Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ASTM: American Society for Testing and Materials.

CA: Central Authority.

CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance.

DSRC: Dedicated Short Range Communication.

IEEE: Institute of Electrical and Electronics Engineers.

MAC: Medium Access Control.

MANET: Mobile Ad Hoc Network.

NS: Network Simulator.

OBU: On Board Unit.

RSU: Road Side Unit.

STI: Systèmes de Transport Intelligents.

SUMO: Simulation of Urban Mobility.

TPD: Tamper Proof Device.

TCP: Transport Control Protocol.

VANET: Vehicular Ad hoc Network.

V2V: Vehicular-to-Vehicular.

V2I: Vehicular-to-Infrastructure.

WAVE: Wireless Access for the Vehicular Environment.

Résumé

Nous proposons dans ce mémoire, un protocole de sécurité basé sur le changement périodique des pseudonymes de communication des véhicules. L'idée est d'éviter la traçabilité illégale des véhicules durant leur communication et ainsi préserver la confidentialité des données échangées. Deux approches d'étude sont proposées. Dans la première approche, chaque véhicule demande après un temps t, un nouveau pseudonyme de communication à la Centrale d'Autorité (CA). Alors que dans l'approche 2, chaque véhicule génère lui-même, après un temps t, un nouveau pseudonyme de communication. Notre objectif est de déterminer un intervalle de temps au cours duquel au moins deux véhicules peuvent changer leurs pseudonymes de communication sans qu'aucun d'eux ne soit localisé par un adversaire. Nous évaluons dans ce travail, le taux de consommation de la bande passante en tenant compte de la vitesse moyenne des véhicules sur la route. Dans le protocole proposé, nous avons disposé les RSUs de manière équidistante. En nous basant sur la plage de vitesses autorisées sur la route, nous avons évalué l'intervalle de temps de changement des pseudonymes de communication.

Pour sécuriser les messages, nous avons considéré l'utilisation des algorithmes cryptographiques. Notre protocole assure l'authentification, la non-répudiation et il permet la gestion de la vie privée des véhicules.

Mots clés: Authentification, vie privée, certificat, distribution équidistante, traçabilité.

Abstract

We propose in this Master thesis, a security protocol based on periodic change of pseudonyms. The idea is to avoid illegal traceability of vehicles during their communications and preserve their privacy and confidential information. Two different approaches are proposed. In the first approach, each vehicle asks the central authority a new communication pseudonym after a time t. While in the second approach, each vehicle generates itself a new communication pseudonym, after a time t. Our objective is to permit at least two vehicles to change their pseudonym in the same time interval. We evaluate in this work, the bandwidth used by considering the vehicle's average speed in each approach. The proposed protocol is based on equidistant distribution of the road side unit and uses the average of the speed permitted on the road to evaluate lifetime t of the communication's pseudonyms and certificates. For securing messages, we have considered the use of cryptographic algorithms. Our protocol provides authentication, non-repudiation and privacy.

Keywords: Authentication, privacy, certificate, equidistant distribution, traceability.

Chapitre 1 - Introduction générale

Les systèmes de transport actuels fournissent très peu d'informations sur les conditions routières. Ils sont l'une des causes des difficultés de circulation entraînant des dégâts environnementaux ainsi qu'une piètre qualité de vie [1]. Selon le rapport réalisé par l'OMS (Organisation Mondiale de la santé) sur la sécurité routière dans le monde en 2013 [2], les traumatismes dus aux accidents de la circulation représentent la huitième cause de décès dans le monde et la première cause de décès de la population dont la tranche d'âge est comprise entre 15 et 29 ans.

En effet, ces systèmes de transport sont à la base des embouteillages qui coûtent près de 266 milliards de dollars par an [1] et ralentissent de façon considérable les usagers dans leurs trajets.

Pour remédier aux handicaps que présentent les systèmes de transport actuels, industriels et universitaires, s'appuyant sur des progrès technologiques, ont introduit la notion de systèmes de transport intelligents (STI). Les systèmes de transport intelligents visent à réduire les risques dans le domaine de transport de façon significative en agissant simultanément sur quatre axes: la prévention des accidents; la réduction des dégâts en cas de collision; la gestion des secours; et enfin la protection des usagers [3]. La mise en place des systèmes de transport intelligents repose sur le déploiement des réseaux véhiculaires sans fil. Ces réseaux permettent aux véhicules d'être informés sur les conditions routières et météorologiques.

Vu l'importance des données échangées sur ces réseaux, un attaquant peut, en absence des mesures de sécurité, modifier le comportement des véhicules par l'ajout de fausses données dans le trafic, ou extraire une information liée à l'identité d'un véhicule dans les messages diffusés.

Pour éviter qu'un adversaire ne localise un véhicule qui communique dans le réseau, nous proposons dans le cadre de notre mémoire, l'étude d'un protocole de gestion de l'anonymat et de la traçabilité.

Ce protocole permet aux véhicules de changer leurs pseudonymes de communication dans un même intervalle de temps afin de préserver la confidentialité des données et d'éviter la traçabilité illégale. Il tient compte de la qualité de service et des exigences de sécurité dans les réseaux véhiculaires sans fil.

L'étude du protocole est faite selon deux approches différentes. Dans la première approche, les véhicules demandent périodiquement les pseudonymes de communication auprès de la Centrale d'Autorité (CA) alors que dans l'approche 2, les véhicules génèrent eux-mêmes leurs pseudonymes de communication. Notre projet est réalisé dans l'espace euclidien. En utilisant la portée de communication autorisée par la norme DSRC (Dedicated Short Range Communication) et la plage de vitesses autorisées sur une route, nous allons d'abord déterminer combien d'unités de bords de routes seront nécessaires et comment les disposer afin d'avoir une bonne connectivité véhicule-infrastructure. Ensuite, nous allons évaluer un intervalle de temps dans lequel au moins deux véhicules puissent changer leurs pseudonymes de communication.

Le présent mémoire est structuré en sept chapitres. Le chapitre 2 porte sur la généralité des réseaux VANETs. Le chapitre 3 présente les résumés de quelques travaux trouvés dans la littérature sur la sécurité des réseaux véhiculaires sans fil. Les étapes de conception du protocole de gestion de l'anonymat et de la traçabilité sont présentées dans le chapitre 4. Le chapitre 5 décrit les simulateurs généralement utilisés pour évaluer les performances des protocoles des réseaux VANETs. Les résultats des simulations de notre étude sont présentés dans le chapitre 6. Le chapitre 7 conclut notre étude en présentant quelques perspectives.

Chapitre 2 - Généralité sur les réseaux véhiculaires sans fil

2.1 Introduction

Les réseaux véhiculaires sans fil dérivent de l'exploitation des technologies conçues pour les réseaux Ad Hoc mobiles (MANETs). Leur élaboration accentue l'émergence des systèmes de transports intelligents (STI) qui ont pour but d'améliorer la sécurité routière et de rendre plus efficace, voire plus convivial, le temps passé sur la route. À l'aide des systèmes embarqués aussi bien dans les voitures qu'installés au bord des routes, les conducteurs peuvent envoyer, ou recevoir des informations sur l'état des routes et des alertes sur des accidents de la route. Aussi les passagers des voitures peuvent s'échanger des données (musique, vidéo) et d'autres informations utiles; ceci pour rendre le temps passé sur la route, moins ennuyeux.

Dans cette première partie de notre mémoire, nous parlerons d'abord de la communication entre les différentes entités du réseau, et des services issus de ces réseaux. Ensuite, nous aborderons la norme et le standard de communication. Enfin, nous présenterons les éléments et concepts de sécurité des réseaux VANETs.

2.2 Communication dans les réseaux VANETs

Dans les réseaux véhiculaires sans fil, les véhicules (entités mobiles) s'organisent pour établir la communication entre eux et aussi entre les entités fixes disposées le long de la route. L'échange des données entre les véhicules est désigné sous le nom de la communication en mode ad hoc alors que celui entre les véhicules et les entités fixes est connu sous l'appellation de communication en mode infrastructure. Dans cette section, nous détaillerons les principes et l'avantage de chaque mode de communication.

2.2.1 Communication en mode Ad hoc

Généralement appelée communication véhicule à véhicule (V2V), la communication Ad Hoc dans les réseaux VANETs est similaire à celle des nœuds mobiles dans les réseaux MANETs. Dans ce mode de communication, chaque véhicule équipé d'une plateforme électronique appelée OBU (On-Board Unit), échange des données avec les véhicules situés dans sa zone radio. La communication Ad Hoc fonctionne en environnement décentralisé et ne nécessite pas d'infrastructure pour son fonctionnement. Il est très efficace pour la diffusion rapide des informations liées aux services de sécurité routière. Cependant à cause de la forte mobilité des véhicules, la connectivité n'est pas permanente entre les véhicules [4].

2.2.2 Communication en mode infrastructure

La communication en mode infrastructure est également connue sous le nom de la communication véhicule-infrastructure. Trois entités s'organisent pour établir ce type de communication:

- **OBU**: ensemble de composants logiciels embarqué dans le véhicule. Il permet aux véhicules de se localiser, de calculer et d'envoyer des données sur l'interface réseau.
- **RSU** (Road Side Unit): Cette entité installée au bord des routes, diffuse aux véhicules des informations sur l'état du trafic et sur les conditions météorologiques. Elle peut être utilisée comme point d'accès au réseau.
- **CA** (Central Authority): C'est la Centrale d'autorité. Elle gère le réseau et joue le rôle de serveur de stockage des données. La CA délivre également des certificats et des clés ou pseudonymes de communication aux véhicules [5].

Le mode de communication infrastructure offre une meilleure connectivité et permet l'accès à divers services (internet, information météorologique...) [6].

Toutefois, le déploiement des entités fixes le long des routes est très coûteux; d'où la combinaison des deux modes de communication dans les réseaux VANETs. Aussi, la communication en mode infrastructure présente un temps de latence dans l'acheminement des paquets [7]. La figure 2.1 décrit les modes de communication présents dans les réseaux véhiculaires sans fil.

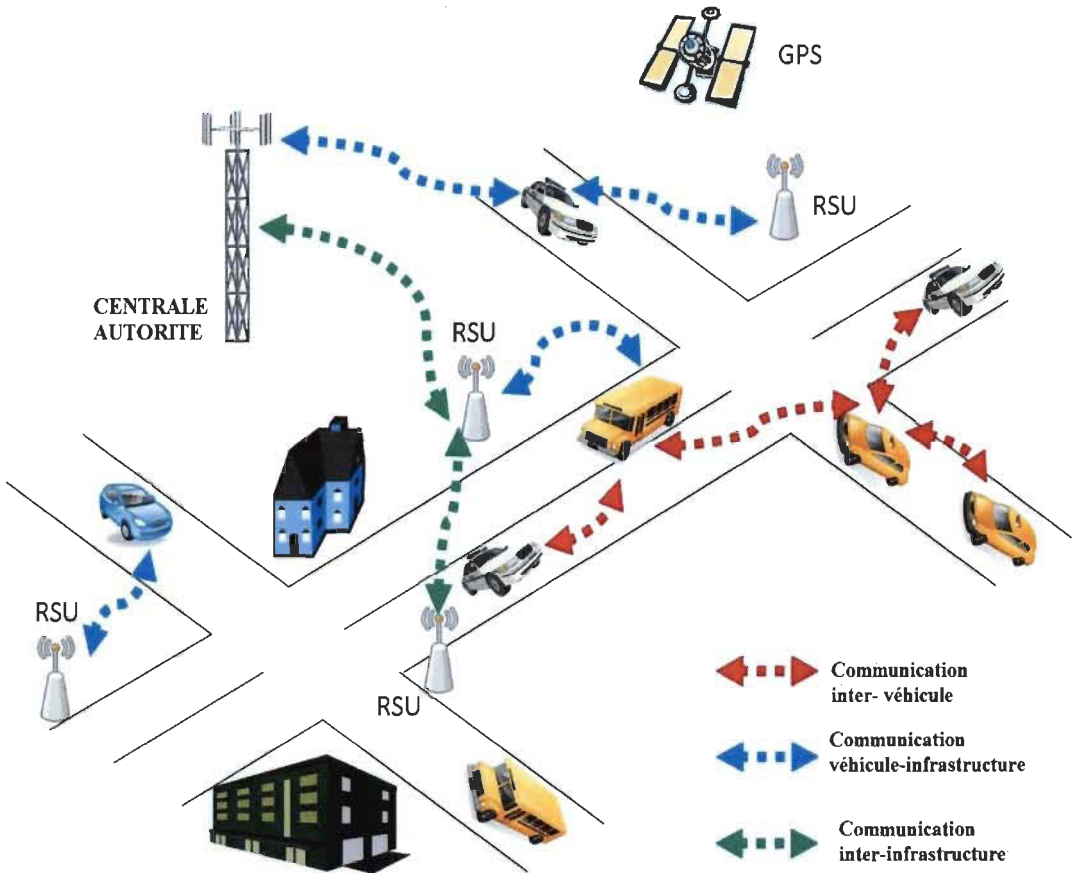


Figure 2.1: Communication dans les réseaux VANETs [8]

2.3 Services dans les réseaux VANETs

Les réseaux véhiculaires sans fil contribueront à réduire le nombre d'accidents sur les routes du fait des différents services que peuvent bénéficier ces utilisateurs. En effet, de la communication entre les diverses entités du réseau découlent trois types de services qui vont de la gestion du trafic routier à l'amélioration du confort des usagers [4, 7].

2.3.1 Services de gestion et d'amélioration du trafic routier

Ces services contribuent à l'amélioration du trafic routier en fournissant des informations sur l'état des routes. Du contenu des messages échangés par les différentes entités du réseau, un véhicule peut être informé de la circulation sur son trajet actuel ou futur. Le conducteur peut donc décider de suivre une autre route lorsque le trafic est dense sur son trajet et éviter ainsi de la congestion.

Les services de gestion du trafic routier permettent de créer le passage pour les voitures d'urgence, ou de proposer des itinéraires aux véhicules qui se dirigent dans une zone de congestion.

2.3.2 Services de prévention et de sécurité du trafic routier

Les services de préventions et de sécurité du trafic routier permettent d'élargir le champ de vision des conducteurs. Par les messages d'alerte diffusés entre les différentes entités, les conducteurs peuvent être avertis des accidents ou autres situations dangereuses (alerte pour les travaux routiers, informations météorologiques) qui ont lieu sur leurs itinéraires. De plus, ces services qui ont un effet direct sur les personnes et les biens contribuent à la diminution du nombre d'accidents sur les routes et par conséquent préserver la vie humaine. Un de ces services est déjà implémenté dans certaines voitures actuelles. Il s'agit du service SOS qui en cas d'accident, envoie un message afin de prévenir le centre de secours le plus proche. Ceci facilite l'arrivée rapide de l'équipe de secours et ainsi prévenir d'un carambolage [7].

2.3.3 Services d'amélioration du confort des usagers

Outre les services de prévention et de gestion du trafic routier, les réseaux véhiculaires sans fil contribuent également à l'amélioration du confort des usagers et leur permettent de bénéficier, grâce à l'accès internet, de plusieurs services. À travers les réseaux VANETs, les conducteurs et les passagers des voitures peuvent recevoir de façon instantanée des offres commerciales (les annonces des restaurants, des services d'informations touristiques, des stations-services), et des informations sur les lieux de stationnement dans leur zone de voisinage. De plus, par l'échange des données les voitures, les passagers peuvent s'échanger des musiques, vidéos ou jouer en réseau. Aussi, on pourra déployer facilement dans ce réseau la conduite assistée entre les conducteurs, la vérification à distance des permis de conduire et des plaques d'immatriculation par les autorités compétentes, et le paiement électronique au niveau des points de péage afin de faire gagner du temps aux utilisateurs.

2.4 Norme et standard de communication

Pour mettre en place la communication entre les différentes entités dans les réseaux véhiculaires sans fil, l'ASTM (American Society for Testing and Materials) a adopté en 2002, une norme de communication appelée DSRC (Dedicated Short Range Communication) [9], dont la couche physique est basée sur la norme IEEE 802.11a [10]. En 2003, l'IEEE s'inspirant des travaux de l'ASTM, a étendu sa famille de standard 802.11 en y ajoutant le 802.11p [7, 9].

Dans cette section, nous allons décrire brièvement la norme DSRC et le standard 802.11p.

2.4.1 DSRC

Dedicated Short Range Communication (DSRC) regroupe un ensemble de technologies dédiées aux communications véhiculaires. Cette technologie a évolué à partir de la norme IEEE 802.11a vers la norme IEEE 802.11p ou WAVE afin de répondre aux caractéristiques des réseaux VANETs.

Le DSRC œuvre dans la bande de fréquence de 5.9 GHZ. Cette bande de fréquence est divisée en 7 canaux de 10 MHZ chacun [9,10]. L'ensemble de ces canaux se répartit fonctionnellement en 1 canal de contrôle et 6 canaux de services. Le canal de contrôle est réservé à la transmission des messages de gestion du réseau et des messages très importants tels que les messages liés à la sécurité routière. Les 6 autres canaux sont dédiés à la transmission des données des services annoncés sur le canal de contrôle [9]. L'étude comparative réalisée sur les technologies d'accès dans [7] prouve que le DSRC peut assurer le bon fonctionnement des applications de sécurité du trafic routier. Le DSRC propose un débit (atteignant 54 Mbit/s) suffisant pour le volume de données transporté. Aussi avec une latence faible (inférieur à 5 ms), la technologie DSRC supporte une forte mobilité (aptitude à la mobilité élevée à 300 km/h) sur une portée maximale théorique de 1000 m, ainsi que le trafic de données temps réel. Il s'adapte à tous les types de communication véhiculaires (IVC/V2V).

2.4.2 IEEE 802.11p

Le standard IEEE 802.11p utilise le concept de multicanaux dans le but d'assurer les communications liées aux applications de sécurité et autres services des transports intelligents [9, 11]. Il dérive de la couche physique du standard IEEE 802.11a, et est adapté au fonctionnement à faible charge du spectre DSRC [11]. Le 802.11p offre un débit compris entre 6 et 27 Mb/s sur une distance de 1000 m et avec une modulation de type OFDM (orthogonal Frequency Division Multiplexing). Aussi la couche MAC du 802.11p reprend le principe du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) développé dans le protocole MAC de l'IEEE 802.11e afin de gérer la qualité de service et le support du protocole de marquage de priorité (priorité d'accès) [9, 11].

2.5 Éléments et concepts de sécurité

Différents éléments sont pris en compte dans le développement des réseaux véhiculaires sans fil afin de respecter les concepts de sécurité. Nous allons présenter, dans cette partie, ces éléments et ensuite décrire les concepts de sécurité qui doivent être pris en compte dans la conception des protocoles de sécurité pour les réseaux VANETs.

2.5.1 Éléments de sécurité

2.5.1.1 Le Tamper-Proof Device (TPD)

C'est un dispositif qui embarqué dans les voitures, permet de stocker les données confidentielles aux véhicules (clés privées, certificats). De plus, le TPD se charge de signer les messages envoyés par les véhicules. Il est conçu de manière à détruire automatiquement toutes les informations stockées lors d'une manipulation matérielle grâce aux capteurs de nature diverse qu'il contient [4, 12].

2.5.1.2 Les certificats dans les réseaux VANETs

L'utilisation des certificats dans les réseaux VANETs vise à renforcer les mesures de sécurité établies par les algorithmes cryptographiques, principalement ceux de la cryptographie asymétrique. On distingue de types de certificats [4].

a. Le certificat à long terme

Chaque véhicule a un certificat à long terme qui contient outre les données qui lui sont propres, les informations personnelles sur son propriétaire (identité du propriétaire). Ce certificat est utilisé pour renouveler les certificats à court terme, faire des demandes de pseudonymes, ou établir une communication avec l'autorité centrale.

b. Le certificat à court terme

Le certificat à court terme ne contient pas des données personnelles du conducteur. Il peut contenir un identifiant virtuel et des pseudonymes de communication permettant de garder l'anonymat du véhicule dans le réseau.

Seule la centrale autorité pourra révéler l'identité réelle du véhicule. Ce type de certificat est utilisé généralement dans les protocoles de routage. Il faut souligner que chaque véhicule possède un seul certificat à long terme et plusieurs certificats à court terme.

2.5.2 Concepts de sécurité

Dans la conception des protocoles de sécurité des réseaux VANETs, les concepts de sécurité tels que la confidentialité, l'authentification, l'intégrité des données, la non-répudiation, la disponibilité, le respect de la vie privée et le contrôle d'accès, doivent être pris en compte.

2.5.2.1 La confidentialité

Le principe de la confidentialité est de rendre l'information du réseau accessible uniquement aux entités autorisées (les entités qui se sont authentifiées dans le réseau). La confidentialité protège donc les données du réseau contre l'écoute clandestine. Deux niveaux de protection sont identifiables [7]:

- Le service global protège toutes les données transmises entre les utilisateurs du réseau pendant une période donnée;
- Le service restreint assure la protection des messages par l'ajout de champs spécifiques à l'intérieur du message.

Les objectifs des applications de sécurité du trafic routier ne peuvent être atteints que si un maximum de véhicules coopère pour mettre en place la politique de confidentialité.
Le chiffrement des données permet de mettre en place le service de confidentialité dans les réseaux VANETs. Généralement, ce sont les algorithmes de cryptographie asymétrique et symétrique qui sont utilisés pour assurer le chiffrement et le déchiffrement des données.

2.5.2.2 L'authentification

L'authentification est le concept de sécurité qui permet de lier un message à son auteur. Elle permet aux différents nœuds d'avoir confiance aux messages diffusés dans le réseau. Pour un message d'alerte par exemple, c'est le principe d'authentification qui permet au destinataire du message d'avoir confiance dans la source du message: c'est-à-dire que l'émetteur est bien une entité du réseau et non une entité externe. L'authentification est assurée par des mécanismes proactifs. Il existe deux types d'authentification: l'authentification des messages et l'authentification des entités. L'authentification des messages permet de retracer la source du message alors que l'authentification des entités permet d'identifier les nœuds du réseau.

La principale particularité des applications de sécurité du trafic routier réside dans l'obligation pour toute entité générant et diffusant des messages d'alerte ou de contrôle d'y adjoindre une preuve d'authenticité (signature) afin d'éviter que les entités malveillantes ou non authentifiées ne puissent générer et diffuser des messages de sécurité [7].

2.5.2.3 L'intégrité

Le principe d'intégrité repose sur deux concepts :

- L'intégrité des messages : Fonction permettant de s'assurer que l'information envoyée par la source n'a pas subi d'altération avant d'arriver au destinataire;
- L'intégrité physique : Elle est liée aux matériels utilisés pour chiffrer et déchiffrer les messages. Cette fonction permet de s'assurer que le dispositif servant à l'envoi ou à la collecte d'informations n'a pas subi de modification.

Le service d'intégrité des messages veille à ce que les messages diffusés entre les entités du réseau ne subissent aucune modification, duplication, réorganisation voire répétition. Contrairement à la confidentialité, l'intégrité s'applique sur certains champs spécifiques du paquet du message.

Les mécanismes proactifs utilisés pour gérer l'intégrité des messages sont les fonctions de hachage et le MAC (Message Authentication Code). Ces mécanismes reposent sur des fonctions mathématiques à sens unique [7].
L'intégrité physique est assurée par le TPD (Tamper-Proof Device), équipement robuste qui est embarqué dans les véhicules et permet d'assurer l'intégrité des messages.

2.5.2.4 Non-répudiation

Dans les réseaux véhiculaires sans fil, il est indispensable que toute entité diffusant des messages soit identifiable avec certitude. En effet compte tenu des conséquences néfastes que peuvent présenter les applications de sécurité routière sur les biens et les personnes, il est important de retrouver la source du message. La mise en place de la politique de non-répudiation dans les réseaux VANETs permet donc d'éliminer toute possibilité pour un attaquant d'injecter des données erronées sans être identifié.
Généralement, c'est la signature numérique qui est utilisée pour garantir la non-répudiation des messages des applications de sécurité et de gestion du trafic routier. Quant aux messages des applications de gestion de confort, la non-répudiation n'est pas aussi nécessaire sauf pour les messages impliquant des transactions financières [13].

2.5.2.5 Disponibilité

Le principe de la disponibilité se définit par l'accès permanent au canal à des services ou ressources pour toute entité du réseau. C'est-à-dire que les services des applications de gestions du trafic routier, de sécurité et de confort doivent être disponibles pour les véhicules légitimes les sollicitant. Pour assurer cette permanence des services, les réseaux véhiculaires doivent résister aux attaques de déni de service. Cependant, il est difficile de contrer une attaque de déni de service provoquée par un attaquant employant les moyens efficaces pour brouiller la totalité du spectre radio. Les techniques comme le saut de fréquence et le changement de technologie (DSRC, Ultra-TDD) [14, 15] permettent d'éviter les attaques opérées avec des capacités réduites.

2.5.2.6 Gestion de la vie privée

Les messages diffusés par les véhicules à travers le réseau véhiculaire peuvent leur être une source de menaces. Un attaquant pourra suivre un véhicule dans le réseau, recueillir toutes les données liées à ce véhicule ou à son propriétaire et les utiliser à des fins néfastes. Vu le danger que représente la traçabilité illégale des véhicules dans le réseau et aussi pour préserver la confidentialité des données, il est important d'adopter des mesures de sécurité afin de gérer la vie privée dans les réseaux véhiculaires sans fil.
L'un des objectifs de notre travail consiste à mettre en place un protocole de gestion de l'anonymat afin d'éviter la traçabilité illégale des véhicules et de préserver par la suite la vie privée des conducteurs des véhicules.

2.5.2.7 Contrôle d'accès

Il est important de contrôler les accès des entités aux ressources et services du réseau. Définir dans un premier temps les nœuds qui peuvent se connecter au réseau et garantir par la même occasion que les utilisateurs se conforment aux politiques de sécurités mises en place; tel est l'objectif du service de contrôle d'accès. Diverses applications se distinguent en fonction des niveaux d'accès accordés aux entités du réseau. Les applications de contrôle des feux tricolores peuvent être installées dans les voitures de police et de secours afin de faciliter le déplacement de ces dernières. On pourrait aussi retirer les privilèges ou exclure du réseau, un véhicule qui a un comportement anormal (non-respect du temps de transmission des messages beacon ou de changement des pseudonymes de communication) ou qui est détecté comme étant un attaquant.

