RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Amar Telidji - Laghouat

Faculté de Sciences

THÈSE DE DOCTORAT EN SCIENCES

Spécialité : Informatique

Présentée et soutenue publiquement

le 09/11/2017

CHAIB Noureddine

THEME

La protection contre les nœuds malveillants dans les réseaux VANET

JURY :

Monsieur Ouinten Youcef,	Président du jury,	Maître de conférences,	Université Amar Telidji - Laghouat
Monsieur Mohamed Benmohammed,	Examinateur,	Professeur,	Université de Constantine
Monsieur Azeddine Bilami,	Examinateur,	Professeur,	Université de Batna
Madame Hadda Cherroun,	Examinateur,	Professeur,	Université Amar Telidji - Laghouat
Monsieur Mohamed Bachir Yagoubi,	Encadreur,	Professeur,	Université Amar Telidji - Laghouat
Monsieur Nasreddine Lagraa ,	Co-encadreur,	Professeur,	Université Amar Telidji - Laghouat

الملخص:

شبكات المركبات تلعب دورا حيويا في زيادة الوعي لدى السائقين. للأسف، نظرا للطبيعة الموزعة لهذه الشبكات ، يمكن أن يسيطر بعض القراصنة بطريقة شرعية على عناصر بها، فيمكن أن تسبب خلل في هذه الشبكات أو حتى تتسبب في حوادث تعرض حياة الناس وممتلكاتهم للخطر . ولذلك، فإن قدرة المهاجم على شن هجمات خارجية قد تكون محدودة، أوتصل حتى إلى السيطرة على البنية التحتية المثبتة على جوانب الطرقات والقدرة على تنسيق الهجمات. لذلك كشف وإزالة هذه العناصر أمر معقد و صعب للغاية.

في هذا العمل، نقترح حلولا للتخلص من عناصر الشبكات المسيطر عليها من القراصنة في على نحو فعال.

أولا اقترحنا نظام أرس لإزالتها دون المساس بتوفرالخدمة في الشبكة. هذا النظام يتميز بصفته نظام هجينا يتميز بقدرته على كشف الهجمات بعدد قليل من الرسائل المتبادلة بين عناصر الشبكة, كما يتميز هذا النظام بقدرته على التكيف مع عدد المهاجمين ليحمي الشبكة و الخدمات المختلفة التي توفرها

النظام المقترح الثاني هو إسديربي الذي هو عبارة عن نظام لكشف وإزالة عناصر الشبكات المسيطر عليها من القراصنة عند طلب هذه الخدمة, و يسمح النظام المقترح بتجنب هذه العناصر على نحو فعال.

في هذا العمل اقترحنا أيضا نظاما جديدا لإلغاء الأسماء مستعارة. على عكس الأنظمة الأخرى، فإنه يشمل جميع الآليات لإزالة هذه الأسماء لعناصر الشبكات المسيطر عليها من القراصنة في أي حالة تتوفر فيها شروط الإلغاء. وتشير نتائج المحاكاة نجاعة أداء حلولنا.

كلمات البحث: إلغاء شبكات المركبات ، اسم مستعار، أدس، الكشف ،التحقق ،أرس، إسديربي.

Abstract:

VANETs (*Vehicular ad hoc networks*) allow communication between vehicles. They play an essential role in increasing the contextual awareness of vehicles. Unfortunately, due to the distributed nature of these networks, a node could be controlled by malicious entities. They could harm the proper functioning of these networks or even cause accidents that threaten the lives of people and properties. A malicious entity could be a person or an organization seeking profit. Therefore, the ability of an attacker might comprise launching limited attacks, controlling roadside infrastructures or coordinating attacks. Thus, the detection and the removal of malicious nodes is complicated and difficult to perform.

In this work, we propose several solutions to revoke malicious nodes efficiently. We propose the revocation scheme ARS (*Adaptive Revocation Scheme*) which allows removing malicious nodes without compromising the network availability.

The second proposed system is SDRP (*Secure Distributed Revocation Protocol*), which is an on-demand system for the detection and the removal of malicious nodes. SDRP allows honest nodes to avoid using malicious nodes as relays. We also propose a new system for the revocation of pseudonyms. Unlike other systems, SDRP includes all mechanisms to revoke malicious nodes whenever the revocation condition is satisfied. The simulation results show the efficiency of our solutions.

The third solution that we propose in this work, is EPRV (*Efficient Pseudonym Revocation in VANETs*) that allows the revocation of pseudonyms of malicious vehicles efficiently. In Fact, unlike previous works, EPRV revokes malicious vehicles whenever the revocation conditions holds against them. Simulation results show the high performance of the our system

Keywords: Revocation, VANET networks, Pseudonym, IDS, detection, verification, ARS, SDRP.

Résumé :

Les VANETs (*Vehicular ad hoc networks*) permettent les communications entre les véhicules. Elles joueront un rôle essentiel pour augmenter la prise de conscience contextuelle des véhicules. Malheureusement, vue la nature distribuée de ces réseaux, un nœud pourrait être contrôlé par des entités malveillantes. Ces dernières pourraient causer le dysfonctionnement de ces réseaux ou, voire même, causer des accidents menaçant la vie des personnes et les biens. Ces entités malveillantes pourraient être une personne ou un organisme qui cherche son profit. Donc, la capacité d'un attaquant à lancer des attaques peut être limitée, ou aller au contrôle sur les infrastructures installées aux abords de routes et à l'aptitude de coordonner les attaques. Donc, la détection et la révocation de nœuds malveillants est un processus compliqué et difficile à effectuer. Dans ce travail, nous proposons des solutions pour révoquer les nœuds malveillants de manière efficace. Le premier système réalisé est ARS (*Adaptive Revocation Scheme*) qui permet de révoquer les nœuds malveillants sans mettre en péril la disponibilité du réseau. Le deuxième système proposé est SDRP qui est un système de détection et de révocation de nœuds malveillants à la demande. SDRP permet aux nœuds honnêtes d'éviter les nœuds relais malveillants. Nous avons aussi proposé un nouveau système EPRV (*Efficient Pseudonym Revocation in VANETs*) pour la révocation des pseudonymes. A la différence des autres systèmes, il comprend l'ensemble de mécanismes qui permettent de révoquer les nœuds malveillants à n'importe quelle situation dans laquelle la condition de révocation est satisfaite. Les résultats de simulations effectuées montrent l'efficacité de nos solutions.

Mots clés : Révocation, Réseaux VANET, Pseudonyme, IDS, détection, vérification, ARS, SDRP.

Table des matières

Table de figures

Liste des Tableaux

Á ma défunte mère,

Á mon père,

Á ma petite famille

Á mes frères,

Á mes sœurs,

Á tous ceux qui me sont chers,...

Je dédie affectueusement ce modeste travail

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à mes encadreurs

Pr. Mohamed YAGOUBI et Pr. Nasreddine LAGRAA. Pour leurs aides sans limite et leurs précieux conseils qu'ils m'ont donnés et sans lesquels ce travail n'aurait pas vu le jour. Ils m'ont guidé pour entamer un travail de recherche passionnant et prometteur : le monde de la sécurité des communications dans les réseaux véhiculaires.

Je remercie les membres de jury qui ont accepté de juger ce travail :

Dr. Ouinten Youcef, maître de conférences à l'université d'Amar télidji de Laghouat, qui me fait le grand honneur d'accepter la présidence du jury.

Pr. Azeddine Billami, professeur à l'université de Batna, Pr. Mohamed Benmohamed, Professeur à l'université de Constantine et Professeur Hadda cherroun professeur à l'université d'Amar télidji de Laghouat, pour l'honneur qu'ils me font en acceptant de participer à ce jury.

Je suis très reconnaissant à Mr. Rabeh BOUCHELGA pour son aide. Je remercie également tous ceux qui de près ou de loin, m'ont accompagné et soutenu pour

Je remercie aussi mes collègues, mes amis et toutes les personnes qui m'ont aidé durant ces années, à préparer cette thèse dans les meilleures conditions.

Introduction générale

Chaque année dans le monde, des millions d'accidents routiers constituent les premières causes de décès et de blessures. Ces accidents ont aussi un impact négatif sur l'économie à cause des pertes de biens correspondants. Ils rendent aussi la situation des routes congestionnées plus grave. Ce qui augmente les heures de conduite et de transport de marchandises.

Avec la prolifération des équipements électroniques et l'émergence de la technologie de communication, il devient possible d'équiper les véhicules d'interfaces de communication, d'appareils GPS, des unités de traitement, de radars, de capteurs,…etc. Donc, les véhicules peuvent détecter les situations dangereuses et diffuser des messages d'alerte pour avertir les véhicules voisins. En conséquence, les conducteurs ou les véhicules eux mêmes peuvent intelligemment décider l'action adéquate à entreprendre. Ces éléments constituent les réseaux véhiculaires VANET (*Vehicular ad- hoc Network*) qui peuvent alléger la congestion routière en informant les conducteurs sur l'état des routes et les espaces de parking libres. Ils permettent aussi d'éviter les fluctuations de vitesse ce qui réduit la quantité de carburant consommée. Donc, les VANETs ont un impact positif sur l'environnement et l'économie.

Les réseaux véhiculaires et leurs applications prometteuses sont devenus un centre d'intérêt de plusieurs entités, que ce soit des organisations gouvernementales ou de standardisation, des entreprises (notamment les constructeurs automobiles et les opérateurs de télécommunication) ou des centres de recherche.

Ces futurs réseaux véhiculaires seraient parmi les plus grands réseaux dans le monde. A cet effet, ils constitueraient une cible idéale aux attaques des entités malveillantes qui pourraient viser à dégrader leur performance, les exploiter à leur profit ou voire même commettre des actions menaçant la vie des personnes et leurs biens.

L'authentification des nœuds du réseau constitue un élément fondamental pour la sécurisation de ces réseaux et l'identification des nœuds malveillants. Pour celà, les différents organismes de standardisation ont traité ce problème et ont défini les outils cryptographiques nécessaires et le format d'un message sécurisé.

L'identification des nœuds malveillants nécessite des mécanismes pour leur détection préalable. En effet, les nœuds peuvent localement coopérer en contrôlant les activités de leurs voisins et en échangeant des messages d'accusation qui conduisent à la révocation d'un nœud si leur nombre dépasse un seuil prédéfini. Les nouveaux voisins peuvent rapidement révoquer les nœuds malveillants. Cette révocation locale consiste à considérer leurs clés cryptographiques comme invalides.

Les systèmes de révocation locale doivent avoir des mécanismes autonomes afin d'empêcher les nœuds malveillants d'exploiter leur aspect distribué dans la révocation de nœuds honnêtes. Ce qui pose plus de contraintes à la sécurisation de ces réseaux.

Avec les travaux de recherches intensifs sur les VANETs et l'émergence de la cryptographie moderne, les chercheurs ont proposé des solutions pour protéger la vie privée des utilisateurs des VANETs. Elles consistent essentiellement à employer les pseudonymes pour assurer l'anonymat de ces réseaux. Ce qui permet d'encourager les décideurs aux déploiements de ces derniers.

Les solutions de l'anonymat protègent la vie privée d'une part, et posent des contraintes sévères à la détection et l'identification de nœuds malveillants.

Dans ce travail, nous avons essentiellement apporté quatre contributions:

Premièrement, nous avons mené une étude sur l'impact des éléments cryptographiques sur l'authentification. Nous avons trouvé à travers les simulations que le taux des paquets perdus et les délais d'acheminements des paquets augmentent avec l'augmentation de la taille de signature numérique.

Le processus de distribution de certificat est très lent car il est centralisé. Donc, les nœuds doivent collaborer pour révoquer les nœuds localement sans l'intervention de l'AC. A cet effet, notre deuxième contribution consiste à proposer un nouveau protocole de révocation de nœuds malveillants que nous avons appelé ARS (*Adaptive Revocation Scheme*) qui est à la différence de la plupart des systèmes de révocation existant n'est pas basé sur un seuil prédéfini. En effet, avec les systèmes existant une configuration appropriée des nœuds malveillants peut conduire à révoquer tous les nœuds du réseau. De plus, l'augmentation de la valeur du seuil minimise les taux de détection, alors que la diminution de cette valeur conduit à la minimisation du nombre de messages d'accusation nécessaire à la vérification de la condition de révocation, d'une part, et à l'augmentation du nombre de nœuds faux-positifs (Des nœuds honnêtes qui sont révoqués par erreur), d'autre part. En effet, l'objectif principal d'ARS est d'éviter l'épuisement des nœuds dans le réseau autant que possible afin qu'il soit possible d'assurer un certain niveau de disponibilité de service dans le réseau. Le principe de notre approche est de minimiser le nombre de nœuds révoqués autant que possible en rendant la condition de révocation plus difficile à satisfaire. Les propriétés particulières d'ARS sont démontrées mathématiquement et ont montré que l'impact de nœuds malveillants sur le système et la rapidité de leur exclusion dépend de leurs taux de présence dans les réseaux. Ainsi, dans le cas d'une attaque isolée, la performance d'ARS est optimale par rapport aux autres systèmes de révocation existants et un seul message d'accusation est suffisant pour révoquer un nœud. Alors que le coût de révocation de nœuds malveillants augmente de manière proportionnelle au nombre de nœuds malveillants. Les résultats de simulation obtenus supportent et mettent en évidence la performance élevée d'ARS.

Notre troisième contribution dans cette thèse consiste à proposer le système de révocation SDRP (*Secure Distributed Revocation Protocol*). La particularité de SDRP par rapport aux autres systèmes est qu'il permet aux nœuds du réseau d'effectuer l'évaluation et la révocation de nœuds malveillants à la demande. En effet, avec SDRP les nœuds honnêtes du réseau sont capables d'éviter les nœuds relais malveillants, ce qui permet d'acheminer les paquets correctement. A la différence des autres techniques existantes, SDRP n'utilise pas nécessairement toutes les accusations contre un nœud pour le calcul du seuil de révocation, ils emploient plutôt une fonction spécifique pour filtrer les accusations malveillantes. La performance de SDRP a été étudiée par des simulations intensives. Les résultats obtenus montrent que SDRP a donné de meilleurs taux de détection et de faux-positifs qui ont contribué à rendre le processus d'acheminement de paquets plus sûr et sécurisé, même en présence d'un nombre élevé de nœuds malveillants qui lancent des attaques coordonnées.

