différents émetteurs. Le problème que pose la CRL est que sa taille augmente à chaque mise à jour vu qu'on ne supprime jamais un certificat révoqué. Ceci induit un dépassement de capacité et la surcharge de la bande passante

lors du parcours de la liste. Afin de remédier à cela différentes approches ont été élaborées :

- Liste différentielle ou la Delta CRL : Cette liste répertorie seulement les certificats ajoutés après la dernière mise à jour de la CRL. Ces listes sont numérotées afin de faciliter la recherche aux nœuds.
- Partitionnement de la CRL : Dans cette approche la liste de certificats révoqués est partitionnée en K-listes dès qu'un certain seuil ou nombre de certificats est atteint. L'ajout d'un indicateur dans le certificat est nécessaire pour trouver la partition à laquelle ce dernier sera attribué lors de sa révocation [10, 32] .

1.2.4.2 Cryptographie symétrique et asymétrique

La cryptographie est un ensemble de méthodes utilisées pour chiffrer ou crypter des données afin d'assurer la confidentialité des informations envoyées. Deux types de cryptographie existent. La cryptographie symétrique et la cryptographie asymétrique [31].

1.2.4.2.1 Cryptographie symétrique

Dans cette approche une seule clé est utilisée pour le chiffrement et le déchiffrement des messages.

1.2.4.2.2 Cryptographie asymétrique

Dans cette approche deux clés sont utilisées :

- La **clé publique** de A est partagée avec tout le monde. Tous les utilisateurs peuvent envoyer des messages chiffrés à l'utilisateur A avec cette clé publique.
- La **clé privée** de A est gardée secrète, elle n'est connue que par A. Il est le seul à déchiffrer les messages qu'il reçoit via cette clé.

Il doit être impossible de déterminer la clé privée à partir de la clé publique.

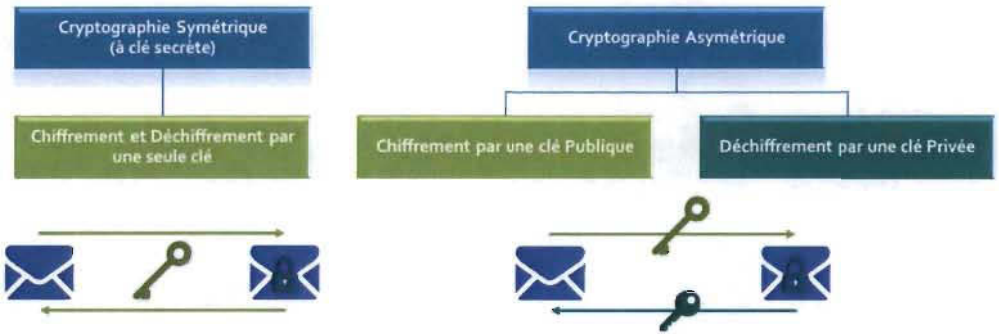

Figure 14 : Cryptographie symétrique et asymétrique

1.2.4.3 Signature numérique

La signature numérique est un procédé de sécurité qui permet d'identifier l'expéditeur d'un message. Elle est analogue à la signature manuscrite sur papier. C'est un mécanisme de base qui permet la mise en œuvre de l'authentification des messages et de l'intégrité des données. Chaque nœud expéditeur signe numériquement son message avant de l'envoyer et chaque nœud récepteur vérifie la signature du message qu'il a reçu. La signature numérique repose sur une fonction mathématique appelée fonction de hachage. Cette fonction génère une empreinte « hash » du message qui sera chiffré par la suite avec la clé privée. Le principe est de signer un message de taille plus petite que l'original[33].

1.2.4.4 Fonction de hachage

La fonction de hachage H est une fonction mathématique qui prend en paramètre un message M de taille quelconque. Elle retourne une empreinte h ou un hash du message qui n'est rien d'autre que le message d'origine compressé.

$$h = H(M) \text{ Où } \begin{cases} h : empreinte\ ou\ le\ hash\ du\ message \\ H : fonction\ de\ hachage \\ M : message\ d'origine \end{cases}$$

La fonction de hachage doit avoir les propriétés suivantes :

- **Résistance à la pré-image** : Il est facile de calculer le hash d'un message en appliquant la fonction de hachage mais il est extrêmement difficile de déduire le message d'origine à partir du hash. Cette propriété reflète l'irréversibilité du calcul de l'empreinte.

- **Résistance à la seconde pré-image** : Etant donné un message M_1, il est difficile de trouver un autre message M_2 ayant le même hash. Aussi, le moindre changement dans le message d'origine engendre un changement dans le hash.
- **Résistance aux collisions** : C'est difficile de trouver deux messages différents $M_1, M_2 \; / \; M_1 \neq M_2 \; et \; H(M_1) = H(M_2)$ [34].

1.2.4.5 Schéma de cryptographie

1.2.4.5.1 Algorithme de hachage dans les signatures numériques

Les algorithmes de hachage peuvent être utilisés conjointement avec les algorithmes à clé publique pour la génération d'une signature numérique. Ces algorithmes sont utilisés pour vérifier l'intégrité des données reçues. Si BOB veut envoyer un message à Alice il commence par :

- Générer une empreinte du message via la fonction de hachage, en d'autres termes réduire la taille du message.
- Crypter le hash grâce à sa clé privée. Le résultat obtenu est considéré comme étant la signature de Bob.
- Envoyer le message original ainsi que la signature à Alice.

Dès qu'Alice reçoit le message elle vérifie son authenticité, pour cela elle procède comme suit :

- Décrypter la signature reçue via la clé publique de Bob et obtenir ainsi la valeur du hash de Bob noté h_1.
- Appliquer la fonction de hachage que Bob a utilisée pour condenser le message original. Le résultat obtenu est noté h_2.
- Comparer l'empreinte calculée h_2 avec h_1.
- $Si \; h_1 = h_2 \Rightarrow$ le message n'a pas été altéré d'où son authenticité [34].

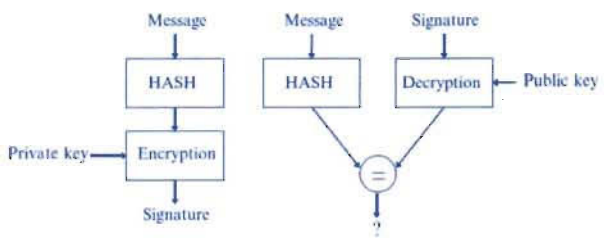

Figure 15: Principe de la signature numérique

1.2.4.5.2 PKI

Le PKI (***Public Key Infrastructure***) repose sur la cryptographie à clé publique. Il comprend une autorité de certification, une autorité d'enregistrement, des répertoires pour lister les certificats ainsi qu'un système de gestion de ces derniers. Cette infrastructure utilise deux clés différentes, où chaque clé est utilisée pour une opération bien précise. La clé privée est réservée au chiffrement et la publique est dédiée à l'opération de déchiffrement. Il est à préciser que la clé de chiffrement est rendue publique dans cet algorithme car on ne peut déterminer la clé de décryptage à partir de la clé de cryptage. Le déroulement de cet algorithme est décrit plus amplement dans la partie qui suit[31, 32].

Pour chaque utilisateur la CA génère les deux clés, publique et privée simultanément. Elle délivre la clé privée à son propriétaire et garde la clé publique dans sa base de données pour la partager.

Supposons qu'Alice veut envoyer un message à Bob. Elle demande la clé publique de Bob à la CA. La CA va par la suite confirmer l'identité du propriétaire (Bob) et s'assure que c'est bien sa clé. D'un autre coté elle vérifie si cette clé n'est pas révoquée et finalement elle la délivre à Alice. Par la suite Alice utilise cette clé publique (de Bob) pour crypter le message puis elle l'envoie à Bob. Ce dernier décrypte le message avec sa clé privée.