2.6 Conclusion

Nous avons présenté dans cette première partie du mémoire les réseaux véhiculaires sans fil et décrit les éléments et concepts de sécurité de ces réseaux. En raison des contraintes temps réel des applications des systèmes de transport intelligents et de la forte mobilité des nœuds, les protocoles de sécurité des réseaux filaires sont inadaptés pour les réseaux VANETs. Il faut donc définir de nouveaux mécanismes de sécurité afin de protéger la vie des différents utilisateurs des réseaux véhiculaires sans fil.

Avant l'étude de notre protocole de gestion de l'anonymat et de la traçabilité, nous allons présenter dans le chapitre suivant, l'état de l'art à travers quelques travaux liés à la sécurité des réseaux VANETs.

Chapitre 3 - Revue de littérature

3.1 Introduction

Le fonctionnement des applications déployées dans les réseaux véhiculaires sans fil dépend des envois de messages entre les véhicules d'une part et entre les véhicules et les infrastructures routières d'autre part. En absence des mesures de sécurité, ces messages peuvent être des sources de menaces pour les entités du réseau. Diverses solutions ont été proposées pour sécuriser les messages et conserver l'identité des utilisateurs du réseau. Ces solutions vont du groupement des véhicules (cluster), aux changements de pseudonymes de communication afin d'assurer l'authentification, la confidentialité des données transmises dans le réseau et d'éviter la traçabilité illégale des voitures.

Dans le présent chapitre, nous résumerons certains travaux réalisés dans le contexte de la gestion des messages, du groupement des véhicules et du changement des pseudonymes de communication afin de répondre aux besoins de sécurité dans les réseaux véhiculaires sans fil.

3.2 Protocoles de sécurité liés à la gestion des messages

La sécurité liée à la gestion des messages vise à authentifier les messages reçus dans le réseau, à localiser les services et leurs fournisseurs à travers l'échange des données. Plusieurs protocoles ont été proposés dans la littérature pour répondre à ces exigences. Yong Hao, Tingting Han et Yu Cheng présentent dans [16] un protocole d'authentification des messages de façon coopérative. Le protocole proposé est adapté à l'environnement interurbain. L'objectif de l'étude est d'alléger la charge de calcul des OBUs dans le processus de vérification des messages échangés à travers le réseau. Ils définissent dans leur étude, deux types de véhicules: les vérificateurs de messages qui ont pour rôles de contrôler les messages diffusés à travers le réseau afin d'identifier ceux qui sont frauduleux.

Le second type de véhicules, qualifié de non-vérificateur de messages, attend les résultats des actions du premier type de véhicules. Dès qu'ils reçoivent des alertes de messages invalides, ils procèdent eux-mêmes à une seconde vérification de ces messages avant de les rejeter. Le protocole proposé permet d'une part d'authentifier les messages et aussi de traiter ces messages afin de diminuer le temps de calcul dû à la vérification des données transmises au sein du réseau. Ce qui conduit à éliminer les données frauduleuses. Kaouther Abrougui et Azzedine Boukerche présentent dans [17], un protocole d'identification et de localisation des fournisseurs de service dans le réseau. Il consiste à une propagation des demandeurs et fournisseurs de services. Ainsi par la découverte des voisins, les véhicules s'identifient en tant que fournisseurs ou demandeurs de services. Leur modèle permet donc aux véhicules de localiser et d'obtenir les services rapidement dans le réseau. Un algorithme basé sur une approche probabiliste est proposé pour sécuriser les messages dans [18]. Ce modèle permet de déterminer le niveau de confiance des messages échangés dans le réseau et de juger de la validité des messages reçus. Contrairement au modèle présenté dans [16], chaque véhicule vérifie le message reçu et juge si ce dernier est valide pour être retransmis ou non. Un modèle de vérification de la position des nœuds dans le réseau véhiculaire sans fil est proposé dans [19]. L'objectif de ce modèle est de détecter la position des nœuds malveillants qui diffusent de fausses informations concernant leur localisation et ainsi sécuriser la diffusion des paquets. Pour détecter la position du nœud malveillant dans le réseau, on tient compte de la position géographique de ses nœuds voisins et la portée de ses messages.

3.3 Sécurité basée sur le groupement des véhicules

Dans l'optique de protéger la vie et les données des utilisateurs du réseau véhiculaire sans fil, différentes études proposent de grouper les entités mobiles afin d'accroître le niveau de sécurité. Yong Hao, Yu Cheng, Chi Zhou et Wei Song proposent dans [20], une méthode de gestion des clés d'authentification basée sur des signatures de groupe.

Cette méthode utilise le protocole de message coopératif afin de réduire la charge de calcul due à l'implémentation de l'algorithme de signature de groupe.

Les groupes sont formés par chaque RSU disposé le long de la route et sont distingués par les clés des RSUs. Ainsi, font partie du même groupe, les véhicules utilisant une même clé RSU. Lorsqu'un véhicule entre dans la zone radio d'un RSU, il reçoit de ce dernier, une clé privée de groupe qu'il utilise pour communiquer avec les autres véhicules. Les auteurs proposent d'attribuer à chaque véhicule une clé privée de groupe et d'avoir une clé publique par groupe. Pour examiner la distribution des clés, identifier les RSUs pouvant être compromis, et les nœuds mobiles malveillants, ils ont développé un modèle analytique pour la couche MAC 802.11. Un modèle de pré-authentification est proposé dans [21]. Ce modèle repose sur le protocole d'authentification SRAP (Scable Robust authentication protocol) qui utilise une clé de groupe pour signer les messages. Les auteurs ont modifié les étapes d'attribution de la clé de groupe du protocole SRAP afin de réduire le nombre de paquets transmis durant la phase d'authentification et de diminuer le temps de calcul des clés. Dans [22], un protocole d'authentification de groupe est proposé. L'objectif de ce modèle est de gérer l'authentification des messages dans les réseaux véhiculaires sans fil en attribuant des clés dynamiques aux groupes de véhicules. Il permet donc d'accroître l'efficacité de l'authentification multicast dans les réseaux VANETs. Un modèle de groupe statique est présenté dans [23] pour gérer l'authentification, la confidentialité et la non-répudiation dans les réseaux véhiculaires sans fil. Bien que ce modèle permet aux véhicules d'échanger des messages sécurisés, il n'est pas très adapté pour les réseaux VANETs à cause de leur topologie dynamique. Un protocole de formation et de diffusion de messages sécurisés dans les réseaux véhiculaires sans fil est proposé dans [24]. Ce protocole utilise les modèles cryptographiques symétriques et asymétriques pour assurer la sécurisation des messages échangés. Quant à la formation de groupes de véhicules, elle découle de l'échange des clés publiques entre les véhicules. L'élection de la tête de groupe est basée sur la vitesse de déplacement des véhicules ainsi que leur portée de communication. Un algorithme de sécurité basé sur la formation des groupes est

présenté dans [25]. Le modèle se base sur la portée de communication des voitures pour former des groupes. Ainsi les véhicules sont liés à un groupe de façon dynamique dès qu'ils sont connectés au réseau. Le véhicule qui se trouve proche du centre du cercle délimité par le groupe auquel il appartient est la tête ou le leader du groupe. Si plusieurs véhicules sont proches du centre, le véhicule qui a un plus petit identifiant est élu tête de groupe.

Krishna Sampigethaya, Mingyan Li, Leping Huang, et Radha Poovendran présentent dans [26] un modèle de gestion de la traçabilité illégale dans les réseaux véhiculaires sans fil. Leur idée est de considérer la navigation des voitures sur la route afin de former des groupes avec des véhicules se trouvant dans une même zone radio. Le protocole proposé est testé dans les milieux autoroutiers et interurbains et présente des résultats significatifs afin de gérer l'authentification, la confidentialité et la traçabilité illégale des nœuds mobiles. Un modèle de transmission des messages d'alerte est proposé dans [27]. Ce modèle se base sur la formation des groupes de véhicules afin d'améliorer la transmission des messages d'alerte dans les réseaux véhiculaires sans fil. Les véhicules qui se trouvent dans une même zone géographique forment un groupe et communiquent par l'intermédiaire du leader de groupe avec les autres véhicules afin de diffuser des informations d'alerte. Dans [28], les auteurs proposent un protocole de signature de groupe afin de préserver la confidentialité des données échangées entre les nœuds mobiles. Leur modèle est très utile et permet de détecter les nœuds malveillants grâce à une approche probabiliste lors de la diffusion des messages par les véhicules. Ils ont étudié les phases suivantes dans leur proposition: la génération de signature de groupe, la vérification de signature, l'autorisation de vérifier les signatures, le contrôle et la détection des anomalies dans les messages ainsi que la gestion du pare-feu. Un système d'authentification dans les réseaux VANETs basé sur la communication de groupe est proposé dans [29]. Ce modèle utilise l'échange des clés publiques cryptographiques (PKC en Anglais) pour former des groupes de véhicules. Après la formation des groupes, chaque tête de groupe ou leader choisit aléatoirement une clé qui est utilisée comme clé de groupe. Il faut noter que chaque véhicule possède un ensemble de clés

cryptographiques. La communication de groupe basée sur la cryptographie à clé symétrique est proposée dans [30]. Malgré que ce modèle permet de gérer l'authentification et de préserver la confidentialité des données, la formation des groupes n'est pas dynamique. Ce qui pose un problème à son adaptation à l'environnement des réseaux véhiculaires sans fil à cause de leur topologie dynamique. Dans [31], les auteurs ont utilisé la cryptographie à clés publiques (PKI en Anglais) pour présenter un modèle de communication de groupe. Dans leur modèle, chaque nœud mobile possède un certificat qui est utilisé pour l'authentification. Les informations de localisation des nœuds sont utilisées pour former les groupes. L'inconvénient de ce modèle est qu'il nécessite plus de temps de calcul dans la phase de chiffrement et de déchiffrement des clés parce que chaque nœud vérifie le message reçu avant de le retransmettre. Dans [32], un protocole de gestion de la vie privée est proposé. Ce protocole utilise les algorithmes de signatures de groupe et de signature basée sur l'identifiant afin de sécuriser les messages échangés entre les différents nœuds du réseau. L'algorithme de signature de groupe est utilisé pour sécuriser la communication entre les OBUs. Alors que l'algorithme de signature basé sur l'identifiant est utilisé pour authentifier les RSUs. Le modèle proposé permet d'assurer l'authentification des nœuds du réseau et d'éviter la traçabilité illégale des véhicules. Cependant si l'envoi de la clé privée du groupe n'est pas sécurisé, un intrus peut l'intercepter et ainsi violer les propriétés de confidentialité des données.

3.4 Sécurité basée sur les pseudonymes de communication

Les clés cryptographiques utilisées par les entités mobiles dans le but de sécuriser les échanges de données dans le réseau peuvent contenir des informations liées à leur identité. Pour éviter qu'un adversaire ne découvre l'identité d'un véhicule ou le localise lorsque ce dernier communique, de nombreux auteurs suggèrent que les nœuds mobiles utilisent différents pseudonymes pour communiquer. Ces pseudonymes ne contiennent pas des informations révélant l'identité réelle du véhicule. Le changement périodique des pseudonymes permettra non seulement de protéger les données transmises sur le réseau;

mais aussi d'éviter la traçabilité illégale des voitures. Dans cette perspective, Huang Lu et autres présentent dans [33], un modèle d'authentification intégrant la gestion de la confidentialité. Le modèle proposé utilise le mécanisme de signature basé sur l'identifiant (IBS: ID-based Signature) et celui basé sur l'identifiant en ligne et hors ligne (IBOSS: ID-based Online/Offline Signature). Le mécanisme de signature basé sur l'identifiant permet de gérer l'authentification entre les véhicules et les RSUs. Celui basé sur l'identifiant en ligne/hors ligne gère l'authentification entre les véhicules. Les deux méthodes d'authentification reposent sur la cryptographie liée à l'identifiant. Cette méthode cryptographique consiste à déduire la clé publique d'une entité à partir de ses données publiques (le nom, l'adresse email,..). Le véhicule reçoit auprès du RTA (Regional Trusted Authority) les identifiants des RSUs présents dans la zone qu'il désire parcourir et les stocke. Pour communiquer avec les autres véhicules, le véhicule génère un pseudonyme qu'il envoie au RSU de sa proximité. À la réception du pseudonyme du véhicule, le RSU génère un nouveau pseudonyme qu'il diffuse aux véhicules de sa zone. Ce nouveau pseudonyme sera utilisé par les véhicules pour communiquer entre eux de façon sécuritaire. Le modèle proposé s'adapte à l'authentification et préserve la confidentialité des informations diffusées dans le réseau. Mais les auteurs n'ont pas expliqué la disposition des RSUs sur la route et le facteur intervenant dans le changement des pseudonymes de communication. Ils proposent que les véhicules changent leurs pseudonymes de manière volontaire. Un protocole d'authentification basé sur l'usage des pseudonymes est présenté dans [34]. Dans ce protocole, chaque véhicule s'enregistre auprès de la centrale d'autorité pour recevoir un ticket. Le véhicule communique le ticket reçu au RSU situé dans sa zone radio qui se charge de transmettre au véhicule un ensemble d'information lui permettant de générer ses pseudonymes de communication. L'inconvénient de ce travail réside dans la gestion des pseudonymes. Les auteurs n'ont pas expliqué comment les véhicules prennent connaissance des pseudonymes de leurs voisins directs afin de décrypter les messages reçus, ni sur quelle base les véhicules changent leurs pseudonymes de communication.

Dans [35], les auteurs proposent un protocole de changement périodique de pseudonymes de communications des véhicules connectés aux réseaux VANETs dans les lieux publics. Chaque véhicule s'enregistre auprès de la centrale d'autorité et reçoit une clé anonyme lui permettant de générer en fonction de son trajet les pseudonymes de communication à utiliser. Durant leur trajet, les véhicules sont invités à changer leurs pseudonymes de communication soit dans les lieux de stationnement ou aux intersections. Ce modèle permet d'empêcher la collecte d'information sur la vitesse et le trajet d'un véhicule par un attaquant lorsque ce dernier change son pseudonyme de communication. Un modèle d'utilisation de différents pseudonymes dans chaque zone radio de RSU est proposé dans [36]. Dans ce modèle, chaque véhicule vérifie et valide le message reçu de ses voisins en communiquant toujours avec le RSU situé à sa portée. Une nouvelle approche basée sur la communication entre OBU et RSU dans le but de générer les pseudonymes est proposée dans [37]. Dans cette approche, le véhicule échange des données avec le RSU situé à sa portée à chaque fois qu'il a besoin d'utiliser un pseudonyme. Ce processus permet de réduire le délai et la surcharge du système causés par le stockage des pseudonymes de communication. Cependant, quand le nombre de véhicules sur la route devient important, ce modèle peut affecter la performance du réseau. Dans [38, 39], les auteurs proposent un mécanisme de changement de pseudonymes de communication. Dans ce modèle, les véhicules génèrent eux-mêmes les pseudonymes. Chaque véhicule s'enregistre auprès de la centrale d'autorité et reçoit une trousse d'information qu'il pourra utiliser pour générer ses pseudonymes de communication. Bien que le modèle présenté dans ces deux articles aide les véhicules à utiliser différents pseudonymes pour communiquer, peu d'explication est fournie sur la diffusion des pseudonymes des véhicules du réseau. Aussi les auteurs n'ont pas analysé l'impact du changement de pseudonymes de communication sur les ressources du réseau en termes de consommation de bande passante et de perte de paquets.

3.5 Conclusion

L'authentification et la confidentialité ont été étudiées sous diverses formes afin d'éviter la traçabilité illégale des véhicules et protéger les informations qu'ils échangent. Même si l'utilisation de différents pseudonymes de communication permet d'avoir un bon niveau de sécurité dans les réseaux véhiculaires sans fil, la plupart des études utilisant ce concept n'ont pas défini un intervalle de temps durant lequel les véhicules peuvent changer leurs pseudonymes en toute discrétion. Afin de pallier cet inconvénient, nous proposons dans le chapitre suivant un protocole de sécurité pour gérer l'anonymat et la traçabilité dans les réseaux véhiculaires en tenant compte du temps de changement des pseudonymes de communication.

Chapitre 4 - Gestion de l'anonymat et de la traçabilité dans les réseaux VANETs

4.1 Introduction

La communication entre les différentes entités du réseau véhiculaire sans fil se fait sur un canal partagé. Pour protéger les données échangées par les entités (les nœuds mobiles en particulier) et leur identité, de nombreuses études suggèrent l'utilisation de différents pseudonymes de communication par les véhicules. Cependant, peu de ces études ont évalué l'impact que pourrait avoir le changement périodique des pseudonymes de communication sur le réseau en matière de la consommation de la bande passante, par exemple. De ce fait, nous proposons dans le cadre de ce mémoire l'étude d'un protocole de changement périodique des pseudonymes de communication afin de gérer l'anonymat et la traçabilité illégale des véhicules.

Dans ce chapitre, nous aborderons dans un premier temps, les exigences de sécurité et les défis auxquels notre proposition répond. Ensuite, nous présenterons notre modèle de gestion de l'anonymat et de la traçabilité et une analyse de sécurité de ce dernier.

4.2 Exigences de sécurité et défis

L'objectif de notre étude pour la gestion de l'anonymat et la traçabilité est de tenir compte d'un certain nombre de principes de sécurité susceptibles de convenir, dans une perspective de déploiement, au contexte de la communication à travers les réseaux VANETs. Pour cela, nous avons retenu les exigences de sécurité suivantes:

- **Authentification**: L'accès aux ressources et services du réseau par le véhicule ou un nœud mobile se fait après que ce dernier ait reçu une autorisation de la centrale d'autorité. Ce qui veut dire que tous les véhicules du réseau s'enregistrent auprès de la centrale d'autorité afin de bénéficier des services du réseau.

- **Sécurité des données d'authentification**: Dans notre proposition, les nœuds mobiles s'authentifient en envoyant leur identifiant réel ou des clés liées à leur identité. Pour éviter toute modification ou altération malveillante de ces données, il est indispensable de mettre en place un contrôle d'intégrité sur les données.
- **L'intimité (privacy en Anglais):** La préservation de l'intimité recouvre les concepts de non-traçabilité et de gestion de l'anonymat. Cependant, il doit être possible de révéler l'identité des véhicules pour satisfaire les requêtes judiciaires.

Compte tenu de la topologie dynamique des réseaux véhiculaires sans fil (due à la forte mobilité des véhicules), notre solution doit faire face aux contraintes temps réel. En effet, si on considère que la majorité des services liés à la sécurité ne pourraient être opérés sans le processus d'authentification, il importe donc que ce processus soit rapide et moins coûteux en termes de latence. Aussi, notre modèle doit permettre d'éviter les attaques sur la vie privée, la cohérence d'information et l'usurpation de l'identité afin de permettre aux entités du réseau de profiter pleinement des services offerts dans le réseau. Pour faire face à ces exigences de sécurité et défis, nous avons tenu compte dans le cadre de notre étude, de l'utilisation des algorithmes de cryptographie symétrique et asymétrique basée sur les courbes elliptiques pour sécuriser les messages. Ces algorithmes offrent un bon niveau de sécurité et nécessitent peu de calcul et de ressource.

4.3 Gestion de l'anonymat et de la traçabilité

Notre proposition pour la gestion de l'anonymat et de la traçabilité illégale dans les réseaux véhiculaires sans fil s'inscrit dans le contexte où tout véhicule après s'être authentifié auprès de la centrale d'autorité, doit changer après un temps son pseudonyme de communication afin d'avoir accès à nouveau aux services du réseau. À la différence des travaux existants, notre contribution permettra d'analyser l'impact de la vitesse des véhicules sur le changement de pseudonymes et de déduire la disposition des RSUs sur la route afin de garantir une meilleure communication RSU-véhicule.

4.3.1 Modèle de gestion de l'anonymat et de la traçabilité

L'apport de notre travail est de définir un intervalle de temps T au cours duquel au moins deux véhicules pourront changer leurs pseudonymes de communication. Ceci dans le but de préserver la confidentialité des données échangées et éviter la traçabilité illégale; tout en tenant compte de la qualité de service et des exigences des réseaux VANETs.

Pour résoudre ce problème, nous proposons dans le cadre de ce mémoire, l'étude d'un protocole basé sur la plage des vitesses de déplacements des véhicules et *la distribution équidistante* des RSUs, afin d'aider les entités mobiles à changer leurs pseudonymes de communication dans un même intervalle de temps. Le protocole proposé est étudié selon deux approches différentes.

Dans cette sous-section, après avoir expliqué la disposition des RSUs sur la route et l'obtention de l'intervalle de changement des pseudonymes de communication, nous allons détailler les deux approches d'étude proposées.

4.3.1.1 Disposition des RSUs

Dedicated Short Range Communication (DSRC) propose des technologies dédiées aux réseaux véhiculaires sans fil. Nous allons nous baser sur la portée de communication proposée par cette norme afin de déduire une distribution équidistante des unités de routes.

Soit X la portée de communication de la norme DSRC (en m); on considère une route de longueur L (en m). Le nombre de RSU à distribuer de façon équidistante sur la route de longueur L est :

$$n_{RSU} = \frac{L}{X} (1)$$

La distance entre chaque RSU est égale à X.

La figure 4.1 montre la disposition des RSUs sur la route de longueur L.

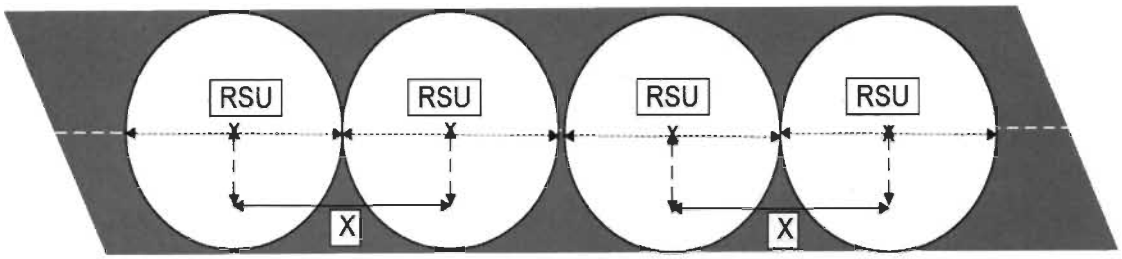


Figure 4.1: Disposition des RSUs sur une route de longueur L

4.3.1.2 Intervalle de changement de pseudonymes de communication

L'objectif dans cette partie est de déterminer l'intervalle de temps pendant lequel au moins deux véhicules peuvent changer leurs pseudonymes de communication.

Soient V_{min} et V_{max} respectivement vitesse minimale et maximale autorisées sur une route. On suppose qu'il y a un véhicule qui roule à la vitesse V_{max} tout au long de son trajet. Soit Veh_A ce véhicule qui roule à la vitesse V_{max}. Pour que Veh_A change au moins une fois ses pseudonymes de communication, la durée d de ces derniers doit être égale à:

$$d = \frac{X}{V_{max}} (2)$$

Admettons qu'au moins deux véhicules roulent avec une vitesse moyenne V_{moy} et qu'il n'y a aucun véhicule qui roule avec une vitesse minimale durant tout son trajet. Ce qui nous permet de dire que la vitesse du déplacement du véhicule varie entre V_{moy} et V_{max}. En considérant ces hypothèses, nous pouvons définir l'intervalle de changement des pseudonymes de communication comme suit:

$$\text{Vitesse moyenne } V_{moy}\text{: } V_{moy} = \frac{V_{max}+V_{min}}{2} (3)$$

La durée (d_{moy}) des pseudonymes pour un véhicule qui roule à la vitesse V_{moy} est:

$$d_{moy} = \frac{X}{V_{moy}} (4).$$

Avec (1) et (4), l'intervalle T de changement de pseudonymes de communication

$$\text{est: } T = \left[\frac{X}{V_{max}}; \frac{X}{V_{moy}}\right] (5).$$

Durant l'intervalle T, la demande de pseudonymes de communication se fera par au moins deux véhicules à chaque distance X parcourue. En plus, nous avons supposé qu'un véhicule ne roule pas avec une vitesse supérieure à la vitesse V_{max}.

4.3.1.3 Approche 1 du protocole de changement de pseudonymes de communication

Dans l'approche 1 de notre étude, les véhicules interagissent avec la Centrale d'Autorité (CA) par l'intermédiaire des RSUs, pour avoir leurs pseudonymes de communication. Les notations utilisées dans cette approche sont expliquées dans le tableau 4.1.