La quatrième contribution de cette thèse se focalise sur la révocation de pseudonymes. Nous avons présenté deux nouveaux mécanismes DAPM (*Duplicate Accusations Prevention Mechanism*) et IRM (*Instantaneous Revocation Mechanism*). Le mécanisme DAPM permet d'éviter d'avoir plusieurs accusations avec un seul accusateur et un seul accusé, alors que le mécanisme IRM assure la révocation des véhicules dès que la condition de révocation est satisfaite. Nous avons aussi proposé un nouveau système de révocation de pseudonyme EPRV (*Efficient Pseudonym Revocation in VANETs*) qui implémente les deux mécanismes DAPM et IRM, ce qui empêche les nœuds malveillants d'amplifier le nombre de leurs accusations et améliore significativement les délais de révocation. Donc, notre système permet d'exclure les nœuds malveillants le plus tôt possible (l'impact du mécanisme IRM), et dispose des techniques qui permettent de faire face aux accusations falsifiées (l'impact du mécanisme DAPM). En effet, les véhicules malveillants possèdent suffisamment de pseudonymes à un moment donné et peuvent les changer sans suivre les démarches appropriées nécessaires à l'opération, et par conséquent ils peuvent causer une attaque de succession d'accusations qui leurs permet d'amplifier leur impact négatif sur la performance du système. Les résultats de simulation et l'analyse de sécurité de EPRV montrent sa performance par rapport à l'approche classique de révocation de pseudonyme. Finalement, nous avons veillé à démontrer toutes les propriétés de sécurité assurées par EPRV.

Cette thèse est organisée en six chapitres. Nous présentons dans le premier chapitre l'environnement véhiculaire. Nous détaillons, plus précisément, ses futures applications, les modes de communication des réseaux VANET, leurs architectures de communication possibles, et nous donnons un aperçu sur les travaux des équipes de recherche et les organismes de standardisation.

Dans le chapitre 2, nous nous focalisons sur l'authentification de nœuds dans les réseaux VANET. À partir du format des messages sécurisés et des problèmes liés à l'authentification, des approches ont été proposées pour améliorer le processus d'authentification de nœuds.

Le chapitre 3 donne les techniques de détection et de révocation de nœuds malveillants existants et présente une contribution pour la révocation adaptative de nœuds malveillants, et nous avons aussi présenté une étude comparative entre les techniques de révocations existantes.

Le chapitre 4 présente un nouveau protocole de révocation que nous avons proposé pour révoquer les nœuds malveillants.

Le chapitre 5 présente les systèmes de pseudonymat dans les VANETs et les différents problèmes de révocation de pseudonymes.

Le chapitre 6 présente notre dernière contribution, qui est la description de l'architecture de notre système de système de révocation de pseudonyme, suivie par la présentation détaillée de chaque composant de cette architecture. Enfin, nous analysons la performance de notre système à travers des simulations.

Nous concluons cette thèse en présentant les conclusions et quelques perspectives.

Chapitre 1

Introduction aux réseaux VANET

1.1 Introduction

L'émergence de la technologie de communication et la baisse du coût des équipements électroniques a encouragé les chercheurs à introduire les VANETs pour qu'ils soient le noyau du STI (Système de Transport Intelligent). En effet, les réseaux VANET représentent une application des réseaux ad hoc mobiles, dans lesquels les véhicules, qui sont équipés de capteurs dédiés et d'interfaces radio, échangent les informations pour notifier les conducteurs suffisamment tôt afin d'éviter le carambolage et les différentes situations dangereuses.

De plus, l'utilité des VANETs n'est pas limitée à améliorer la sécurité routière, mais à permettre aussi d'offrir de nouveaux services de confort aux occupants de véhicules, ce qui rend la conduite plus agréable.

Dans ce chapitre, nous présentons la technologie véhiculaire et ses applications prometteuses. Ensuite, nous décrivons les éventuelles attaques contre les VANETs, et enfin nous passons en revue les travaux de standardisation et les différents projets et groupes de recherche dans la communauté VANET.

1.2 Pourquoi les réseaux véhiculaires ?

Les réseaux véhiculaires ont été introduits pour résoudre deux problèmes principaux :

1.2.1 Problème de la sécurité routière

Les accidents de la route représentent la 8ème cause de décès dans le monde et la première cause de décès chez les jeunes (âgés de 15 à 29 ans). Les tendances actuelles indiquent que les accidents de la route passeront au cinquième rang des causes des décès à l'horizon 2030 [1].

Le tableau suivant montre l'estimation de l'évolution de décès de route par région :

Estimation de l'évolution des décès de la route par région (1)						
Région	Nombre de pays	Décès (par millier)		Changement (%) 2000–2020	Décès/million d'habitants	
		2000	2020		2000	2020
Afrique subsaharienne	46	80	144	+80%	123	149
Amérique latine et Caraïbes	31	122	380	+48%	261	310
Asie de l'Est et Pacifique	15	188	337	+79%	109	168
Asie du Sud	7	135	330	+144%	102	189
Europe de l'Est et Asie centrale	9	32	38	+19%	190	212
Moyen-Orient et Afrique du Nord	13	56	94	+68%	192	223
Total partiel	**121**	**613**	**1124**	**+83%**	**133**	**190**
Pays à revenu élevé	35	110	80	-27%	118	78
TOTAL	**156**	**723**	**1204**	**+67%**	**130**	**174**

Tableau 1 : Estimation de l'évolution des décès de la route par région [2]

1.2.2 Problème économique

La congestion de la route engendre des coûts importants sur le plan économique. Les prix des produits et des services sont directement liés à la durée de transport nécessaire et à la quantité des carburants consommés. Une gestion intelligente du trafic routier va certainement permettre la réduction des dépenses annuelles.

La congestion réduit la qualité de vie des individus et engendre des coûts environnementaux importants. Les embouteillages entraînent un gaspillage d'énergie et une production de gaz à effet de serre et d'autres polluants qui sont néfastes pour l'environnement.

1.3 Qu'est ce qu'un réseau VANET

Un réseau VANET constitue une nouvelle forme de réseaux MANET « pour *Mobile Ad-hoc NETworks* ». Il permet aux véhicules de communiquer entre eux (cf. Figure 1.1), ou avec des infrastructures installées aux bords de routes appelées RSU (Road Side Units). Par rapport à un MANET, un réseau VANET est caractérisé par une forte mobilité de nœuds rendant le système difficile à concevoir.

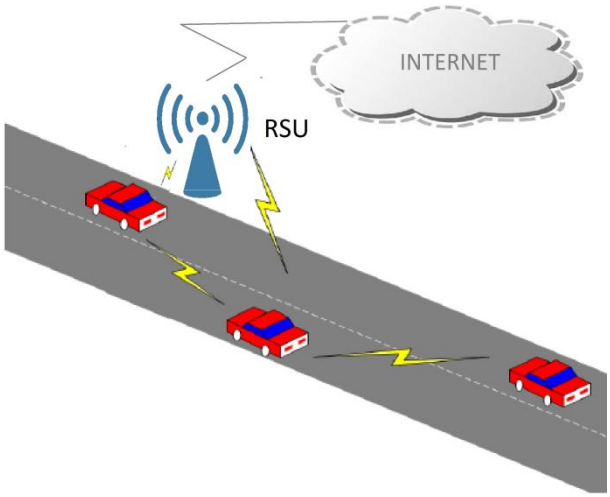


Figure 1.1: Exemple d'un réseau VANET

La mise en œuvre d'un réseau VANET nécessite des équipements électroniques (Des exemples de ces équipements électroniques sont illustrés dans la Figure 1.2) spécifiques tels les radars, les caméras, le système de positionnements GPS, une plateforme de communication, … etc.

Figure 1.2 : Equipements électroniques d'un véhicule intelligent [3]

1.4 Les applications des réseaux VANET

Les applications des réseaux VANET, aux fins d'illustration, peuvent être divisées en trois catégories [4]:

1.4.1 Les applications liées à la sécurité routière

Ces applications peuvent jouer un rôle important pour éviter les accidents ou au moins minimiser l'impact des accidents inévitables. Les VANETs ont comme objectif principal de fournir un système d'avertissement anticipé intelligent afin de prévenir les conducteurs des situations dangereuses et d'ajuster automatiquement, au besoin, le régulateur de vitesse ou les freins pour éviter ou minimiser les dommages lors d'un accident.

Selon des études effectuées par une commission européenne, l'avertissement d'un conducteur avant l'impact une demi-seconde plus tôt, pourrait réduire le nombre de collisions par l'arrière de 60 % [2].

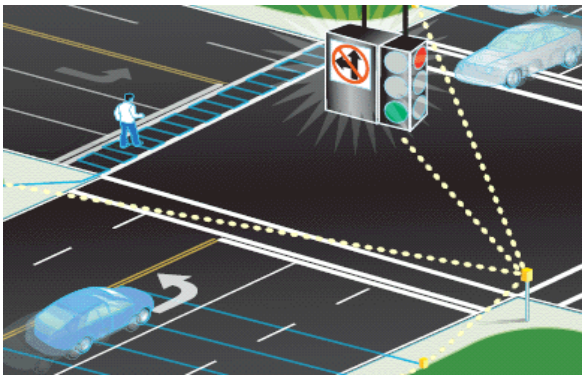
Une autre étude effectuée par l'agence fédérale de la sécurité routière américaine (appelée le NHTSA « abréviation de *National Highway Traffic Safety Administration* »), montre que 40 % des accidents surviennent aux intersections avec des impacts de côté des piétons la plupart du temps[5]. Le nombre de ces accidents peut être réduit de manière efficace par l'utilisation d'un système d'avertissement anticipé, en se basant sur des capteurs et les différents équipements embarqués dans les véhicules.

1.4.2 Les applications liées à la gestion de trafic

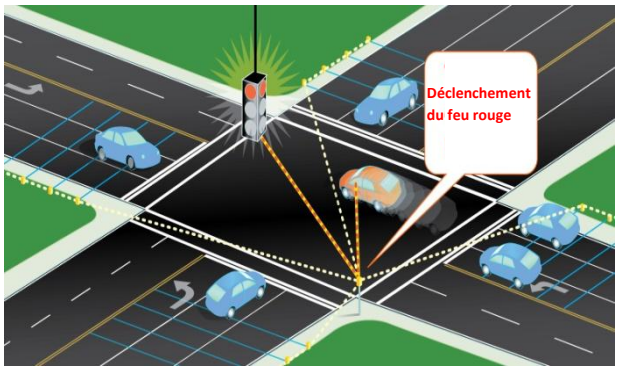
Une des applications importantes pour les VANETs est de lutter contre les congestions routières et de fournir aux conducteurs des chemins avec de bonnes conditions. De plus, avec un système de contrôle de variation de vitesses, les véhicules peuvent aussi améliorer la sécurité routière et réduire la consommation de carburants[6].

Il y a aussi une autre possibilité pour diminuer la congestion et améliorer la sécurité routière. En effet, les intersections sont souvent une cause de congestion, et l'amélioration de leur fonctionnement à l'aide des feux de circulation adaptés (cf. Figure 1.3) [7].

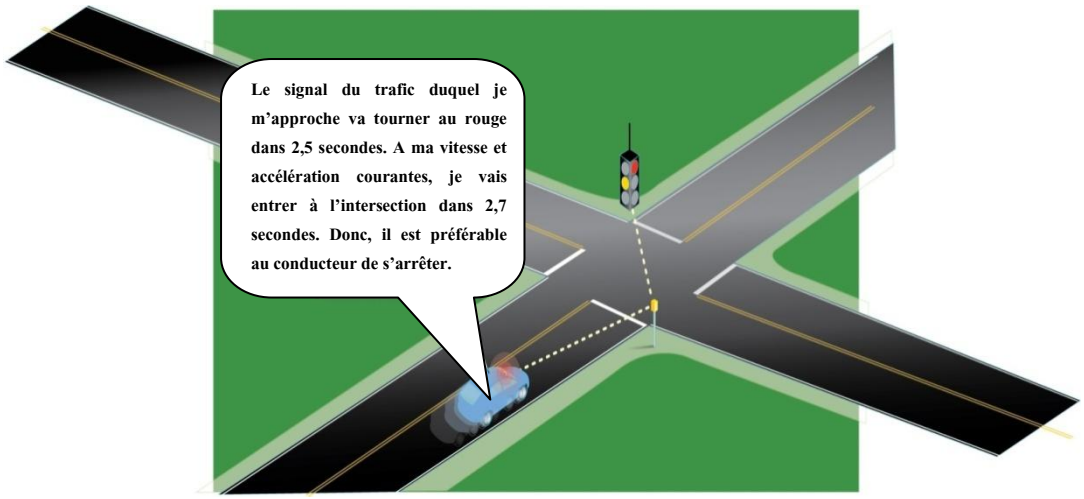
Il existe une autre application intéressante qui permet aux voitures d'éviter la recherche d'un espace de parking libre et de payer automatiquement les frais nécessaires[8][9].



a) Détection des piétons dans les intersections



b) Détection de violation du code de la route



c) Assistance de conducteurs

Figure 1.3 : Gestion des intersections dans les VANETs[10]

1.4.3 Les applications de confort

Les réseaux VANET offrent aussi des applications qui permettent d'assurer le confort des occupants de véhicules durant leurs voyages; ces applications comprennent : la messagerie instantanée, le partage de fichiers, les jeux en réseau, le streaming, l'accès à Internet, … etc (cf. Figure 1.4).

Le champ d'application des réseaux véhiculaires est large et permet aux opérateurs de télécommunications de réaliser des bénéfices supplémentaires.

Figure 1.4 : Un exemple d'application de confort dans les VANETs[3]

1.5 Les modes de communication dans les réseaux VANET

Dans les réseaux de véhicules, plusieurs modes de communication peuvent être distingués, nous citons: les communications Véhicule-à-Véhicule (V2V), les communications Véhicule-à-Infrastructure (V2I) et les communications véhicule-à-piétons (V2P) (cf. Figure 1.6). Les véhicules peuvent utiliser un de ces modes ou bien les combiner s'ils ne peuvent pas communiquer directement avec les infrastructures. Dans cette section, nous donnons le principe et l'utilité de chaque mode :

A. **Mode de communication Véhicule-à-Véhicule (V2V)**

Ce mode de communication est caractérisé par une architecture décentralisée, et représente un cas particulier des réseaux ad hoc mobiles. Les communications avec ce mode sont effectuées par les véhicules et ne nécessitent aucune infrastructure. En effet, une communication directe est possible entre deux véhicules, suivant ce mode, si un véhicule se situe dans la zone radio de l'autre, ou bien par le biais d'un protocole multi-sauts qui se charge d'acheminer les messages de bout en bout en utilisant les véhicules intermédiaires qui les séparent comme relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission.

B. Mode de communication de Véhicule à Infrastructure (V2I)

Ce mode de communication permet aux utilisateurs de multiplier les services fournis par exemple : il permet d'avoir un accès à Internet, d'échanger des données de voiture-à-domicile ou de voiture-à-garage de réparation pour le télé-diagnostic, ...etc.). Les infrastructures nécessaires pour ce mode de communication sont appelés RSUs(Road Side Units). La figure suivante illustre un spécimen d'un RSU (le ZXRIS 8900) fabriqué par l'entreprise chinoise ZTE. Ce RSU conçu suivant le standard DSRC (Dedicated Short-Range Communications).

Figure 1.5 : Un spécimen d'un RSU[11]

Un exemple de ce mode de communication est illustré dans la Figure 1.6 grâce à des points d'accès RSU (*Road Side Units*) déployés aux abords des routes.