Cependant, l'infrastructure à clé publique présente certains inconvénients qui se résument dans les deux points suivants :

- Plus le nombre d'utilisateurs croît plus la capacité de stockage pose problème,
- Plus le nombre d'utilisateurs croît plus l'utilisation des ressources pour la gestion des CRL augmente [27].

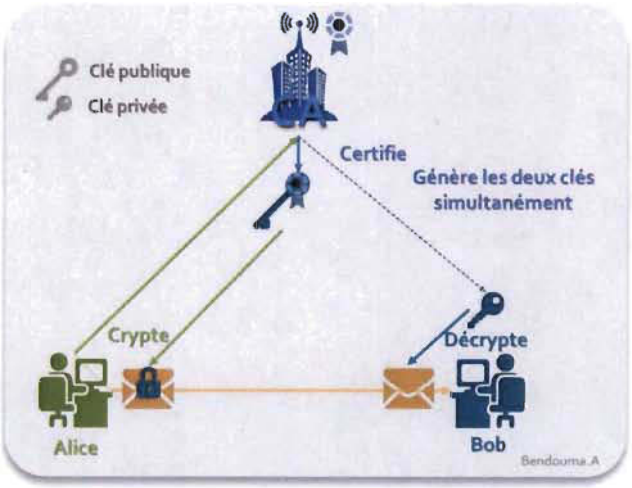

Figure 16 : Infrastructure à clé publique

1.2.4.5.3 Id-Based Encryption

En 1984 Shamir propose un nouveau concept de cryptographie basé sur l'identité. Il s'agit d'une méthode qui repose sur le principe du chiffrement asymétrique.

Le PKG (Private key generator) appelé aussi TTP (Third Trusted Party) est une tierce personne de confiance qui se charge de générer les clés à partir des identifiants (ID) dans l'ID-based Encryption. La clé publique d'un utilisateur peut être extraite à partir de certaines de ses informations d'identification, uniques et publiques comme le SSN, ou l'adresse e-mail. Elle est utilisée pour signer et vérifier les messages. Chaque utilisateur a un identifiant unique, en premier temps, il s'authentifie au niveau du PKG pour avoir sa clé privée.

Supposons qu'Alice veut envoyer un message à Bob :

- Elle utilise sa clé publique préalablement générée pour signer le message,
- Elle envoie l'ID de Bob au PKG à partir duquel il va générer la clé publique de Bob en deuxième temps,
- Alice utilise cette clé publique (celle de Bob) pour crypter le message, puis elle l'envoie,
- Bob envoie l'ID d'Alice au PKG à partir duquel il va générer la clé publique d'Alice,
- Bob utilise cette clé publique (celle d'Alice) pour vérifier si le message a bien été signé par Alice,

- Bob utilise sa clé privée pour décrypter le message [33, 35].

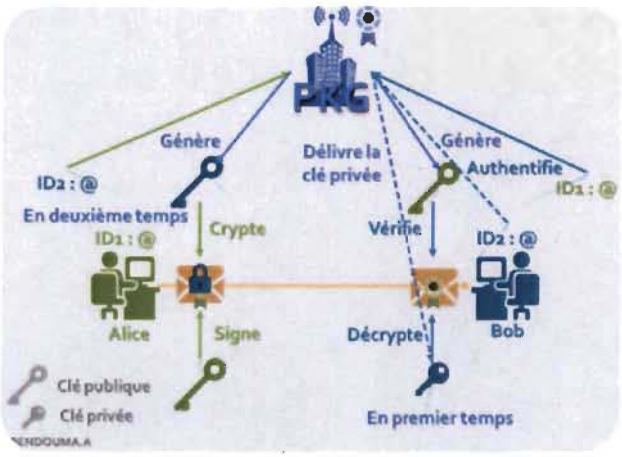

Figure 17 : Cryptographie basée sur l'identité

1.2.4.5.4 Comparaison entre PKI et IBC

Chaque schéma de cryptographie a ses propres caractéristiques. Nous les listons et les comparons dans le tableau ci-dessous [35].

Tableau 1 : Comparaison entre le PKI et l'IBC

PKI	ID-Based Cryptography
Chiffrement symétrique	Chiffrement asymétrique
Les clés publiques et privées sont générées simultanément	Les clés publiques et privées sont générées en deux temps différents
Les clés sont générées par la CA	Les clés sont générées par le PKG
La CA génère les clés et les stocke	Le PKG génère les clés à partir des identificateurs IDs
La CA certifie les clés	Les utilisateurs signent et vérifient les messages à l'aide de la clé publique

1.2.4.6 Échange de clés Diffie-Hellman (DH et ECDH)

Les deux parties souhaitant communiquer entre elles, se mettent d'accord sur deux nombres a et p tel que $1 \leq a < p$, p doit être un nombre premier suffisamment grand. Ces deux nombres sont choisis publiquement et ne doivent pas être secrets.

Elles passent ensuite au calcul de la multiplication de la valeur de a par elle-même, un certain nombre de fois. Soit n_1 pour l'un et n_2 pour l'autre. Il est aussi à préciser que les deux nombres n_1 et n_2 doivent être choisis secrètement.

Le $y_1 = a^{n1} mod\ p$ calculé par l'entité 1 est envoyé à l'entité 2 et le $y_2 = a^{n2} mod\ p$ est envoyé à l'entité 1. Cet échange se fait aussi publiquement.

La dernière étape consiste à calculer la clé secrète K_s par les deux entités parallèlement. Où $K_s = y_1^{n_2} = a^{n_1 n_2} mod\ p = y_2^{n_1} = a^{n_2 n_1}\ mod\ p$

Cette méthode permet le calcul d'une clé secrète commune et assure que même si une tierce personne espionne la communication, elle ne peut procéder au calcul de la clé secrète K_s en possédant les valeurs de $a, p, y_1 et\ y_2$ ce qui est connu par le problème de l'algorithme discret[25, 33].

L'échange de clés Diffie-Hellman basé sur les courbes elliptiques (ECDH) suit le même raisonnement mais consiste à choisir les deux points qui représentent les clés privée et publique sur une courbe elliptique.

Une des failles du Diffie-Hellman est que les deux entités communicantes doivent être connectées en même temps pour pouvoir choisir les paramètres et s'échanger les valeurs calculées. Par contre, dans les réseaux véhiculaires VANET, les RSU sont en tout temps disponibles et connectés. Aussi cet algorithme ne permet pas l'authentification à cause de l'absence de la signature dans les messages échangés. De ce fait, nous avons décidé de le fusionner à l'algorithme ECDSA.

1.2.4.7 ECDSA

L'algorithme ECDSA (*Elliptic Curve Digital Signature Algorithm*) est un algorithme de signature numérique qui se compose de deux parties distinctes. La première consiste en la génération de la clé publique et de la clé secrète, la deuxième concerne le calcul de la signature du message comme suit [36-40]:

Partie 1 : Génération de la signature

1) Choisir un point K_s aléatoirement où $1 \leq K_s \leq n - 1$ où n est un nombre entier,
2) Calculer $K_{pub} = K_s \times G$ où G est un point de la courbe elliptique E $(G \in E)$

3) Soit K_{pub} la clé publique et K_s la clé secrète.

Partie 2 : Génération de la signature

1) Choisir un nombre entier d aléatoirement où $1 < d < n - 1$
2) Calculer le point $(i, j) = d \times G$
3) Calculer $x = entier\ (i)\ mod\ n$
4) Si $x = 0$ revenir à l'étape 1
5) Calculer $y = d^{-1} \times (h(m) + K_s \times x)\ mod\ n$ où $h(m)$ est le résultat de la fonction de hachage ayant comme paramètre le message m à signer. Dans notre cas c'est le SHA-256 qui a été utilisé.
6) Si $y = 0$ revenir à l'étape 1
7) Finalement la signature est la paire (x, y).