Termes	Explication
V_rid	Identifiant réel du véhicule
V_cert	Certificat du véhicule
V_prpseudo	Pseudonyme privé du véhicule
V_vid	Identifiant virtuel du véhicule
R_prKey	Clé privée du RSU
R_pbKey	Clé publique du RSU
E_RpbKey(V_rid)	Fonction asymétrique pour chiffrer l'identifiant réel du véhicule avec la clé publique du RSU
E_V_rid(V_prpseudo+V_vid)	Fonction symétrique pour chiffrer le pseudonyme privé et l'identifiant virtuel du véhicule avec son identifiant réel
Br(V_cert)	Diffusion broadcast du certificat du véhicule
E_V_rid(V_vid)	Fonction symétrique pour chiffrer l'identifiant virtuel du véhicule avec son identifiant réel.
E_V_rid(V'_prpseudo+V'_vid)	Fonction symétrique pour chiffrer le nouveau pseudonyme du véhicule et son nouvel identifiant virtuel avec l'identifiant réel du véhicule
V'_cert	Nouveau certificat du véhicule
Br(V'_cert)	Diffusion broadcast du nouveau certificat du véhicule
V_pbpseudo	Pseudonyme public du véhicule
T_{V_cert}	Temps de validité du certificat du véhicule
V'_prpseudo	Nouveau pseudonyme privé du véhicule
V'_vid	Nouvel identifiant virtuel du véhicule

Tableau 4.1: Termes utilisés dans l'approche 1

a. Hypothèses de l'approche 1

- Chaque véhicule a un identifiant (V_rid) qu'il utilise pour s'authentifier auprès de la CA.
- Les clés publiques des RSUs sont accessibles aux véhicules tout au long de leurs trajets. Ces clés sont certifiées et périodiquement mises à jour par la CA.
- La CA déchiffre tout message chiffré avec la clé publique du RSU.
- La clé publique du RSU est certifiée et périodiquement mise à jour par la CA.
- La CA est toujours accessible et contrôle les RSUs.

b. Description de l'approche 1

Pour avoir ses pseudonymes de communication, chaque véhicule utilise la clé publique du RSU pour chiffrer son identifiant réel et l'envoyer à la CA. La CA déchiffre le paquet reçu du véhicule avec la clé privée du RSU correspondant et enregistre l'identifiant du véhicule. Après avoir enregistré l'identifiant du véhicule, la CA génère à ce dernier un identifiant virtuel plus un pseudonyme privé. La CA envoie au véhicule un paquet crypté avec l'identifiant réel du véhicule contenant son pseudonyme privé et son identifiant virtuel. En parallèle, la CA génère le certificat du véhicule et l'envoie au RSU proche de ce dernier. Ce certificat contient les données relatives au véhicule (son identifiant virtuel, son pseudonyme public et le temps d'expiration du certificat) qui a fait la demande de pseudonyme. À la réception du certificat du véhicule, le RSU diffuse le certificat reçu. Lorsque les véhicules situés à la portée du RSU reçoivent le certificat diffusé, ils récupèrent le pseudonyme public du nœud qui s'est enregistré auprès de la CA et ils peuvent donc communiquer avec ce dernier en envoyant des messages chiffrés avec son pseudonyme public. Pour récupérer son pseudonyme privé et son identifiant virtuel, le véhicule utilise son identifiant réel pour déchiffrer le paquet reçu de la CA.

À l'expiration du certificat, le véhicule envoie son identifiant virtuel chiffré avec son identifiant réel à la CA.

Après vérification des informations reçues, la CA génère un nouveau pseudonyme privé pour le véhicule ainsi qu'un nouvel identifiant virtuel qu'il envoie au véhicule.

Dans le même temps, la CA transmet au RSU, le nouveau certificat du véhicule. Ce certificat est diffusé aux autres véhicules par le RSU.

c. Schémas descriptifs de l'approche 1

Nous allons présenter les schémas descriptifs des étapes de l'approche 1 dans cette section.

- **Authentification**

Pour s'authentifier, le véhicule envoie à la CA, son identifiant réel (V_rid) crypté avec la clé publique du RSU (R_pbKey). Le véhicule utilise la fonction E_RpbKey(V_rid) pour sécuriser son message. Cette fonction asymétrique permet de chiffrer l'identifiant réel du véhicule avec la clé publique du RSU. La figure 4.2 montre la phase d'authentification de l'approche 1.

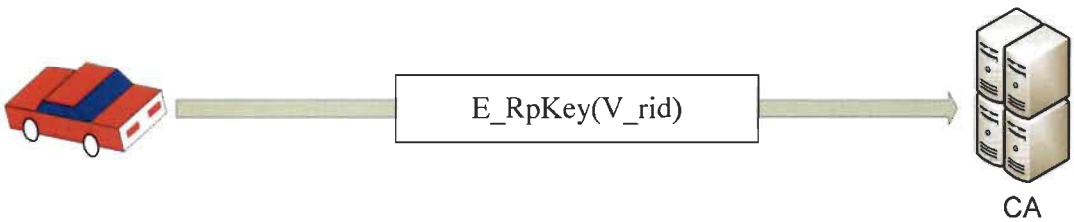


Figure 4.2: Authentification dans l'approche 1

- **Réception du pseudonyme privé**

À la réception du message d'authentification du véhicule, la CA envoie au véhicule son pseudonyme privé ainsi que son identifiant virtuel. Elle utilise la fonction E_V_rid(V_prpseudo+V_vid). Cette fonction permet de chiffrer le pseudonyme privé du véhicule et son identifiant virtuel avec l'identifiant réel du véhicule. La figure 4.3 décrit l'étape de réception du pseudonyme privé par le véhicule.

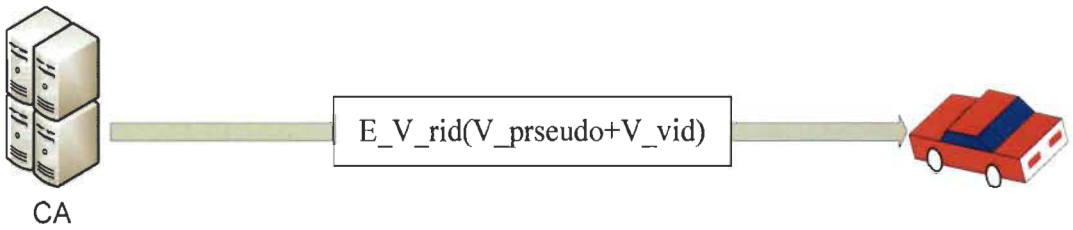


Figure 4.3: Réception du pseudonyme privé dans l'approche 1

- **Réception du certificat**

Après avoir envoyé le pseudonyme privé au véhicule, la CA envoie au RSU le certificat du véhicule (V_cert). Ce dernier diffuse le certificat du véhicule dans le réseau. La réception du certificat est décrite à la figure 4.4.

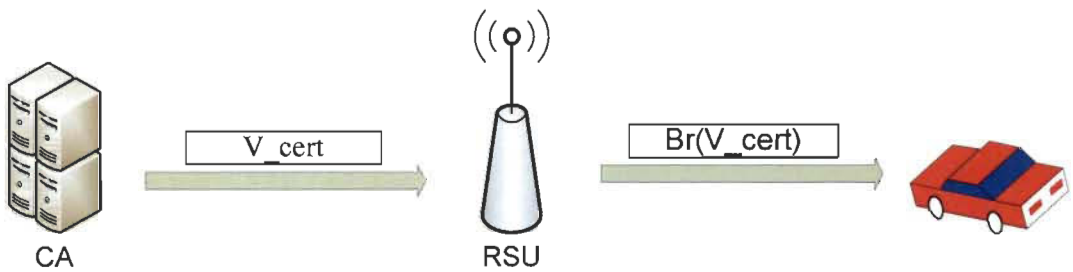


Figure 4.4: Réception du certificat dans l'approche 1

- **Mise à jour du pseudonyme privé et du certificat**

La mise à jour du pseudonyme privé et du certificat se déroule en trois étapes :

- Le véhicule envoie à la CA son identifiant virtuel chiffré avec son identifiant réel (E_V_rid(V_vi)). La figure 4.5 illustre cette étape.

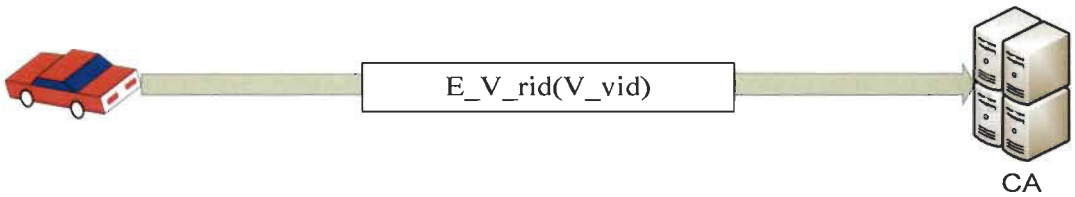


Figure 4.5: Envoi de l'identifiant virtuel

- La CA, à la réception de l'identifiant virtuel du véhicule, délivre au véhicule un nouveau pseudonyme privé (V'_prpseudo) et un nouvel identifiant virtuel (V'_vid). Cette étape est présentée sur la figure 4.6.

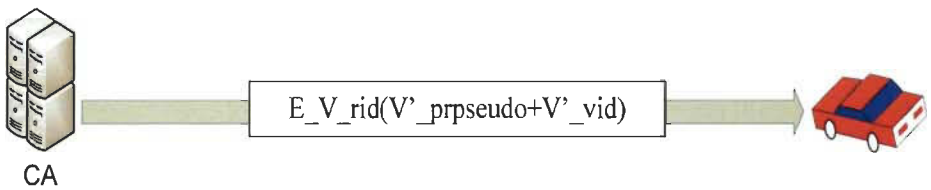


Figure 4.6: Mise à jour du pseudonyme privé et de l'identifiant virtuel

- après la CA envoie le nouveau certificat du véhicule (V'_cert) au RSU qui le diffuse (Br(V'_cert)). La figure 4.7 décrit cette étape.

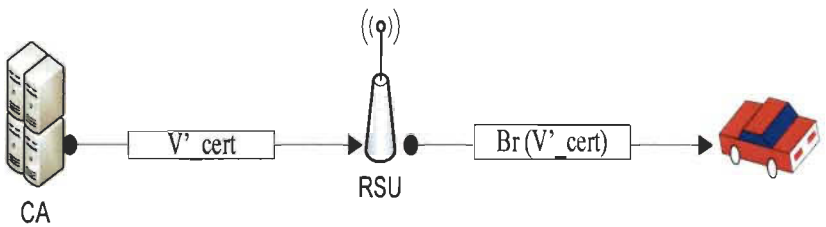


Figure 4.7: Diffusion du nouveau certificat du véhicule

d. Enregistrement des données par la CA et le véhicule

Lors des échanges des messages concernant des pseudonymes de communication, les entités (véhicules et CA) enregistrent les données qu'ils reçoivent. Les CA sauvegardent les données relatives aux véhicules dans une table. De même chaque véhicule enregistre les pseudonymes publics de ses voisins tout le long de son trajet.

Présentation de la table d'enregistrement des données:

- **Chez la CA**

Identifiant Véhicule	Pseudonyme privé	Certificat
V_rid_{V1}	$V\_prpseudo_{V1}$	V_cert_{V1}
V_rid_{V2}	$V\_prpseudo_{V2}$	V_cert_{V2}
...	...	...
V_rid_{Vn}	$V\_prpseudo_{Vn}$	V_cert_{Vn}

Tableau 4.2: Enregistrement des données des véhicules chez la CA (approche 1)

La CA enregistre pour chaque véhicule son identifiant réel, le pseudonyme privé et le certificat qu'elle a attribué au véhicule. Le tableau 4.2 résume les données enregistrées par la CA.

- **Chez le véhicule**

À la réception du certificat, chaque véhicule le décompresse et extrait le contenu dans une table. Le tableau 4.3 présente les informations enregistrées par le véhicule.

Identifiant virtuel	Pseudonyme public	Temps d'expiration
V_vid_{V1}	$V\_pbpseudo_{V1}$	$T_{V\_cert_{V1}}$
V_vid_{V2}	$V\_pbpseudo_{V2}$	$T_{V\_cert_{V2}}$
...	...	...
V_vid_{Vn}	$V\_pbpseudo_{Vn}$	$T_{V\_cert_{Vn}}$

Tableau 4.3: Enregistrement des données chez le véhicule (approche 1)

N. B. Pour éviter une surcharge des données chez le véhicule, nous proposons que les véhicules ne conservent que les informations en cours d'utilisation; c'est-à-dire que les véhicules ne gardent que les contenus du certificat valide.

4.3.1.4 Approche 2 du protocole de changement de pseudonymes de communication

Dans l'approche 2, les véhicules sont moins dépendants des RSUs. En effet, dans cette approche, les véhicules génèrent leurs propres pseudonymes privés et certificats. Aussi chaque véhicule diffuse son propre certificat. Les termes utilisés dans cette approche sont définis dans le tableau 4.4.

Termes	Explication
V_prKey	Clé privée du véhicule
V_pbKey	Clé publique du véhicule
R_prKey	Clé privée du RSU
R_pbKey	Clé publique du RSU
Vpseudcertif	Paquet de données permettant au véhicule de générer pseudonyme et certificat
V_cert	Certificat du véhicule
V_prpseudo	Pseudonyme privé du véhicule
V'_prpseudo	Nouveau pseudonyme privé du véhicule
V'_cert	Nouveau certificat du véhicule
E_RpbKey(V_prkey+V_pbkey)	Fonction asymétrique permettant de chiffrer la clé privée et publique du véhicule avec celle du RSU
E_VpbKey(Vpseudcertif)	Fonction asymétrique permettant de chiffrer le paquet de données avec la clé publique du véhicule
V_pbpseudo	Pseudonyme public du véhicule
T_{V_cert}	Temps de validité du certificat du véhicule

Tableau 4.4: Termes utilisés dans l'approche 2

a. Hypothèses de l'approche 2

- Chaque véhicule est identifié par une paire de clés privées/publiques
- Les clés publiques des RSUs sont accessibles aux véhicules tout au long de leurs trajets.
- La CA connaît la clé privée du RSU.
- La clé publique du RSU est certifiée et périodiquement mise à jour par la CA.
- La CA est toujours accessible et contrôle les RSUs.

b. Description de l'approche 2

Lorsqu'un véhicule souhaite avoir ses pseudonymes de communication, il envoie sa paire de clés (privée/publique) cryptées avec la clé publique du RSU à la CA. Après avoir déchiffré le paquet, la CA enregistre la paire de clés du véhicule et envoie à ce dernier un paquet de données lui permettant de générer ses pseudonymes et certificats à chaque intervalle de temps. Pour protéger le contenu message envoyé au véhicule, la CA chiffre le message avec la clé publique du véhicule. À la réception du message de la CA, le véhicule qui a fait la demande, déchiffre le message avec sa clé privée et extrait le paquet d'information. Il utilise le paquet d'information pour générer son pseudonyme privé ainsi que le certificat associé. Après il diffuse le certificat généré aux entités localisées dans sa zone radio. Comme dans l'approche 1, le certificat généré contient le pseudonyme public du véhicule, et le temps de validité du certificat.

À l'expiration de son certificat, le véhicule génère un nouveau pseudonyme privé ainsi qu'un certificat associé qu'il diffuse. En résumé dans l'approche 2, les véhicules communiquent une seule fois avec la CA afin d'avoir le paquet de données leur permettant de générer les pseudonymes privés et les certificats.

c. Schémas descriptifs de l'approche 2

Les schémas descriptifs des différentes étapes de l'approche 2 seront présentés dans cette partie.

- **Authentification**

Le véhicule envoie ses clés privée et publique (V_prkey et V_pbkey) chiffrées avec la clé publique du RSU à la CA. La figure 4.8 résume cette phase d'authentification.

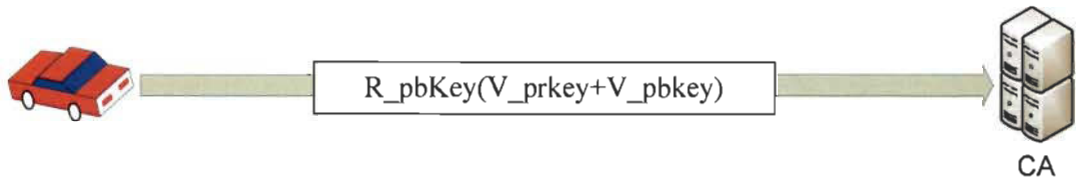


Figure 4.8: Authentification dans l'approche 2

- **Réception du paquet de génération de pseudonyme privé et certificat**

La CA délivre au véhicule un paquet de données lui permettant de générer ses pseudonymes privés et certificats (Vpseudcertif) après avoir enregistré le véhicule. La figure 4.9 décrit la phase de réception du pseudonyme privé et du certificat.

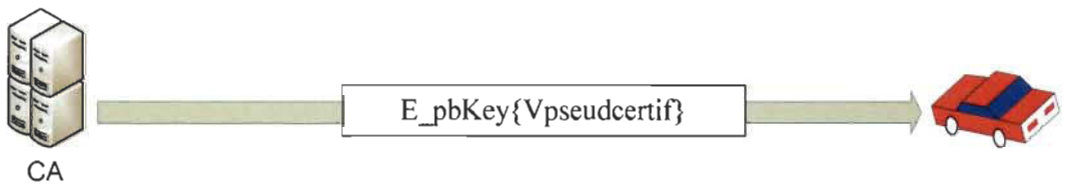


Figure 4.9: Réception du paquet de génération de pseudonymes privés et certificats

- **Diffusion du certificat**

Lorsque le véhicule reçoit le paquet d'information, le véhicule génère son pseudonyme privé et le certificat correspondant périodiquement et diffuse son certificat afin de créer son groupe de communication. La figure 4.10 résume la diffusion du certificat.

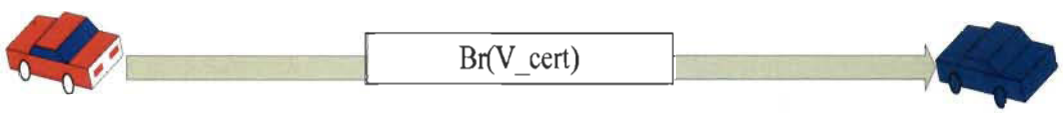


Figure 4.10: Diffusion du certificat par le véhicule dans l'approche 2

À l'expiration du certificat, le véhicule génère un nouveau pseudonyme privé ainsi qu'un nouveau certificat qu'il diffuse (voir figure 4.11).

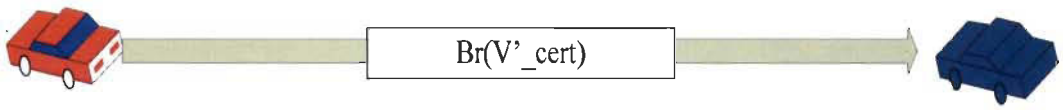


Figure 4.11: Diffusion du certificat par le véhicule dans l'approche 2

e. Enregistrement des données par la CA et le véhicule

Comme dans l'approche 1, la CA et les véhicules tiennent à jour chacun, une table dans laquelle sont enregistrées les données concernant les pseudonymes.

Présentation de la table d'enregistrement des données

- **Chez la CA**

Clé privée du Véhicule	Clé publique du véhicule	Forfait de données
V_prKey_{V1}	V_pbKey_{V1}	$Vpseudcertif_{V1}$
V_prKey_{V2}	V_pbKey_{V2}	$Vpseudcertif_{V2}$
...	...	...
V_prKey_{Vn}	V_pbKey_{Vn}	$Vpseudcertif_{Vn}$

Tableau 4.5: Enregistrement des données par la CA (approche 2)

La CA enregistre les clés privées et publiques des véhicules ainsi que le paquet de données leur permettant de générer le pseudonyme privé et le certificat (Tableau 4.5).

- **Chez le véhicule**

À la réception du certificat, chaque véhicule le décompresse et extrait le contenu dans une table (Tableau 4.6).

Pseudonyme public	Temps d'expiration
$V\_pbpseudo_{V1}$	$T_{V\_cert_{V1}}$
$V\_pbpseudo_{V2}$	$T_{V\_cert_{V2}}$
...	...
$V\_pbpseudo_{Vn}$	$T_{V\_cert_{Vn}}$

Tableau 4.6: Enregistrement des données par le véhicule (approche 2)

N. B. Les véhicules conservent uniquement les données du certificat valide (en cours d'utilisation).

4.4 Analyse de sécurité du protocole

Après avoir décrit les deux approches du protocole proposé, nous allons dans cette partie, analyser la sécurité du modèle par rapport à quelques concepts de sécurité présentés dans le premier chapitre.

4.4.1 Authentification

Dans les deux approches de notre étude, seuls les véhicules qui se sont enregistrés auprès de la CA, peuvent utiliser les services du réseau. En d'autres termes, la CA connaît l'identité de tous les véhicules du réseau. Aussi, les RSUs sont sous le contrôle de la CA. On peut déduire que notre protocole répond au concept de l'authentification.

4.4.2 Non-répudiation

Les véhicules communiquent avec un pseudonyme certifié reçu de la CA. En cas de conflit, la CA peut facilement révéler l'identité réelle du véhicule. Les véhicules sont identifiés auprès de la CA dans l'approche 1 par leur identifiant alors que dans l'approche 2, ils sont identifiés par leurs clés privée et publique.

4.4.3 Gestion de la vie privée

Chaque véhicule communique avec des pseudonymes de courte durée (durée exprimée dans notre étude en seconde). Les pseudonymes sont mis à jour périodiquement et ne sont pas liés. En plus le changement de pseudonymes se fait par au moins deux véhicules. Un attaquant ne pourra pas avec certitude identifier le véhicule qui a changé son pseudonyme de communication. Les pseudonymes utilisés par les véhicules ne contiennent pas leurs identités réelles. Même si un attaquant intercepte le message contenant le pseudonyme du véhicule, il ne pourra pas l'utiliser pour révéler l'identité du véhicule, le localiser ou bien connaître les données de son propriétaire. On voit bien donc que notre modèle permet d'éviter la traçabilité illégale.

4.5 Conclusion

L'étude conceptuelle du protocole de gestion de l'anonymat et de la traçabilité a été réalisée dans ce chapitre. Les analyses de sécurité prouvent que les deux approches du modèle proposé répondent aux concepts de sécurité suivant: l'authentification, la non-répudiation et la gestion de la vie privée.

Avant de présenter les résultats des simulations de notre modèle, nous allons décrire brièvement, dans le chapitre suivant, les simulateurs généralement utilisés pour évaluer les performances des protocoles dans les réseaux VANETs.

Chapitre 5 - Présentation des simulateurs

5.1 Introduction

L'étude des performances d'un protocole de réseau véhiculaire sans fil, fait appel à deux types de simulateurs: le simulateur de trafic routier et le simulateur réseau. Le simulateur de trafic routier permet de générer la mobilité des véhicules sur une carte. Le simulateur réseau modélise le comportement des différentes entités du réseau; c'est-à-dire qu'il permet de gérer les interactions entre les différents nœuds du réseau.

Dans ce chapitre, nous allons présenter le simulateur de trafic routier SUMO et deux simulateurs réseau NS2 et OMNET++ qui sont souvent utilisés pour simuler des réseaux VANETs.

5.2 Le simulateur de trafic routier: SUMO

SUMO (Simulation of Urban Mobility) est un progiciel de simulations de trafic routier open source sous licence GNU public (GPL), dont le développement a commencé en 2002. L'objectif des développeurs est de mettre à la disposition du monde académique un outil leur permettant de modéliser le réseau routier aussi bien en milieu urbain qu'environnement autoroutier. Le progiciel SUMO contient une suite d'applications qui aident à préparer et à exécuter la simulation d'un scénario de trafic routier. Les différentes applications incluses dans la suite SUMO seront présentées dans cette sous-section en fonction de leur objet d'étude [41].

5.2.1 Génération du réseau routier

Les réseaux routiers du monde réel sont reproduits dans SUMO comme un graphe où les sommets (nœuds) correspondent aux intersections tandis que les arêtes représentent les routes. Le réseau routier SUMO comprend des plans de feux de circulation et les connexions entre les voies à travers des intersections. Les réseaux routiers peuvent être directement générés à l'aide de l'application « netgenerate » ou par importation des fichiers de carte routière de l'OpenStreetMap [40] avec l'application « netconvert ». En outre, netconvert permet de lire les fichiers XML représentant un graphe réseau routier. On distingue 5 types de fichiers XML qui décrivent les nœuds, les routes, les types de routes, les connexions entre les voies et le plan des feux de circulation. Les applications netgenerate et netconvert partagent la même bibliothèque pour générer ou importer les réseaux routiers dans le simulateur. Elles utilisent les méthodes heuristiques pour corriger les données manquantes dans les fichiers XML. L'étape de génération d'un réseau routier est résumée sur la figure 5.1.

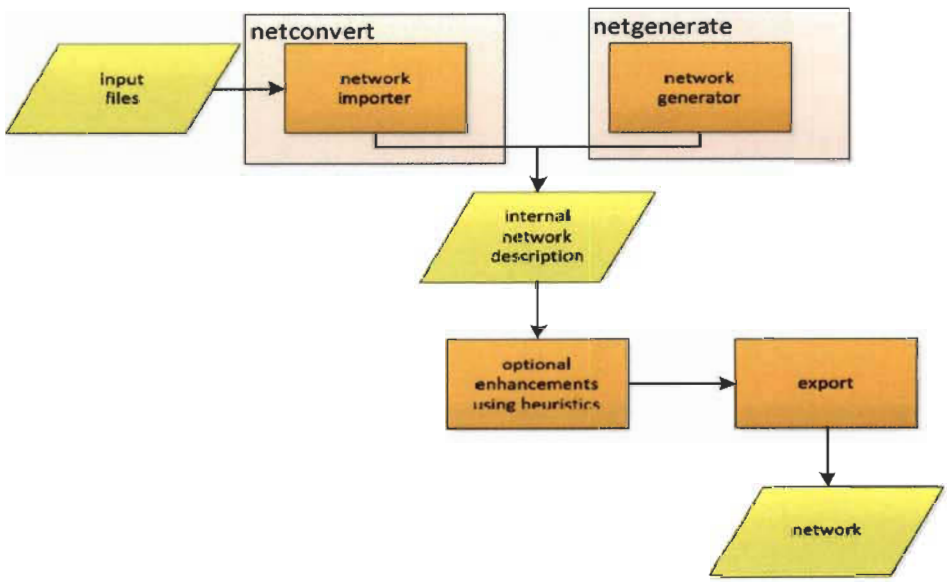


Figure 5.1: Génération du réseau routier avec netgenerate et netconvert dans SUMO [41].

5.2.2 Simulation

Le progiciel SUMO effectue des simulations à temps discret. La longueur du pas par défaut est de 1s mais cette valeur peut être réduite jusqu'à 1ms. Dans le simulateur, l'unité de mesure du temps est la microseconde. La position de chaque véhicule est décrite par sa localisation sur la voie en partant du début de son trajet. La vitesse de déplacement (m/s) d'un véhicule est évaluée en utilisant une extension du modèle stochastique. Deux versions de la simulation de trafic routier existent dans le simulateur SUMO :

- Sumo : une application qui permet d'exécuter les simulations en ligne de commande;
- Sumo-gui permet de simuler le trafic routier grâce à une interface graphique utilisant OpenGL. La visualisation peut être personnalisée de plusieurs manières : gérer la vitesse des véhicules, le temps d'attente, et l'interaction avec les programmes de signalisation routière.