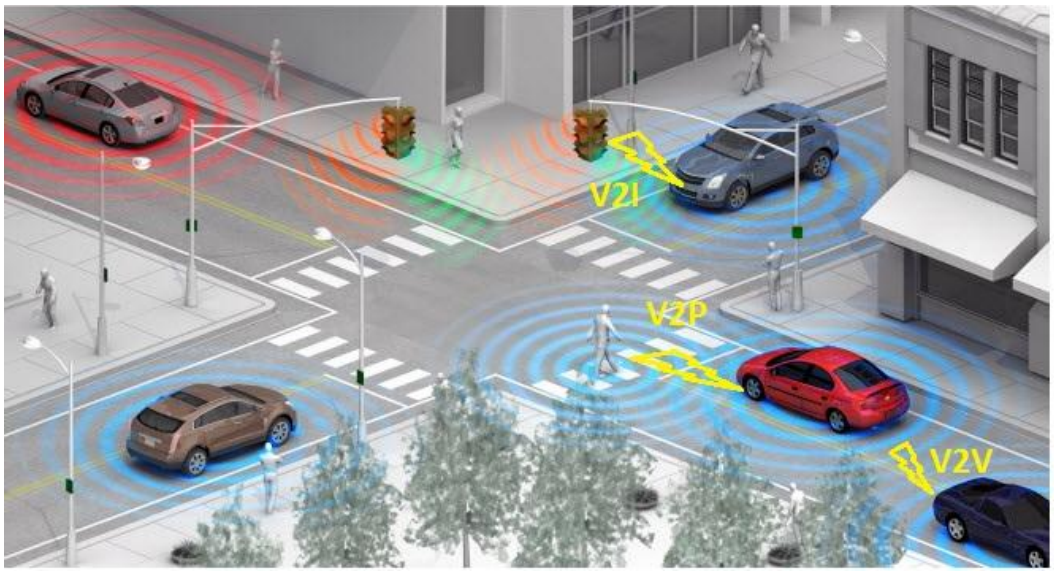


Figure 1.6 : Les modes de communication dans les réseaux VANET[12]

C. Mode de communication de Véhicule à piéton (V2P)

Ce mode de communication a été introduit pour permettre l'échange des messages de sécurité entre les véhicules et les piétons qui utilisent des téléphones ou n'importe quel appareil sans fil, intelligent. Ces messages peuvent comporter par exemple des informations sur les piétons qui s'approchent de la route. Les véhicules peuvent aussi émettre des messages d'avertissement vers les appareils intelligents des piétons qui déclenchent des alertes sonores ou via des vibrations.

General Motors a réalisé un projet dans ce domaine en 2010 pour réduire le nombre d'accidents avec les piétons et les cyclistes. VOLVO y a aussi investi, et a déjà dévoilé son nouveau concept d'un système des airbags automatiques pour protéger les piétons[13].

La figure suivante montre une démonstration de l'implémentation de HONDA pour les communications V2P.

Figure 1.7 : Démonstration de HONDA pour V2P[14]

1.6 Le beaconing

Le beaconing (cf. Figure 1.8) qui est une opération effectuée par chaque véhicule consiste à diffuser des messages périodiques (appelés « Beacons ») aux autres nœuds dans sa zone radio. L'objectif de beaconing est de permettre à chaque véhicule d'informer les autres de son contexte tel l'identité, la position géographique, la vitesse et la direction. Les beacons peuvent comporter d'autres informations nécessaires pour les communications et les différents services dans les VANETs.

Il est à noter que les beacons dans les VANETs sont des messages à un saut, donc ils ne doivent pas être relayés.

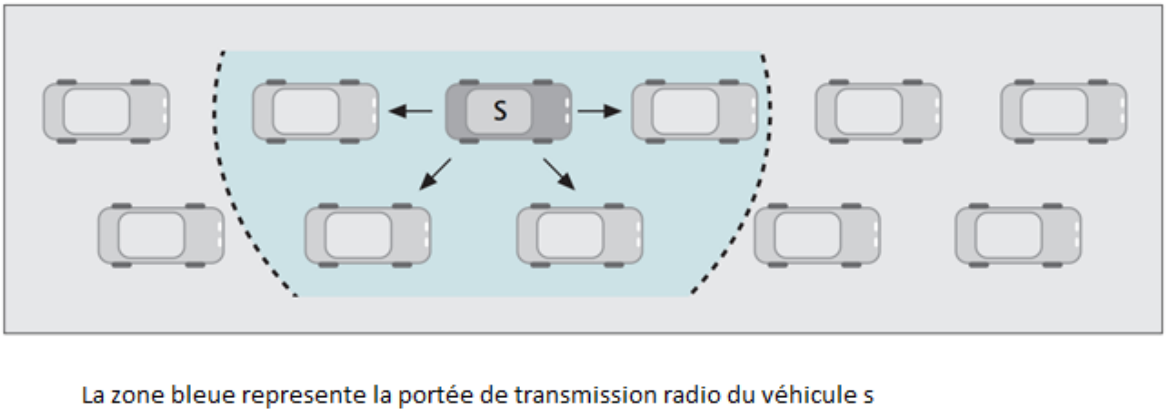


Figure 1.8 : Le beaconing dans les VANETs

1.7 Les caractéristiques des réseaux VANET

Les réseaux véhiculaires ont leurs propres caractéristiques qui les distinguent des réseaux MANET. Ces caractéristiques doivent être considérées lors de la conception des architectures et des protocoles pour les réseaux VANET.

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

- **La capacité d'énergie et de stockage**: dans les réseaux VANET, les véhicules disposent suffisamment d'énergie pour alimenter les différents équipements électroniques nécessaires à la constitution d'un réseau VANET. Vue la grande capacité de traitement et de stockage de données, des complexes opérations arithmétiques et cryptographiques peuvent être mises en œuvre pour assurer la sécurité et le bon fonctionnement de ces réseaux[15].
- **La topologie et la connectivité**: les réseaux VANET sont caractérisés par une topologie très dynamique et un temps d'interaction entre les véhicules très court. De plus, la topologie est souvent constituée de plusieurs ilots séparés[15], ce qui complique la conception des systèmes efficaces pour les VANETs.
- **Le modèle de mobilité**: dans les réseaux VANET, la mobilité des nœuds est affectée par plusieurs facteurs : type de route, panneaux de signalisation, ainsi que le comportement des conducteurs et leurs réactions face aux différentes situations rencontrées tels : les embouteillages de la route, les accidents,… etc. [16].
- **Les contraintes temps réel** : les applications liées à la sécurité routière nécessitent la transmission de données dans des délais très courts. Ce qui limite le choix d'outils et de techniques à utiliser pendant la conception d'un protocole ou une d'architecture pour les VANETs[17].
- **Une taille illimitée du réseau** : les VANETs peuvent être mis en œuvre au niveau d'une ville, un pays ou voire même plusieurs pays. Ce qui signifie que les VANETs ne sont pas limités géographiquement[17].
- **Echange des messages fréquents**: dans les réseaux VANET, les véhicules doivent émettre périodiquement des messages beacons, ce qui nécessite un échange fréquent de données entre les différents véhicules[17].

1.8 Les défis dans les réseaux VANET

Les défis dans les réseaux VANET peuvent être classés en deux catégories[17]:

a) Les défis techniques

- **La gestion du réseau** : à cause de la forte mobilité des nœuds, le changement rapide de la topologie et les conditions du canal (canal sans-fil partagé), il est difficile de concevoir un protocole de communication efficace.
- **Le contrôle de la congestion et des collisions** : dans les zones rurales et pendant la nuit, le trafic routier est faible, ce qui mène à partitionner le réseau. Cependant durant les heures

de pointe dans les zones urbaines, le réseau est congestionné et les collisions de paquets sont fréquentes.

- **L'impact environnemental**: les VANETs utilisent des ondes électromagnétiques pour les communications. Ces ondes sont affectées par l'environnement (par exemple à cause de réflexion des signaux). Donc, l'impact environnemental doit être considéré avant le déploiement des VANETs.
- **La sécurité et l'anonymat:** l'importance des informations échangées via les communications véhiculaires rend l'opération de sécurisation de ces réseaux cruciale qui constitue un pré-requis au déploiement des VANETs.

b) Les défis sociaux économiques

Outre les défis techniques que nous avons déjà mentionnés, les défis socio-économiques doivent aussi être envisagés. Il est difficile de convaincre le fabricant de construire un système qui ne préserve pas la vie privée des utilisateurs (leurs identités et leurs activités quotidiennes), car ce dernier va rejeter ce type de surveillance.

1.9 La sécurité dans les réseaux VANET

La sécurité dans les VANETs est obligatoire avant leur déploiement. En effet, l'adversaire peut attaquer le système pour bénéficier de plus de services du système, rediriger le trafic routier, et voire même causer un accident. Plusieurs recherches ont été effectuées dans ce domaine. Dans cette section, nous présentons les objectifs de la sécurité dans les VANETs, puis nous donnons les types d'attaquants, ensuite nous décrivons les différentes catégories d'attaques contre les VANETs, enfin nous présentons le matériel utilisé pour protéger les données.

1.9.1 Les objectifs de la sécurité dans les réseaux VANET

La sécurisation des communications dans les réseaux VANET nécessite la mise en œuvre de technique permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent[18] :

- **L'authentification** : cet objectif assure que les messages sont générés par des entités légitimes, et les récepteurs peuvent identifier leurs origines.
- **La disponibilité** : elle permet d'avoir une qualité de service adéquate d'accès aux ressources du réseau véhiculaire.
- **La confidentialité** : elle s'agit d'un ensemble de règles à appliquer pour garantir que seules les personnes autorisées peuvent accéder aux ressources. Cet objectif peut être achevé en utilisant le cryptage de données et l'échange de messages spécifiques entre les véhicules et les RSUs.

- **La non-répudiation**: elle assure que les émetteurs ne peuvent pas nier d'être à l'origine d'un message qu'ils génèrent.
- **L'intégrité**: cet objectif de sécurité permet de s'assurer que les informations échangées ne sont pas soumises à une modification volontaire ou accidentelle.
- **La vie privée et l'anonymat** : cet objectif permet de cacher l'identité et la position géographique des nœuds, et d'autres informations qui mettent en péril la vie privée des utilisateurs.
- **La révocabilité** : cet objectif permet d'avoir les mécanismes nécessaires pour exclure les nœuds malveillants et de révéler leurs vraies identités.
- **Le contrôle d'accès** : il permet de s'assurer que les nœuds accèdent aux ressources suivant des règles et de privilège bien déterminés.

1.9.2 Les types d'attaquants

Les attaquants peuvent être classées suivant les dimensions suivantes [19]:

- **Interne/Externe :** l'attaquant interne possède les clés cryptographiques qui lui permettent de communiquer avec d'autres nœuds dans le réseau. Les techniques cryptographiques seules ne sont pas suffisantes pour se défendre contre ce type d'attaquant. Ce dernier est capable de dégrader considérablement la performance du réseau. Par contre, l'attaquant externe est perçu par les membres du réseau comme un intrus, il est donc limité dans la diversité des attaques qu'il peut provoquer.
- **Malveillant/Rationnel:** un attaquant malveillant emploie tous les moyens pour le dysfonctionnement du réseau quels que soient les coûts et les conséquences correspondants. Par contre, un attaquant rationnel cherche un profit personnel, et par conséquent, les cibles d'attaques et les moyens employés peuvent être prévus.
- **Passif /Actif :** l'attaquant passif écoute simplement les données échangées dans le réseau, tandis que l'attaquant actif peut agir sur les données échangées.

1.9.3 Les attaques contre les VANETs

Les attaques contre les VANETs peuvent être classées comme suit [20]:

1. **Attaques contre la disponibilité :** les attaques suivantes contre la disponibilité de communication véhiculaire ont été identifiées:
    - **Déni de service**: les attaques DoS (*Denial of Service*) peuvent être effectuées par des participants malveillants du réseau ou des entités étrangères pour rendre un service indisponible aux utilisateurs de réseau par les inondations inutiles de messages et de brouillage du canal (cf. Figure 1.9). Cette attaque est dangereuse car elle profite de l'aspect distribué et coopératif du système VANET pour causer son disfonctionnement[21].

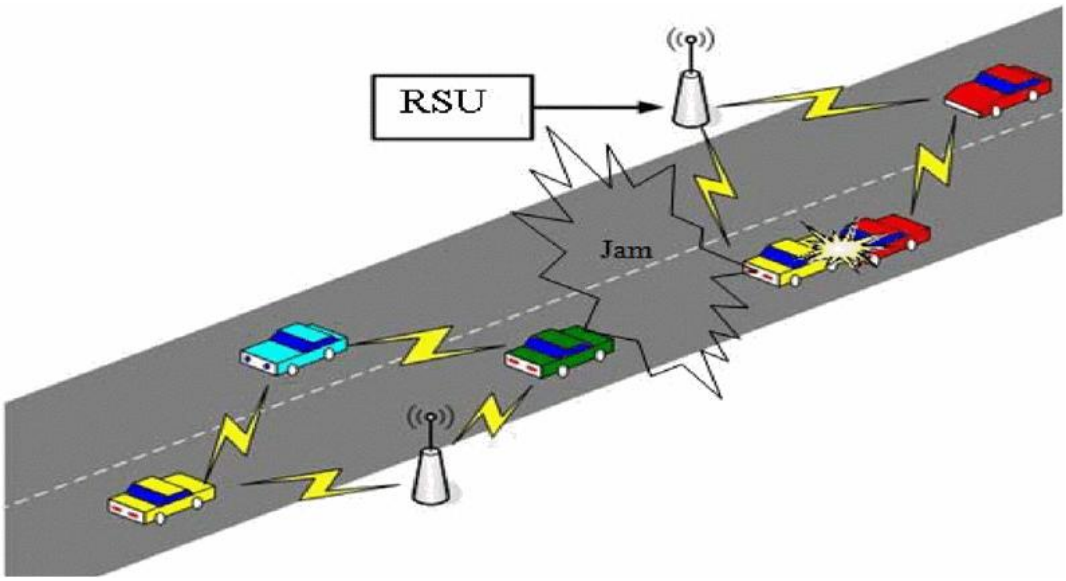


Figure 1.9 : Attaque DoS [22]

- **Falsification de données diffusées**: dans cette attaque, l'adversaire compose un message contenant des informations erronées sur l'état de la route, un message de freinage d'urgence ou un autre sur les conditions du trafic routier par exemple. Ces informations falsifiées affectent la disponibilité de données correctes pour l'assistance du conducteur[18].
- **Malware**: l'introduction de logiciels malveillants, tels que des virus ou des vers dans les VANETs, peut causer des perturbations au bon fonctionnement des réseaux. Les attaques par des logiciels malveillants sont plus susceptibles d'être effectuées par des attaquants internes plutôt que des externes. Les Malwares peuvent être injectés dans les OBUs[1] (On Board Unit), lorsque ces derniers reçoivent les mises à jour logicielles. Dans ces attaques, il se peut que l'entité malveillante vise à dégrader l'efficacité du réseau[18].
- **L'attaque trou noir (*Blackhole*)**: dans les réseaux VANET, un blackhole est formé lorsque le trafic est redirigé vers un ou plusieurs nœuds qui ne relient pas ces paquets à leurs destinations (cf. Figure 1.10). Cette attaque est très dangereuse car l'attaquant aura un contrôle important sur le réseau[23].