1.2.5 Conclusion

Dans la première partie de ce chapitre, nous avons présenté les réseaux VANET, leurs entités et leur architecture afin de donner une vue globale du sujet étudié. Dans la seconde partie, nous avons discuté les attaques dont les réseaux VANET sont victimes. Nous avons donné également un aperçu des bases de la sécurité et leurs applications dans les réseaux VANET.

Dans le prochain chapitre nous présenterons les différents scénarii de sécurité issus de la littérature qui explorent le domaine de la sécurité et de l'authentification dans les réseaux VANET.

CHAPITRE 2

ÉTAT DE L'ART

2.1 Introduction

Plusieurs recherches ont été proposés dans le domaine de la sécurité des réseaux véhiculaires ces derniers temps. Dans le présent chapitre, nous listons des études qui portent sur l'authentification des entités du réseau VANET et nous introduisons globalement les différents algorithmes et approches de sécurité utilisées, ainsi que leurs forces et leurs limites.

2.2 L'authentification dans les réseaux VANET

Raya et Hubaux, ont montré que l'algorithme RSA créé en premier lieu par Shamir, est un algorithme de cryptographie robuste, qui procure un haut niveau de sécurité. Toutefois, en raison de la grande taille des clés générées, le système prend beaucoup d'espace de stockage et nécessite énormément de temps pour le processus de chiffrement / déchiffrement. Ces demandes affecteront négativement la bande passante et le temps de transmission du message, ce qui rend le schéma RSA inapproprié pour les réseaux VANET notamment lorsque le message est volumineux. D'un autre côté, Raya et Hubaux ont montré que l'algorithme de courbe elliptique (EC) génère des clés plus courtes et prend moins de temps pour exécuter les tâches de cryptage et de décryptage. Ce qui le rend plus approprié pour les réseaux VANET [23].

Jonathan Petit a implémenté dans le cadre de son travail, l'algorithme d'authentification ECDSA dans les réseaux VANET et a exploré ses dépassements de capacité. Il a analysé la variable « complexité du temps » ainsi que le délai de traitement de cet algorithme. Il a proposé également quelques techniques pour réduire les dépassements de capacité, comme l'utilisation d'une clé de taille P-224 à la place de P-256 afin de minimiser le retard de transmission de données [37].

Vijayabharathi et Malarchelvi ont mis en œuvre le protocole EMAP (Expedite Message Authentication Protocol) pour assurer l'authentification. Leur travail repose aussi sur l'utilisation du Hash Message Authentication Code (HMAC) dans le réseau VANET. Ils ont utilisé un processus de vérification de la liste de révocation, plus rapide, donc plus efficace que les anciennes méthodes. Leur protocole d'authentification leur a permis de réduire le temps de calcul et de prévenir par la suite les problèmes de dépassement de capacité [41].

Sakhreliya et Pandya sont venus avec une nouvelle conception du PKI (Public Key Infrastructure) pour le processus d'authentification. Ils ont mis en œuvre cette infrastructure en utilisant la cryptographie à clé symétrique (PKI-SC), ce qui leur a permis de réduire le temps de traitement et d'empêcher les dépassements de capacité du CPU pour l'authentification. Ils ont également fait une comparaison entre les algorithmes ECDSA et MAC. Leurs simulations ont prouvé que la génération de messages dans PKI-SC ne prend que 26 us comparée à 2 ms dans l'ancien PKI. De plus, la vérification des messages ne prend que 26 us contre 5 ms dans l'ancien PKI [42].

En 2007, Calandriello et al. A proposent un mécanisme d'authentification par pseudonyme pour les réseaux VANET. Ce mécanisme a réduit à son tour les dépassements de capacité et a conservé la robustesse de la sécurité du transport tout en permettant aux OBU des véhicules de générer leurs propres pseudonymes sans surcharger le système de sécurité [43].

En 2008, Zhang et al. ont introduit la notion de RSU-AIDED, un système d'authentification de messages assisté par un RSU qui à son tour délègue la vérification de l'authenticité des messages envoyés par les véhicules aux autres RSU. Le schéma montre un faible taux de perte de message et un retard de message[44].

En 2011, Huang et al. A proposent un schéma qui repose sur le principe d'authentification basé sur un pseudonyme de confidentialité conditionnelle appelé

(PACP). Ce système permet aux véhicules des réseaux VANET d'utiliser des pseudonymes au lieu de leur véritable identité afin d'offrir et d'assurer l'anonymat des nœuds du réseau véhiculaire[45].

L'ensemble des travaux précédents n'étudient pas l'authentification du RSU. Les chercheurs ont utilisé aussi des listes de révocation pour gérer les certificats ou / et les pseudonymes qui utilisent et consomment énormément d'espace de stockage et demandent plus de temps de traitement et de calcul informatique, los du processus de vérification. Cela a souvent induit des coûts au niveau des ressources et a affecté le délai et le taux de perte de message etc.

En 2009, Studer et al. ont utilisé des clés temporaires anonymes certifiées (TACK) pour concevoir leur système de gestion de clés dans les réseaux véhiculaires. Ce système leur a permis d'empêcher les intrus ou les nœuds malveillants, de lier les différentes clés d'un véhicule à l'identité réelle ou au lieu exact du conducteur. Leurs résultats démontrent aussi que le schéma proposé permet de gérer la révocation en temps opportun sans causer la surcharge de la communication [46].
L'étude précédente n'étudie pas l'authentification du RSU et les auteurs ont utilisé des listes de révocation pour gérer des certificats ou des pseudonymes en utilisant plus d'espace de stockage et plus de temps de traitement pour l'authentification pouvant induire des rallongements dans le délai de message et une augmentation dans le taux de perte de message.

En 2009, Zhang et al. sont venus avec l'idée du protocole d'authentification de groupe décentralisé. Ils ont modifié l'architecture du réseau véhiculaire en retirant l'autorité centrale et en déléguant la gestion en permanence aux RSU. Les résultats ont démontrés que le schéma proposé ne dégrade pas de façon significative les performances du réseau lorsque plus de véhicules rejoignent le réseau [47].
La décentralisation du réseau en déléguant le travail d'autorité centralisée au RSU est une bonne idée, mais le schéma proposé ne prend pas en compte que le RSU peut lui aussi être compromis.

En 2011, Hao et al. ont développé des protocoles de sécurité capables, non seulement de détecter les RSU compromis mais aussi de détecter leurs nœuds malveillants en collusion. Dans ce schéma, les auteurs ont fait en sorte que chaque véhicule vérifie seulement une partie des messages afin de réduire la surcharge causée par le dépassement de capacité lors des calculs. Cela en utilisant un autre protocole celui qui permet le contrôle d'accès aux supports [48].

La vérification d'une partie des messages envoyés n'est pas un solide schéma de sécurité, car il y a une probabilité de passer outre et de ne pas détecter un RSU compromis. Sachant que dans les normes, ECDSA est recommandé comme algorithme de signature numérique dans le réseau VANET, ils ne l'ont pas utilisé même s'il peut présenter des performances plus rapides.

2.3 Conclusion

Sachant que les études sur l'authentification des RSU dans les réseaux VANET sont rares et très limitées et que l'utilisation des certificats et des listes de révocations engendrent des dépassements dans les capacités de stockage et dans les temps de traitement, substituer l'autorité de confiance par le RSU, sans en assurer l'authentification, résout les problèmes des délais et du stockage mais n'assure pas une sureté fiable, car le RSU peut être compromis à son tour, d'où l'intérêt d'assurer l'authentification du RSU. Toutefois, le schéma de sécurité doit se baser sur des algorithmes rapides qui garantissent un réseau plus fluide. Nous allons donc proposer un schéma de sécurité, sans une tierce autorité de confiance, sans les certificats et sans les listes de révocation, où, chaque RSU identifié se porte garant de la vraie identité de son voisin. Quant au véhicule, il pourra vérifier la signature du message envoyé par le RSU en utilisant un algorithme de signature numérique.