5.2.3 Interaction en ligne

Le simulateur SUMO est intégré d'un socket appelé Traci (Interface Traffic Control). Cette API permet au simulateur d'interagir avec une application externe. Pour permettre une interaction en ligne, SUMO doit être démarré avec l'option supplémentaire qui prend en compte le numéro de port réseau. L'interaction en ligne du simulateur permet de modifier les valeurs des objets de simulation tels que les intersections, les routes, les voies, les feux de circulation et les vitesses des voitures. On pourrait également instancier un nouveau programme de feux de circulation, ou forcer les véhicules à changer de voies. Cette propriété du simulateur permet la synchronisation en ligne des feux de circulation ou la modélisation du comportement d'un véhicule.

5.3 Simulateur réseau NS2

NS2 est un logiciel de simulation de réseaux informatiques. Il est essentiellement élaboré avec les idées de la conception objet, de la réutilisation du code et de la modularité. Le simulateur NS2 est une extension du langage de programmation Tcl (Tool Command Language) qui sert à contrôler les applications décrites dans NS2. Du point de vue de l'utilisateur, la mise en œuvre du simulateur se fait en 3 étapes: étape de programmation qui décrit la topologie du réseau et le comportement de ses composants; étape de simulation et enfin l'étape d'interprétation des résultats. La dernière étape est prise en charge par un outil annexe appelé NAM (Network Animator).

NAM est un outil de visualisation qui permet de faire une analyse des éléments simulés. Il présente deux intérêts principaux: représenter la topologie d'un réseau décrit avec NS2 et afficher temporellement les résultats d'une trace d'exécution NS2. C'est-à-dire qu'il est capable de représenter les paquets TCP ou UDP, la rupture des liens entre les nœuds ou de représenter les paquets rejetés lorsque la file d'attente est pleine [42, 43].

5.3.1 Les composants de NS2

Le simulateur NS2 est adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille. Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés et d'application. La liste des principaux composants disponibles dans le simulateur NS2 est présentée dans le tableau 5.1.

Application	Web, FTP, Telnet, générateur de trafic (CBR...)
Transport	TCP, UDP, RTP, SRM
Routage	Statique, dynamique (vecteur distance) et routage multipoint (DVMRP, PIM)
Gestion des files d'attente	RED, DROP Tail, Token bucket
Discipline de service	CBQ, SFQ, DRR, Fair queueing
Système de transmission	CSMA/CD, CSMA/CA, lien point à point

Tableau 5.1: Liste des principaux composants disponible dans NS2 [33]

5.3.2 Modèle de mobilité

NS2 implémente deux modèles de mobilité.

5.3.1.1 Le Random Waypoint Mobility Model

Ce modèle génère un mouvement aléatoire du nœud qui choisit ensuite, aléatoirement, sa prochaine destination. Aussi dans ce modèle, le nœud se déplace avec une vitesse aléatoire constante.

5.3.1.2 Le Trajectory based Mobility Model

Ce modèle est défini par un scénario dans lequel l'utilisateur précise une destination et la vitesse de déplacement des nœuds. La vitesse de déplacement des nœuds est constante.

5.3.3 Modèle de propagation dans NS2

Les modèles de propagation implémentés dans NS2 ont pour objectif de prédire la puissance de réception du signal des paquets. À la couche physique de chaque nœud, il existe un seuil de réception du signal de paquets. Quand la puissance de réception du signal du paquet reçu par un nœud est inférieure au seuil, le paquet est marqué comme erroné et il est abandonné dans la couche MAC. Dans NS2, on trouve 4 principaux modèles de propagation [44, 45].

5.3.3.1 Free Space model

Ce modèle dit modèle d'espace libre suppose dans la condition de propagation qu'il n'existe qu'un chemin clair (sans obstacle) entre l'émetteur et le récepteur. H.T. Friis a présenté l'équation suivante pour calculer la puissance du signal du paquet reçu.

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (6)$$

où P_t représente la puissance du signal transmis. G_t et G_r sont respectivement le gain d'antenne (le pouvoir d'amplification passif de l'antenne) de l'émetteur et du récepteur. L ($L \geq 1$) est la perte de système et d la distance. λ : la longueur d'onde.

Le modèle de propagation Free space représente la portée de communication sous forme d'un cercle autour de l'émetteur. Ainsi, les nœuds qui se trouvent à l'intérieur du cercle reçoivent tous les paquets. Dans le cas contraire, les paquets sont perdus.

5.3.3.2 Two-ray ground reflection model

Contrairement au modèle Free space, le modèle Two-ray ground reflection considère à la fois le trajet direct entre l'émetteur et le récepteur et aussi le trajet de réflexion au sol. Il est démontré que ce modèle donne une prévision plus précise sur la distance que le modèle Free space. La puissance de réception du signal à une distance d est donnée par l'équation suivante:

$$P_r(d) = \frac{P_t G_t h^2{}_t h^2{}_r}{d^4 L} \quad (7)$$

où:

P_t: la puissance du signal transmis.

G_t et G_r sont respectivement le gain d'antenne (le pouvoir d'amplification passif de l'antenne) de l'émetteur et du récepteur.

h_t et h_r sont respectivement la hauteur de l'antenne de l'émetteur et du récepteur.

L ($L \geq 1$) est la perte de système.

Avec ce modèle, la puissance du signal diminue au fur et à mesure que la distance augmente. Mais il ne donne pas de bons résultats sur une courte distance. Pour cette raison le modèle Free space est plus utilisé.

5.3.3.3 Shadowing model

Les modèles Free space et Two-ray ground reflection prédisent la puissance du signal reçu avec une fonction déterministe basée sur la distance. Ils représentent tous les deux la portée de communication par un cercle. En réalité, la puissance reçue à une certaine distance est une variable aléatoire à cause des effets de propagation des trajets multiples. En fait, les deux modèles ci-dessus prédisent la puissance moyenne du signal reçu à une distance.

Les tableaux 5.2 et 5.3 présentent respectivement les valeurs de pertes de trajet et de déviation d'ombre des modèles Free space et Two-ray ground reflection.

Environnement		β
Outdoor	Free space	2
	Shadowed urban area	2.7 to 5
In building	Line-of-sight	1.6 to 1.8
	Obstructed	4 to 6

Tableau 5.2: Quelques valeurs de perte de trajet [45]

Environnement	$\sigma_{dB}(dB)$
outdoor	4 to 12
Office, hard partition	7
Office soft partition	9.6
Factor, line-of-sight	3 to 6
Factory, obstructed	6.8

Tableau 5.3: Quelques valeurs de déviation d'ombre en dB [45]

Le modèle Shadowing (modèle d'ombre), généralement utilisé, est constitué de deux sous modèles. Le premier connu sous le nom de modèle de perte de trajet, prévoit la puissance moyenne du signal reçu à une distance d qui est notée $P_r(d_0)$:

$$\left[\frac{\overline{P_r(d)}}{P_r(d_0)}\right]_{dB} = -10\beta \log(\frac{d}{d0}) \quad (8)$$

β est appelé exposant de l'affaiblissement du chemin et est généralement déterminé de façon empirique par la mesure de champ.

Le second sous-modèle reflète la variation de la puissance du signal reçue à une certaine distance. L'ensemble du modèle Shadowing est représenté par:

$$\left[\frac{\overline{P_r(d)}}{P_r(d_0)}\right]_{dB} = -10\beta \log(\frac{d}{d0}) + X_{dB} \quad (9)$$

X_{dB} est une variable aléatoire gaussienne avec moyenne nulle et écart-type σ.

Le modèle étend le modèle idéal de cercle à un modèle statistique plus riche. Les nœuds peuvent communiquer de façon probabiliste lorsqu'ils sont près du bord de la plage de communication.

5.3.3.4 Nakagami model

C'est un modèle probabiliste utilisé fréquemment dans le simulateur NS2. La puissance de réception du signal du paquet suit la loi de distribution gamma.

$$P_{rNakagami}(d;m) \sim Gamma(m, \frac{P_{rdet}(d)}{m}) \quad (10)$$

Le paramètre m spécifie l'intensité des effets de transition et couvre une large gamme d'intensités de fluctuation. Le choix $m = 1$ reflète la de distribution de Rayleigh, alors que pour une grande valeur de m, on a un comportement similaire au model Free space mais probabiliste.

5.4 Simulateur réseau OMNET++

OMNET++ est un simulateur à évènements discrets orienté objet, basé sur le langage C++. Il a été conçu pour simuler les systèmes réseaux de communication, les systèmes multi processeurs et d'autres systèmes distribués [43]. Bien qu'il fournit un Framework de simulation puissant, il ne permet pas une bonne simulation des réseaux de communication sans fil [56]. Pour pallier ce déficit, la communauté scientifique suggère d'intégrer à OMNET++ le Framework MIXIM.

MIXIM est un Framework créé pour la modélisation des réseaux filaires et mobiles (réseaux de capteurs sans fil, les réseaux véhiculaires) dans OMNET++ [48]. Il propose de manière détaillée les modèles de propagation des ondes radio, d'estimation d'interférence, de consommation d'énergie et les protocoles MAC sans fil. MXIM intégré à OMNET++.Il permet à ce dernier de supporter la couche MAC IEEE 802.11p et 1609.4.

Ce qui permet de réaliser aisément la simulation des protocoles de réseaux véhiculaires sans fil. En outre, OMNET++ supporte facilement les modèles de propagation probabilistes tels que Log-Normal-Shadowing, Nakagami, Rayleigh, ainsi que d'autres modèles de propagations.

5.4.1 Architecture d'OMNET++

Le simulateur OMNET++ est composé de modules. Un module peut être soit simple ou composé. À chaque module simple correspond un fichier .cc et un fichier .h. Un module composé regroupe en son sein des modules simples ou d'autres modules composés connectés entre eux. Les paramètres, les sous modules et les ports de chaque module sont spécifiés dans un fichier .ned. La communication entre les différents modules se fait par échanges de messages. Les messages sont envoyés et reçus à travers les ports qui représentent les interfaces d'entrée et de sortie de chaque module. La conception d'un réseau se fait dans un fichier .ned et les différents paramètres de chaque module sont spécifiés dans le fichier de configuration (.ini). À la fin de chaque simulation, OMNET++ génère deux nouveaux fichiers .vec et .sca. Ces fichiers permettent de faire les statistiques [43].

5.5 Comparaison entre les simulateurs NS2 et OMNET++

Après avoir brièvement décrit les deux simulateurs réseau (NS2 et OMNET++), nous allons faire une étude comparative des deux simulateurs dans cette section. Les résultats de cette étude sont présentés dans le tableau 5.4.

Propriétés	OMNET++	NS2
Flexibilité	Très flexible et générique. Il peut simuler n'importe quel type de réseau.	Il est difficile de simuler autres choses que les réseaux de commutations de paquets et protocoles
Mobilité	Plusieurs modes de mobilités sont fournis (Random Waypoint Mobility Model, Constant Speed Mobility Model, Basic Mobility Model, ...)	Supporte que Random Waypoint Mobility Model et le Trajectory Based Mobility Model.

Propriétés	OMNET++	NS2
La gestion de modèle	Les modèles sont indépendants du noyau de simulation	La limite entre les modèles et le noyau de simulation n'est pas très considérable
Support de traçage	Visibilité de la transmission de paquets lors de la simulation	Pas de traçage
Habileté à couvrir les grands réseaux	Peut simuler une grande topologie de réseaux	Beaucoup de problèmes dans la simulation des grandes topologies de réseaux

Tableau 5.4: Comparaison entre NS2 et OMNET++ [43, 47]

5.6 Conclusion

Dans ce chapitre, nous avons présenté les simulateurs utilisés pour simuler les réseaux véhiculaires sans fil. L'étude comparative réalisée entre les deux simulateurs réseau (NS2 et OMNET++) montre qu'OMNET++ présente de très nombreux avantages par rapport à NS2. Pour cette raison, nous avons choisi le simulateur OMNET++ pour évaluer les performances du protocole. Le simulateur SUMO est utilisé pour la génération du trafic routier.

Dans le chapitre suivant, nous allons présenter et analyser les résultats de simulation de notre modèle de gestion de l'anonymat et de la traçabilité.

Chapitre 6 - Évaluation de performances

6.1 Introduction

Les simulateurs permettent d'étudier le comportement des entités des réseaux véhiculaires sans fil et d'évaluer les performances des protocoles conçus pour ces réseaux.

Après avoir présenté au chapitre précédent trois simulateurs utilisés pour modéliser les protocoles des réseaux VANETs, nous allons décrire dans ce chapitre, l'environnement de simulation de notre modèle. Ensuite, nous allons présenter les différents scénarios de chaque approche et enfin analyser les résultats des simulations.

6.2 Environnement de simulation pour notre étude

Pour analyser la performance de notre protocole, nous avons utilisé le simulateur de trafic routier SUMO-0.15.0 et le simulateur réseau OMNET++ 4.2.2. Le choix du simulateur réseau OMNET++ est dû aux nombreux avantages qu'il présente par rapport au simulateur NS2 [43, 47]. L'évaluation des protocoles de réseaux véhiculaires sans fil avec le simulateur OMNET++ nécessite l'utilisation d'un Framework qui permet de le faire fonctionner en parallèle avec le simulateur de trafic routier. Ce Framework connu sous le nom de Veins [49] (Vehicles in network Simulation) a pour objectif d'assurer le couplage bidirectionnel des simulateurs OMNET++ et SUMO, dans le but d'avoir des résultats de simulation significatifs proches de l'environnement réel. Dans le cadre de notre étude, nous avons utilisé Veins-2.0.

Le protocole proposé est évalué dans deux milieux différents: milieu urbain et autoroutier. Les propriétés de l'environnement de simulation sont renseignées dans le tableau 6.1.

Simulateur réseau	OMNET++-4.2.2
Simulateur de trafic routier	SUMO-0.15.0
Plateforme de couplage entre OMNET++ et SUMO	Veins-2.0
Nombre de RSU	4
MAC protocole	IEEE 802.11p
Portée du signal des OBUs	150 m
Taille des paquets	1024 bits
Modèles de propagation	SimplePathlossModel TwoRayInterferenceModel SimpleObstacleShadowing
Débit binaire	6 Mbps

Tableau 6.1: Propriétés de l'environnement de simulation

6.3 Les métriques de simulation

L'évaluation des performances de notre protocole a été faite en utilisant les métriques suivantes:

- Taux de véhicules ayant reçu le pseudonyme privé dans chaque approche;
- Taux de véhicules ayant changé de pseudonyme durant la simulation;
- Bande passante consommée en fonction de la vitesse moyenne des véhicules durant le processus de demande et de renouvellement de pseudonymes de communication.

Pour simuler notre protocole en environnement urbain, nous avons considéré une carte (1200 m x 1200 m) de la ville de Manhattan. Pour l'environnement autoroutier, nous avons utilisé une carte d'autoroute de 5 km.

Nous présenterons dans ce qui suit, les résultats de simulations de chaque environnement en tenant compte des métriques mentionnées ci-dessus, dans les deux approches.

6.3.1 Simulation en milieu urbain

Chacune des approches de l'étude du protocole a été évaluée en milieu urbain avec les paramètres suivants (Tableau 6.2). À ces paramètres, il faut ajouter les propriétés de l'environnement de simulation du tableau 6.1.

Élément	Valeur
Carte routière: Manhattan city	1200 m x 1200m
Intervalle de vitesse sur la route	5 m/s -14 m/s
Temps de changement de pseudonymes et de certificats	30 s
Portée de communication RSU	300 m
Temps de simulation	100 s

Tableau 6.2: Paramètres de simulation en milieu urbain

Justification du temps de changement de pseudonymes et certificats

Comme discuté dans le chapitre précédant, l'objectif dans cette étude est de trouver un intervalle de temps au cours duquel au moins deux véhicules peuvent changer leurs pseudonymes de communication. Pour définir le temps de changement de pseudonymes et de certificat, nous avons considéré les paramètres suivants:

X = 300 m

V_{max}= 14 m/s

V_{min}=5 m/s

$V_{moy=}(V_{max} + V_{\min})/2$. (i)

D'après (i), $V_{moy} = \frac{14+5}{2}$

V_{moy}= 9.5 m/s.

L'intervalle T de changement de pseudonymes de communication défini dans le chapitre précédent sous la forme: $T = \left[\frac{X}{V_{max}}; \frac{X}{V_{moy}}\right]$ (j) est:

T=[21.43; 31.58]

En tenant compte du délai de cryptages, de décryptages et de signature des messages présentés dans [50] et aussi pour que les véhicules puissent avoir de nouveaux pseudonymes avant l'expiration de ceux utilisés, nous avons fixé le temps de changement de pseudonymes de communication à 30 s.

Pour la simulation du protocole dans le milieu urbain, nous avons considéré 2 scénarios.

6.3.1.1 Scénario avec 50 nœuds mobiles

Dans cette section, nous allons présenter les résultats des simulations réalisées avec 50 véhicules.

Évaluation de l'intervalle de confiance des simulations de ce scénario

L'intervalle de confiance permet d'évaluer la précision de l'estimation d'un paramètre statistique sur un échantillon [51].

Pour un degré de confiance égale à 95 %, le coefficient dépendant $Z_{\alpha/_2}$=1.96

L'intervalle de confiance $I_c = \left[\bar{X} - \frac{1.96*S}{\sqrt{n}}; \bar{X} + \frac{1.96*S}{\sqrt{n}}\right]$ (11)

$\bar{X}$: moyenne des simulations.

S: écart type des simulations.

n: nombre de simulations.

Nous avons réalisé les simulations 20 fois dans notre étude. Pour le calcul de l'intervalle de confiance, nous avons considéré l'ensemble des véhicules qui ont envoyé un message d'authentification à la CA; c'est-à-dire les véhicules qui ont reçu la clé publique du RSU.

n= 20

$\bar{X}$=42.25

S=6.40

L'intervalle de confiance I_c =[39.44; 45.06]

- **Taux de véhicules ayant reçu le pseudonyme privé dans chaque approche**

Nous supposons dans toutes les simulations qu'un véhicule ne reçoit son pseudonyme privé que si son certificat est diffusé par le RSU (approche 1) ou lorsque le véhicule diffuse son propre certificat (approche 2). Les résultats des simulations sont représentés sur la figure 6.1.

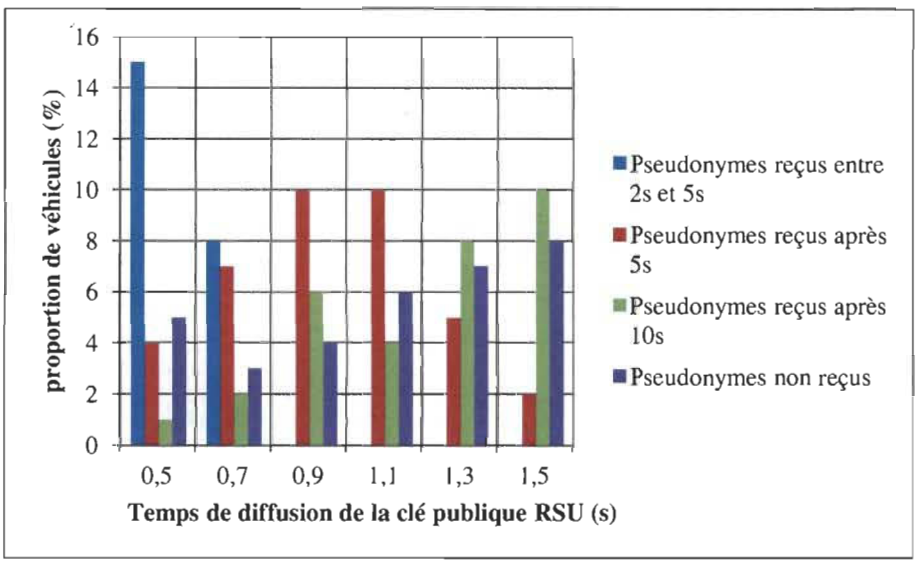


Figure 6.1: Phase de distribution des pseudonymes en milieu urbain (50 véhicules)

La diffusion des clés publiques des RSUs commencent à 500 ms. Et à chaque 200 ms, les RSUs diffusent de nouveau leurs clés publiques jusqu'à la fin de la simulation. 15 % des véhicules reçoivent leurs pseudonymes privés entre 2 s et 5 s après un temps de diffusion de la clé publique RSU égale à 0,5 s. 5 % des véhicules n'ont pas reçu leurs pseudonymes privés pendant ce temps de diffusion de la clé publique RSU. Après un temps de diffusion de la clé publique RSU égale à 0,7 s, 8 % des véhicules ont reçu leurs pseudonymes privés au-delà de 5 s alors que 3 % des véhicules n'ont pas reçu leurs pseudonymes. À 1,5 s (temps de diffusion de la clé publique RSU), 10 % des véhicules ont reçu leurs pseudonymes privés après 10 s alors 8 % des véhicules n'ont pas reçu leurs pseudonymes privés.

Ces constats s'expliquent par des pertes importantes de paquets lors de l'envoi des données de la CA vers le véhicule et aussi du temps de validité d'un paquet (1 s) que nous avons définie dans le simulateur.

- **Taux de véhicules ayant changé de pseudonyme durant la simulation**

Nous avons considéré dans cette partie, les véhicules qui ont reçu leurs pseudonymes privés dans durant la diffusion de la clé publique RSU entre 0,5 s et 1,5 s.

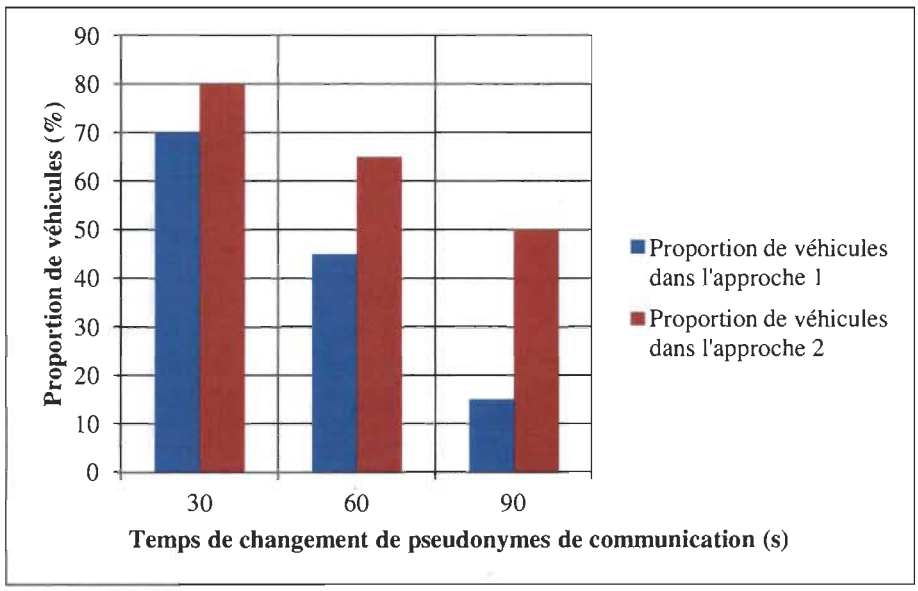


Figure 6.2: Proportion de véhicules ayant changé de pseudonymes de communication durant la simulation (50 véhicules) en milieu urbain

Sur la figure 6.2, on constate que 70 % des véhicules ont changé leurs pseudonymes privés et leurs certificats dans l'approche 1 contre 80 % des véhicules dans l'approche 2 après 30 s. Le taux de véhicules dans l'approche 1 à changer de pseudonymes privés et de certificats diminuent à 15 % (approche 1) contre 50 % (approche 2) après 90 s. Ce constat s'explique par la dépendance des véhicules de la CA lors du changement de pseudonymes de communication et aussi par un nombre faible de véhicules qui retransmet le message provenant des entités fixes dans l'approche 1.

- **Bande passante consommée en fonction de la vitesse moyenne des véhicules durant le processus de demande et renouvellement de pseudonymes de communication**

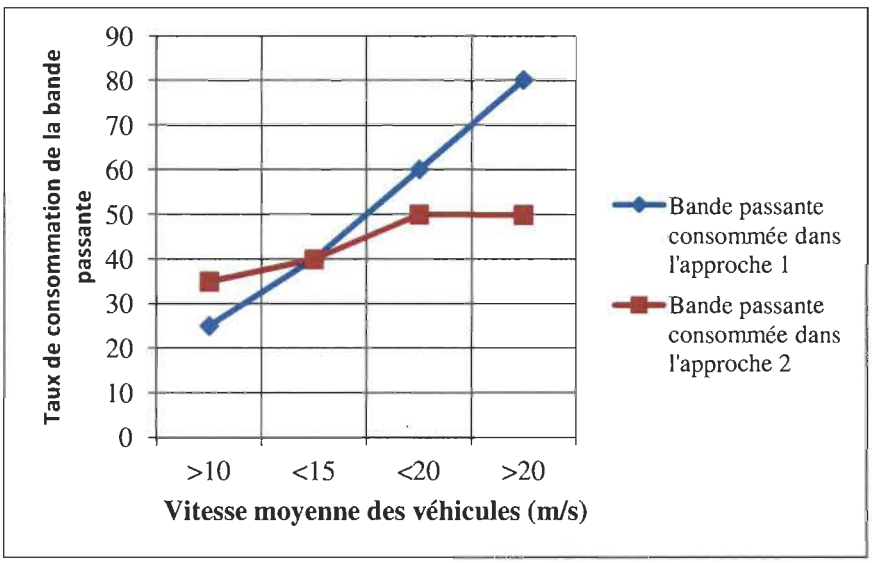


Figure 6.3: Taux de consommation de la bande passante en fonction de la vitesse moyenne des véhicules en milieu urbain (50 véhicules)

La différence entre le taux de consommation de la bande passante dans les deux approches est moins importante (voir figure 6.3). Même si les véhicules qui roulent à une vitesse moyenne comprise entre 15 m/s et 20 m/s dans l'approche 1 consomment plus de bande passante que les véhicules roulant à cette même vitesse dans l'approche 2.