[1] On Board Unit (OBU) : c'est l'équipement nécessaire pour enregistrer et traiter les différentes données nécessaires pour les communications dans les VANETs.

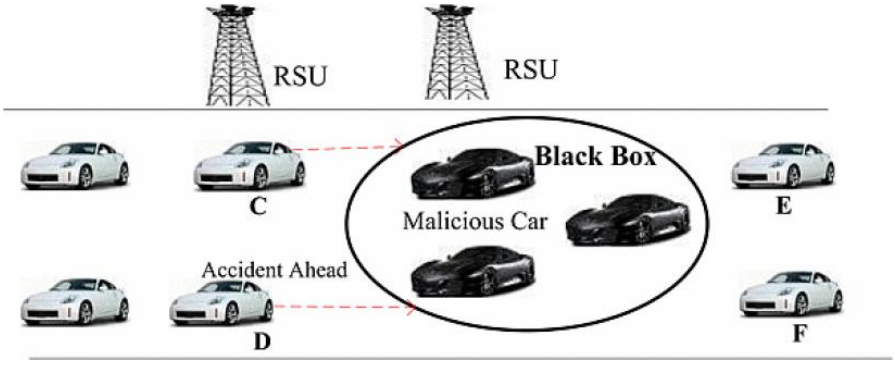


Figure 1.10 : Attaque Blackhole [23]

2. **Attaques liées à l'authentification** : assurer l'authentification dans un réseau véhiculaire consiste à protéger les nœuds légitimes contre les entités étrangères du réseau. L'authentification avec d'autres mécanismes appropriés permet d'éviter la communication avec des nœuds ayant une fausse identité, la réémission illégitime du message et l'injection des informations erronées. Celles-ci comprennent:

   - **Attaque d'usurpation de l'identité d'un nœud** (en anglais, *Spoofing* ou *Impersonation*) : dans cette attaque, l'adversaire prend l'identité d'un autre nœud afin d'exercer des activités malveillantes. Par exemple : pour faire vite, l'attaquant prend l'identité d'une ambulance afin que les autres véhicules, automatiquement, lui libèrent la route. L'attaquant peut montrer qu'il a un comportement malveillant sous les identités des autres nœuds afin de dégrader leurs degrés de confiance, et par conséquent, dégrader la performance du réseau[24].
   - **Attaque *Replaying***: dans cette attaque, l'attaquant réinjecte des messages déjà émis par d'autres nœuds pour causer, par exemple, l'empoisonnement des tables de routage et de voisins.
   - **Attaque GPS Spoofing**: cette attaque consiste à utiliser un générateur de signaux GPS qui émet des signaux plus forts que ceux émis par les satellites, afin de forcer les nœuds victimes à injecter des données géographiques falsifiées[23]. Un exemple de cette attaque est celle contre le *White Rose of Drachs* qui est un super-yacht de 80 millions de dollars. Cette attaque a été effectuée par Todd Humphreys, professeur de l'université de Texas, en juin 2013. Les attaquants ont contrôlé ses mouvements à distance(cf. Figure 1.11)[25].

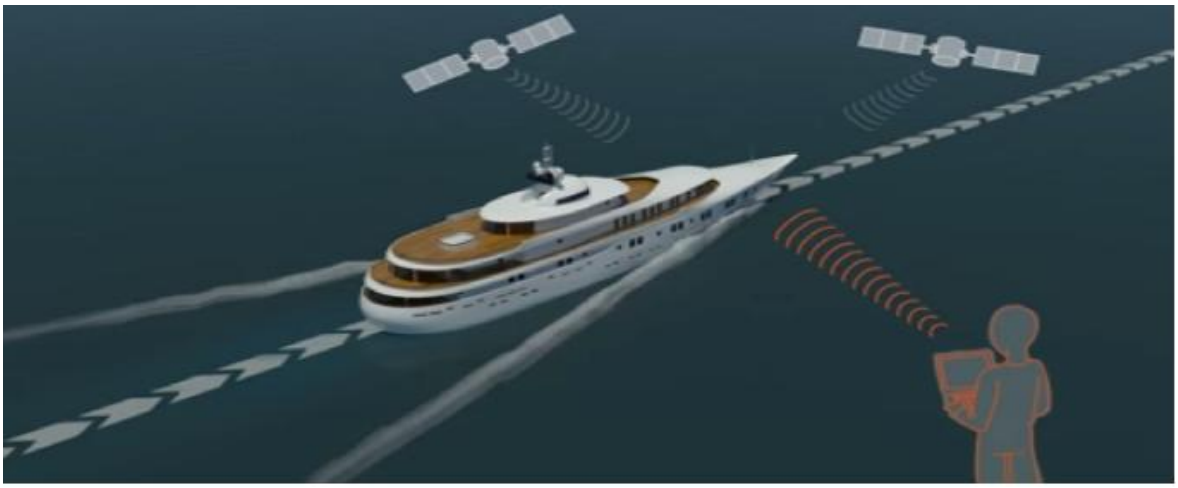


Figure 1.11 : L'attaque contre le « White Rose of Drachs »[26]

- **Attaque Tunneling**: un attaquant peut exploiter la perte momentanée par un véhicule de l'information de positionnement géographique lorsque ce dernier entre dans un tunnel pour lui injecter de fausses données géographiques.
- **Attaque Sybil** : c'est une variante très dangereuse de l'attaque « *Spoofing* », où l'attaquant est physiquement un seul nœud, mais il utilise l'identité de plusieurs autres nœuds à la fois pour pouvoir contrôler le système et facilement monter d'autres attaques. Dans l'attaque Sybil un nœud peut prétendre être sur plusieurs positions stratégiques à la fois[27].
- **Attaque sur l'intégrité d'un message :** un nœud intermédiaire dans une communication véhiculaire peut modifier le contenu d'un message légitime pour tromper son récepteur[22].
- **Attaque de réplication de certificats et de clés cryptographiques :** elle consiste à accéder au contenu d'OBU pour récupérer les données cryptographiques. Cette attaque met le système VANET en péril, car l'entité malveillante peut générer des signatures numériques autant qu'elle veut sans qu'il y ait la possibilité de l'identifier[20].

3. **L'attaque contre la confidentialité :** cette attaque permet à un nœud, de manière illégitime, d'établir un profil sur les communications effectuées par les autres nœuds. Ce type d'attaque menace la vie privée des utilisateurs des réseaux VANET, du fait que l'adversaire est capable d'analyser les paquets (la destination, le timestamp, les informations géographiques nécessaires pour le routage, ..etc.) pour avoir une idée sur les activités des autres nœuds[20].

1.9.4 Le TPD (Tamper Proof Device)

Le TPD est un équipement hardware capable d'effectuer des opérations cryptographiques, de protéger et de sauvegarder les données secrètes, comme les clés cryptographiques, les journaux d'événements. Ce module est équipé par des mécanismes qui empêchent la manipulation non autorisée de données. En effet, des programmes de sécurité spécifiques ont été implémentés : ils suppriment les données sensibles s'ils détectent des manipulations physiques non autorisées à l'aide des capteurs spécifiques appelés « *Tamper sensing membrane* ».

Ce module est connu aussi sous d'autres noms : « *Tamper resistant devices* »[28]. Un exemple de cet équipement est l'IBM 4758 (cf. Figure 1.12).

Figure 1.12 : Un exemple de TPD[28]

1.10 Les problèmes législatifs

Un réseau VANET concerne une large communauté de consommateurs, des partenaires industriels, des fabricants de matériel, les assurances et les gestionnaires de trafic routier (par exemple : le département de transport, la police, .. etc.). Ces derniers doivent collaborer pour réviser les lois existantes et en créer d'autres.

La loi doit protéger la vie privée des utilisateurs des VANETs, elle doit ainsi garantir la possibilité de poursuivre judiciairement les personnes responsables des attaques contre les VANETs.

1.11 Les travaux de standardisation dans les VANETs

Plusieurs standards de communication ont été développés dans le cadre de communication véhiculaire. Dans cette section, nous présentons les travaux de standardisation les plus connus.

1.11.1 DSRC

L'ASTM « *American Society for Testing and Materials* » a adopté en 2002 une norme appelée DSRC (*Dedicated Short Range Communication*) pour normaliser l'accès sans fil dans l'environnement véhiculaire.

Selon le DSRC, les transmissions sur le canal radio sont effectuées dans la bande situé entre 5.850 GHz à 5.925 GHz allouée par l'US FCC « *United States Federal Communications Commission* »; les communications qui suivent ce standard sont caractérisées par une faible latence [7].

Selon le DSRC, la bande passante est divisée en sept canaux radio (cf. Figure 1.13) de 10 MHz chacun. Ces canaux se répartissent fonctionnellement en un canal de contrôle et six canaux de service (quatre de ces canaux pouvant être regroupés en deux-à-deux afin d'avoir un plus grand débit), chacun pouvant offrir des débits allant de 6 à 27 Mbps (pour des distances allant jusqu'à 1000 mètres). Le canal de contrôle est utilisé pour la transmission des messages de gestion du réseau et des messages de très haute priorité à l'instar de certains messages critiques liés à la sécurité routière. Les six autres canaux sont, quant à eux, dédiés à la transmission des données de différents services annoncés sur le canal de contrôle [8].

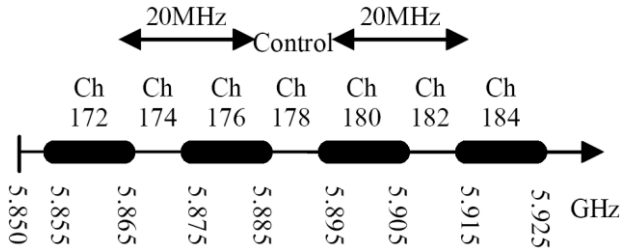


Figure 1.13 : La bande radio de DSRC en Amérique du nord [9]

1.11.2 WAVE

Plusieurs protocoles et standards dédiés aux communications véhiculaires ont été regroupés afin de définir le nouveau standard WAVE *(Wireless Access for the Vehicular Environment).* La partie basse de la pile protocolaire de WAVE comprend le standard IEEE 802.11p qui a défini les couches Physique et MAC, tandis que la partie se situant entre la couche liaison et la couche application comprend plusieurs standards qui ont été définis par le groupe de travail IEEE 1609[29].

La famille des standards IEEE 1609 pour WAVE, se décompose en quatre standards (cf. figure 1.14):

- IEEE 1609.1 - *WAVE Resource Manager(WRM)*: il décrit les principaux éléments (comme le format de données et les types de dispositifs supportés) de l'architecture WAVE et gère les flux de données entre ses composants.
- IEEE 1609.2 – *WAVE Security Services for Applications and Management Messages*: il décrit le format de message et les traitements nécessaires pour la sécurisation des messages échangés.
- IEEE 1609.3 – *WAVE Networking Services*: il standardise les services réseau et transport pour les communications véhiculaires, et définit les services de routage pour les communications inter-véhiculaires. Le 1609.3 inclut le protocole WSMP (*Wave Short Messages Protocol*) qui est réservé à la transmission des messages qui doivent passer par le canal de contrôle.
- IEEE 1609.4 -*WAVE Multi-Channel Operation*: il apporte des améliorations à la couche MAC, notamment, la gestion d'accès aux sept canaux DSRC.

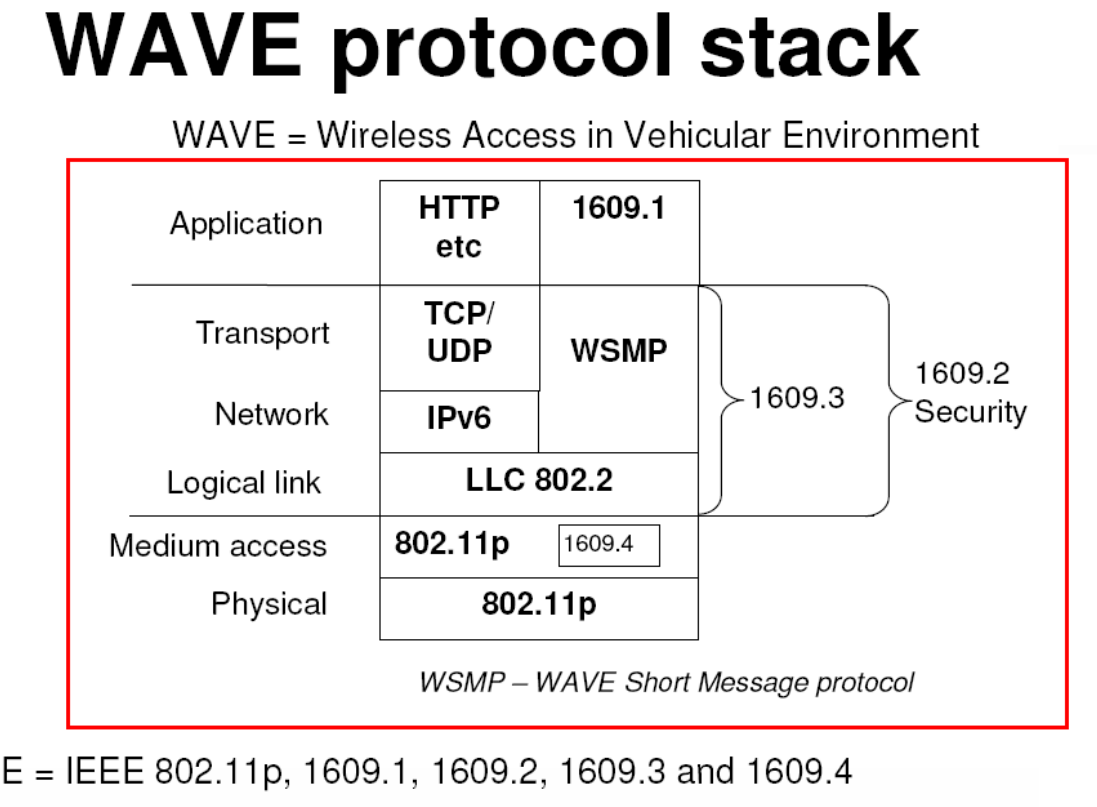


Figure 1.14 : Vue d'ensemble sur la pile protocolaire WAVE proposée par l'IEEE [15]

1.11.3 ETSI

Au niveau Européen, l'ETSI (European Telecommunications Standards Institute) a créé un comité technique TC ITS pour établir des standards et spécifications pour les ITS. Cette comité est organisée en cinq groupes de travail : WG1 - User and Application requirements, WG2 - Architecture and cross layer issues, WG3 - Transport and Network, WG4 - Media and related issues, et le WG5 - Security.