CHAPITRE 3
OBJECTIFS ET METHODOLOGIE

3.1 Objectif

Dans le cadre de ce mémoire, nous avons proposé d'une part un schéma de sécurité sans une tierce autorité de confiance, où, chaque RSU garantit l'identification du RSU voisin et d'une autre part l'authentification du message du RSU expéditeur par le véhicule via le processus de signature et de vérification de signature. Pour y parvenir, nous avons défini deux objectifs :

- Tout d'abord, assurer l'identification du RSU par un algorithme *Elliptic Curve Diffie-Hellman* (ECDH) où le véhicule confirme que les deux voisins RSU ont le même secret partagé,
- Deuxièmement, le véhicule authentifie le message préalablement signé par le RSU, en utilisant l'algorithme de signature numérique sur courbe elliptique (ECDSA).

3.2 Méthodologie

Notre schéma de sécurité se base sur deux algorithmes, l'algorithme d'échange de clés ECDH et l'algorithme de signature numérique ECDSA. Tous les deux s'appuient sur le concept des courbes elliptiques qui leur confère plus de rapidité de traitement comparé à leurs semblables non basés sur les courbes elliptiques. Le fonctionnement des deux algorithmes est résumé dans les paragraphes qui suivent.

3.2.1 ECDH

L'ECDH assure un échange de clés sécurisé sans passer par un transfert de la clé dans le réseau faisant ainsi échouer toute tentative d'interception.
Chaque paire de "*RSU* voisins" appliquent l'algorithme ECDH :

- Ils choisissent secrètement deux clés privées (points) $r1$ et $r2$ à partir de la même courbe elliptique E,

- Ils calculent leurs clés publiques $R1$, $R2$ en multipliant la clé privée par G, le point générateur de la courbe ($R = r \times G$),
- Ils échangent leurs clés publiques calculées,
- Ils calculent le secret partagé $Ss1$, $Ss2$ ($Ss1 = r1 \times R2$, $Ss2 = r2 \times R1$).

3.2.2 ECDSA

L'ECDSA assure l'authentification, la non-répudiation et l'intégrité des messages envoyés où des signatures uniques sont produites par l'expéditeur pour chaque message et sont vérifiées par le destinataire.

Le processus de signature ECDSA du message envoyé par le RSU au véhicule est le suivant :

- Chaque RSU génère ses propres clés publique ($Kpub$) et privée (Ks), sur une courbe elliptique prédéfinie.
- Chaque RSU génère une signature en utilisant la clé privée (Ks), la fonction de hachage h (m) et le message m à envoyer.

3.2.3 Schéma de sécurité proposé

Le schéma proposé assure une agrégation d'identification des RSU en s'appuyant sur des zones d'interaction sans l'intervention d'un tiers de confiance :

- Le véhicule signale sa présence dans la zone d'interaction, en envoyant un message Beacon et il demande un secret partagé.
- Les deux RSU concernés appliquent un schéma ECDH et chacun envoie son secret partagé au véhicule pour qu'il confirme que les RSU sont fiables.
- L'authentification du RSU est assurée par l'ECDSA.

La communication entre le RSU et le véhicule est réalisée comme suit :

- Chacun des deux "RSU voisins" envoie son secret partagé Ss au véhicule et un message signé par l'algorithme ECDSA,
- Le véhicule compare les deux secrets partagés reçus $Ss1$, $Ss2$. S'ils sont égaux ($Ss1 = Ss2$), les RSU sont identifiés comme étant des entités fiables.

- Le véhicule vérifie la signature ECDSA en utilisant la clé publique du RSU ($Kpub$), la fonction de hachage h (m) et le message.

Dans le chapitre suivant, nous présentons notre papier soumis à la conférence **IEEE International Conference on Communications 21-25 May 2017 // Paris // France, IEEE ICC 2017 Mobile and Wireless Networking.**

CHAPITRE 4
ARTICLE SCIENTIFIQUE

Résumé : Le réseau ad-hoc véhiculaire (VANET) est une innovation qui modifiera notre vision du trafic routier et qui améliorera la sécurité et l'efficacité du transport. VANET représente une cible pour les attaques, qui peuvent causer des pertes humaines et matérielles. Cela souligne la nécessité d'un système de sécurité robuste, qui doit sécuriser efficacement les communications entre les véhicules et le reste des entités du réseau, mais doit également garantir la disponibilité et la fluidité de la transmission.

Notre schéma de sécurité vise à assurer l'identification, l'authentification, la non-répudiation et l'intégrité de l'unité de bord de route (RSU) lors de la transmission des messages du (RSU) aux véhicules (R2V). Une agrégation d'identification sera réalisée par plusieurs RSU et sans l'intervention d'un tiers de confiance.

Notre algorithme assure d'abord l'identification des RSU par l'algorithme Elliptic Curve Diffie-Hellman (ECDH) où le véhicule vérifie que les deux RSU voisins ont le même secret partagé, ensuite, le véhicule procède à l'authentification du message préalablement signé, en utilisant l'Elliptic Curve Digital Signature (ECDSA). Pour les simulations nous avons utilisé l'environnement combiné OMNET ++, SUMO et VEINS, et nous avons intégré la bibliothèque Crypto++ afin d'atteindre les exigences de sécurité. Le modèle que nous avons proposé parachève une plus haute sécurité.

Mots-clés : réseau sans fil ; VANET ; Sécurité ; ECDSA.

Article présenté à la conférence IEEE International Conference on Communications 21-25 May 2017 // Paris // France, IEEE ICC 2017 Mobile and Wireless Networking.

Numéro de papier : 1570321205.

IEEE ICC 2017 Mobile and Wireless Networking

RSU authentication by aggregation in VANET using an interaction zone

Amina Bendouma

Laboratoire de Mathematiques et Informatique Appliquées (LAMIA)
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres
Trois-Rivières, QC, Canada
amina.bendouma@uqtr.ca

Boucif Amar Bensaber

Laboratoire de Mathematiques et Informatique Appliquées (LAMIA)
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres
Trois-Rivières, QC, Canada
Boucif.Amar.Bensaber@uqtr.ca

***Abstract*—Vehicular ad-hoc network (VANET) is an innovation that will change our vision of road traffic, it will improve the safety and the efficiently of transport. VANET represent a target for attacks that can cause human and material losses. This, highlights the need for a robust security system, who must secure effectively communications between vehicles and the different network's entities, but also, it must guarantee availability and fluidity in the transmission.**

Specifically, in transmission of messages from Road Side Unit (RSU) to vehicle (R2V), our security aims to ensure identification, authentication, non-repudiation and integrity for the RSU. An aggregation of identification will be achieved by multiples RSU and without asking for the intervention of a trusted third party.

In this paper, we proposed a security schema to firstly ensure identification for RSU by an Elliptic Curve Diffie-Hellman (ECDH) algorithm where the vehicle confirms that the two neighbours RSU have the same shared secret, then secondly the vehicle authenticates the message beforehand signing, using Elliptic Curve Digital Signature Algorithm (ECDSA). To simulate the vehicle scenario, we used the OMNET++, SUMO and VEINS combined environment, and we integrated on it the Crypto++ library to achieve the security requirement. Our proposed model ensures stronger security.

***Keywords*—Wireless network; VANET; Security; ECDSA.**

I. INTRODUCTION

VANET is characterized by mobile nodes moving at high speed and exchanging information in wireless environment, while the network topography changes continuously and rapidly. Moreover, one of his assets is the high capacity energy and the powerful computing of the nodes [1-3].