6.3.1.2 Scénario avec 100 nœuds mobiles

Comme dans le scénario avec 50 nœuds, l'intervalle de confiance des simulations pour le scénario avec 100 véhicules est obtenu à partir des nœuds qui ont reçu la clé publique du RSU et ont envoyé un message d'authentification à la CA.

L'intervalle de confiance est: I_c =[47.5; 52.91].

- **Taux de véhicules ayant reçu le pseudonyme privé dans chaque approche**

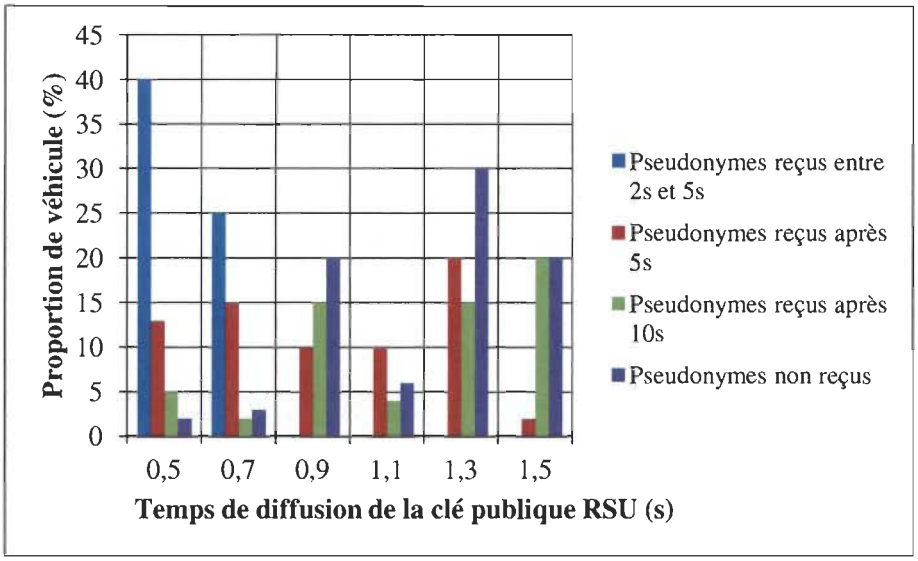


Figure 6.4: Phase de distribution des pseudonymes en milieu urbain (100 véhicules)

Le taux de véhicules à changer de pseudonymes privés entre 2s et 5 s dans ce scénario (40 %) est le double (voir figure 6.4) de celui du scénario avec 50 nœuds (6.1) pour un temps de diffusion de la clé publique RSU égale à 0,5 s. La raison est que dans ce scénario chaque véhicule possède un nombre important de voisins lui retransmettant l'information venant soit de la CA ou du RSU que dans le scénario avec 50 nœuds mobiles. Par contre le taux de véhicules n'ayant pas reçu de pseudonymes privés dans le scénario avec 50 nœuds est moins considérable par rapport à celui du scénario avec 100 nœuds. Le fait est que la CA traite plus de demandes dans le second cas (scénario avec 100 nœuds) que dans le premier (scénario avec 50 nœuds).

- **Taux de véhicules ayant changé de pseudonymes durant la simulation**

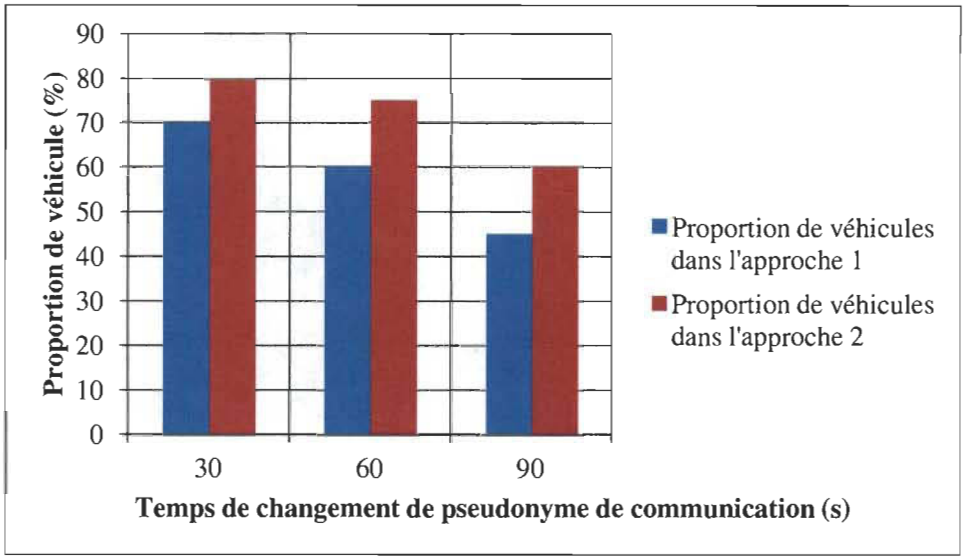


Figure 6.5: Proportion de véhicules ayant changé de pseudonymes de communication durant la simulation (100 véhicules) en milieu urbain

Sur la figure 6.5, on remarque que 70 % des véhicules dans l'approche 1 ont changé de pseudonymes privés et de certificats contre 80 % des véhicules dans l'approche 2, après 30 s. Après 90 s, le taux de véhicules à changer de pseudonymes privés et de certificats dans l'approche 1 diminue à 45 % alors que celui de l'approche 2 diminue à 60 %. Si l'on compare les résultats de la figure 6.5 à ceux de le figure 6.2, on peut déduire que le nombre de véhicules présents dans le réseau a un impact important sur le taux de véhicules à changer de pseudonymes de communication dans l'approche 1. Alors que dans l'approche 2, ce constat est moins significatif.

- **Bande passante consommée en fonction de la vitesse moyenne des véhicules durant le processus de demande et renouvellement de pseudonymes de communication**

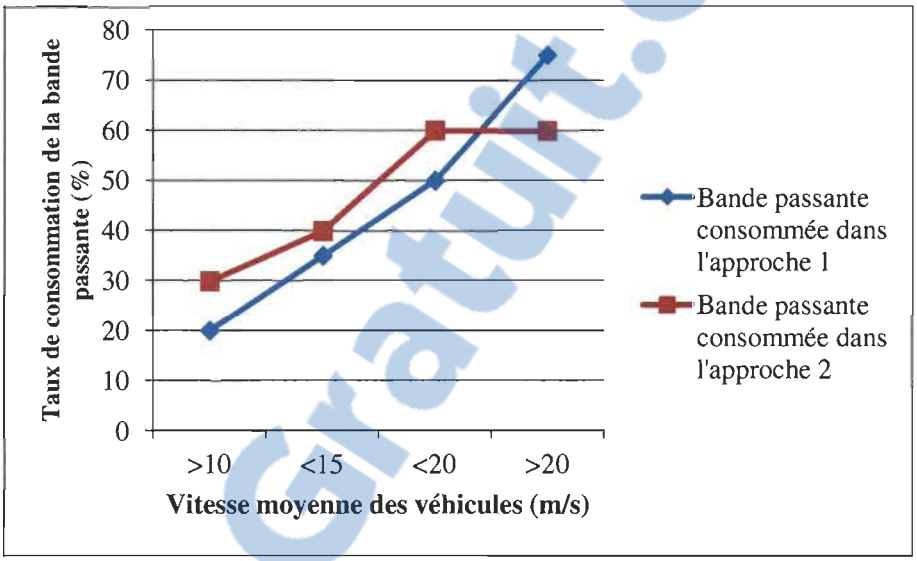


Figure 6.6: Taux de consommation de la bande passante en fonction de la vitesse moyenne des véhicules (100 véhicules) en milieu urbain

Le taux de consommation de la bande passante dans l'approche 2 est supérieur à celui de l'approche 1 (voir figure 6.6) si l'on considère les véhicules qui roulent à une vitesse moyenne comprise entre 15 m/s et 20 m/s. La raison est que chaque véhicule dans l'approche 2 diffuse son certificat afin de créer un nombre important de voisins. L'augmentation du taux de consommation de la bande passante au-delà de 50 % pour les véhicules roulant à une vitesse moyenne supérieure à 20 m/s dans l'approche 1 est due aux nombreux échanges de paquets entre les véhicules et les entités fixes pour l'obtention de leurs pseudonymes privés.

6.3.2 Simulation sur autoroute

Pour la simulation en milieu autoroutier, nous avons considéré les paramètres suivants:

Élément	Valeur
Carte autoroute	5000 m x 3000m
Intervalle de vitesse sur la route	16 m/s -28 m/s
Temps de changement de pseudonymes et de certificats	30 s
Portée de communication RSU	700 m
Temps de simulation	100 s

Tableau 6.3: Paramètres de simulation en milieu autoroutier

Justification du temps de changement de pseudonymes et certificats

$X = 700$ m

V_{max}= 28 m/s

V_{min}=16 m/s

D'après (i), $V_{moy} = 22m/s$

D'après (j), l'intervalle T de changement de pseudonymes de communication est:

T=[25; 31,81]

Dans la simulation, nous avons fixé, comme dans le cas de la simulation en milieu urbain, le temps de changement de pseudonymes de communication à 30s.

Deux scénarios ont été également considérés dans cette partie:

6.3.2.1 Scénario avec 50 nœuds mobiles

Pour la simulation avec 50 nœuds mobiles, nous avons considéré le même intervalle de confiance que dans le cas de la simulation de 50 nœuds mobiles dans le milieu urbain.

- **Taux de véhicules ayant reçu le pseudonyme privé dans chaque approche**

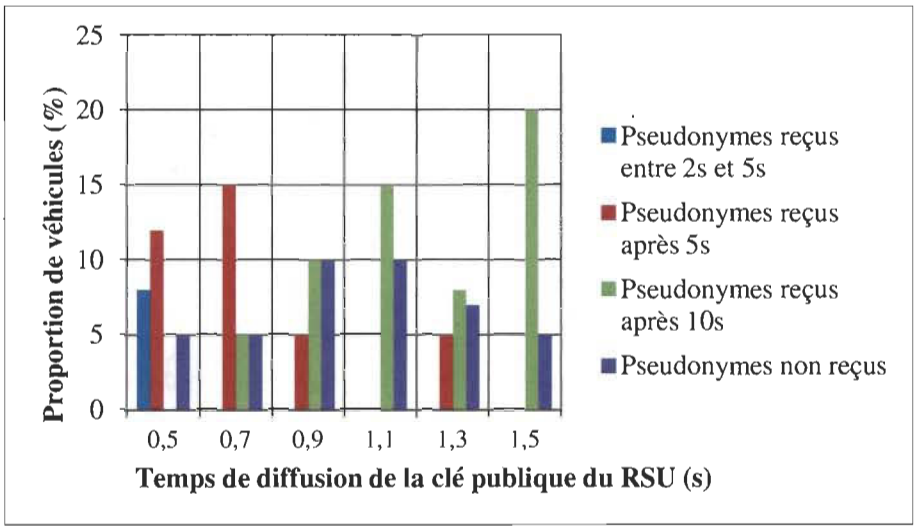


Figure 6.7: Phase de distribution des pseudonymes sur autoroute (50 véhicules)

sur la figure 6.7, on remarque que 8 % des véhicules reçoivent leurs pseudonymes entre 2 s et 5 s après un temps de diffusion de la clé publique RSU égale à 0,5 s. Contrairement au scénario de 50 nœuds mobiles en milieu urbain (**Figure 6.1**), le taux de véhicules authentifiés (ayant reçu le pseudonyme) dans le réseau est très faible sur autoroute. Ceci est dû à la vitesse des véhicules dans ce milieu.

- **Taux de véhicules ayant changé de pseudonymes durant la simulation**

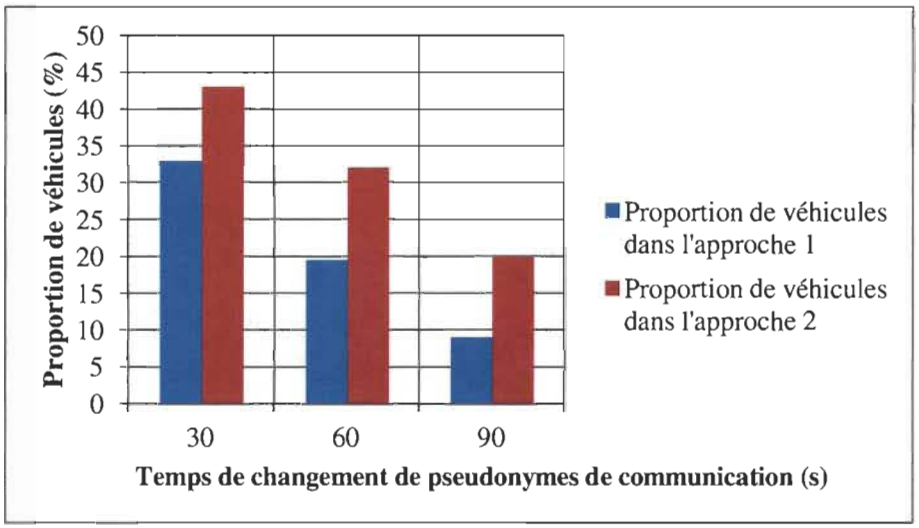


Figure 6.8: Proportion de véhicules ayant changé de pseudonymes de communication durant la simulation (50 véhicules) sur autoroute

Si l'on compare le taux de véhicules ayant changé de pseudonyme dans le scénario de 50 nœuds mobiles en milieu urbain (figure 6.2) à celui sur autoroute (voir figure 6.8), on constate qu'en milieu urbain, un nombre important de véhicules changent leurs pseudonymes de communication. Nous avons considéré dans les simulations sur autoroute le même temps de validité des paquets (1 s) utilisé dans les simulations en milieu urbain. Or sur autoroute, à cause de leurs vitesses de déplacement, beaucoup de véhicules reçoivent des paquets invalides. C'est-à-dire que les paquets arrivent après 1 s. Les paquets invalides sont donc considérés comme paquets perdus. Pour corriger cette situation, nous allons dans notre travail futur, augmenter le temps de validité des paquets sur autoroute et définir une autre méthode de distribution des RSUs afin d'avoir une bonne liaison de communication véhicule-RSU.

- **Bande passante consommée en fonction de la vitesse moyenne des véhicules durant le processus de demande et renouvellement de pseudonymes de communication**

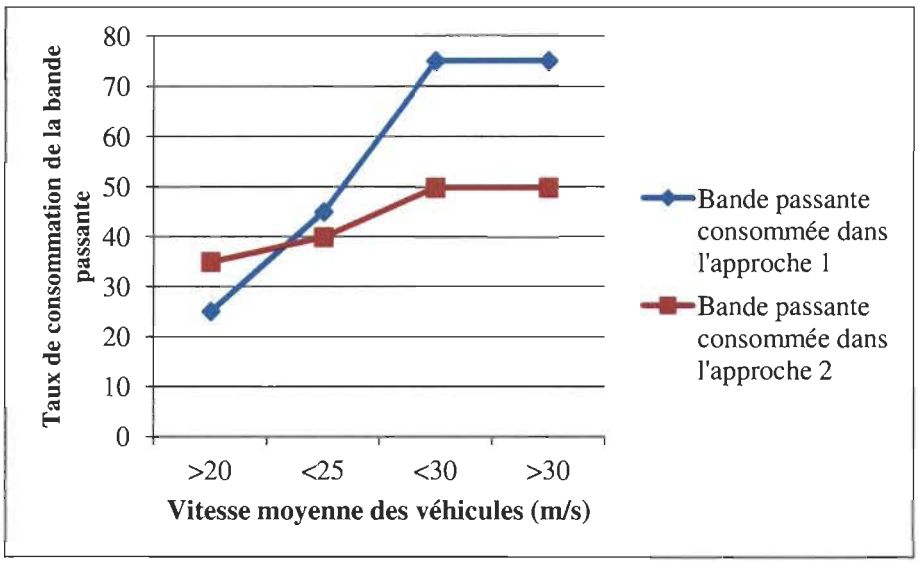


Figure 6.9: Taux de consommation de la bande passante en fonction de la vitesse moyenne des véhicules sur autoroute (50 véhicules)

Même si le taux de véhicules authentifiés dans le réseau dans ce scénario est faible par rapport à celui du milieu urbain avec 50 nœuds mobiles, le taux de consommation de la bande passante est assez important sur autoroute (voir figure 6.9). Le nombre assez conséquent des pertes de paquets oblige les véhicules à faire plusieurs demandes dans les phases d'authentification et de changement de pseudonymes.

6.3.2.2 Scénario avec 100 nœuds mobiles

Dans cette partie, l'intervalle de confiance est le même que celui de la simulation du scénario avec 100 véhicules dans le milieu urbain.

- **Taux de véhicules ayant reçu le pseudonyme privé dans chaque approche**

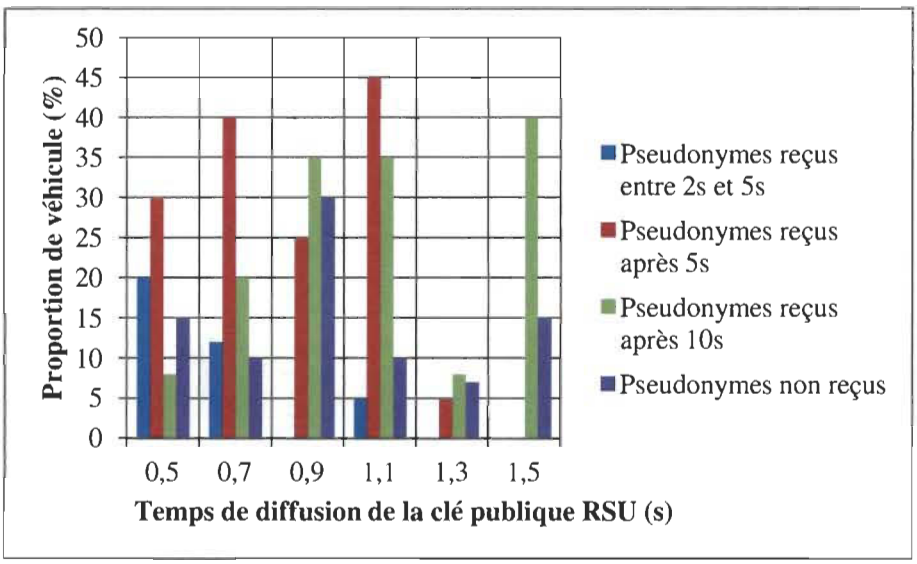


Figure 6.10: Phase de distribution des pseudonymes sur autoroute (100 véhicules)

Sur la figure 6.10, on voit a une nette différence entre le taux de véhicules authentifiés (véhicule ayant son pseudonyme privé et certificat connu par les autres véhicules du réseau) dans le réseau durant le temps de diffusion de la clé publique RSU (de 0,5 s à 1,5 s) si l'on compare les résultats de la figure 6.4 à ceux de la figure 6.10. Même si nous avons considéré une portée de communication des RSU jusqu'à 700 m sur autoroute contre 300 m en milieu urbain, cela n'influence pas positivement le résultat. Ce qui nous permet de dire que la vitesse des voitures et la distance séparant les véhicules sur la route sont à l'origine des pertes de paquets dans les échanges de données dans le milieu autoroutier.

- **Taux de véhicules ayant changé de pseudonymes durant la simulation**

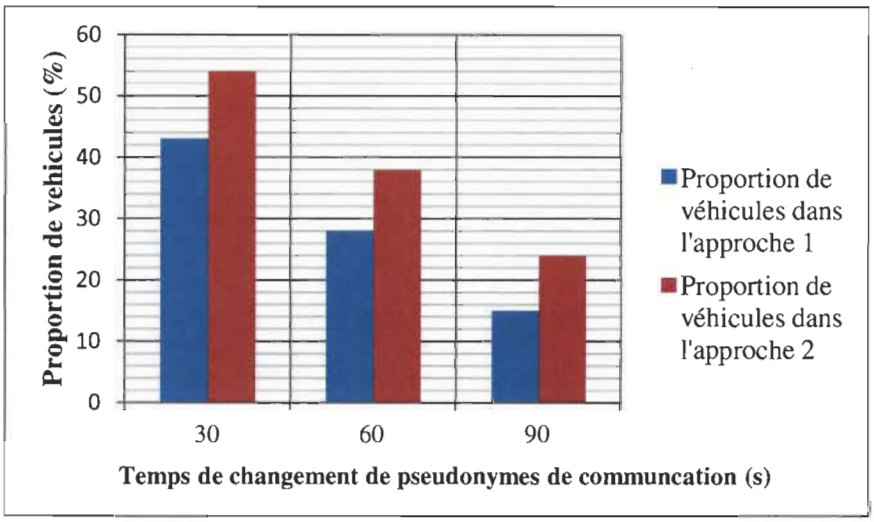


Figure 6.11: Proportion de véhicules ayant changé de pseudonymes de communication durant la simulation sur autoroute (100 véhicules)

Sur la figure 6.11 on remarque que 43 % des véhicules changent leurs pseudonymes de communication dans l'approche 1 contre 54 % des véhicules dans l'approche 2 après 30 s. Si l'on compare les résultats de la figure 6.8 à ceux de la figure 6.11, on peut déduire que le nombre de véhicules authentifiés dans le réseau influence positivement la réception des paquets parce qu'ils permettent de réacheminer le paquet vers le destinataire du message dans le réseau. Plus on a un nombre important de véhicules dans le réseau, moins on aura de perte de paquets.

- **Bande passante consommée en fonction de la vitesse moyenne des véhicules durant le processus de demande et renouvellement de pseudonymes de communication**

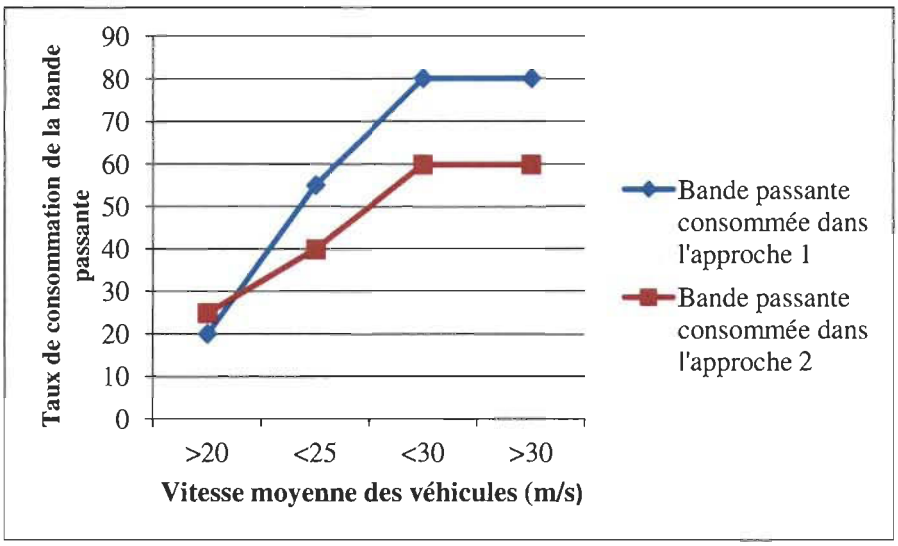


Figure 6.12: Taux de consommation de la bande passante en fonction de la vitesse moyenne des véhicules sur autoroute (100 véhicules)

Pour une vitesse moyenne comprise entre 25 m/s et 30 m/s, les véhicules dans l'approche 1 consomment plus de bande passante que ceux de l'approche 2 (voir figure 6.12). Aussi, la différence entre le taux de consommation de la bande passante dans le scénario de 50 nœuds mobiles (Figure 6.9) et celui de 100 nœuds mobiles (Figure 6.12) sur autoroute n'est pas si importante. On pourra donc déduire que le nombre de véhicules dans le réseau n'est pas un facteur important de consommation de la bande passante.

6.4 Conclusion

L'évaluation des performances du protocole de gestion de l'anonymat et de la traçabilité a été réalisée dans ce chapitre. Eu égard aux différents résultats des simulations, nous avons constaté que l'approche 2 (génération des pseudonymes par le véhicule) présente un avantage considérable dans le cas de changement de pseudonymes de communication et dans la consommation de la bande passante dans les deux milieux de simulations (urbain et autoroutier) par rapport à l'approche 1 (génération des pseudonymes par la Centrale d'Autorité). Aussi, nous avons remarqué que le taux de pertes des paquets est inversement proportionnel au taux de véhicules authentifiés dans le réseau. Dans les simulations, nous avons considéré un temps de validité des paquets égale à 1 s. Ce temps influence négativement l'authentification des véhicules qui roulent avec des vitesses supérieures ou des véhicules se situant à une distance importante par rapport aux autres véhicules du réseau. En effet, la plupart de ces véhicules reçoivent les paquets d'authentification après la durée de validité définie. Ce qui fait que les paquets reçus sont invalides et considérés comme perdus.

Dans nos travaux futurs, afin d'augmenter le nombre de véhicules authentifiés dans le réseau, nous allons redéfinir le temps de validité des paquets en tenant compte des vitesses des véhicules, ensuite faire une étude sur le nombre de RSUs à utiliser et leurs dispositions sur la route tout en respectant la qualité de service. Enfin, nous allons utiliser un protocole de trafic qui gère la densité pour tester notre modèle.