De manière similaire au modèle OSI(Open Systems Interconnection), l'ETSI a défini son architecture en couches (cf. Figure 1.15).

La couche *Access* définit les interfaces avec les technologies de communication disponibles telles que ITS-G5, Wi-Fi, 3G et DSRC. ITS-G5 est l'équivalent de l'IEEE 802.11p et permet une communication directe (V2V et V2I) et à faible latence.

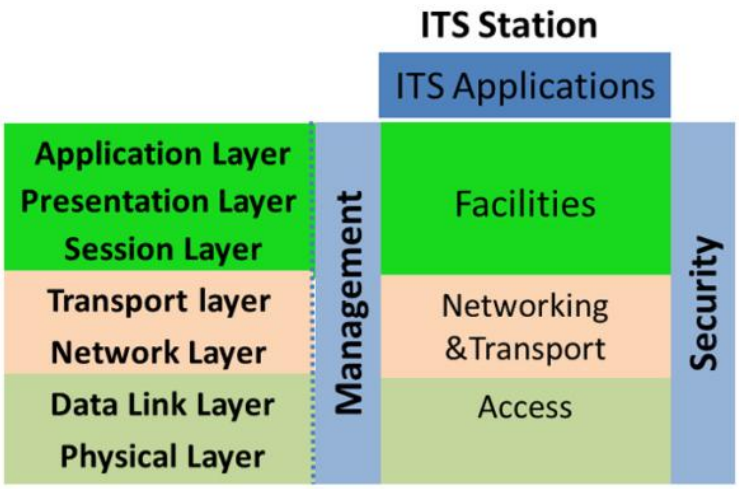


Figure 1.15 : Architecture ETSI [18]

1.12 Conclusion

Les réseaux VANET sont des réseaux prometteurs qui ont un large éventail d'applications, que ce soientt celles qui visent à améliorer la sécurité routière ou celles qui augmentent le confort des utilisateurs des VANETs durant le voyage. Le nombre de projets de recherche et les efforts énormes déployés par les équipes de standardisation à ce stade montrent l'importance de ces réseaux et leur permet de voir la lumière. Néanmoins, plusieurs défis techniques et économiques font face au déploiement des VANET. La sécurité est le souci principal qui préoccupe les concepteurs vue l'importance des données échangées. Dans le chapitre suivant, nous présenterons l'authentification de données dans les VANETs qui est un mécanisme fondamental pour sécuriser les VANETs.

Chapitre 2

L'authentification dans les réseaux VANET

2.1 Introduction

Les messages liés à la sécurité dans les réseaux VANET nécessitent l'authentification de leurs origines afin de filtrer ceux qui contiennent des données falsifiées. Cette opération exige la mise en œuvre des solutions logicielles et matérielles spécifiques. Les projets de standardisation ont défini l'architecture générale d'authentification, la structure de certificat et les algorithmes cryptographiques, mais un besoin s'avère nécessaire pour optimiser leurs solutions afin d'encourager le gouvernement à déployer des VANETs avec de faibles coûts.

Dans ce chapitre, nous décrivons l'architecture et l'organisation de base pour l'authentification des véhicules, puis nous présentons la problématique d'authentification dans les VANETs, suivie par les solutions de base qui ont été mises en œuvre pour résoudre ce problème.

2.2 Les éléments de base de la sécurité dans les VANETs

Dans cette section, nous présentons les éléments de base de la sécurité dans les VANETs. Nous présentons le PKI, ensuite nous présentons l'algorithme ECDSA et la spécification des éléments cryptographiques.

a) PKI (Public Key infrastructure)

Le PKI est une infrastructure qui comporte les composants de base suivants(cf. Figure 2.1) [18] :

- L'autorité de certification root : dans les réseaux VANET, on doit avoir au minimum une autorité de certification root principale, d'autres autorités peuvent exister pour distribuer la charge et pour ajouter une couche de sécurité supplémentaire contre les attaques [18].
- Subordinate authority (*Registration Authority*) : il est certifié par l'autorité root, il permet d'authentifier l'identité des véhicules.
- La base de données de certificats : elle contient les demandes de certificats, les certificats à délivrer et la liste de révocation de certificats.
- L'entrepôt de certificats : il existe au niveau des OBUs des véhicules, un entrepôt de certificats à clés publiques et leurs clés privées correspondantes.

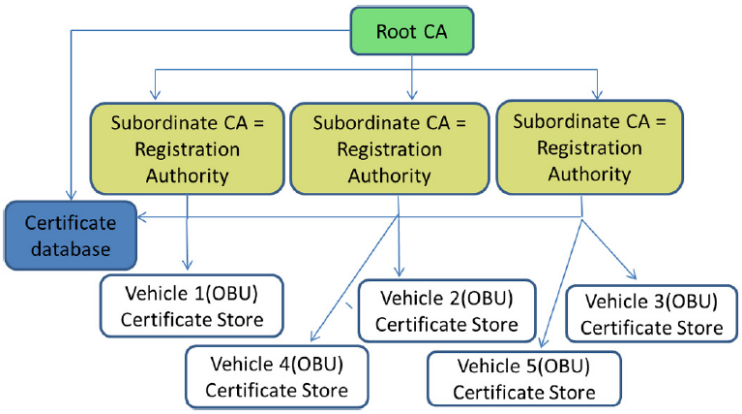


Figure 2.1 : Architecture d'un PKI dans les VANETs [18]

b) L'algorithme ECDSA et la spécification des éléments cryptographiques

L'algorithme de cryptage spécifié par le standard IEEE Standard 1609.2[30] est le cryptage à base de courbes elliptiques. En effet, une signature numérique générée avec cet algorithme (elle est appelée ECDSA « *Elliptic curve digital signature algorithm* »)[31]. Cette dernière nécessite une clé de 224 bits pour les OBUs et 256 bits pour les RSUs et les certificats.

Les tailles des éléments cryptographiques sont illustrées (en octets) dans le tableau 2. Nous pouvons remarquer que les tailles des éléments cryptographiques de l'AC (*Autorité de Certification*) ou de RSU (qui ont des ressources de traitement et de stockage plus puissantes) sont plus grandes par rapport à celles de l'OBU.

Type	**AC ou RSU** **ECDSA-256**	**OBU** **ECDSA-224**
Clé publique	33	29
Clé privée	32	28
Signature	64	56
Certificat	135	125
Identifiant de certificat	10	8

Tableau 2 : Tailles des éléments cryptographiques en utilisant ECDSA [32]

Les certificats peuvent être gérés d'une façon hiérarchique suivant deux possibilités (cf. Figure 2.2)[19] : La première possibilité consiste à laisser le contrôle des certificats aux gouvernements. Chaque gouvernement distribue la tache de gestion sur plusieurs AC régionales, et ces dernières peuvent aussi utiliser des divisions administratives qui gèrent directement les certificats des véhicules. Une telle hiérarchie pour la gestion des certificats nécessite une longue chaine de certification pour l'authentification. Ainsi, les véhicules doivent être recertifiés au niveau des frontières avant d'accéder à un pays diffèrent.

Le deuxième choix consiste à faire confiance aux fabricants d'automobiles pour gérer les certificats, mais avec ce choix, l'authentification nécessite que chaque véhicule doit disposer de tous les certificats valides des fabricants d'automobiles dans le monde.

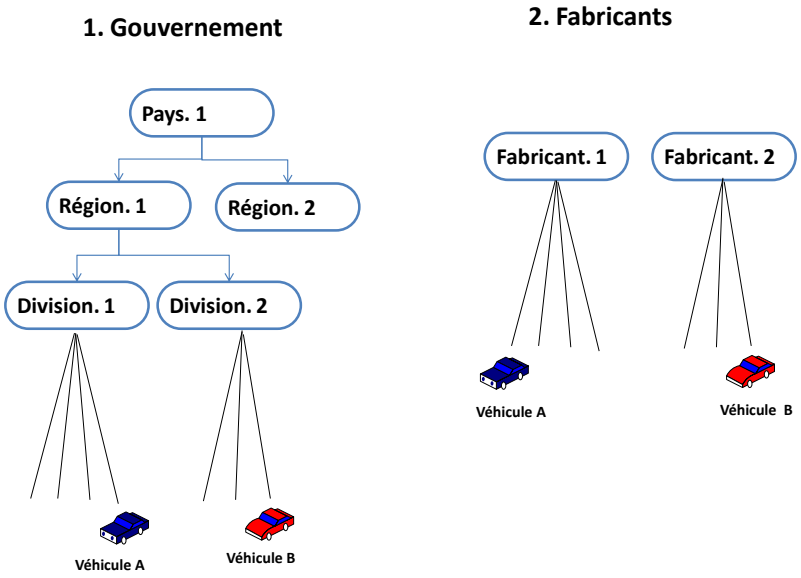


Figure 2.2 : Gestion hiérarchique des certificats

2.3 Le cycle de vie des dispositifs qui utilisent la sécurité

Afin de mieux comprendre le contexte de l'authentification des VANETs, nous devons avoir une idée sur le cycle de vie des dispositifs dans les VANETs. Ce cycle de vie est illustré dans la Figure 2.3; il comprend les étapes suivantes[30] :

a) **Fabrication** : le dispositif est physiquement créé.

b) **Acquisition**: le dispositif est acquis par un opérateur qui fournit les paramètres système communs à tous ses dispositifs.

c) **Configuration**: le dispositif est configuré pour un ensemble d'applications spécifiques.

d) **Déploiement**: le dispositif est mis en place et peut être exploité dans son environnement d'exploitation. Une configuration supplémentaire appropriée à son environnement peut y être effectuée.

e) **Exploitation**: le dispositif est en fonctionnement. Celà comprend les étapes suivantes, en série ou en parallèle:

   1) Les opérations de base: ce sont les opérations d'application.

   2) La maintenance: c'est une simple reconfiguration qui est mise à jour.

3) L'administration: elle consiste à effectuer une reconfiguration importante pour prendre en considération des contremesures ou intégrer de nouveaux protocoles.

f) **Redéploiement**: il consiste à déplacer le dispositif vers un autre emplacement.

g) **Reconfiguration**: l'appareil est configuré pour supporter les différentes applications ou utilisations.

h) **Revente**: le dispositif est transféré vers un autre opérateur. Des contremesures liées à la certification doivent être prises en compte.

i) **Déclassement**: à ce stade, le dispositif est physiquement en fin de cycle de vie.

Le processus du cycle de vie comprend deux types de paramètres de sécurité à gérer: l'un à long terme et l'autre à court terme :

- Les paramètres de sécurité à long terme: il s'agit essentiellement de certificats racines; une clé qui permet de mettre à jour la liste des certificats racine de confiance; des coordonnées nécessaires pour communiquer avec les ACs qui créent les certificats des dispositifs; création de clés cryptographiques qui permettent d'authentifier les dispositifs.
- Paramètres de sécurité à court terme: il s'agit notamment des certificats et des clés qui sont nécessaires pour les communications anonymes entre les différents nœuds dans les VANETs.

Les paramètres de sécurité avec différentes durées de vie seront naturellement installés ou mis à jour aux différents stades du cycle de vie du dispositif.

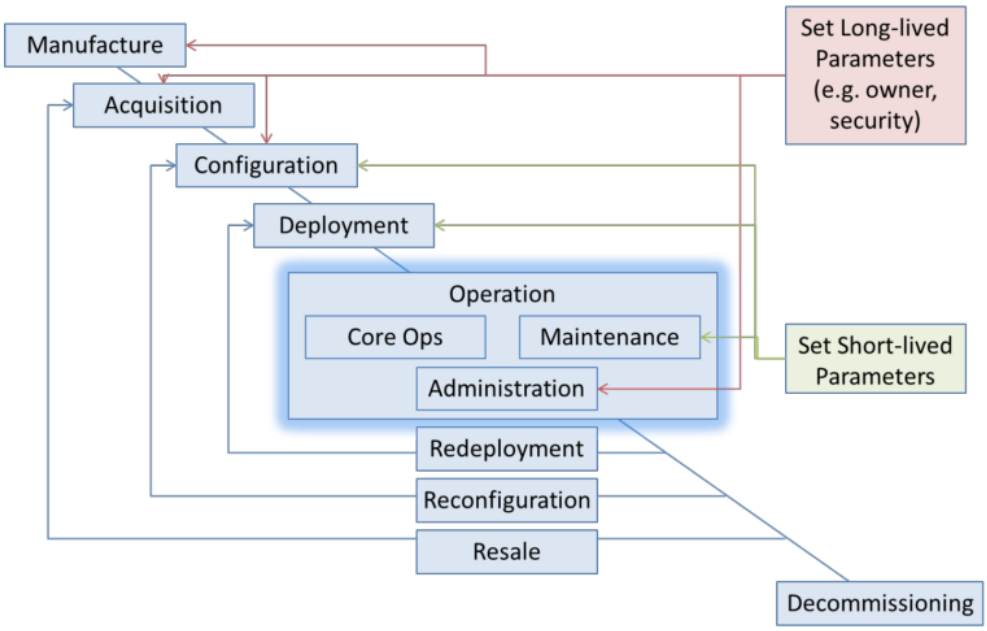


Figure 2.3 : Le cycle de vie des dispositifs qui utilisent les services de la sécurité [30]

2.4 Standardisation des messages sécurisés dans les VANETs

Dans cette section, nous présentons le format du certificat numérique, ensuite nous décrivons le format d'un message sécurisé dans les VANETs.

2.4.1 Le format du certificat numérique

Le standard ETSI duplique pratiquement les mêmes champs du certificat numérique du standard IEEE 1609.2[30] et ajoute quelques champs supplémentaires.

La Figure 2.4 montre le format du certificat numérique suivant la spécification technique 103 097 du standard ETSI[33].

- *Version* : ce champ est constitué de 8 bits de données, il représente la version du certificat.
- *Signer_info* : ce champ indique des informations concernant le signataire du certificat numérique pour pouvoir vérifier la validité de certificat.
- *Subject_info* : il indique le type du certificat et le contexte de son utilisation.
- *Subject_attributes* : c'est un champ de 8 bits indiquant des informations supplémentaire au champ précédent.
- *Subject_restriction* : il spécifie la période de validité de certification ainsi que la région géographique dans laquelle le certificat est valide.

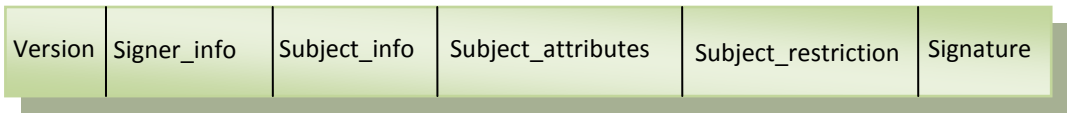


Figure 2.4: Format du certificat numérique

2.4.2 Le format de message sécurisé

Les deux standards IEEE 1609.2 et ETSI ont définit le format d'un message sécurisé (cf. Figure 2.5) qui comprend la donnée à authentifier, la signature numérique générée à l'aide de la clé privée de l'émetteur et le certificat numérique qui permet de vérifier la validité de la clé publique.