The VANET is basically constituted of two distinct entities, the vehicle and the road-side unit (RSU). The vehicle integrates an on-board unit (OBU), a wireless device that allows the transmission of data between vehicles or between vehicles and RSU through the Dedicated Short Range Communication (DSRC) radio [1-4].

DSRC is a wireless communication based on IEEE 802.11p designed for intelligent transport system (ITS), in order to allow high data transfer (more than 27Mbps) with low latency. It works in 5.9GHz band with bandwidth of 75MHz and have a range of 300-1000m [5, 6].

We distinguish three modes of communication that can be identified in VANET. The first mode is established between two vehicles using their OBU (V2V), the second is between two infrastructures (R2R) and the third is between vehicle and infrastructure (V2R) [4] as shown below in Fig. 1. The communication can be done directly as one-hop or indirectly by retransmitting the message until it reached the final destination as multi-hop [7].

Fig 1 : VANET architecture and communication

For all this communications, the security system implemented in VANET have to grantee privacy, integrity, authentication and non-repudiation [7].

The authentication ensures that a message was received from a legitimate node [1]. This is achieved by the verification of the message signature. This last also certifies the non-repudiation, by preventing the entities to deny being the sender of the message or to have been a part of the conversation [7-9].

The digital signature involves two elements: a hash function and a secret key. The hash function deals with the concept of integrity by guaranteeing that the transmitted in the network aren't damaged by a technical problem or tampered by malicious attack[9].

Furthermore, a symmetric or an asymmetric key can be used to encrypt messages to satisfy the required property of confidentiality. This property means that the information exchanged between nodes is kept secret and is protected from spying, in other words confidentiality ensures that only

978-1-4673-8999-0/17/$31.00 ©2017 IEEE

authorized parties have access to the information through an encryption and decryption process [7, 10].

All information (pair key, identity, hash function and other information) are regrouped and saved in an electronic file known as certificate. It's a secure way to publish the public key and to bind it with the identity of his owner which is known by identification in security [11]. Intelligent vehicle will be equipped with Tamper Proof Device (TPD) which allows the vehicle to storage securely the different keys and information but also to sign the sent vehicle message[10].

The reminder of this paper is organized as follows. In section II, we discuss the related works on VANET Security. In section III, we present our security model. In section IV, we skim through the main tools and describe the parameters of simulation. In section V, we present some simulation results and a performance analysis. Finally, we conclude in section VI.

II. RELATED WORKS

To ensure security in VANET, researchers used a variety of encryption/decryption algorithms, hashing and signature methods. Each one has its own advantages/ disadvantages and its applicability. We discuss them briefly in this section.

Raya and Hubaux [12] showed that RSA is a robust cryptography algorithm created firstly by Shamir and al. [13], which procures a high level of security. However, due to the large size of the generated keys, the system will take up much storage space and will require a long time for the computation process of encryption/decryption. These demands will affect negatively the bandwidth and the transmission time of the message, making RSA scheme inappropriate for VANET notably when the message is bulky. By opposition Raya and Hubaux showed that Elliptic curve (EC) algorithm generates shorter keys and takes less time to perform encryption and decryption tasks, making it more suitable for VANET [12].

Jonathan Petit [14] implements ECDSA authentication processing on VANET and explores his overhead. He analysed the time complexity and the processing delay. He also gives some techniques to reduce the overhead, like the use of the P-224 size key in place of P-256 in order to minimize the data transmission delay.

Vijayabharathi and Malarchelvi [15] implement Expedite Message Authentication Protocol (EMAP) using the Hash Message Authentication Code (HMAC) for VANET. They used a fast revocation checking process instead of the old one. Their authentication protocol has reduced computation process and thereby avoid the overhead problems.

Sakhreliya and Pandya [16] came with a new conception of PKI for the authentication process. They implement public key infrastructure using symmetric key cryptography (PKI-SC), which allows them to decrease the processing time and avoid overhead for the authentication. They also made a comparison between ECDSA and MAC algorithms. Their simulations prove that message generation in PKI-SC takes only 26 us comparing to 2 ms in old PKI. Moreover, the message verification takes 26 us versus 5 ms.

Many studies proposed authentication schemes using the certificate revocation list (CRL), unfortunately CRL consumed storage resources, calculation processing and increase communication overhead. Besides, they did not explore the authentication of RSU. Our study attempts to reduce processing time by excluding a CA, removing the CLR checking, and consolidating the security of the RSU by using an ECDH-ECDSA scheme and a P-256 key.

III. MODEL DESCRIPTION

In this section, we present our security model, which aims to ensure identification, authentication, non-repudiation and integrity for the RSU. In our proposed model, we assume that the CA is not part of our scheme. The RSU is the only authority that we focused on. An aggregation of identification using an interaction zone will be achieved by multiples RSU and without asking for the intervention of a trusted third party.

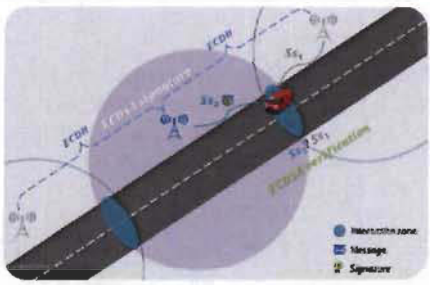

Fig. 2 : Security exchange between different entities

As described above, our solution is based on three main steps illustrated in Fig.2:

- The vehicle reports its presence in the interaction zone, by sending a beacon message and asks for a shared secret.
- The two concerned RSU apply ECDH schema and each one sends its shared secret to confirm that they are a trusted RSU.
- The authentication is ensured by an ECDSA algorithm.

All symbols used in our sequence diagram algorithm are presented in Table I.

TABLE I : Notation algorithm description

Symbol	Description
	ECDH
R	*RSU's public key*
$genR()$	*Generating public key function*
S_s	*Shared secret*
$genS_s()$	*Generating shared secret function*
	ECDSA
k_s	*Secret key*
$genK_s()$	*Generating shared secret function*
K_{pub}	*RSU's public key*
$genK_{pub}(k_s)$	*Generating public key function*
m	*message*
$sig()$	*Generating signature function*
$h()$	*hashing function SHA − 256*
m'	*signed message*

Establishment of a shared secret between two RSU using ECDH:

Each two pairs of neighbours *RSU* apply ECDH algorithm. They choose two points r_1 and r_2 respectively for RSU_1, RSU_2 from the same elliptic curve E, already agreed before [17, 18]. The secp256r1 (Type of elliptic curve used in cryptography and in Crypto++ library) have been chosen as elliptic curve.

Let's be the point r_1 extracted from the curve, the private key of the first RSU_1 and r_2 the private key of the second one.

RSU_1, RSU_2 calculate their public keys R_1, R_2 respectively which will be the multiplication of the private key with G, the generator point of the curve.

$$RSU_1\ Public\ Key: R_1 = r_1 \times G$$

$$RSU_2\ Public\ Key: R_2 = r_2 \times G$$

It should be noted that both numbers r_1 *and* r_2 must be chosen secretly.

Both RSU_1 *and* RSU_2 exchange their calculated public keys. So the public key R_1 is sent to the RSU_2 and conversely R_2 is sent to the RSU_1. This exchange is done publicly.

The last step in the key agreement consists in the calculation of the shared secret: [17, 18]

$$RSU_1\ calculates: S_{s_1} = r_1 \times R_2$$

$$RSU_2\ calculates: S_{s_2} = r_2 \times R_1$$

Communication R2V:

The vehicle asks for the shared secret S_s from the *RSU* whenever he approaches one of it.

The RSU_1 sends the shared secret S_{s_1} to the vehicle.

The RSU_2 signs a message m by the ECDSA algorithm and sends it with the shared secret S_{s_2} to the vehicle.

The ECDSA algorithm is composed from two parties, firstly the public and the secret key are generated and secondly the signature is calculated [9, 14, 18, 19].