Chapitre 7 - Conclusion générale et perspectives

Le déploiement des systèmes de transport intelligent permettra de prévenir de nombreux accidents, de réduire les dégâts en cas de collision et de gérer les secours sur les routes. Ces systèmes vont améliorer de façon significative le trajet des véhicules par l'accès instantané aux informations sur l'état des routes et aussi, leur permettre d'échanger entre eux des informations visant à rendre plus conviviale leurs trajets. Le fonctionnement de ces systèmes repose sur les réseaux véhiculaires sans fil. Ces réseaux sont vulnérables aux attaques en absence des mesures de sécurité adéquates. Pour éviter la traçabilité illégale des véhicules et rendre confidentielles les données échangées par ces derniers, nous avons réalisé dans le cadre de notre mémoire un protocole de gestion de l'anonymat et de la traçabilité. Ce protocole vise à définir un intervalle de temps au cours duquel, les véhicules pourront changer leurs pseudonymes de communication. L'idée est d'éviter qu'un véhicule soit ciblé par un attaquant durant le processus de changement de pseudonymes de communication. Dans notre étude, nous avons disposé les unités de routes de façon équidistante et ensuite nous nous sommes basés sur deux approches différentes pour évaluer les performances du protocole. Après une analyse de sécurité du protocole, il en ressort qu'il répond aux concepts de sécurité suivants: l'authentification, la non-répudiation et la gestion de la vie privée. De l'analyse des résultats obtenus après simulations, on retient que l'approche 2 (génération des pseudonymes par le véhicule) présente plus de résultats positifs en termes de pourcentage de véhicules ayant changé de pseudonymes de communication, et des taux de consommation de la bande passante par rapport à l'approche 1 (génération des pseudonymes par la Centrale d'Autorité).

Le travail réalisé dans ce mémoire a permis d'analyser l'impact de la vitesse des véhicules dans les échanges de données et d'apporter une piste de réflexion sur la disposition des RSUs sur la route afin d'avoir une meilleure connectivité OBU-RSU et aussi sur le temps d'exploitation des pseudonymes de communication.

Notre travail futur se situera sur trois axes. Dans un premier temps, nous allons faire l'étude d'une approche probabiliste sur la disposition des RSUs; ensuite nous allons considérer les vitesses des véhicules pour définir le temps de validité des paquets et aussi le temps de changement des pseudonymes de communication des nœuds mobiles. Enfin, nous allons comparer notre méthode à celles existantes dans la littérature. Aussi, une étude se fera en parallèle sur l'utilisation d'un protocole de routage de trafic qui gère la densité afin de minimiser les pertes de paquets dans notre modèle en considérant les deux milieux de simulations (urbain et autoroutier).

Ce travail a donné lieu à une communication dans un colloque national [52], à deux publications dans des conférences internationales avec comité de lecture [53, 54] et ainsi qu'à deux posters dans des colloques internationaux [55, 56].

Références bibliographiques

[1] http://www.rfi.fr/economie/20130309-prix-exorbitant-embouteillages-cabinet-roland-berger-tokyo-mexico-seoul-caire?ns_campaign=editorial&ns_source=FB&ns_mchannel=reseaux_sociaux&ns_fee=0&ns_linkname=20130309_prix_exorbitant_embouteillages_cabinet_roland_berger (accédé le 03/12/2013).

[2] www.who.int/violence_injury_prevention/road_safety_status/2013/report/ (accédé le 03/12/2013).

[3] http://www.michelinchallengebibendum.com/publication/roulons-connecte (accédé le 03/12/2013).

[4] Noureddine CHAIB, "La sécurité des communications dans les réseaux VANET", Mémoire, Université Elhadj Lakhder-Batna, faculté des sciences de l'ingénieur département d'informatique, 05 Septembre 2011.

[5] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri, "Short-lived Key Management for Secure Communications in VANETs", 11th International Conference on ITS Telecommunications (ITST), pp. 613-618, August 23-25, 2011- St. Petersburg, Russia.

[6] Hsin-Te, Wu, Wei-Shuo Li, Tung-Shih and Wen-Shyong Hsieh, " A Novel RSU-based Message Authentication Scheme for VANET", 50th International Conference on System and Networks Communications (ICSNC), pp.111-116, August 22-27, 2010-Nice, France.

[7] Jonathan Petit, "Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", Thèse de Doctorat, Université de Toulouse, 13 juillet 2011.

[8] http://www.cs.nthu.edu.tw/~jungchuk/research.html.

[9] Moez JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections", Thèse de Doctorat, Université d'Evry val d'Essonne, 06 novembre 2008.

[10] Arijit Khan, Shatrugna Sadhu, and Muralikrishna Yeleswarapu, "A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks".

[11] Ahizoune Ahmed, " Un protocole de diffusion des messages dans les réseaux véhiculaires", Mémoire, Université de Montréal, Département d'informatique et de recherche opérationnelle, Faculté des arts et sciences, avril 2011.

[12] Surabhi Mahajan, Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks", International Journal of Computer Applicatuions (0975-8887), Volume 1-N°20, février 2010.

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

[14] Maxime Raya, Jean-Pierre Hubaux, ''The Security of Vehicular Ad Hoc Networks'', pp. 11-21, Proceedings of the 3rd ACM workshop on Security of Ad Hoc and Sensor Networks (SASN '05), ACM New York, NY, USA, 2005.

[15] Maxime Raya, Jean-Pierre Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security-Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, N°1, pp. 39-68, 2007.

[16] Yong Hao, Tingting Han and Yu Cheng, "A Cooperative Message Authentication Protocol in VANETs", Global Communication Conference (GLOBECOM), 2012 IEEE, pp. 5562-5566, 3-7 December, 2012-Anaheim, California.

[17] Kaouther Abrougui and Azzedine Boukerche, "Secure Service Discovery Protocol for Intelligent Transport Systems: Proof of Correctness", 1st NSERC DIVA WORKSHOP, Developing the next Generation Intelligent Vehicular Network and Applications, pp. 51-57, September 9, 2011-Ottawa-Canada.

[18] Danda B. Rawat, Bhed B. Bista, Gongjun Yan and Michele C. Weigle, "Securing Vehicular Ad-Hoc Network against Malicious Drivers: A Probabilistic Approch", International Conference on Complex, Intelligent, and Software Intensive Systems, pp. 146-151, 2011.

[19] Tim Leinmuller, Elmar Schoch, Frank Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks", IEEE Wireless Communications, Vol. 13, Issue: 5, pp. 16-21, 2006.

[20] Yong Hao, Yu Cheng, Chi Zhou and Wei Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE journal vol 29, pp. 616-629, 2011.

[21] JaeHyu Kim and JooSeok Song, "A Pre-authentication Method for Secure Communications in Vehicular Ad Hoc Networks", 8th International Conference on Wireless Communication, Networking and Mobile Computing (WiCom), pp. 1-6, 2012.

[22] You Lu, Biao Zhou, Fei Jia and Mario Gerla, "Group-based Secure Source Authentication Protocol for VANETs", IEEE Globecom 2010 Workshop on Heterogenous, Multi-hop Wireless and Mobile Networks, pp. 202-206.

[23] Ayman Tajeddine, Ayman Kayssi and Ali Chehab, "A Privacy-Preserving Trust Model for VANETs", 10th IEEE International Conference on Computer and Information Technologie (CIT 2010), pp.832-837.

[24] Asif Ali Wagan, Bilal Munir Mughal, Halabi Hashullah, "VANET Security Framework for Trust Grouping using TPM Hardware: Group Formation and Message Dissemination", IEEE Information Technology, pp. 607-611, June 15-17, 2010, Kuala Lumpur, Malaysia.

[25] Maxim Raya, Adel Aziz, Jean-Pierre Hubaux, "Efficient Secure Aggregation in VANETs", VANET '06 Procedings of 3rd International workshop on Vehicular ad hoc networks, pp. 67-75, August 20 — 23, 2006, New York, USA.

[26] Krishna Sampigethaya, Mingyan Li, Leping Huang, Radha Poovendran "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE JSAC, Special issue on Vehicular Networks, Vol. 25, No. 8, pp. 1569-1589, 2007.

[27] Ambuj Kumar, Rajendra Prasad Nayak, " An Efficient Group-Based Safety Message Transmission Protocol for VANET", IEEE, International Conference on Communication and Signal Processiing (ICCSP), pp. 270-274, April 3-5, 2013, Melmaruvathur, India.

[28] Jinhua Guo, John P. Baugh, and Shengquan Wang, "A GroupSignature Based Secure and Privacy- Preserving Vehicular Communication Framework". Proc. of the Mobile Networking for Vehicular Environment (MOVE) works-hop in conjunction with IEEE INFOCOM. May 2007.

[29] Marshall Riley, Kemal Akkaya , Kenny Fong, "Delay-Efficient Geodynamic Group-Based Authentication in VANETs" IEEE 35th Conference on Local Computer Networks (LCN), pp. 280-283, October, 10- 14, 2010, Denver, Colorado, USA.

[30] Albert Wasef and Xuemin Shen, "Ppgcv: Privacy preserving group communications protocol for vehicular ad hoc networks," in Proceedings of IEEE ICC'08, 2008, pp. 1458–1463.

[31] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure Multicast Groups on Ad Hoc Networks," Proc. of the 1st ACM workshop on security of ad hoc and sensor networks, NY, USA, ACM, pp. 94-102, 2003.

[32] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen, GSIS: A secure and Privacy-Preserving Protocol for Vehicular Communications, IEEE Transactions on Vehicular Technologie, Vol.56, N06, pp.3342-3456, November 2007.

[33] Huang Lu, Jie Li and Mohsen Guizani, "A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs" Computing, Communication and Applications Conference (ComComAp), pp. 345-350, 2012.

[34] Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs" IEEE Transaction on Intelligent Transportation Systems, Volume 12, pp. 736-746, september 2011.

[35] Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang and Xuemin Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE Transactions on Vehicular technology, Vol.61, N01, January 2012, pp.86-96.

[36] Bharati Mishra, Saroj Kumar Panigrahy, Tarini Charan Tripathy, Debasish Jena and Sanjay Kumar Jena, "A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation", Information and Communication Technologies (WICT), pp. 880-885, 2011.

[37] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han, Xuemin Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications" IEEE the 27th Conference on Computer Communications, pp. 1903-1911, April 13-18, 2008, Phoenix, Azizona, USA.

[38] F. Armknecht, A. Festag, D. Westhoff and K. Zang, "Cross-layer privacy enhancement and non-repudiation in vehicular communication", In 4th Workshop on Mobile Ad hoc networks, WMAN 07, February 26 - March 02, 2007, Bern, Switzerland.

[39] C.I Fan, R. H. Hsu and C. H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network", Proceeding of the International Conference on Mobile Technology, Applications, and Systems, ACM 2008, Article No 82, ISBN: 978-1-60558-089-0.

[40] http://www.openstreetmap.org/ (accédé le 03/12/2013).

[41] Daniel Krajzewicz, Jakob Erdmann, Michael Behrisch, and Laura Bieker. Recent Development and Applications of SUMO - Simulation of Urban MObility. International Journal On Advances in Systems and Measurements, 5 (3&4):128-138, December 2012.

[42] http://y-baddi.developpez.com/tutoriels/ns2/ (accédé le 03/12/2013).

[43] http://www.memoireonline.com/04/10/3394/Greedy-perimeter-stateless-routing-sur-omnet.html (accédé le 03/12/2013).

[44] A. Kuntz, F. Schmidt-Eisenlohr, O. Graute, H. Hartenstein, M. Zitterbart, "Introducing Probabilistic Radio Propagation Models in OMNeT++ Mobility Framework and Cross Validation Check with NS-2" Proceedings of the 1st International Conference on Simulation tools and technique for communications, networks and system & workshop, ACM 2008, Article No. 72, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium.

[45] http://kom.aau.dk/group/05gr1120/ref/Channel.pdf (accédé le 03/12/2013).

[46] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. T. Klein Haneveld, T. E. V. Parker, O. W. Visser, H. S. Lichte, S. Valentin, "Simulating wireless and mobile networks in OMNeT++ the MiXiM vision", 1st International Conference on Simulation tools and techniques for communications, networks and system & workshops, Article No. 71, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium ©2008.

[47] http://ctieware.eng.monash.edu.au/twiki/bin/view/Simulation/OMNeTppComparison (accédé le 03/12/2013).

[48] http://mixim.sourceforge.net/index.html (accédé le 03/12/2013).

[49] Christoph Sommer, Reinhard German andFalko Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," IEEE Transactions on Mobile Computing, vol. 10 (1), pp. 3-15, January 2011.

[50] Jung-Yoon Kim, Hyoung-Kee Choi, John A. Copeland, "An Efficient Authentication Scheme for Security and Privacy Preservation in V2I Communications", IEEE, 72nd Conference on Vehicular Technology, pp. 1-6, Sept 6-10, 2010, Ottawa-Ontario, CANADA.

[51] http://fr.wikipedia.org/wiki/Intervalle_de_confiance (accédé le 03/12/2013).

[52] Adetundji Adigun. Boucif Amar Bensaber, Ismail Biskri, "Protocole de sécurité basé sur le changement périodique des pseudonymes de communication dans les VANETs", 81e Congrès de l'ACFAS 2013,6 -10 mai 2013, Université de Laval, Québec-CANADA

[53] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, " Protocol of Change Pseudonyms for VANETs ", 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks,(The 38th IEEE Conference on Local Computer Networks (LCN)), Sydney, Australia, 21-24 October 2013, Pages 111-114, ACM New York, NY, USA, ISBN: 978-1-4503-1625-5.

[54] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, " Proof of Concept of a Security Based on Lifetime of Communication's pseudonyms for VANETs ", DIVANet '12, Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications (15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems), Pages 111-114, ISBN: 978-1-4503-1625-5, Paphos, Cyprus Island, October 2012.

[55] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, "A Model of change pseudonyms of communication on Highway", 3rd Annual NSERC DIVA Workshop, 12-13 November 2013, Ottawa — CANADA.

[56] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, "A Security Based on Lifetime of Communication's Pseudonyms for the VANETs", 2nd Annual NSERC DIVA Workshop, 30-31 August. 2012, Ottawa — CANADA.

Annexes: Diffusions reliées au sujet de la maîtrise

A. Publications

1. Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, " Protocol of Change Pseudonyms for VANETs ", 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks,(The 38th IEEE Conference on Local Computer Networks (LCN)), Sydney, Australia, 21-24 October 2013, Pages 111-114, ACM New York, NY, USA, ISBN: 978-1-4503-1625-5.

9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, 2013

Protocol of Change Pseudonyms for VANETs

Adetundji Adigun[1], Boucif Amar Bensaber[2], Ismail Biskri[3]
Laboratoire de Mathématiques et Informatique appliquées (LAMIA)
Departement of Mathematics and Computer Science
University of Quebec at Trois-Rivières
Trois-Rivières, QC, Canada
[1]Adigun@uqtr.ca, [2]Boucif.Amar.Bensaber@uqtr.ca, [3]Ismail.Biskri@uqtr.ca

***Abstract*—We propose in this paper a security protocol based on periodic change of pseudonyms. The idea is to avoid illegal traceability of vehicles during their communications and preserve their privacy and confidential information. Two different approaches are proposed. In the first approach, each vehicle asks the central authority a new communication pseudonym after a time t. While in the second approach, each vehicle generates itself after a time t, a new communication pseudonym. Our objective is to permit at least two vehicles to change their pseudonym in the same time interval. We evaluate in this work, the bandwidth used by considering the vehicles speed in each approach. The proposed protocol is based on equidistant distribution of the road side unit and uses the average of speed permitted on the road to evaluate lifetime t of the communication's pseudonyms and certificates. The exchange of information is based on asymmetric and symmetric cryptography scheme and it uses hash function. Our protocol provides authentication, non-repudiation and privacy.**

***Index Terms*—VANET security, authentication, privacy, certificate, equidistant distribution, traceability.**

I. INTRODUCTION

There are two types of applications in Vehicular Ad Hoc Network (VANET). The first type is called security applications; it provides real time information about the conditions of the road to the drivers. This information can be collision warning, emergency report, or congestion information. The second type is qualified as non-safety application. It is a series of applications that make the journey on road pleasant such as video streaming, music, hotels information. Furthermore, a VANET offers two fundamental types of communications: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Each vehicle is equipped with a wireless communication device called an on-board unit (OBU) and at the road side location road-side units (RSU) are installed. The system is coordinated by a trusted third entity called, Central Authority (CA), which could be the department of transportation [1]. Because of the important aspect of the information shared through the network, it is necessary to develop the security protocols to make VANETs applications helpful. Especially, sensitive information such as identity and location privacy must be preserved through vehicular communications [2]. For this purpose, we propose a security protocol based on periodic change of communication pseudonym. Two different approaches are proposed. In the first approach, each vehicle asks the central authority (CA) a new communication pseudonym after a time t. In the second approach each vehicle generates itself, after a time t, a new communication pseudonym. In each approach, the road side units (RSU) are distributed equidistantly (the distance between each RSU is the same), so the RSUs can communicate with each other. The distance between each RSU is their communication range. Thus when a vehicle enters into another RSUs communication range, it will ask for a new pseudonym in first approach, or will generate a new pseudonym and certificate in the second approach. The time for a vehicle traveling at the average speed to cover the distance between each RSU, is the lifetime (t) of pseudonym and certificate. Our objective is to permit at least two vehicles to change their pseudonym in the same time interval. We use the cryptography scheme to secure the information shared through the network. Our aim is to evaluate the bandwidth used, and the bit error rate by considering the vehicles speed in each approach. The remainder of this paper is organized as follows. In section II, we discuss the state of art on the security in VANET networks. In section III, we introduce our model. In section IV, we will present a short security analysis and describe the parameters of simulation for the two approaches, and we will conclude in section V.

II. STATE OF THE ART

In [2], Youngho Park, Kyung-Hyune Rhee and Chul Sur present a secure and Location Assurance Protocol for Location-Aware Services in VANETs which provides anonymous authentication and avoid illegal movement tracking of vehicles in VANET as well as location assurance. The proposed scheme permits to the vehicle to have confidence that the received information originated from the vehicles that actually passed through the target location area. But if the private key generated by the MA (Master Authority) is not sent to the vehicle in a secure way, the attacker can intercept it and use it to threaten the life of drivers, violating confidentiality properties and authentication. In [3], the authors propose a novel ID-based authentication framework with adaptive privacy preservation for VANETs. In this framework, the vehicles use pseudonym to communicate and the update of pseudonym depends on vehicles demands. A cooperative message authentication protocol in VANETs is proposed in [4]. The idea of this work is to alleviate vehicles computation burden during the authentication stage and reduce the number of safety messages that each vehicle needs to verify. In [5], JaeHyu Kim and JooSeok Song propose a pre-

978-1-4799-0540-9/13/$31.00 ©2013 IEEE

authentication method based on scalable robust authentication protocol (SRAP) to reduce the number of packets transmitted in the key request stage. They also use symmetric key encryption function to decrease calculation time. In [1], the authors propose ID-based Safety Message Authentication for Security and Trust in Vehicular Networks. They incorporate an ID-based proxy signature framework with the standard ECDSA for VANETs road-side unit (RSU) originated safety application messages. The proposed protocol is appropriate for authentication and trust management but may suffer of the traceability problem. Because, if an attacker intercepts the message exchanged by two OBUs and if it contains the OBU location, then he could trace a vehicle in the network. A Secure and efficient data acquisition method in VANETs is proposed in [15]. The idea of the authors is to allow each vehicle user (driver and passengers) to communicate individually in the network. The road side unit assigns to each user who is connected a pseudonym per packet to avoid attacks. In [6], the authors propose a privacy-preserving trust model that respects the privacy of the users through groups and offers security through trust and reputation. Although the proposed protocol permits to exchange secure messages among vehicles and helps them to assess the reliability of receiving message. It is based on a static group of vehicles assigned offline. This protocol doesnt provide a better security algorithm because of dynamic topology in vehicular network. In [7], an efficient pseudonym authentication-based conditional privacy protocol for VANETs is proposed. It allows each vehicle in the network to use pseudonyms to obtain privacy. The vehicles interact with road units to generate their communication pseudonyms. The authors propose in [8] a secure and efficient protocol for VANETs. Their scheme ensures both message authentication and privacy preservation. But a vehicle needs to communicate to road side unit before verifying the signature of a message it has received. In [16], a distributed key management framework based on group signature to preserve privacy in vehicular ad hoc network is presented. Each group is formed by the vehicles which get keys from the same road side unit. The proposed scheme preserves the privacy and permits to detect compromised road side units and vehicles. A privacy preservation authentication scheme for communication between vehicle and infrastructure in VANETs is proposed in [17]. The scheme permits to a vehicle and a road side unit to authenticate each other without returning to the trust authority. Although the proposed scheme satisfies most of the security requirements, it can be used to a communication between vehicles. In [18], the authors present a secure and efficient protocol for position-based routing in VANETs, The proposed scheme improves the security of position-based protocol. Group-based Source Authentication protocol (GSA) is proposed in [9] to handle the message authentication in VANETs. GSA makes use of group attributes as dynamic group key to protect data transmission in intra-group communication. The results of this implementation can guarantee multicast source authentication and boost the efficiency of authentication for multicast communication in VANETs. An innovative scheme for generating series of-lived secret keys that are shared by all the subscribers of the service is presented in [12]. The proposed algorithm is based on a couple of hash-chains generated from the master key. In [13] the authors present a security architecture which helps achieve all the security attributes without introducing complex or multi-transaction procedure. This proposed protocol doesnt require a tamper-proof-device (TPD) which stores the vehicles communication keys. In [19], Kaouther Abrougui and Azzedine Boukerche present a Secure Location based Service Discovery Protocol (SecLocVSDP). The proposed protocol permits secure discovery of service providers in VANET. It consists of a location based propagation of service requests and service reply messages; in other words, it permits to discover service providers located in a region of interest specified by the service requester. An algorithm to secure vehicular communication based on a probabilistic approach is proposed in [14]. This scheme helps to determine the trust level of vehicles communication messages and to check the validity of the received messages. Security architecture is proposed in [10]. This protocol is based on two new concepts: an extend PKI called PKI+ and secure geographical routing. In the proposed scheme, the user acts autonomous after receiving one master key and a master certificate from the CA. The user can create his own certified pseudonyms without interaction with the CA. In [11] the authors propose an efficient pseudonym PKI mechanism based on bilinear mapping to improve the performance of the message authentication protocol, and permits certificate tracing and certification revocation. The proposed solutions in [10, 11] permit to the vehicles to generate themselves their keys for communication but they dont mention the expiration time of the certificate. Authentication and privacy have been studied in various forms to prevent illegal vehicle traceability and protect users' information in the network. But few of these studies have defined a change time of the pseudonyms of communication for vehicles and analyzed the impact of the speed of vehicles on the use of pseudonyms communication. For it, we evaluate in this work, the bandwidth used, and the bit error rate by considering the vehicles speed in the periodic change of the pseudonyms of communication.

III. SYSTEM MODEL

A. overall idea

Our proposed protocol preserves authentication, non repudiation, and privacy. It permits to the vehicles to change their pseudonyms in the same interval time. We have also place the road side unit at the same distance to permit the communication between them and the vehicles.

B. assumptions

In our proposed protocol, we assume that: in the first approach, each vehicle has an ID (unique information that identifies the vehicle) which it shares with the Central Authority (CA) to request for the communication pseudonyms. In the second approach, each vehicle is identified by a private/public keys which it uses to get its private pseudonym and its certificate from the CA. The Road side units are trusted and

are under the CAs control. The RSUs public key is available to all vehicles and it is certified by the CA. Each RSU broadcasts the publics pseudonym of the vehicles in its range as soon as it receives them from the CA. The CA is always online and reachable. It knows the RSUs private keys so it can decipher a message encrypted with the RSUs public key. Also the CA certifies the RSUs public key and frequently updates it.

C. description of the model

1) approach 1: In this approach, each vehicle is registered at the CA to get its private pseudonym and its virtual identity. The CA, after sending to the vehicle its private pseudonym and its virtual identity, sends the vehicles certificate to the road side unit which broadcasts this certificate. The vehicles certificate contains its virtual identity, public pseudonym and the lifetime of the certificate. The lifetime of the certificate is time for a vehicle traveling at an average speed to cover distance between two road side units. Upon expiry of the certificate, the vehicle sends to the CA its virtual identity. When the CA receives the virtual identity of the vehicle, it sends to this vehicle an update private pseudonym and communicates to the road side unit the vehicles certificate. Then the road side unit will broadcast the certificate. The virtual identity is used to identify the vehicles on the road, while the pseudonym permits them to communicate.

TABLE I
NOTATIONS USED THROUGHOUT THIS PAPER

Notation	Description
$Vrid$	Vehicle's real identity.
$VprKey$	Vehicle's private. key
$VpbKey$	Vehicle's public key.
$Vcert$	Vehicle's certificate.
$Vprpseudo$	Vehicle's private pseudonym.
$Vvid$	Vehicle's virtual identity.
$Vpseudcertif$	Vehicle's pseudonym and certification information.
$RprKey$	RSU's private key.
$RpbKey$	RSU's public key.
$ERpbKey(Vrid)$	Asymmetric encryption function that encrypts the vehicle real identity with RSU public key.
$EVrid(Vprpseudo + Vvid)$	Symmetric encryption function that encrypts the vehicle private pseudonym and its virtual identity with the real identity of the vehicle.
$ERpbKey(VprKey + VpbKey)$	Asymmetric encryption function that encrypts the vehicle private and public key with RSU public key.
$EVpbKey(Vpseudcertif)$	Asymmetric encryption function that encrypts the set of information (which permit at the vehicle to generate its pseudonym and certificate) with its public key.
$Br(Vcert)$	Broadcast the vehicle certificate.
$EVrid(Vvid)$	Symmetric encryption function that encrypts the vehicle virtual identity with its real identity.
$E_VVrid(V'prpseudo + V'vid)$	Symmetric encryption function that encrypts the new private pseudonym and virtual identity of the vehicle with its real identity.
$V'cert$	Vehicle's new certificate.
$Br(V'cert)$	Broadcast the new certificate.

The design as shown in figure 1, describes the different steps of the approach 1. Related steps are offered as follows:

1. RSU broadcasts periodically its public key.
2. Vehicle sends to CA a $E_{RpbKey}(Vrid)$ message.
3. CA sends to the applicant vehicle a $EVrid(Vprpseudo + Vvid)$ message.
4. CA sends to RSU a $Vcert$ message.
5. RSU broadcasts $Vcert$ message.
6. Vehicle sends a $EVrid(Vvid)$ message to the CA.
7. CA delivers a $EVrid(V'prpseudo + V'vid)$ message to the vehicle.
8. CA sends to RSU a $V'cert$ message.
9. RSU broadcasts $V'cert$ message.