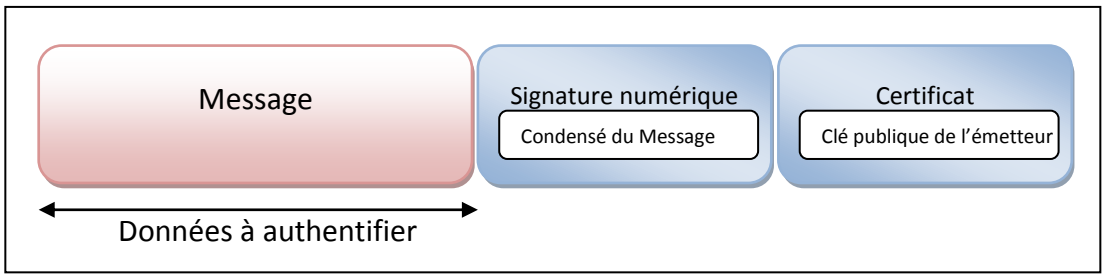


Figure 2.5 : Format simplifié d'un message sécurisé dans les VANETs

La Figure 2.6 montre le format d'un message sécurisé suivant le standard 1609.2, l'entête du message comprend la version du protocole et le type de message, les informations du signataire, les données à signer, et la signature numérique calculée suivant l'algorithme ECDSA (elle est composée de deux nombres entiers r,s[31]). Un exemple d'un message sécurisé suivant le standard ETSI est illustré dans la Figure 2.7.

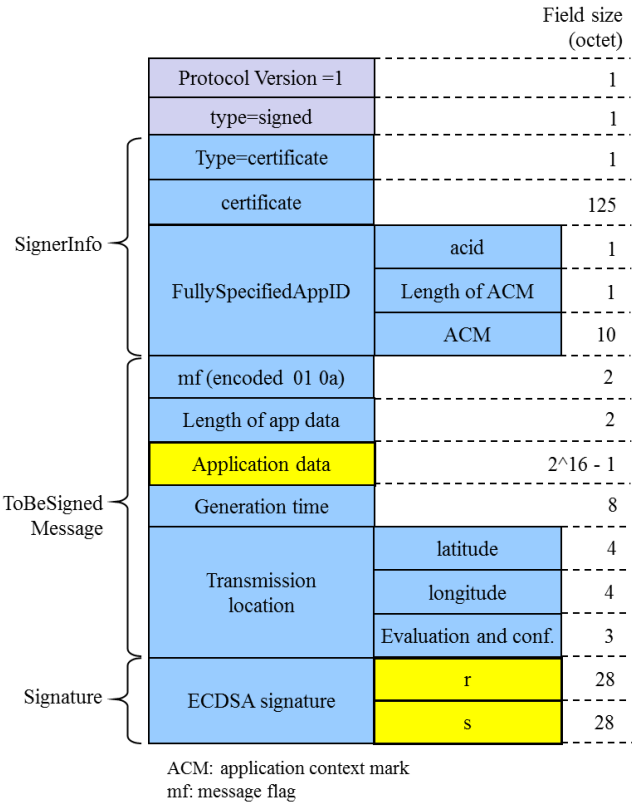


Figure 2.6 : Format d'un message sécurisé suivant le standard 1609.2 [34]

Element	Value	Description	Length
SecuredMessage			
protocol_version	0x02		1
header_fields <var>	0x8091	Length: 145 octets	2
type	0x80	=signer_info	1
type	0x02	=certificate	1
certificate	...	certificate of signer	141
type	0x05	=its_aid	1
its_aid	...		1
payload			
type	0x01	=signed	1
data <var>	0x01	Length: 1 octet	1
[data]	...	payload	1
trailer_fields <var>	0x43	Length: 67 octets	1
type	0x01	=signature	1
signature			
algorithm	0x01	=ecdsa_nistp256_with_sha256	1
ecdsasignature			
R			
type	0x00	=x_coordinate_only	1
x	...		32
s	...		32
Total size: 219 bytes			

Figure 2.7: Exemple d'un message ETSI sécurisé [35]

2.5 Les problèmes liés à l'authentification dans les VANETs

Suivant le standard IEEE 1609.2[30], chaque véhicule diffuse périodiquement à ses voisins entre 1 et 10 messages beacons. Les messages beacons peuvent être directement traités par une application qui génère par exemple un avertissement d'une collision imminente, ou bien qui construit une carte utilisable pour donner des conseils aux conducteurs.

Ces applications peuvent être visées par des attaquants qui y injectent des informations falsifiées. Il se peut que leurs objectifs soit de tromper, par exemple, les conducteurs et les amener à commettre des manœuvres non appropriées. Pour faire face à ces attaques, les standards proposent l'utilisation des signatures ECDSA. Donc, les véhicules ont des clés cryptographiques publiques et privées et des certificats gérés par des ACs qui déclarent que ces véhicules sont des participants valides. Chaque véhicule peut donc signer des messages beacons et leur ajouter des certificats (cf. Figure 2.5). Donc, n'importe quel véhicule récepteur doit vérifier le certificat et la signature avant n'importe quel traitement supplémentaire des informations qui y sont incluses. Par conséquent, l'overhead ajouté à cause de la sécurité augmente la bande passante consommée (à cause de la taille du message beacon), ainsi que les délais de communication (cf. Figure 2.8).

Ces deux derniers aspects causent un problème de scalabilité, et par conséquent, on ne peut pas avoir une communication fiable dans les scénarios de haute densité de nœuds.

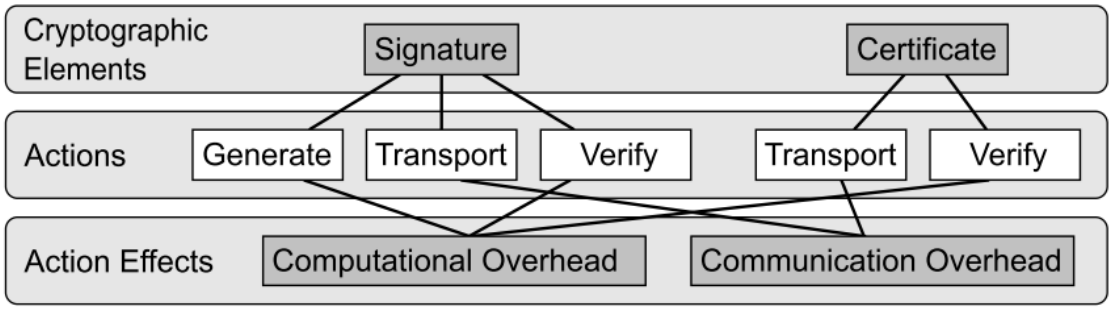


Figure 2.8 : L'overhead de l'authentification [36]

À titre illustratif, nous donnons un exemple d'un véhicule ayant 100 voisins. Donc, ce dernier est sensé recevoir environ 100×10= 1000 messages par seconde pour une fréquence de messages de 10 Hz, et par conséquent ce véhicule doit faire une vérification de 1000 signatures par seconde et encore 1000 autres vérifications pour les certificats numériques. En outre, les signatures et les certificats ajoutent environ 200 octets supplémentaires à la taille du message beacon, ce qui charge ainsi le canal de communication partagé et augmente les risques d'avoir des collisions.

Afin de remédier à ce problème, le projet Preserve a proposé d'intégrer dans l'OBU un module afin d'accélérer les opérations cryptographiques. Ce module est capable d'effectuer jusqu'à 1000 vérifications par seconde[37]. Malheureusement, cette solution est coûteuse et n'encourage pas l'accélération du déploiement des VANETs.

Pour avoir une idée sur l'impact de la complexité spatiale entrainée par l'ajout d'un certificat et d'une signature numériques sur le système de beaconing, nous donnons le tableau suivant :

Nombre de nœuds voisins	**30 octets charge utile**	**211 octets charge utile**
1	4901,96	2225,52
50	98,04	44,51
100	49,02	22,26
250	19,61	8,90
500	9,80	4,45

Tableau 3 : Taux de paquets par nœud par seconde[36]

A partir de la table précédente, nous pouvons remarquer que dans les scénarios à haute densité, un nœud ne peut pas atteindre la fréquence 10 hertz pour les beacons s'il attache des informations cryptographiques (voir Tableau 3, considérer les cas où le nombre de nœuds est supérieur ou égal à 250). En effet, le canal a une capacité limitée qui ne peut jamais être dépassée. Tous les nœuds voisins doivent partager le canal, et chacun d'eux doit attendre que ce dernier soit libre avant la transmission.

2.6 L'impact de la signature numérique sur le routage dans les VANETs

Le routage est un élément fondamental pour les communications véhiculaires, ce qui le rend une cible idéale pour les attaques dans les VANETs. En effet, les nœuds malveillants peuvent effectuer des actions malveillantes afin de perturber le bon fonctionnement des VANETs. L'authentification est une opération indispensable à la sécurisation de routage. Dans cette section, nous allons étudier l'impact de l'authentification sur les protocoles de routage dans les VANET. A cet effet, nous avons considéré le routage géographique glouton[38], pour étudier l'impact de l'authentification. Cette stratégie de routage est très utilisée pour évaluer la performance de différentes propositions de protocoles dans les VANETs, à cause de sa haute performance dans les réseaux très dynamique[39].

Durant la simulation, nous avons utilisé les paramètres suivants :

Paramètre	Valeur
Simulateur	NS-2 [40]
La portée de transmission(m)	300m
Dimension du champ de mouvement	1000 m × 1000 m
Nombre d'intersection	6
Le nombre de nœuds	250
L'intervalle de temps minimum entre deux beacons	1 seconde
Vitesse de véhicule (m/s)	[0..40]

Tableau 4 : Environnement et paramètres de simulation

La Figure 2.9 représente le délai moyen d'acheminement de paquets de bout en bout en fonction de la taille de la signature numérique. C'est le temps moyen écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Il comprend éventuellement les retards causés dans les files d'attente et les retransmissions de paquets. Par contre, les paquets de données qui sont perdus en route ne sont pas considérés.

Les résultats obtenus montrent que le délai moyen de bout-en-bout croît à l'augmentation de la taille de la signature numérique. Nous remarquons aussi que le délai d'acheminement a augmenté de façon considérable au-delà d'une taille de signature supérieure à 1024 bits, car cette dernière nécessite un temps de génération, de vérification et de transmission important, et cause en plus une charge importante sur le canal.

Pour un système d'authentification plus simple, les délais d'acheminement de bout en bout peuvent être exprimés de la manière suivante :

$$D = (n-1)\left(TV_{sign} + TG_{sign} + TR + TV_{cert}\right)$$

Avec :

D : le délai moyen d'acheminements des paquets

n : le nombre de nœuds intermédiaires +nœud source+ nœud destination

TV_{sign} , TV_{cert} **:** le temps de vérification de la signature et du certificat, respectivement.

TG_{sign} **:** le temps de génération de la signature numérique.

TR : le temps de transmission.

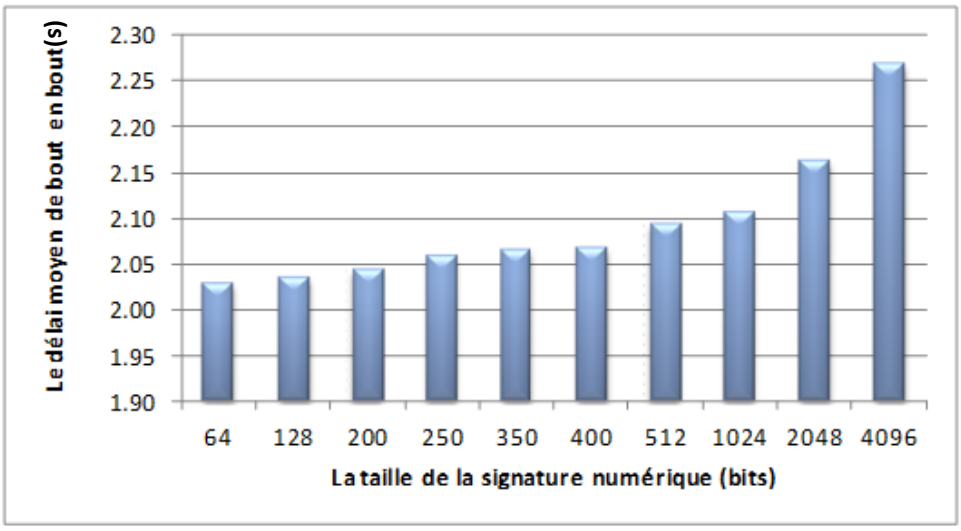


Figure 2.9 : Délai moyen d'acheminement des paquets

Nous remarquons dans la Figure 2.10 que le taux des paquets perdus augmente avec l'augmentation de la taille de signature numérique. De la même manière, avec le graphe précédent, le taux de perte augmente d'une façon exponentielle au-delà la taille de la signature numérique 1024 bits à cause de la charge sur le canal. Nous remarquons aussi que le taux de perte des paquets est presque le même pour les valeurs de la taille de signature numérique de l'intervalle allant de 64 à 1024 bits.

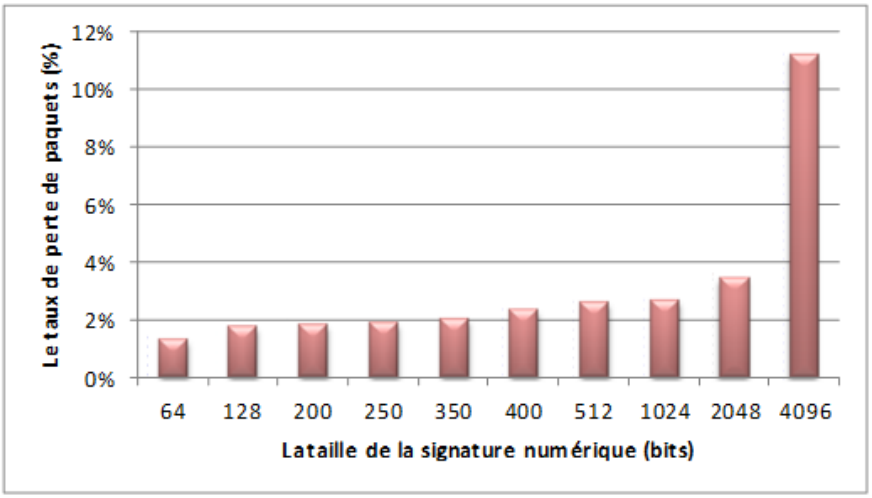


Figure 2.10 : La perte de paquets

2.7 L'omission de certificat

Dans les scénarios de haute densité de véhicule, les paquets peuvent être perdus à cause de la limitation de puissance de calcul des OBUs, et donc certains paquets ne seront pas traités. Par conséquent, ils seront surement éliminés. Ce type de perte de paquets est connu sous le nom CPL (pour « *Cryptographic Packet Loss* »). Il faut noter que l'omission de certificat a été officiellement prise en compte par les travaux de standardisation ETSI[35].