Part 1, each *RSU* generates his own elliptic curve public and private keys as follows:

1) Choose K_s randomly where $1 \leq K_s \leq n-1$ *where* n is an integer number already agreed before.
2) Compute $K_{pub} = K_s \times G$ where G is a base point from the elliptic curve E $(G \in E)$
3) Let take K_{pub} as a public key and K_s as a secret one.

Part 2, the message's sender (RSU) generates a signature as follows:

1) Choose a random integer d where $1 < d < n-1$
2) Compute the point $(i, j) = d \times G$
3) Compute $x = integer\ (i)\ mod\ n$
4) If $x = 0$ return to step 1
5) Compute $y = d^{-1} \times (h(m) + K_s \times x)\ mod\ n$ where $h(m)$ is the result of a cryptographic hash function applied on the message m to be signed; in our case, we used SHA-256.
6) If $y = 0$ return to step 1
7) Finally, the signature is the pair (x, y).

The vehicle compares the two received shared secrets $S_{s_1} ? S_{s_2}$. If they are equals $(S_{s_1} = S_{s_2})$ then the RSUs are identified as trusted entities.

The vehicle proceed then, to the authentication by verifying the message's signature using the ECDSA algorithm as below [9, 14, 18, 19].

1) Check if $K_{pub} \neq 0$ and $K_{pub} \epsilon E$
2) Compute the value of $w = y^{-1} mod\ n$
3) Compute the value of $u_1 = w \times h(m)\ mod\ n$
4) Compute the value of $u_2 = w \times x\ mod\ n$
5) Compute $P = u_1 \times G + u_2 \times K_{pub}$
6) Compute $V = P\ mod\ n$
7) If $V = x$ then, the signature is verified.

The Fig.3 below summarizes the steps of our algorithm in sequence diagram format:

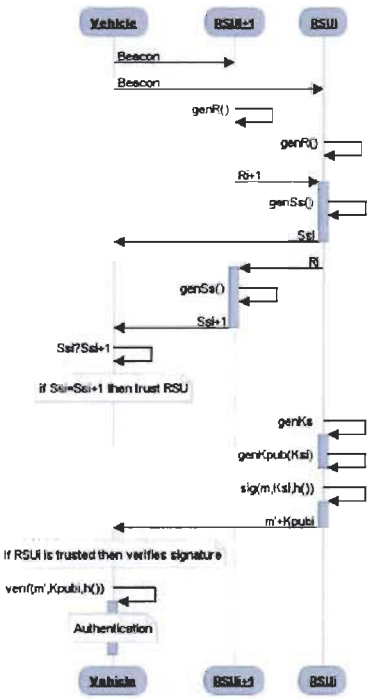

Fig. 3 : Sequence diagram

IV. SIMULATION ENVIRONMENT

In our simulation we use a combined environment for VANET composed of OMNET++ 5.0 [20] which is a network simulation C++ library, SUMO 0.25.0 [21] which is road traffic simulation and the event-based network simulator Veins 4.4 [22]. To achieve security requirement, we implemented Crypto++ 5.6.3 [23]. The all running on Ubuntu 16.04.1.

The parameters of the chosen scenario are described in Table II.

TABLE II : Simulation parameters

Parameter	Value
number of RSU	5
number of vehicle	5 – 30
Vehicle's speed	20 – 60 km/h
Wireless protocol	IEEE 802.11p
Channel bitrate	18$Mbps$
Carrier frequency	5.89 × 10^9 Hz
Thermal noise	−110dBm
Header length	256 bit
Message sending time in the interaction zone	2s
Distance between RSU	100 – 300m
Intersection zone	10m

V. RESULTS

A. Security analysis:

ECDH allows the calculation of a shared secret. It ensures that even if an eavesdropper spies the communication, it can't calculate the secret key (which is known by Elliptic curve Diffie-Hellman problem ECDHP [24]). However, it can be broken by a brute-force attack with sufficiently large computational resources and time. In this scenario, the vehicle receives the two shared secrets from two neighboring RSUs. If they are equals, the second RSU is identified to be a true one. The first RSU is already identified to be a true one, in the precedent ECDH. Hence, we called an aggregation identification. Also, the shared secret is used only one time to not be subject of a MITM attack or a brute-force attack.

ECDSA provides message integrity by using the hash function on the message. If the message was altered, the message digest will not be the same and the value of the variable V will not be equal to the value of the variable x. This last makes failed the verification of the signature. Also, ECDSA provides message authentication using a signature, that can't be only forged by the private key owner and verified by the public key. By the same way, ECDSA provides non-repudiation.

B. Performance analysis:

ECDSA has the advantage over RSA in that the signatures are much shorter (256 bits) and achieves the same security levels then RSU and DSA.

The Table III below resumes the time of signature and verification in ECDSA.

TABLE III : Operation times on AMD Opteron 8354 2.2 GHz processor under Linux using Crypto ++

ECDSA signature generation (ms)	ECDSA signature verification (ms)	SHA-256 (MiB/s)	ECDH key agreement (ms)
2.88	8.53	111	2.82

End to end delay or message delay is the time taken by the message to transit from the source (RSU) to the destination (vehicle) [25].

We calculate the mean of the mean of the message delay MMMD (1) by the formula bellow:

$$MMMD = \frac{1}{N} \times \sum_{1}^{N} \sum_{1}^{M} \frac{(T_{arrived} - T_{sent})}{M_{msg}} \quad (1)$$

Where T_{sent} is the time when the message is sent by the RSU and $T_{arrived}$ is the time when the message arrives to the vehicle. N is the number of the RSU (N=5) and M is the number of the messages sent by the RSU and received by the vehicle in the interaction zone.

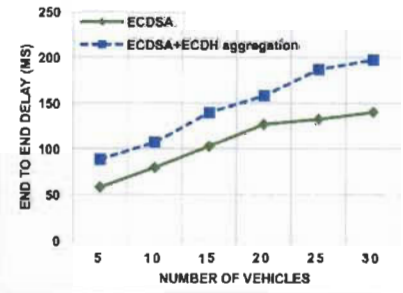

Fig. 4 : End to end delay

Through the Fig.4 above, we can see that generally the end-to-end delay increases gradually with the number of vehicles. It can be explained by the fact that, the rise of the number of the packets transmitted, is due to the rise of the number of the vehicles, which by the way increases the data processing time. We can also see that the ECDSA+ECDH aggregation schema have a superior end-to-end delay than ECDSA schema. The difference in means (m_D) (2) [26] calculated between the two schemas is 39.580 ms with a confident interval (CI) (3) [26.034 - 53.125].

$$m_D = \sum_{1}^{N} \frac{d_i}{N} = m_{ECDSA+ECDH\ aggr} - m_{ECDSA} \quad (2)$$

$$95\%\ CI: m_D \pm z_{\alpha/2} \frac{S_D}{\sqrt{N}} \quad (3)$$

RSU RSA

The average of end-to-end delay of the ECDSA+ECDH aggregation schema is higher 39.580 ms than the average of end-to-end delay of the ECDSA schema. The confidence interval does not include the value zero, so this difference is statistically significant at alpha level of 0.05.

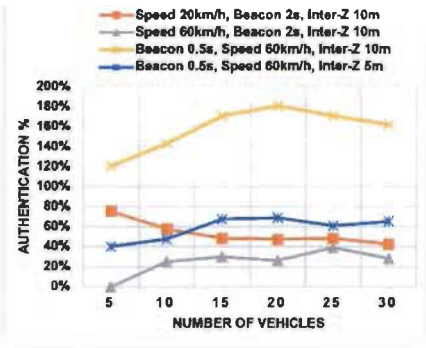

Fig. 5 : Authentication percentage

We used five RSU so we have four authentications for four interaction zones between them. This represent 100% of authentication. Having a proportion over 100% means, that multiple authentication had been done by the same vehicle in the same interaction zone.