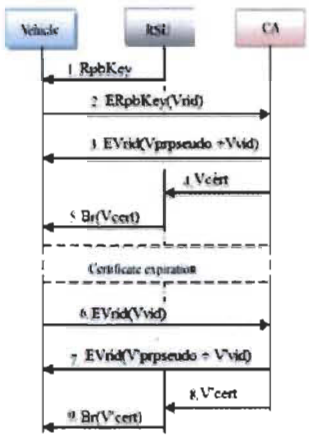


Fig. 1. Description of the main steps in approach 1.

In this approach, the vehicle always communicates with the CA to obtain its private communication pseudonym. We will analyze the bandwidth used between the request and the reception of pseudonym by vehicle in section IV.

2) approach 2: In the second approach, each vehicle has a private and public key. If the vehicle receives the RSUs public key, it will send to the CA, its private and public keys by encrypting them with RSUs public key. The CA will register the vehicles pair key (private/public) and will send to the vehicle a set of information by encrypting them with the vehicle public key. This set of information contains data that permits to the vehicle to generate its private pseudonym and certificate. When the vehicle receives this set of information, it will generate its private pseudonym and certificate. After that, it will broadcast its certificate. Upon the expiration of the certificate, it will generate a new private pseudonym and certificate that it will broadcast. The vehicles are identified in this approach by the pseudonyms.

Figure 2 describes the different steps of the approach 2. The steps are as follows:

1. RSU broadcasts periodically its public key.
2. Vehicle sends to CA a $ERpbKey(VprKey + VpbKey)$ message.
3. CA sends to the applicant vehicle a $EVpbKey(Vpseudcertif)$ message.
4. Vehicle generates its private pseudonym and certificate.
5. Vehicle broadcasts its certificate.
6. Vehicle updates its private pseudonym and certificate.
7. Vehicle broadcasts the new certificate.

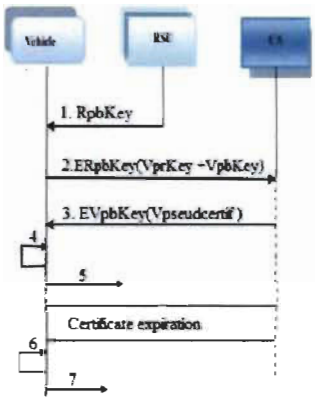


Fig. 2. Description of main steps in approach 2.

The vehicles, in the second approach are autonomous to update their private pseudonyms and certificates, once they have been authenticated by the CA. As in the first approach, we evaluate in section IV the bandwidth used and the bit error rate for this approach. We will compare the results for each approach.

D. Evaluation of the expiration time of certificate and private pseudonym

In both approaches, the road side units are distributed equidistantly. Consider d the distance between each road side unit. d is also the communication range of each road side unit. V_max and V_min are respectively the maximum and minimum speed authorized on the road. We suppose, there will be at least two vehicles which will roll at an average speed. Our idea is to permit at least two vehicles to get the pseudonym on road in the same interval time. Denote V_m=$(V_max + V_min)/2$. The expiration time of certificate and private pseudonym t, will be the ratio between d and V_m; $t = d/V_m$. Also, as the communication range of each road side unit is equal road side unit has a communication range equal d, any vehicle, whatever its speed, can communicate at least with one road side unit and could change at least once its pseudonym on the road.

IV. ANALYSIS

A. Security Analysis

1) Authentication: In our two approaches, only a vehicle which has certified pseudonyms by the CA, can communicate with the others. This means that all vehicles in the network are registered and trusted by the CA. CA is the one who can decipher a message encrypted with the RSUs public key and all the RSUs are under the CAs control.

2) Non-repudiation: The vehicles communicate with certified pseudonyms received from the CA. In case of dispute, the CA can easily find the real identity of the vehicle because in the first approach, a vehicle requests private pseudonyms with its secret (identity), while in the second approach, the private and public key of vehicle permit to identify it.

3) Privacy: Each vehicle communicates with short lifetime pseudonyms. The pseudonyms are renewed periodically and are not linked. Furthermore the change of pseudonym has done by at least two vehicles. So an attacker cant identify precisely which vehicle has changed its pseudonym.

B. Performance Analysis

Assessment parameters:

1) Number of vehicles which have gotten the private pseudonym in each approach.
2) Number of vehicles which have changed their pseudonym in each approach.
3) The bandwidth used in each approach according to the vehicle velocity.

The scheme is tested by OMNET++ 4.2.2 [20] with veins-2.0 [21] and SUMO-0.15.0. [22]. We have run the simulation five times. Network parameters are set as in table 2.

TABLE II
SIMULATION PARAMETERS

Item	Value
Map Manhattan city	1.2 km x 1.2 km
Number of RSU	4
Distance between RSU	300 m
Simulation time	100 s
Packet size	1024 bytes
Number of vehicles in each approach	100
Interval of speed on the road	$5m/s$ - $14m/s$.
Time for changing the pseudonym and certificate	30 s
Bit rate	6 Mbps
MAC Protocol	IEEE 802.11p
Analogue Models	SimplePathlossModel TwoRayInterferenceModel SimpleObstacleShadowing
Communication range of RSU	300 m
Communication range of vehicle	150 m
*.nic.phy80211p.thermalNoise	-110 dBm

1) Number of vehicles which have gotten the private pseudonym in each approach.
In both approaches, 40% of vehicles didn't get their privates pseudonyms. 60% of them have gotten their private pseudonym in different time. We suppose, in the first approach, a vehicle receives its private pseudonym if its certificate has been broadcasted. The results are presented in figure 3.

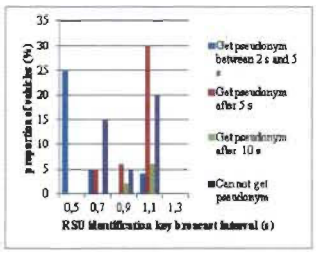


Fig. 3. Private pseudonym distribution phase

2) Number of vehicles which have changed their pseudonym in each approach.
The aim of our study is to evaluate the change of pseudonyms vehicles. As described previously in subsection D, the expiration time of certificate and private pseudonym t = 300/9.5. t = 31.5 s. But we have considered in our simulations that the vehicles will begin to change their pseudonyms every 30 s. This will allow them to have new pseudonyms before expirationy of the current ones.
During the first period for change the communication pseudonym, 80% of vehicles which have been authenticated in the second approach have changed their pseudonyms while 75% of vehicles have received a new pseudonym in the first approach. We remark that the number of vehicles in first approach decreases until 50%, in time; while proportion of vehicles in the second approach is above 50%. This is due to the lost of packets. The result is presented in figure 4 below.

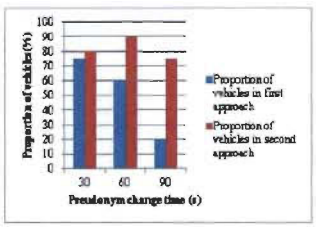


Fig. 4. Change of pseudonym in each approach

3) The bandwidth used in each approach according to the vehicle velocity.
We consider in this section the average velocity of vehicles. In figure 5, the bandwidth used by vehicles in first approach is increasing quickly depending on the velocity. While in the second approach, the consumption of bandwidth is less significant depending on the speed. The used of bandwidth in first approach is more important than the second approach. This is the fact in the first approach; a vehicle needs to communicate always with the central authority to get its private pseudonym.

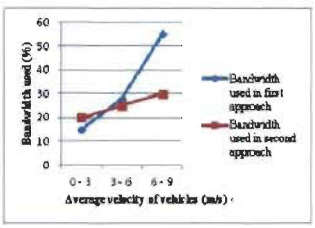


Fig. 5. Bandwidth consumption in each approach based on average velocity

V. Conclusion

We have presented in this paper, a protocol of change pseudonyms for VANETs, using urban environment for simulation. The bandwidth used and the update of pseudonyms have been considered in each approach. In our future work, we will evaluate the bit error rate and take in to operation of our protocol in highway scenario. After that we will propose a dissemination routing protocol to fit best our method.

Acknowledgment

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

References

[1] Subir Biswas, Jelena Misic and Vojislav Misic, ID-based Safety Message Authentication for Security and Trust in Vehicular Networks, 31st International Conference on Distributed Computing System Workshops, pp.323-331, 2011.

[2] Youngho Park and Kyung-Hyune Rhee, Chul Sur, A Secure and Location Assurance Protocol for Location-Aware Services in VANETs, 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.456-461, 2011.

[3] Huang Lu, Jie Li and Mohsen Guizani, A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs Computing, Communication and Applications Conference (ComComAp), pp. 345-350, 2012.

[4] Yong Hao, Tingting Han and Yu Cheng, A Cooperative Message Authentication Protocol in VANETs, Global Communication Conference (GLOBECOM), IEEE, pp. 5562-5566, 2012.

[5] JaeHyu Kim and JooSeok Song, A Pre-authentication Method for Secure Communications in Vehicular Ad Hoc Networks, 8th International Conference on Wireless Communication, Networking and Mobile Computing (WiCom), pp. 1-6, 2012.

[6] Ayman Tajeddine, Ayman Kayssi and Ali Chehab, A Privacy-Preserving Trust Model for VANETs, 10th IEEE International Conference on Computer and Information Technologie (CIT 2010), pp.832-837. [7] Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue, PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs Intelligent Transportation Systems, IEEE Transaction on Volume 12, pp. 736-746, 2011.

[8] Bharati Mishra, Saroj Kumar Panigrahy, Tarini Charan Tripathy, Debasish Jena and Sanjay Kumar Jena, A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation, Information and Communication Technologies (WICT), pp. 880-885, 2011.

[9] You Lu, Biao Zhou, Pei Jia and Mario Gerla, Group-based Secure Source Authentication Protocol for VANETs, IEEE Globecom 2010 Workshop on Heterogenous, Multi-hop Wireless and Mobile Networks, pp.202-206.

[10] F. Armknecht, A. Festag, D. Westhoff and K. Zang, Cross-layer privacy enhancement and non-repudiation in vehicular communication, In 4th Workshop on Mobile Ad hoc networks, WMAN 07, February 26 - March 02, 2007, Bern, Switzerland.

[11] C.I Fan, R. H. Hsu and C. H. Tseng, Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network, Proceeding of the International Conference on Mobile Technology, Applications, and Systems, ACM 2008, Article No 82, ISBN: 978-1-60558-089-0.

[12] StefanoBusanelli, Gianluigi Ferrari and LucaVeltri, Short-lived Key Management for Secure Communications in VANETs, Security and Applications IEEE, pp.613-618, 2011.

[13] Baber Aslam and Cliff C.Zou, One-way-linkable Blind Signature Security Architecture for VANET, The 8th Annual IEEE Consumer Communication and Networking Conference-Smart Spaces and Personal Area Networks, pp.745-750, 2011.

[14] Danda B. Rawat, Bhed B. Bista, Gongjun Yan and Michele C. Weigle, Securing Vehicular Ad-Hoc Network against Malicious Drivers: A Probabilistic Approch, International Conference on Complex, Intelligent, and Software Intensive Systems, pp.146-151, 2011.

[15] Khaleel Mershad and Hassan Artail, REACT: Secure and Efficient Data Acquisition in VANETs, 7th International Conference IEEE, Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 149-156, 2011.

[16] Yong Hao, Yu Cheng, Chi Zhou and Wei Song, A Distributed Key Management Framework with Cooperative Message Authentication in VANETs, IEEE journal vol 29, pp. 616-629, 2011.

[17] Ming-Chin Chuang and Jeng-Farn Lee, PPAS: A Privacy Preservation Authentication Scheme for Vehicle-to-Infrastructure Communication Networks, Consumer Electronic, Communicatins and Networks (CECNet), International Conference, pp. 1509-1512, 2011.

[18] Jie Hou, Lei Han, Jiqiang Liu and Jia Zhao, Secure and Efficient Protocol for Position-based Routing in VANETs, Intelligent Control Automatic Detection and High-End Equipment, (ICADE), IEEE International Conference, pp. 142-148, 2012.

[19] Kaouther Abrougui and Azzedine Boukerche, Secure Service Discovery Protocol for Intelligent Transport Systems: Proof of Correctness, 1st NSERC DIVA WORKSHOP, Developing the next Generation Intelligent Vehicular Network and Applications, pp.51-57, September 9, 2011-Ottawa-Canada.

[20] http://www.omnetpp.org/

[21] http://veins.car2x.org/

[22] http://sumo.sourceforge.net/

2. Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri, " Proof of Concept of a Security Based on Lifetime of Communication's pseudonyms for VANETs ", DIVANet '12, Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications (15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems), Pages 111-114, ISBN: 978-1-4503-1625-5, Paphos, Cyprus Island, October 2012.

Proof of Concept of a Security Based on Lifetime of Communication's Pseudonyms for the VANETs

Adetundji Adigun
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivières, Trois-Rivières, Qc, Canada
1 819 3765011 ext. 3831
Adigun@uqtr.ca

Boucif Amar Bensaber
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivières, Trois-Rivières, Qc, Canada
1 819 3765011 ext. 3807
Boucif.Amar.Bensaber@uqtr.ca

Ismail Biskri
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivières, Trois-Rivières, Qc, Canada
1 819 3765011 ext. 3837
Ismail.Biskri@uqtr.ca

ABSTRACT

To make Vehicular Ad Hoc Network (VANET) applications useful to the users, the security problem must be solved. Recent researches have suggested the use of a set of anonymous keys certified by the issuing CA (Central authority) to preserve privacy, authentication, and confidentiality of the communicating entities. But how to determine the right time for the vehicles to exchange their communication pseudonyms and what would be the impacts on the network resources such as time processing and memory. In this paper, we propose a protocol that preserves authentication, non repudiation, and location privacy and helps vehicles to exchange their pseudonyms at roughly the same time. It is based on calculating the Euclidean distance and the average of the speed permitted on the path to evaluate the lifetime of the communication's pseudonyms. The exchange of the information is based on asymmetric and symmetric cryptography scheme and it uses hash function. The protocol permits to determine the expiration time of pseudonyms and how to make the distribution of all the road side units along the road in order to establish a good communication between them and the vehicles.

Categories and Subject Descriptors

C.2.2 [Network Protocols]

General Terms

Security

Keywords

VANET security, privacy, keys management, Euclidean distance.

1. INTRODUCTION

There are two types of applications in Vehicular Ad Hoc Network (VANET). The first type called security applications provides real time information about the road conditions to the drivers. This information can be collision warning, emergence reporting, and congestion information. The second type qualified by non-safety application is a series of applications that make pleasant the journey on road such as video streaming, music, hotels information. Furthermore, a VANET offers two fundamental types of communications: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Each vehicle is equipped with a wireless communication device called an on-board unit (OBU) and at the road side location are installed road-side units (RSU). The system is coordinated by a trusted third entity Central Authority (CA) which could be the department of transportation [1].

Because of the important aspect of the information shared through the network, it is necessary to develop the security protocols to make VANET's applications helpful. Especially, sensitive information such as identity and location privacy must be preserved through vehicular communications [2].

To achieve location privacy, a popular approach is recommended to change periodically the vehicle's pseudonyms in VANETs when they broadcast messages. Because a vehicle uses different pseudonyms on the road, the unlinkability of pseudonym can guarantee a vehicle's privacy [3]. But how can we determine a right time for the vehicle to exchange his pseudonyms and what would be the impacts of these actions on the network.

To resolve this problem, we present in this paper a secure protocol based on calculating the Euclidean distance and the average of the speed permitted on the path to evaluate the lifetime of the communication's pseudonyms and which uses a cryptography scheme for the exchanging of the information. We propose two different approaches. One based on the generation of pseudonyms by the central authority and the second one based on the pseudonyms generation by each vehicle. Our aim is to compare the latency and the bandwidth of each approach.

The remainder of this paper is organized as follows. In section II, we discuss the state of art of the security in VANET networks. In section III, we introduce our model. In section IV, we will present a short security analysis and we will conclude in section V.

2. STATE OF THE ART

In [2], Youngho Park and Kyung-Hyune Rhee, Chul Sur present a secure and Location Assurance Protocol for Location-Aware Services in VANETs which provides anonymous authentication and avoid illegal movement tracking of vehicles in VANET as well as location assurance. The proposed scheme permits to the vehicle to have confidence that the received information were originated from the vehicles actually passed through the target location area. But in their proposition, they don't explain in which way the private key is generated by the MA (Master Authority) and sent to the vehicle. If this information is not secure, an attacker can intercepts it and use it to threaten the life of drivers, violating confidentiality properties and authentication. In [3], the authors propose an effective pseudonym changing at social spot (PCS) strategy to achieve the provable location privacy. In their scheme, the user by using authorized anonymous key received from the trusted authority (TA)

DIVANet'12, October 21–22, 2012, Paphos, Cyprus.

generates anonymous short-life keys according to his trip. After that, he installs the generated keys in his vehicle and conserves an authorized anonymous key in a secure place. During the trip, the driver will change the communication key frequently in social spot. The vehicle uses different pseudonyms on the road; the unlinkability of pseudonyms can guarantee a vehicle's location privacy. The fact that all vehicles present at social spot change simultaneously their pseudonyms, the location and velocity information could still clue to the adversary. The protocol permits to guarantee confidentiality properties and untraceability but the user is limited in his journey in case he forgets the authorized anonymous key, he can't generate news keys for a direction he had not programmed before.

In [4], Kaouther Abrougui and Azzedine Boukerche present a Secure Location based Service Discovery Protocol (SecLocVSDP). The proposed protocol permits secure discovery of service providers in VANET. It consists of a location based propagation of service requests and service reply messages; in other words, it permits to discover service providers located in a region of interest specified by the service requester. In [5], the authors propose GSIS: A secure and Privacy-Preserving Protocol for Vehicular Communications. Their ideas are based on group signature and identity based signature technique. Each vehicle is in a group and uses a group key pair to communicate. They propose a protocol that includes correctness, unforgeability, anonymity and unlinkability, but doesn't resolve the man in the middle attack. Because if the ID of a vehicle or the vehicle's group private key were not sent in a secure way, an intruder can intercept this information which is very important to preserve the confidential and the usurpation properties. In [1], the authors propose ID-based Safety Message Authentication for Security and Trust in Vehicular Networks. They incorporate an ID-based proxy signature framework with the standard ECDSA for VANET's road-side unit (RSU) originated safety application messages. The proposed protocol is appropriate for authentication and trust management but can be suffered by the traceability problem. Because if an attacker intercepts the message exchanged by two OBUs and if it contains the OBU location, then he could trace a vehicle in the network. In [6], the authors propose a privacy-preserving trust model that respects the privacy of the users through groups and offers security through trust and reputation. Although the proposed protocol permits to exchange secure messages among vehicles and helps them to assess the reliability of receiving message; it is based on a static group of vehicles assigned offline. This protocol doesn't provide a better security algorithm for VANET because of its dynamic topology. In [7], the authors propose a message authentication scheme which enables the message authentication in intra and inter RSU range and the hand-off within the different RSUs. The protocol proposed can be able to satisfy authentication, message integrity, privacy but it can allow a spoofing attack of RSU. The authors propose in [8] a privacy-aware location service by integrating Chaum's mix network. The proposed protocol is vulnerable against denial of service attack, secures location inquiry and can easily integrate to others securities protocols. But this scheme requires an infrastructure including RSU, if not there will be a collision problem in the different operators for the mixes. Group-based Source Authentication protocol (GSA) is proposed in [9] to handle the message authentication in VANETs. GSA makes use of group attributes as dynamic group key to protect data transmission in intra-group communication. The results of this implementation can guarantee multicast source authentication and boost the efficiency of authentication for multicast communication in VANETs. An innovative scheme for generating series of-lived secret keys that are shared by all the subscribers of the service is presented in [12]. The proposed algorithm is based on a couple of hash-chains generated from the master key. In [13] the authors present a security architecture which helps to achieve all the security attributes without introducing complex or multi-transaction procedure. This proposed protocol doesn't require a tamper-proof-device (TPD) which stores the vehicle's communication keys. An algorithm to secure vehicular communication based on a probabilistic approach is proposed in [14]. This scheme helps to determine the trust level of vehicles' communication messages and to check the validity of the received messages.

Security architecture is proposed in [10]. This protocol is based on two new concepts: an extend PKI called PKI+ and secure geographical routing. In the proposed scheme, the user acts autonomous after receiving one master key and master certificate from the CA. The user can create his own certified pseudonyms without interaction with the CA. In [11] the authors propose an efficient pseudonym PKI mechanism based on bilinear mapping to improve the performance of the message authentication protocol, and permits certificate tracing and certification revocation.

The proposed solutions in [10, 11] permit to the vehicles to generate themselves their keys for communication but they don't mention the expiration time of the certificate.

3. SYSTEM MODEL

Overall idea

Our proposed protocol preserves authentication, non repudiation, and location privacy and helps vehicles to change their pseudonyms at roughly the same time. It permits to determine the expiration time of pseudonyms and how to make the distribution of all the road side units along the road in order to establish a good communication between them and the on-board unit equipped in each vehicle.

Assumptions

In our proposed protocol, we assume that every vehicle is equipped with a GPS to be able to determine its location. Then each vehicle has a secret (unique information that identifies the vehicle) which it shares with the Central Authority (CA) to request for the communication pseudonyms. The Road side units are trusted and are under the CA's control. The RSU's public key is available to all vehicles and it is certified by the CA. Each RSU broadcasts the public's pseudonym of the vehicles in its range as soon as it receives them from the CA. The CA is always online and reachable. It knows the RSU's private keys so it can decipher a message encrypted with the RSU's public key. Also the CA certifies the RSU's public key.

Description of the model

In the section below, we present our first model by describing the actions of each entity.

Table 1: Notations

Notation	Description
VPpe	Vehicle's Public pseudonym
VPrpe	Vehicle's private pseudonym
Vsecret	Secret of the vehicle
Lx;y	Location information of the vehicle on the road
tabVPpe	Table containing the publics pseudonyms
PkeyRSU	Public key of the road side unit

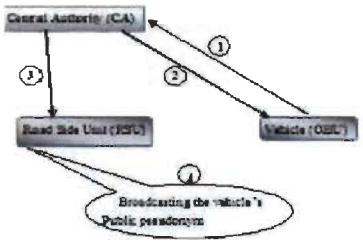


Figure 1: The process of generating pseudonyms by the CA

Legend

1: vehicle requests for certified pair of pseudonyms of communication by sending the secret and localisation

2: CA sends the private pseudonym certified to the requester vehicle

3. CA sends the public pseudonym of the requester to the RSU

4: RSU broadcasts the received public pseudonym.

Step1: **Actions of the vehicle**

Before a vehicle V communicates with its neighbors, it will send to the CA its secret (Vsecret) and its location (Lx,y) encrypted with the RSU's public key. After that, it receives from the CA, its certified private pseudonym (VPrpe) and gets by RSU's broadcasting the certified publics pseudonyms of its neighbors.

Upon expiry of the pseudonym, the vehicle requests another valid pseudonym from the CA by sending again its secret. In our model, a vehicle keeps during the lifetime of its pseudonyms, its private pseudonym and the public's pseudonym of its neighbors.

Algorithm of receiving a communication's keys:

/*sending the secret and location information*/

V.Send ((Vsecret, Lx,y), PkeyRSU)

/*Reception of communication keys*/

VPrpe =CA.message

for all V neighbors in RSU broadcast message do

tabVPpe [i]=RSU.broadcast

end

/*Communication time*/

While (VPrpe.time>0)

V.communication

end

V. Send ((Vsecret, Lx,y), PkeyRSU).

Step2: **the process of generating of communication's pseudonym**

Upon receiving the request message of vehicle, the CA generates a pair of pseudonym (private/public) for the vehicle by including the expiration time. Then the CA encrypts the private pseudonym of the vehicle with a secret received before and sends to the vehicle. Also it sends to RSU located in the vehicle area, the public pseudonym of this vehicle.

Algorithm of generating a communication's pseudonyms

While (vehicle.request=true)

Decipher (vehicle.request,RSU.private Key)
Calculate expiration time of pseudonym ( )
Generatepairepseudonym( )
Sendprivatepseudonym( );
Sendpublicpseudonym ( ).

End

Evaluation of the expiration time of pseudonym

(X', Y'): coordinates of vehicle in Euclidean space.
(X, Y): coordinates of the CA in Euclidean space.
V_1: maximum speed permitted on the path of the vehicle.
V_2: minimum speed permitted on the path of the vehicle.
τ: lifetime of pseudonym.

$$\tau - \frac{\sqrt{(X - X')^2 + (Y - Y')^2}}{\frac{(V1 - V2)}{2}}$$

Even if the vehicle stops the pseudonym would stay active. The lifetime of the pseudonym is independent of the vehicle state.

Step3: **Broadcasting the vehicle's publics' pseudonyms.**

When the road side unit (RSU) received the public pseudonym of the vehicle, it broadcasts the receiving pseudonym to all the vehicles located in its range.

Algorithm3: broadcasting the vehicle's publics pseudonym

While (CA.receive=true)

Broadcast (VPpe)

end

Our protocol permits to determine the valid time for a vehicle communication's pseudonyms and guarantees the authentication and privacy location because even if an attacker eavesdrops the communication, he can't identify exactly which vehicle make the pseudonym request. The CA stores each pair of pseudonyms it generates for the vehicles and in case of a dispute, it will find the real identity of the vehicle by using the information containing in the vehicle's secret.

To measure the effect of expiration communication's pseudonyms on the network and before doing the simulations, we propose a second approach based on the idea developed in [10, 11].