Trois stratégies ont été proposées pour remédier au problème précédent :

2.7.1 La technique POoC (Periodic Omission of Certificates)

La stratégie POoC[41] consiste à ne pas ajouter le certificat qu'au n^{ème} beacon, après avoir envoyer n-1 beacons sans l'inclure. La Figure 2.11 illustre un exemple de la stratégie POoc, avec une période n=5, σ la signature numérique, cert le certificat numérique et m_i le i^{ème} message beacon. L'inconvénient majeur de cette approche est qu'il permet de créer dans les pires des cas, une fenêtre de perte de messages égale à $(\mathrm{n}-1)T_b$ (T_b est la période qui sépare deux beacons consécutifs) dans laquelle un nouveau voisin qui n'a pas de certificat en cache pourrait être incapable d'authentifier les beacons reçus. $(\mathrm{n}-1)T_b$ est la durée de la fenêtre où une situation dans laquelle le véhicule V_1 est considéré comme voisin de V_2 à l'instant t, et V_2 a émis le n^{éme} beacon qui contient le certificat à l'instant $t-\varepsilon$. La valeur moyenne de la fenêtre dans cette approche est donc $\frac{(n-1)}{2}T_b$. Si $T_b = 0{,}1$ s et n=10 la valeur moyenne de la fenêtre sera donc 0,45 s. Durant cet intervalle de temps, un véhicule avec une vitesse de 120 km/h pourrait parcourir une distance de 15 mètres sans être capable d'authentifier les messages envoyés. Nombreuses applications liées à la sécurité n'accepte pas cette situation. Il faut noter que ce problème pourrait aussi avoir lieu dans les situations de changement de pseudonymes.

Un autre problème de cette stratégie est que la valeur n est statique et ne dépend pas du nombre de voisins. Considérant le même scénario précédent, mais avec une table de voisins vide à l'instant t, le nouveau voisin V_1 ne sera capable d'authentifier V_2 qu'après un délai de $(\mathrm{n}-1)T_b$, bien qu'il soit son seul voisin.

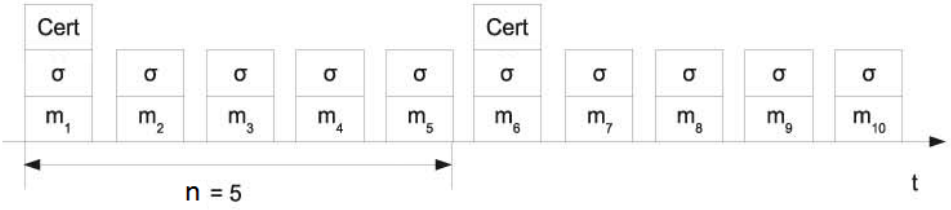


Figure 2.11 : La stratégie POoc[41]

2.7.2 La technique NbCO (Neighbor-based Certificate Omission)

La technique de NbCO a été proposée par Schoch et al. [36], elle prend en considération le changement de table de voisins. Elle consiste à intégrer le certificat dans le beacon d'un nœud n1 si et seulement s'il reçoit le beacon d'un autre nœud n2 qui ne figure pas dans sa table de voisins (cf. Figure 2.12)

.

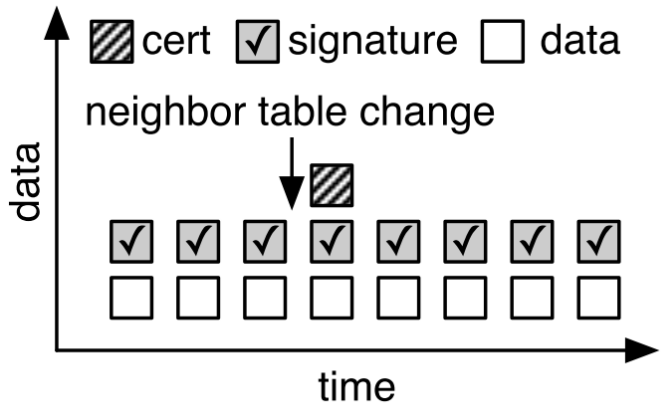


Figure 2.12 : Un exemple de la tehnique NbCO [42]

Cette technique est plus efficace et permet de réduire l'overhead dans une certaine mesure. En effet, un nœud peut être incapable d'authentifier un nouveau nœud voisin dans un laps de temps de $2.T_b$ (T_b est la période qui sépare deux beacons consécutifs). Cet intervalle de temps peut être beaucoup plus long en cas de présence de collisions. Ainsi, si le paquet d'un nœud n1 comportant le certificat destiné au nœud n2, est perdu, ce dernier nœud doit attendre une opportunité pour que n1 inclut son certificat pour un autre nouveau nœud voisin. Pour remédier à ce problème, les auteurs de cette approche ont proposé de solliciter les certificats à la demande. Les auteurs n'ont pas pris en compte les attaques de déni de service, dans lesquelles les attaquants peuvent demander les certificats malgré qu'ils aient des copies dans leurs caches.

2.7.3 La technique CbCO (Congestion based Certificate Omission)

L'approche POoC et NbCO souffrent dans le cas de perte de paquets CPL. A cet effet, l'approche CbCO a été proposée pour remédier à leurs problèmes. Elle consiste à rendre la technique POoC adaptative. En effet, le choix de la valeur de n est adaptatif et dépend du nombre de voisins, $n = \Omega(N)$ avec :

— N est le nombre de voisins.

Ω est la fonction de pondération.

Il existe trois variantes pour la fonction Ω : linéaire, quadratique et trigonométrique:

— $\Omega_{lin\,éaire} : y = min(\frac{x}{n_{max}} O_{max}, O_{max})$

— $\Omega_{quad} : y = min(\left(\frac{x}{n_{max}} O_{max}\right)^2, O_{max})$

— $\Omega_{trig} : y = \begin{cases} -\cos\left(\frac{\pi}{n_{max}} O_{max}\right) \frac{O_{max}}{2} + \frac{O_{max}}{2}, & x < n_{max} \\ O_{max}, & x \geq n_{max} \end{cases}$

n_{max} est la taille de la table de voisins qui entraine une omission maximale de certificats O_{max} , et x est la taille de la table de voisins courante.

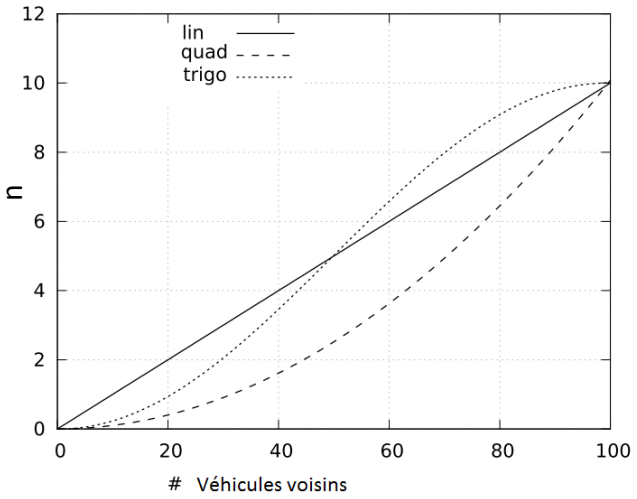


Figure 2.13 : L'omission des trois techniques CbCO [42]

La Figure 2.13 montre l'évolution de la valeur n en fonction du nombre de voisins. Nous remarquons que l'omission des certificats croît à l'augmentation du nombre de voisins. Ceci permet de diminuer la charge sur le canal avec un nombre élevé de voisins. Dans la même figure, nous remarquons aussi que la technique quadratique présente le nombre minimum de certificats omis. Donc, cette technique augmente la charge sur le canal par rapport aux autres techniques. Tandis que la technique trigonométrique maximise l'omission de certificats avec un nombre élevé de voisins qui dépasse 50.

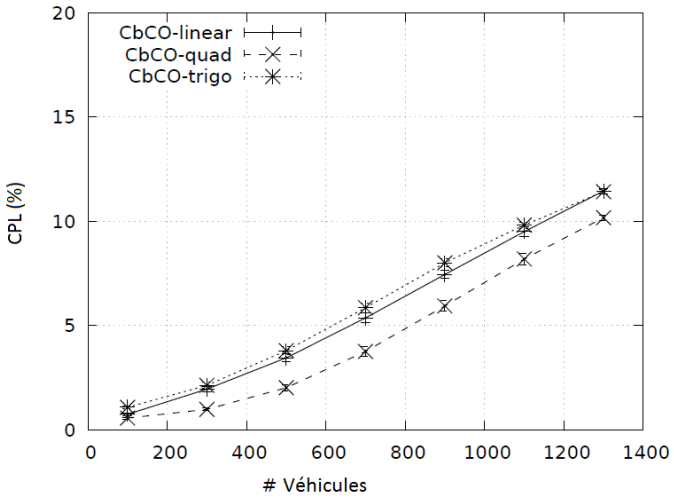


Figure 2.14 : Taux de CPL [42]

La Figure 2.14 illustre le taux de CPL en fonction du nombre de véhicules. Nous remarquons que le taux de perte CPL augmente lorsque le nombre de véhicules augmente. Car, avec un nombre élevé de voisins, les nœuds doivent augmenter le taux d'omission comme on l'a vu dans la figure précédente. La technique quadratique a minimisé le taux de pertes CPL, parce que cette technique assure une omission minimale de certificats.

2.8 L'authentification rapide

A cause de l'ouverture de l'environnement VANET, les différents standards exigent que les signatures numériques et les certificats soient utilisés pour l'authentification. Ces deux outils cryptographiques augmentent la complexité spatiale et temporelle, ce qui entrave le déploiement des VANETs. D'autres techniques cryptographiques peuvent être envisagées pour réduire cette complexité. Dans cette section, nous en présentons quelques une:

2.8.1 La techniques OTS (One-Time Signature)

La technique OTS a été proposée par Lamport [43] . L'OTS est une technique spécifique basée sur la cryptographie symétrique qui est 1000 fois plus rapide que des techniques similaires à l'ECDSA. Cependant, cette vitesse de traitement vient au détriment de la complexité spatiale. En effet, les messages signés avec l'OTS sont volumineux et nécessitent aussi l'échange de clés cryptographiques très longues. De plus, chaque clé ne peut être utilisée qu'une seule fois. Cette technique nécessite les trois étapes suivantes :

1. **Génération** :

   Pour chaque $i \in [1, l], b \in \{0,1\}$, choisir indépendamment $x^{i,b} = \{0,1\}^n$.

   Soit $y^{i,b} = f(x^{i,b}),\ sk = \{x^{i,b}\}$ la clé de signature et $vk = \{y^{i,b}\}$ la clé de vérification. Ces clés peuvent être représentées de la manière suivante :

$$sk = \begin{array}{|c|c|c|c|} \hline x^{1,0} & x^{2,0} & \cdots & x^{l,0} \\ \hline x^{1,1} & x^{2,1} & \cdots & x^{1,1} \\ \hline \end{array}$$

$$vk = \begin{array}{|c|c|c|c|} \hline y^{1,0} & y^{2,0} & \cdots & y^{l,0} \\ \hline y^{1,1} & y^{2,1} & \cdots & y^{1,1} \\ \hline \end{array}$$

2. **Signature :** $Sign\ (sk,\ m \in \{0,1\}^l)$, nécessite $\sigma = \{x^{1,m_1}, x^{2,m_2}, .., x^{l,m_l}\}$.
3. **Vérification :** $Ver\ (v,\ m \in \{0,1\}^l$ signature valide si $y^{i,b} = f(\sigma_i)$ pour chaque $i \in [0, l-1]$.

La complexité spatiale peut être réduite en utilisant le hachage itératif ce qui permet de réduire la complexité n fois, avec n le nombre de fois d'application itérative de la fonction de hachage[44].

2.8.2 MTS (Merkle Tree Signature)

Le MTS est un mécanisme de signature basé sur l'arbre de Merkle ou arbre de hachage proposé par Merkle . Cet arbre est une structure de données qui contient un condensé d'information d'un volume de données, généralement grand (comme un fichier).

Le principe d'un arbre de hachage consiste à décomposer les données d'entrée en un ensemble de blocs de même taille. Ces blocs sont considérés comme les feuilles de l'arbre. Ils sont généralement complétés par des valeurs neutres, comme des zéros, de façon à obtenir des blocs de la taille souhaitée.

A partir de nœuds d'un niveau i, on peut en obtenir d'autres de niveau supérieur i+1 en appliquant la fonction de hachage sur les nœuds de niveau inferieur i (cf. Figure 2.15). Cette opération est itérative jusqu'à l'obtention d'un seul nœud à la racine.

La signature numérique consiste à montrer les différentes valeurs de hachage qui mène à obtenir la racine. Des valeurs aléatoires $r_i$sont concaténées avec les blocs de données pour avoir les condensés h_i .

Nous remarquons que cette technique est beaucoup plus performante par rapport à l'OTS, car chaque arbre construit permet d'authentifier plusieurs messages.

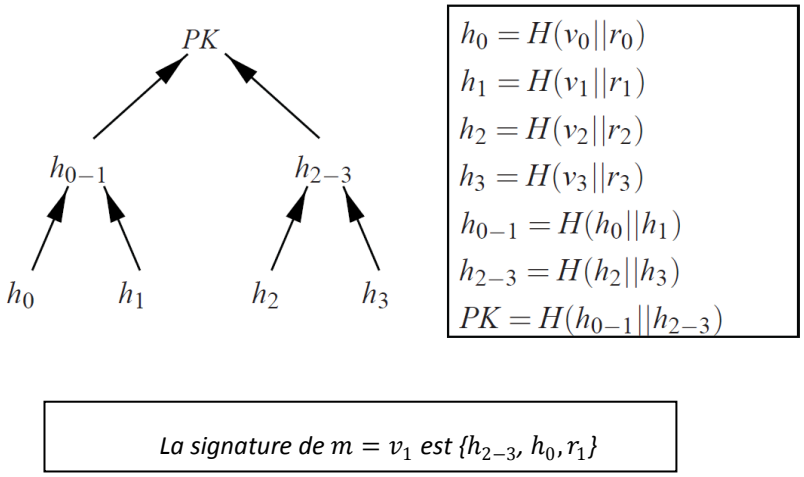


Figure 2.15 : Illustration de l'arbre de Merkle [45]

2.9 Les techniques basées sur la prédiction de mouvements

Les messages de broadcast sont les messages qui dominent les échanges dans les VANETs. C'est pour cette raison que les chercheurs se concentrent sur l'optimisation du processus d'authentification de ces messages. Parmi les techniques les plus connues est celle proposée par Hsiao et al.[45]. Cette technique considère que les véhicules peuvent prévenir leurs contextes dans le futur. En effet, l'entropie de messages beacons est relativement faible du point de vue de l'émetteur. Ce dernier peut tirer avantage des lois physiques : la vitesse est connue, la trajectoire peut être prévue avec une grande probabilité. Le véhicule peut prévenir et construire à l'avance les deux prochains messages beacons, sachant qu'il peut prévenir la position géographique, l'horodateur qui marque le temps d'émission de ces messages beacon.