Through the Fig.5 above, we can see that, when keeping the parameters constant and changing only the speed of vehicles (20-60km/h), we notice that the higher the speed, the higher the proportion of authentication. This is because the vehicle goes through the interaction zone quickly, without sending a beacon to RSU and asking for S_s.

When keeping the parameters constant and changing only the beacon interval of vehicles (2-0.5s), we notice that the lower beacon interval, the higher the number of sent beacon and the higher the proportion of authentication. This is because the vehicle has more chance to send a beacon in the interaction zone to RSU and asks for S_s.[3]

When keeping the parameters constant and changing only the size of the interaction zone (5-10m), we notice that, the bigger the size of the interaction, the higher the proportion of authentication. This is because the vehicle has enough time, while crossing the zone, to send a beacon to RSU and to ask for S_s.

VI. CONCLUSION

This paper proposes a new security schema based on ECDH-ECDSA aggregation schema, by specifying an interaction zone, where a secret shared resulting from ECDH algorithm have been compared before the authentication step. Our simulation proves that even if ECDH-ECDSA aggregation schema takes about 40ms more than the simple ECDSA schema, our model provides higher levels of security. Moreover, being also CA-less and certificate-less make this model faster than other schema who spends time in cheeking the revocation list.

Choosing the beacon interval value equal to 0.5s and an interaction zone between 5 and 10m seems to be the optimal choice to implement ECDH-ECDSA aggregation schema. These parameters and the integration of Multi-party Diffie-Hellman method can be studied in future work to improve this security scheme and to reduce the authentication delay. Instead of calculating a key each time between two neighboring RSU, we will calculate it just once for a group consisting of more than two RSU.

ACKNOWLEDGMENT

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

REFERENCES

[1] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications*, vol. 5, p. 95, 2013.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of network and computer applications*, vol. 37, pp. 380-392, 2014.

[3] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, pp. 53-66, 2014.

[4] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, pp. 164-171, 2008.

[5] Y. L. Morgan, "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics," *IEEE Communications Surveys & Tutorials*, vol. 12, pp. 504-518, 2010.

[6] Y. Toor, P. Muhlethaler, A. Laouiti, and A. D. L. Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues," *IEEE Communications Surveys & Tutorials*, vol. 10, pp. 74-88, 2008.

[7] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1-13, 5/15/ 2014.

[8] E. A. M. Anita and J. Jenefa, "A survey on authentication schemes of VANETs," in *2016 International Conference on Information*

~~higher~~ lower

Communication and Embedded Systems (ICICES), 2016, pp. 1-7.

[9] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, pp. 574-588, 2009.

[10] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 2985-2996, 2015.

[11] R. E. Blahut, *Cryptography and Secure Communication*: Cambridge University Press, 2014.

[12] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," presented at the SASN 2005, Alexandria, VA, USA, 2005.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[14] J. Petit, "Analysis of ECDSA Authentication Processing in VANETs," in *2009 3rd International Conference on New Technologies, Mobility and Security*, 2009, pp. 1-5.

[15] V. Vijayabharathi and P. S. K. Malarchelvi, "Implementing HMAC in expedite message authentication protocol for VANET," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, 2014, pp. 1-5.

[16] S. C. Sakhreliya and N. H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs," in *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, 2014, pp. 1-6.

[17] H. Hartenstein and K. Laberteaux, *VANET: vehicular applications and inter-networking technologies* vol. 1: Wiley Online Library, 2010.

[18] S. Manvi, M. Kakkasageri, and D. Adiga, "Message authentication in vehicular ad hoc networks: Ecdsa based approach," in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*, 2009, pp. 16-20.

[19] A. Abidi, B. Bouallegue, and F. Kahri, "Implementation of elliptic curve digital signature algorithm (ECDSA)," in *Computer & Information Technology (GSCIT), 2014 Global Summit on*, 2014, pp. 1-6.

[20] OpenSim. (2016). *OMNeT++ Discrete Event Simulator*. Available: omnetpp .org

[21] S. Alike. (2016). *Sumo*. Available: sumo.dlr .de/wiki/Main_Page

[22] C. Sommer. (2016, 01/01/2016). *Veins*. Available: veins.car2x .org

[23] W. Dai. (2016). *Crypto++ Library 5.6.3*. Available: cryptopp .com

[24] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*: Springer Science & Business Media, 2006.

[25] S. Ibrahim and M. Hamdy, "A comparison on VANET authentication schemes: Public Key vs. Symmetric Key," in *Computer Engineering & Systems (ICCES), 2015 Tenth International Conference on*, 2015, pp. 341-345.

[26] M. J. Panik, *Statistical Inference: A Short Course*: John Wiley & Sons, 2012.

DISCUSSION

1 Analyse de la sécurité

L'ECDH permet le calcul d'un secret partagé. Il assure que même si un malveillant espionne la communication, il ne peut calculer la clé secrète (Ce qui est connu par le problème du Diffie-Hellman basé sur les courbes elliptiques). Cependant, il se peut que cette clé soit trouvée grâce à une attaque de force brute avec suffisamment de ressources informatiques et de temps.

Dans notre schéma de sécurité, le véhicule reçoit les deux clés secrètes de deux RSU voisins. Si ces clés sont égales, le deuxième RSU est identifié comme étant une entité de confiance. Le premier RSU est déjà identifié comme étant une entité de confiance dans le précédent ECDH, d'où l'appellation identification par agrégation. En outre, le secret partagé est utilisé une seule fois pour ne pas être exposé à une attaque MITM ou une attaque de force brute.

ECDSA fournit l'intégrité du message en appliquant la fonction de hachage sur le message. Si ce dernier a été modifié, le hash du message ne sera pas le même et par conséquent, la vérification de la signature du message échoue. En résumé, nous concluons que l'algorithme ECDSA fournit l'authentification du message en utilisant une signature, qui ne peut être forgée que par le propriétaire de la clé privée et ne peut être vérifiée que par la clé publique correspondante, et dans cette même logique, ECDSA assure la non-répudiation.

2 Analyse des performances

L'algorithme ECDSA a de meilleures performances que l'algorithme RSA en vue des signatures qui sont beaucoup plus courtes (256 bits) et qui atteignent les mêmes niveaux de sécurité que RSA et DSA. Par ailleurs, l'algorithme ECDSA sans les certificats a eu l'avantage d'optimiser les délais d'envoi et d'authentification puisqu'il n'est plus nécessaire de gérer une liste de révocation. Toutefois, il a augmenté le temps d'envoi de 39.580 ms, un compromis pour assurer

l'authentification et une protection contre les MITM et la non répudiation ainsi que l'intégrité des messages.

Nous avons observé que le temps d'authentification varie selon la vitesse du véhicule, de l'intervalle Beacon et du diamètre de la zone d'interaction. Nous avons également déduit qu'avec un intervalle Beacon de 0,5s et une zone d'interaction entre 5 et 10m, nous obtenions le temps d'authentification le plus optimal.

CONCLUSION GENERALE

L'implémentation de nouvelles technologies dans la vie quotidienne ne cesse d'accélérer. Ainsi, les réseaux VANET incarnent l'évolution du véhicule et de la conduite moderne, permettant aux conducteurs de bénéficier d'un réseau sans fil qui leur assure une connectivité continue et en tout temps en vue de garantir leur confort et leur sécurité.