Second approach

In this approach, each vehicle generates its pair of pseudonyms (private/public) of communication and sends them to the central authority by encrypting them with the RSU's public key, for being certified. The CA deciphers the package of the request vehicle with the RSU's private key. After certifying the pair of pseudonyms of the vehicle, the CA sends them to the request vehicle by encrypting them with the public key of RSU located in the vehicle range. When the vehicle received the package containing its certified communication's pseudonym, it deciphers the package with the RSU's public key and it will broadcast its public pseudonym to its neighbors. The expiration time of the communication's pseudonym is the same like in first approach. But the difference between this model and the previous one is that in the second model a RSU doesn't broadcast the vehicle's public pseudonym. Each vehicle is autonomous to generate its private and public pseudonym and broadcasts its public pseudonym to its neighbors, after it certified its pseudonym by the CA.

Second Model

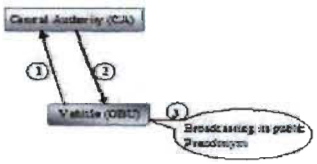


Figure 2: The process of generating pseudonyms by the vehicle

Legend

1: vehicle sends its pair of pseudonyms (private and public) for be certified by the CA

2: CA sends the certified pair of pseudonyms to the requester vehicle

3: vehicle broadcasts its certified public pseudonym.

We want to compare: to compare the latency, amount of messages and the time for receipt of public pseudonym in each approach.

4. SECURITY ANALYSIS

- Authentication

In our two protocols, only a vehicle which has certified pseudonyms by the CA, can communicate with the others. This means that all vehicles in the network are registered and are trusted by the CA. All the RSU are also registered and trusted by CA.

- Non-repudiation

The vehicles communicate with certified pseudonyms received from the CA. In case of dispute, the CA can easily find the real identity of the vehicle because in the first protocol a vehicle requests the pair of pseudonyms with its secret (identity). In the second protocol, a private pseudonyms generated by a vehicle contains its identity.

- Location privacy

Each vehicle communicates with short lifetime pseudonyms. The probability that a new request for communication's pseudonyms will be done by several vehicles and not one is important. In that case, an intruder can't have the location information of a special vehicle because he doesn't know when this vehicle requests for communication's pseudonyms.

5. CONCLUSION

In this paper, we present briefly our protocol based on periodically communication's pseudonym exchange in VANET. We precise the validity time of pseudonym and based on the literature, we have proposed a second approach that will allow us to evaluate our idea. Our goal is to evaluate our schemes in terms of network resources as time processing and memory, so our future work will include the results of the performance metrics of each scheme. We will use traffic simulation SUMO (Simulation of Urban Mobility) and NS-3 (a discrete-event network simulator) to compare and evaluate the feasibility of our approaches.

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

6. REFERENCES

[1] Subir Biswas, Jelena Misic and Vojislav Misic, *ID-based Safety Message Authentication for Security and Trust in Vehicular Networks*, 31st International Conference on Distributed Computing System Workshops, pp.323-331, 2011.

[2] Youngho Park and Kyung-Hyune Rhee, Chul Sur, *A Secure and Location Assurance Protocol for Location-Aware Services in VANETs*, 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.456-461, 2011.

[3] Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang and Xuemin Shen, *Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs*, IEEE Transactions on Vehicular technology, Vol.61, N°1, January 2012, pp.86-96.

[4] Kaouther Abrougui and Azzedine Boukerche, *Secure Service Discovery Protocol for Intelligent Transport Systems: Proof of Correctness*, 1st NSERC DIVA WORKSHOP, Developing the next Generation Intelligent Vehicular Network and Applications, pp.51-57, September 9, 2011-Ottawa-Canada.

[5] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen, *GSIS: A secure and Privacy-Preserving Protocol for Vehicular Communications*, IEEE Transactions on Vehicular Technologie, Vol.56, N°6, pp.3342-3456, November 2007.

[6] Ayman Tajeddine, Ayman Kayssi and Ali Chehab, *A Privacy-Preserving Trust Model for VANETs*, 10th IEEE International Conference on Computer and Information Technologie (CIT 2010), pp.832-837.

[7] Hsin-Te, Wu, Wei-Shuo Li, Tung-Shih, Su and Wen-Shyong Hsieh, *A Novel RSU-based Message Authentication Scheme for VANET*, 50th International Conference on Systems and Networks Communications, pp.111-116, 2010.

[8] Florian Scheuer, Matthias Brecht and Hannes Federrath, A Privacy-Aware location service for VANETs using Chaum's mixes, 6th International Conference on wireless and Mobile Computing, Networking and Communications, pp.159-164, 2010.

[9] You Lu, Biao Zhou, Fei Jia and Mario Gerla, *Group-based Secure Source Authentication Protocol for VANETs*, IEEE Globecom 2010 Workshop on Heterogenous, Multi-hop Wireless and Mobile Networks, pp.202-206.

[10] F. Armknecht, A. Festag, D. Westhoff and K. Zang, *Cross-layer privacy enhancement and non-repudiation in vehicular communication*, In WMAN 07.

[11] C.I Fan, R. H. Hsu and C. H. Tseng, *Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network*, In WMAN 08

[12] StefanoBusanelli, Gianluigi Ferrari and LucaVeltri, *Short-lived Key Management for Secure Communications in VANETs*, Security and Applications IEEE, pp.613-618, 2011.

[13] Baber Aslam and Cliff C.Zou, *One-way-linkable Blind Signature Security Architecture for VANET*, The 8th Annual IEEE Consumer Communication and Networking Conference-Smart Spaces and Personal Area Networks, pp.745-750, 2011.

[14] Danda B. Rawat, Bhed B. Bista, Gongjun Yan and Michele C. Weigle, *Securing Vehicular Ad-Hoc Network against Malicious Drivers: A Probabilistic Approch*, International Conference on Complex, Intelligent, and Software Intensive Systems, pp.146-151, 2011.

B. Communications libres

1. 3rd Annual NSERC DIVA Workshop, "A Model of change pseudonyms of communication on Highway", 12-13 November 2013, Ottawa — CANADA.

UQTR
Savoir Surprendre.

A Model of Change Pseudonyms Communication on Highway

Presented by Adetundji Adigun

Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri
LAboratoire de Mathématiques et Informatique Appliquées LAMIA
Department of Mathematics and Computer Science
University of Québec à Trois-Rivières.
{Adetundji.adigunlBoucif.Amar.BensaberIIsmail.Biskri} @uqtr.ca

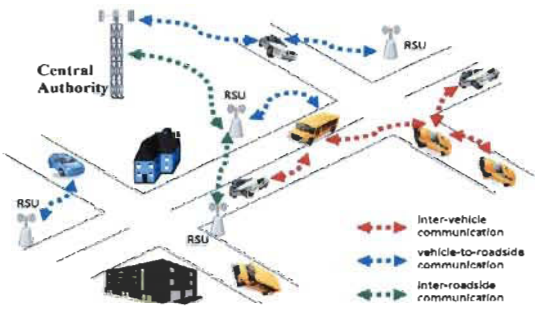
Outline

- Introduction
- Problematic
- Motivation
- Model of change pseudonyms
- Simulations and results
- Conclusion

Introduction

- Vehicular Ad Network offers two types of applications:
  - Security application
    - Collision warning
    - Accident reporting
    - Congestion information
  - Non-safety application
    - Video streaming
    - Sharing music
    - Hotels or packing information

Vehicular Ad hoc Networks (VANETs)



Example of VANET [1]

Problematic

- Protect information exchanged between network users
- Protect the identity of users
- Location privacy

Motivation

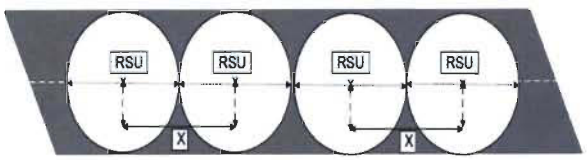
- Achieve location privacy
- Determine an interval time to change pseudonyms
- Analyse the impact on the network in term of bandwidth consumption

Model of change pseudonyms

- Disposition of RSUs
- The speeds authorized on the road
- Two approaches are studied:
  - Generating pseudonyms by the CA
  - Generating pseudonym by the vehicle

Disposition of Road Side units

- Position of RSUs on a road



X: distance between each RSU.

LIFETIME OF PSEUDONYM AND CERTIFICATE

- Vmax , Vmin: respectively maximum and speed authorized on the road
- Interval time to change pseudonyms and certificate is:

  I: [X/Vmax; 2X(Vmax+Vmin)]

Approach 1

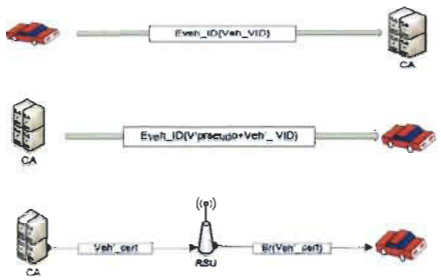
- Authentication

- Reception of private pseudonym

- Getting the certificate

Approach 1

- Update of private pseudonym and certificate



Approach 1

- Content of certificate
  - Virtual identity of the vehicle
  - Public pseudonym
  - Lifetime of the certificate
  - Signature of CA

Approach 2

- Authentication

- Steps of generating private pseudonyms and certificate

- After the expiration of certificate

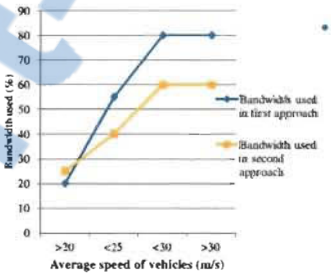
Approach 2

- Content of certificate
  - Public pseudonym
  - Lifetime of the certificate
  - Signature of vehicle

Simulation and results

- OMNet++: network simulator
- SUMO: simulate urban mobility
- Number of nodes: 100
- Number of RSU: 4
- Map: 5km x 3 km
- X=700m
- Vmax=28m/s and Vmin=16m/s
- I=[25s ; 31.81s]

Bandwidth used in function of vehicle's average speed



- The consumption of bandwidth is important in the first approach than in the second approach
  - Number of requests for the pseudonyms communication
  - Forwarding of packets

Conclusion and future works

- Model of change pseudonym
- Develop a probabilistic model to improve the time to change pseudonyms
- Propose a dissemination routing protocol

References

- [1]: www.cs.nthu.edu.tw/~jungchuk/research.html
- [2]: Hsin-Te, Wu, Wei-Shuo Li, Tung-Shih, Su and Wen-Shyong Hsieh, A Novel RSU-based Message Authentication Scheme for VANET, 50th International Conference on Systems and Networks Communications, pp.111-116, 2010.
- [3]: You Lu, Biao Zhou, Fei Jia and Mario Gerla, Group-based Secure Source Authentication Protocol for VANETs, IEEE Globecom 2010 Workshop on Heterogenous, Multi-hop Wireless and Mobile Networks, pp.202-206.

2. 81e Congrès de l'ACFAS 2013, "Protocole de sécurité basé sur le changement périodique des pseudonymes de communication dans les VANETs" 6 -10 mai 2013, Université de Laval, Québec-CANADA.

UQTR
Savoir Surprendre.

Protocole de sécurité basé sur le changement périodique des pseudonymes de communication dans les VANETs

Présenté par Adetundji Adigun

Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri
LAboratoire de Mathématiques et Informatique Appliquées LAMIA
Département de Mathématiques et Informatique
Université du Québec à Trois-Rivières.
{Adetundji.adigun|Boucif.Amar.Bensaber|Ismail.Biskri} @uqtr.ca

Plan

- Introduction
- Systèmes de transport intelligents
- Réseaux véhiculaires sans fil: VANETs
- Problématique
- Notre proposition
- Conclusion

Introduction

- Les systèmes de transport actuels
  - Augmentation de la congestion du trafic routier

  266 milliards de dollars/an : étude du cabinet Roland Berger [1].
  - Les accidents de route

  Environ 1.24 million de décès/an: rapport de l'étude sur la sécurité routière 2013 [2].
  - Absence d'information en temps réel sur les conditions de la route et météorologiques.

Introduction

- Conséquences
  - Dégâts environnementaux: pollution, émission du gaz à effet de serre.
  - Augmentation du taux de mortalité.
  - Perte de temps considérable par les usagers dans les transports.

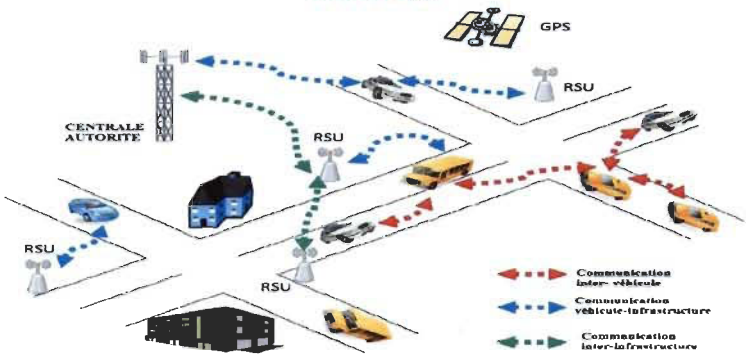
Les systèmes de transport intelligents

- Gérer le trafic routier
- Prévenir les accidents de la route
- Réduire les dégâts en cas de collision
- Gestion des secours
- Aide à la navigation
- Gestion énergétique
- Amélioration du confort des usagers de la route

Les réseaux de transports véhiculaires sans fil VANETs

- Entités communicantes
  - Voitures équipées de OBU
  - Infrastructure routière: RSU
  - Équipement central ou Centrale autorité
- Technologie: DRSC (Dedicated Short range Communication)
  - Norme IEEE 802.11a – IEEE 802.11p
  - Portée maximale théorique: 1000m

Les réseaux de transports véhiculaires sans fil VANETs



Exemple de réseaux VANETs [3]

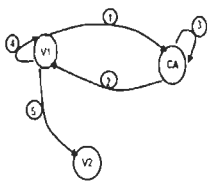
Problématique

- Protéger les informations échangées entre les utilisateurs du réseau
- Protéger l'identité des utilisateurs
- Éviter la traçabilité illégale des utilisateurs

Notre proposition : Protocole de sécurité de changement de pseudonymes

- Plage de vitesses sur les routes
- Cryptographie asymétrique basée sur les courbes elliptiques
- Cryptographie symétrique
- Distribution équidistante des centrales autorités

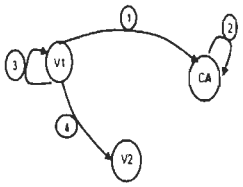
Approche 1: Authentification



Légende

1. Envoi de l'ID plus nonce1 et nonce2 crypté avec la clé publique de CA
2. Envoi (pseudonyme privé+nonce1) crypté avec le nonce2
3. Diffusion du certificat
4. Génération du pseudonyme de session
5. Envoi du pseudonyme de session crypté avec son pseudonyme privé

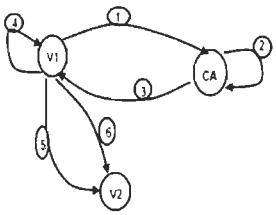
Approche 1: Mise à jour de pseudonyme de session



Légende

1. Envoi pseudonyme privé crypté avec la clé publique de CA
2. Diffusion du certificat après vérification du pseudonyme privé du véhicule
3. Génération du pseudonyme de session
4. Envoi du pseudonyme de session crypté avec son pseudonyme privé

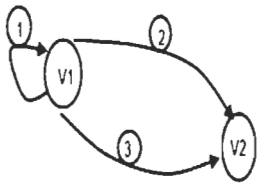
Approche 2: Authentification



Légende

1. Envoi de la paire de pseudonymes (privé/public) crypté avec la clé publique de CA
2. Enregistrement de la paire de pseudonymes
3. Envoi du certificat au véhicule crypté avec le pseudonyme public du véhicule
4. Génération du pseudonyme de session
5. Diffusion du certificat
6. Envoi du pseudonyme de session crypté avec son pseudonyme privé

Approche 2: Mise à jour de pseudonyme de session



Légende

1. Génération du pseudonyme de session
2. Diffusion du certificat
3. Envoi du pseudonyme de session crypté avec son pseudonyme privé

Protocole de sécurité de changement de pseudonymes

- Simulateurs
  - SUMO 0.15
  - OMNETT++ 4.2.2
- Carte routière: Ville de Manhattan (1.5 km x1 km)
  - Plage de vitesse: 20-60 km/h

Protocole de sécurité de changement de pseudonymes

- Paramètres de simulations

Paramètre	Valeur
Taille paquet	1024 bits
Débit du canal	6 Mbps
Fenêtre de collision	20
Taille paquet entête	40 bits
Fréquence	5.890e9
Temps de simulations	100 s
Nombre de véhicules	50
Nombre de CA	4

Protocole de sécurité de changement de pseudonymes

- Résultats

Métriques	Valeur
Réception de la clé publique de CA	37/50
Envoi de message d'authentification	37/50
Réception de pseudonyme privé	2/37
Réception de certificat	2/37
Diffusion de pseudonyme de session	2/2

Conclusion

- Sécuriser les messages échangés à travers le réseau.
- Protéger l'identité des utilisateurs du réseau.
- Analyser l'impact du changement de pseudonymes de communication sur le réseau.
- Réduction de 10% du taux de mortalité sur les routes [4].
- Réduction de 25% de la durée et le coût des transport [4].

Références

- [1]: http://www.rfi.fr/economie/20130309-prix-exorbitant-embouteillages-cabinet-roland-berger
- [2]:http://www.who.int/violence_injury_prevention/road_safety_status/2013/report/summary_fr.pdf
- [3]: http://www.cs.nthu.edu.tw/~jungchuk/research.html
- [4]: Les Cahiers du Challenge Bibendum: Véhicules connectés et systèmes de transport intelligents, Berlin 2011.

C. Posters

1. 3rd Annual NSERC DIVA Workshop, "A Model of change pseudonyms of communication on Highway", 12-13 November 2013, Ottawa — CANADA.

A Model of change pseudonym of communication on Highway

ADETOSOJI ADIGON[1], SOUCIF AMAR BENSABER[1], ISMAIL BISKRI[1], AZZEDINE BOUKERCHE[2]
[1]LABORATOIRE DE MATHEMATIQUES ET INFORMATIQUE APPLIQUEES LAMIA
[1]DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
[1]UNIVERSITY OF QUEBEC AT TROIS-RIVIERES
(ADIGON|SOUCIF.AMAR.BENSABER|ISMAIL.BISKRI)@UQTR.CA
[2]UNIVERSITY OF OTTAWA

INTRODUCTION

To avoid illegal traceability of vehicles and preserve their privacy and confidential information, we propose a model of change pseudonym of communication. The model is based on distribution of Road Side units (RSU), range of speed authorized on the road, and cryptography scheme . Two different approaches are considered in this study.

Approach I

1. RSU broadcasts periodically its public key
2. Vehicle sends to CA a ERpbKey(V rid) message.
3. CA sends to the applicant vehicle a EV rid(V pseudo + V vid) message.
4. CA sends to RSU a V cert message.
5. RSU broadcasts V cert message.
6. Vehicle sends a EV rid(V vid) message to the CA.
7. CA delivers a EV rid(V pseudo + V vid) message to the vehicle
8. CA sends to RSU a V cert message.
9. RSU broadcasts V cert message

Assumptions
- Each vehicle has an ID
- Each RSU broadcasts its public key every 200ms
- CA deciphers all messages encrypted with the RSU public

Content of certificate
- Virtual identity of the vehicle
- Public pseudonym
- Lifetime of the certificate
- The CA's signature

Approach II

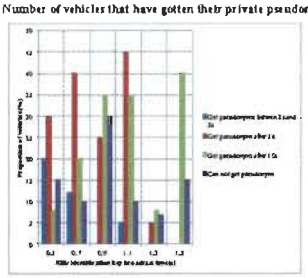
1. RSU broadcasts periodically its public key
2. Vehicle sends to CA a ERpbKey (V prKey + VpbKey) message.
3. CA sends to the applicant vehicle a EVpbKey(Vpseudo cert).
4. Vehicle generate its private pseudonym and certificate.
5. Vehicle broadcasts its certificate
6. Vehicle updates its private pseudonym and certificate
7. Vehicle broadcasts the new certificate

Assumptions
- Each vehicle is identified by a private and public key
- Each RSU broadcasts its public key every 200ms
- CA deciphers all messages encrypted with the RSU public
- Each vehicle is able to generate its pseudonyms

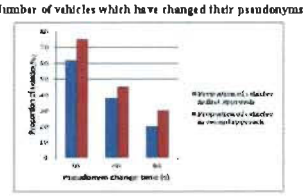
Content of certificate
- Public pseudonym
- Lifetime of the certificate
- The Vehicle's signature

Performance analysis

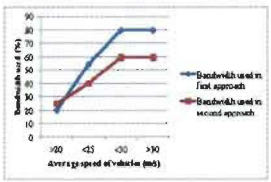
Number of vehicles that have gotten their private pseudonyms



Number of vehicles which have changed their pseudonyms



The bandwidth is used in function of the average vehicle speed



Lifetime of pseudonyms and certificate

Vmax, Vmin: maximum and minimum speed on the road

X: Communication range of RSU

Interval time of change pseudonyms and certificate is:

$$t=[X/Vmax;\ 2X/(Vmax+Vmin)]$$

Simulation environment

- OMNET++ 4.2.2
- SUMO 0.15.0
- Number of nodes: 100
- Number of RSU: 4

Security analysis

Authentication. In both approaches, only a vehicle which has certified pseudonyms by the CA, can communicate with others. This means that all in the network are registered and trusted by the CA.

Non-repudiation: The vehicles communicate with certified pseudonyms received from the CA. In case of dispute, the CA can easily find the real identity of the vehicle.

Privacy: Each vehicle communicates with short lifetime pseudonyms. The pseudonyms are renewed periodically and are not linked. Furthermore, the change of pseudonyms has done at least by two in the same interval time. An attacker can't identify precisely which vehicle has changed its pseudonym.

Conclusion

We have presented in this paper, a protocol of change pseudonyms for VANETs, using urban environment for simulation. The bandwidth used and the update of pseudonyms have been considered in each approach. In our future work, we will propose a dissemination routing protocol to fit best our method.

References

F Armknecht, A. Festag, D. Westhoff and K. Zeng. *"Cross-layer privacy enhancement and non-repudiation in vehicular communication."* In WMAN 07.

C.I Fan, R. H. Hsu and C. H. Tseng. *Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network*, In WMAN 08

2. 2nd Annual NSERC DIVA Workshop, "A Security Based on Lifetime of Communication's Pseudonyms for the VANETs", 30-31 August. 2012, Ottawa — CANADA.

A Security Based on Lifetime of Communication's Pseudonyms for the VANETs

Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri
Laboratoire de Mathématiques et Informatique Appliquées (LAMIA)
Department of Mathematics and Computer Science
University of Québec at Trois-Rivières, Trois-Rivières, Qc, Canada
{Adigun|Boucif.Amar.Bensaber|Ismail.Biskri} @uqtr.ca

Abstract

- The use of a set of anonymous keys certified by the issuing CA (Central authority) has been suggested to preserve privacy, authentication, and confidentiality of the communicating entities in VANETs.
- Evaluate the lifetime of pseudonyms used by the vehicles to communicate and measure the impact on the network resources (time processing and memory) is our goal.
- The lifetime of pseudonym is obtained from the calculation of Euclidean distance and the average of speed permitted on vehicle's path.
- The exchange for the information is based on asymmetric and symmetric cryptography scheme and hash function.

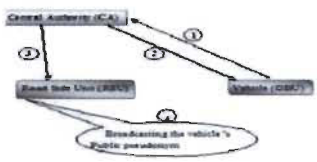
Introduction

- Two types of applications are considered in VANETs:
  - Security applications
  - Non-safety applications
- The security is needed to enjoy of the full information shared through the network.
- We present a secure protocol based on lifetime of pseudonyms.
- Two approaches are presented to evaluate our idea:
  - Generation of pseudonym by the central authority.
  - Generation of pseudonym by each vehicle.

Assumptions

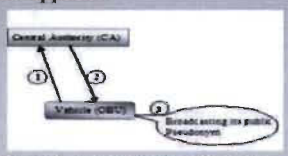
- Every vehicle is equipped with a GPS.
- Each vehicle has a secret (unique information that identifies the vehicle).
- Road Side Units are trusted and are under the CA's control.
- The RSU's public key is available to all vehicles. This public key is certified by the CA.
- CA is always online and reachable and knows all RSU's private keys.

First approach



1. Vehicle requests for certified pair of pseudonyms of communication by sending the secret and the localisation
2. CA sends the private pseudonym certified to the requester vehicle
3. CA sends the public pseudonym of the requester vehicle to the RSU
4. RSU broadcasts the received public pseudonym.

Second approach



1. Vehicle sends its pair of pseudonyms (private and public) to be the CA requesting a certification.
2. CA sends the certified of pseudonyms to the requester vehicle.
3. Vehicle broadcast its certified public pseudonym.

Evaluation of the expiration time of the pseudonym

(X^1, Y^1) : coordinates of the vehicle in Euclidean space.
(X^2, Y^2) : coordinates of the CA in Euclidean space.
V_2 : maximum speed permitted on the path of the vehicle.
V_1 : minimum speed permitted on the path of the vehicle.
τ_1 lifetime of pseudonym.

$$\tau = \frac{\sqrt{(X^2 - X^1)^2 + (Y^2 - Y^1)^2}}{\frac{(V_2 - V_1)}{2}}$$

Security analysis

- **Authentication**: Only a vehicle which has certified pseudonyms by the CA, can communicate with the others. This means that all vehicles in the network are registered and are trusted by the CA.
- **Non repudiation**: The vehicles communicate with certified pseudonyms received from the CA. In case of dispute, the CA can easily find the real identity of the vehicle.
- **Location privacy**: An intruder can't have the location information of a special vehicle because he doesn't know when this vehicle requests for communication's pseudonyms.

Future works

- Present the results of our two approaches by using traffic simulation SUMO and NS-3.
- Expose the results of the performance metrics of each scheme.

References

1 F. Armknecht, A. Festag, D. Westhoff and K. Zang, *Cross-layer privacy enhancement and non-repudiation in vehicular communication*, In WMAN 07.

2 C.I Fan, R. H. Hsu and C. H. Tseng, *Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network*, In WMAN 08