Comme tout réseau informatique, le réseau VANET constitue une cible pour les attaquants. Nous nous sommes intéressés dans cette étude à une des entités du réseau VANET qu'est le RSU, plus précisément à son authentification, sa non-répudiation et à l'intégrité de ses messages. Ces paramètres peuvent être victimes de plusieurs attaques telles que l'attaque Sybil, l'attaque du trou noir, la réplication de certificat, la modification ou la suppression de message, etc... Nous avons élaboré un schéma de sécurité sans l'entité CA, permettant de contrer ce genre d'attaques et nous l'avons nommé « authentification ECDH-ECDSA du RSU par agrégation ». Ce schéma consiste à amener deux RSU voisins à envoyer au véhicule, qui se trouve dans leur zone d'interaction, un secret partagé établi par l'ECDH et à le renouveler à chaque tentative d'émission. Ceci afin de faire face à l'attaque MITM. Pour procéder à l'authentification du RSU, le véhicule compare les deux secrets reçus et s'ils s'avèrent identiques, il poursuit l'authentification par la vérification de la signature par l'ECDSA préalablement amorcée par les RSU. Nous avons choisi les courbes elliptiques (EC) car elles apportent une bonne rapidité dans les processus de calcul. Nous avons également favorisé les clés de taille 256 bits afin d'optimiser la sécurité en dépit des performances. D'après les résultats des simulations effectuées lors de notre étude, nous avons démontré que le temps d'authentification et le délai d'envoi des messages dépendent de la vitesse, du temps de l'intervalle Beacon et du diamètre de la zone d'interaction. Nous avons pu établir aussi, que la valeur d'intervalle Beacon 0,5s et d'une zone d'interaction fixée entre 5 et 10m semblent être un choix optimal pour implémenter le schéma d'agrégation ECDH-ECDSA. En comparaison avec un schéma sans certificat et sans CA basé sur l'ECDSA seul, un test-T a démontré qu'il y avait une augmentation significative dans le délai d'envoi des messages de 39.580 ms. A travers cette étude, nous avons pu explorer les points forts

et les limites de notre schéma et aussi examiner le terrain pour d'éventuelles améliorations dans des travaux futurs. Nous proposons par exemple d'optimiser les délais par l'intégration de la méthode Multi-party Diffie-Hellman sur un groupe de RSU à la fois au lieu de seulement une paire de deux RSU.

RÉFÉRENCES

[1] S. Khan and A. K. Pathan, *Wireless networks and security*: Springer, 2013.

[2] T. Jesus and Z. Sherali "Security in vehicular ad hoc networks," *Dynamic Ad Hoc Networks,* 2013.

[3] H. F. Rashvand and H.-C. Chao, *Dynamic ad hoc networks*: Institution of Engineering and Technology, 2013.

[4] H. Moustafa and Y. Zhang, *Vehicular networks: techniques, standards, and applications*: Auerbach publications, 2009.

[5] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications,* vol. 44, pp. 1-13, 5/15/ 2014.

[6] M. A. Razzaque, A. S. S., and S. M. Cheraghi, "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead," in *Wireless Networks and Security: Issues, Challenges and Research Trends*, S. Khan and A.-S. Khan Pathan, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 107-132.

[7] F. Domingos Da Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. A. F. Loureiro, "Data Communication in VANETs: A Survey, Challenges and Applications," INRIA Saclay
INRIA2014-03-28 2014.

[8] Y. L. Morgan, "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics," *IEEE Communications Surveys & Tutorials,* vol. 12, pp. 504-518, 2010.

[9] Y. Toor, P. Muhlethaler, A. Laouiti, and A. D. L. Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues," *IEEE Communications Surveys & Tutorials,* vol. 10, pp. 74-88, 2008.

[10] H. Hartenstein and K. Laberteaux, *VANET: vehicular applications and inter-networking technologies* vol. 1: Wiley Online Library, 2010.

[11] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of network and computer applications,* vol. 37, pp. 380-392, 2014.

[12] R. Naja, *Wireless vehicular networks for car collision avoidance* vol. 2013: Springer, 2013.

[13] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications,* vol. 1, pp. 53-66, 2014.

[14] M. Nekovee, "Sensor networks on the road: the promises and challenges of vehicular adhoc networks and vehicular grids," in *Proceedings of the Workshop on Ubiquitous Computing and e-Research*, 2005, pp. 1-5.

[15] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives," in *2006 6th International Conference on ITS Telecommunications*, 2006, pp. 761-766.

[16] 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 & tutorials,* vol. 13, pp. 584-616, 2011.

[17] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications,* 2017.

[18] H. La Vinh and A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," *International journal on AdHoc networking systems (IJANS),* vol. 4, pp. 1-20, 2014.

[19] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *International Workshop on Communication Technologies for Vehicles*, 2013, pp. 59-74.

[20] V. Bibhu, R. Kumar, B. S. Kumar, and D. K. Singh, "Performance analysis of black hole attack in VANET," *International Journal Of Computer Network and Information Security,* vol. 4, p. 47, 2012.

[21] N. R. Siddiqui, K. A. Khaliq, and J. Pannek, "VANET Security Analysis on the Basis of Attacks in Authentication," in *Dynamics in Logistics*, ed: Springer, 2017, pp. 491-502.

[22] Y. Kim, I. Kim, and C. Y. Shim, "A taxonomy for DOS attacks in VANET," in *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on*, 2014, pp. 26-27.

[23] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security,* vol. 15, pp. 39-68, 2007.

[24] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications,* vol. 5, p. 95, 2013.

[25] R. E. Blahut, *Cryptography and Secure Communication*: Cambridge University Press, 2014.

[26] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets," in *4th Workshop on Embedded Security in Cars (escar 2006)*, 2006.

[27] L. Qingzi, W. Qiwu, and Y. Li, "A hierarchical security architecture of VANET," in *International Conference on Cyberspace Technology (CCT 2013)*, 2013, pp. 6-10.

[28] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," *International Journal of Computer Theory and Engineering,* vol. 4, p. 1007, 2012.

[29] J. M. d. Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," 2010.

[30] V. Yadav, S. Misra, and M. Afaque, "Security in Vehicular Ad Hoc Networks," in *Security of Self-Organizing Networks*, ed: Auerbach Publications, 2010, pp. 227-250.

[31] J. R. Vacca, *Public key infrastructure: building trusted applications and Web services*: CRC Press, 2004.

[32] J. A. Buchmann, E. Karatsiolis, and A. Wiesmaier, *Introduction to public key infrastructures*: Springer Science & Business Media, 2013.

[33] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*: CRC press, 2016.

[34] Z. Shi, C. Ma, J. Cote, and B. Wang, "Hardware implementation of hash functions," in *Introduction to Hardware Security and Trust*, ed: Springer, 2012, pp. 27-50.

[35] N. I. Shuhaimi and T. Juhana, "Security in vehicular ad-hoc network with Identity-Based Cryptography approach: A survey," in *2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2012, pp. 276-279.

[36] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks,* vol. 11, pp. 574-588, 2009.

[37] J. Petit, "Analysis of ECDSA Authentication Processing in VANETs," in *2009 3rd International Conference on New Technologies, Mobility and Security*, 2009, pp. 1-5.

[38] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach," presented at the Proceedings of the 2009 International Conference on Future Computer and Communication, 2009.

[39] A. Abidi, B. Bouallegue, and F. Kahri, "Implementation of elliptic curve digital signature algorithm (ECDSA)," in *Computer & Information Technology (GSCIT), 2014 Global Summit on*, 2014, pp. 1-6.

[40] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*: Springer Science & Business Media, 2006.

[41] V. Vijayabharathi and P. S. K. Malarchelvi, "Implementing HMAC in expedite message authentication protocol for VANET," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, 2014, pp. 1-5.

[42] S. C. Sakhreliya and N. H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs," in *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, 2014, pp. 1-6.

[43] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," presented at the Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, Montreal, Quebec, Canada, 2007.

[44] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," *IEEE Transactions on Vehicular Technology,* vol. 57, pp. 3357-3368, 2008.

[45] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, pp. 736-746, 2011.

[46] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2009, pp. 1-9.

[47] 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.

[48] 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.