A titre d'illustration, les véhicules qui roulent à une vitesse de 130 Km/h peuvent parcourir une distance de 3,3 mètres dans un intervalle de temps de 0.1 seconde.

Hsiao a remarqué que, la plupart de temps, les véhicules ont tendance à avancer le long de la route plutôt que de se déplacer latéralement. Il a considéré trois actions possibles pour un véhicule qui se déplace :

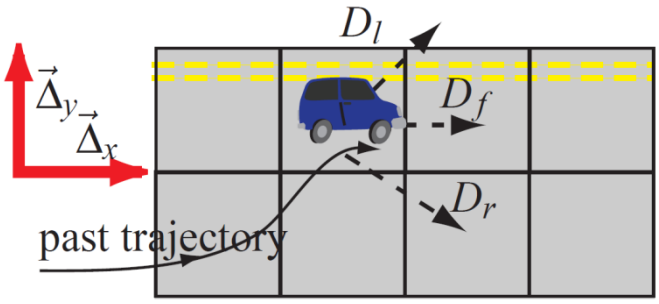


Figure 2.16 : Les possibilités de déplacement d'un véhicule[45]

D_f : Il désigne le déplacement vers l'avant.

D_l : Il désigne le déplacement vers la gauche.

D_r : Il désigne le déplacement vers la droite.

La figure suivante définit l'arbre de Merkle pour les actions précédentes :

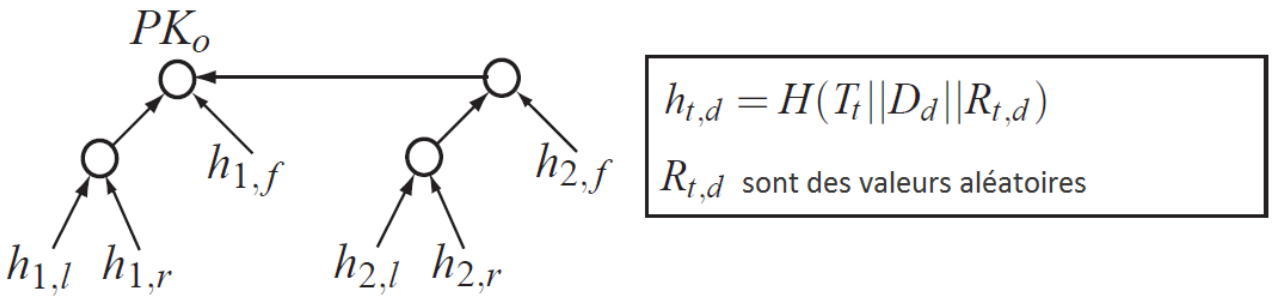


Figure 2.17 : L'arbre de Merkle pour les déplacements d'un véhicule

Dans ce qui suit, nous donnons un exemple illustratif qui montre le déroulement de cette technique. A cet effet, trois phases peuvent être identifiées :

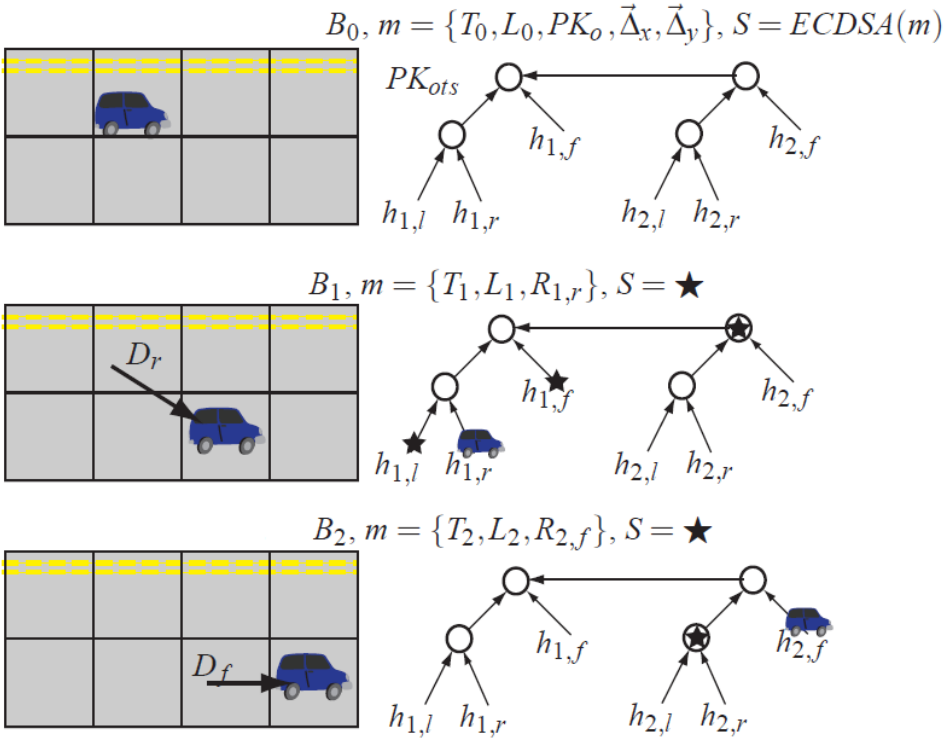


Figure 2.18 : Exemple illustratif du mécanisme d'authentification de Hsiao[45]

- **Phase 0** : elle consiste à diffuser un message B_0 signé de l'algorithme ECDSA comportant la valeur de la racine de l'arbre de Merkle, l'horodateur T_0 qui marque le temps d'émission de message, L_0 la position géographique courante et les vecteurs de déplacement abscisse et ordonnée $\overrightarrow{\Delta x}$ et $\overrightarrow{\Delta y}$, respectivement.
- **Phase 1** : elle consiste à diffuser un message B_1 à l'instant T_1. Ce message comporte $T_1, L_1,$ et $R_{1,r}$. Il fournit le chemin d'authentification qui prouve que le véhicule s'est déplacé vers la droite.
- **Phase 2** : elle consiste à diffuser un message B_2 à l'instant T_2. Ce message comporte T_2, L_2 et $R_{2,f}$. Ce message fournit le chemin d'authentification qui prouve que le véhicule s'est déplacé vers l'avant.

Afin de vérifier la signature numérique, le vérificateur doit reconstruire l'arbre de Merkle. La signature d'un nœud est considérée valide si la valeur calculée de la racine PK_0 correspond à celle diffusée dans la phase 0.

2.10 Conclusion

L'authentification des messages dans les réseaux VANET est une opération fondamentale pour se protéger contre les nœuds malveillants. Elle consiste à ajouter des signatures numériques et à rattacher des certificats numériques aux messages beacons échangés entre les véhicules. Les certificats ont un impact négatif sur les réseaux dans les scénarios de haute densité de nœuds. En effet, le rattachement de certificats aux messages beacons peut causer les pertes cryptographiques de paquets. Une solution à ce problème consiste à omettre le rattachement de certificats aux messages beacons. Cette opération peut être envisagée si le taux de perte de paquets est acceptable.

Prévenir le futur contexte de véhicules et employer la cryptographie symétrique, est une autre solution qui pourrait être aussi envisagée pour améliorer le processus d'authentification.

Chapitre 3

La détection et la révocation des nœuds malveillants

3.1 Introduction

Les réseaux VANET sont vulnérables aux attaques. En effet, un attaquant peut falsifier sa position géographique afin de dégrader la performance du réseau, provoquer une réorientation du trafic routier, ou voire même causer des accidents qui entrainent des dommages concernant des personnes et des biens. Donc, la détection rapide de ces nœuds est indispensable pour assurer le bon fonctionnement de ces réseaux. Une technique habituelle pour annuler la validité des certificats est de distribuer les listes de révocation de certificats crées par l'AC. Mais, le problème réside dans le processus de distribution centralisé qui nécessite beaucoup de temps vu que la collecte de données de révocation nécessite un processus de détection décentralisée.

Dans ce chapitre, nous présentons d'abord les techniques permettant de détecter les nœuds falsifiant leurs positions géographiques. Ensuite, la problématique de révocation suivie de notre contribution sur l'amélioration du processus de révocation de nœuds.

3.2 Les techniques de vérification de position géographique

Il en existe deux grandes catégories pour vérifier la position géographique d'un nœud: la première est basée sur l'estimation de la distance, alors que la deuxième est basée sur les tests de plausibilité. Dans ce qui suit, nous donnons la description de chaque catégorie :

3.2.1 Les techniques basées sur l'estimation de distance

Ces techniques se basent sur les mesures des distances entre les nœuds afin de vérifier leurs positions géographiques; elles consistent à utiliser les techniques suivantes :

a) La technique de la puissance du signal

L'énergie des ondes radio diminue au cours de leur propagation à cause de leur interaction avec l'environnement. Il existe plusieurs modèles décrivant la relation entre cette perte d'énergie et la distance parcourue. Donc, ils peuvent être exploités pour estimer les distances entre deux nœuds. La technique utilisant ce principe est appelée RSS (*Received Signal Strength*)[46]. Elle consiste à calculer la puissance du signal reçu et de conclure l'atténuation du signal lors de la propagation. Le problème de cette technique est qu'elle est vulnérable aux attaques d'allongement et de réduction de distance estimée si l'émetteur est un nœud compromis qui ajuste le signal afin de tromper le récepteur.

b) La technique ToA

Cette technique consiste à mesurer la durée de propagation du signal afin de retrouver la position géographique. Elle est souvent dénotée ToA (*Time of Arrival*). Il existe trois variantes pour cette technique[47].

- La première est coopérative : elle est utilisée dans la technologie de GPS et nécessite une synchronisation entre l'émetteur et le récepteur qui peut estimer la durée de propagation en récupérant la valeur de l'horodateur incluse dans le message qui marque l'instant de son émission. Supposons que t_s est l'instant d'émission du message m, t_r est l'instant de sa réception et c la vitesse de la lumière, alors d_{ABm} qui est la distance à estimer est donnée par l'équation suivante :

$$d_{ABm} = (t_r - t_s)c$$

- Dans la deuxième variante, dite non-coopérative, le nœud à localiser agit comme un réflecteur ou une cible (c'est la technique des radars). Ici, pour l'estimation de la durée de propagation du signal, on se base sur le temps d'aller- retour. Le signal réfléchi par la cible revient vers la source qui l'a envoyé. Dans cette variante, la synchronisation n'est pas obligatoire puisque le nœud source connaît le moment où il a émis le signal (cf. Figure 3.1), la durée de propagation serait alors la moitié du temps estimé.

Supposons que t_{procB} est le temps de traitement au niveau du nœud B, l'équation d'estimation de distance est donnée par l'équation suivante :

$$d_{ABm} = \frac{(t_r - t_s - t_{procB})c}{2}$$

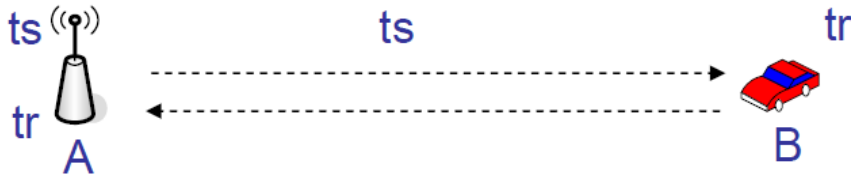


Figure 3.1 : Estimation de la distance avec la variante 2 du ToA

- La troisième variante est basée sur les signaux ultra-sonores. Son avantage réside dans leur vitesse de propagation d'environ 1243 km/h qui est évidemment très faible par rapport à celle de l'infrarouge et des ondes radio qui sont d'environ 300000 km/s. Par conséquent, l'ultra-son fournit une base très pratique pour les mesures de temps et peut donc être utilisé pour l'estimation de distances. Les systèmes de positionnement ultra-sonores peuvent atteindre une précision de l'ordre de quelques centimètres. Les systèmes Active Bat [48] et Cricket [49][50] sont quelques exemples de systèmes de localisation par ultra-son.

La technique du temps d'arrivée est vulnérable aux attaques d'allongement et de réduction de distance. En effet, pour la première variante un attaquant interne peut falsifier la valeur de t_s pour convaincre le récepteur qu'il se situe à n'importe quelle distance (La deuxième variante est vulnérable, seulement, aux allongements de distance vu les contraintes physiques liées à la vitesse de la lumière). Alors qu'un attaquant externe peut effectuer son attaque en deux étapes, comme suit :

Dans la première étape, l'attaquant brouille le canal, juste après la réception du message de localisation. Ensuite, après un certain délai de retard Δt bien déterminé, il réémet le message à la destination B qui estime une distance plus longue que la réelle.

c) Angles d'arrivée (AoA)

La technique AoA (Angle of Arrival) consiste à utiliser des antennes directionnelles ou un réseau d'antennes aux stations de bases pour estimer la direction d'arrivée du signal. L'intersection des trajets des signaux donne la position du nœud. Cependant, étant donnée la présence d'une marge d'erreurs d'autres techniques de localisation peuvent être utilisées pour estimer plus précisément la localisation du nœud dans une région. La précision de cette technique se dégrade donc au fur et à mesure que le nœud à localiser s'éloigne du nœud vérificateur.

La technique AoA donne des erreurs de localisation importantes en milieu urbain. En effet, à cause de présence des obstacles, le signal direct n'atteint pas les nœuds vérificateurs. De plus, l'angle d'arrivée d'un trajet réfléchi est alors considéré comme étant celui du trajet direct. Suivant Fascista et al. la technique AoA peut être utilisée pour localiser, précisément, les véhicules les plus proches des RSU[51].

3.2.2 Les techniques basées sur les tests de plausibilité

Au lieu de se baser sur les techniques d'estimation de position précédentes qui nécessitent des équipements spécifiques et couteux, Leinmuler et al.[52] ont proposé un ensemble de capteurs qui consistent à effectuer des vérifications afin que le nœud vérificateur s'assure que l'information géographique annoncée soit concordante avec les informations dont il dispose. Ces approches sont modélisées sous la forme de capteurs qui génèrent des observations spécifiques. Ces dernières sont utilisées pour calculer le degré de confiance r_t (qui doit être normalisé à une valeur appartenant à l'intervalle [-1,1]) d'un nœud suivant l'équation suivante :

$$r_t = \sum_{i \in S} w^i \sum_{j \in N_i} wt(t, t_j^i)\, \sigma_j^i$$

Où σ_j^i est la $j^{ème}$ observation du capteur i qui est captée à l'instant t_j^i ;

La fonction wt est définie de la manière suivante :

$$wt\left(t, t_j^i\right) = 1 - \left(\frac{t - t_j^i}{T}\right)^x$$

Avec T, la durée maximale des observations stockées et x le facteur de pondération de l'âge.

Les capteurs d'observations précédents peuvent être catégorisés en deux grandes classes : les capteurs de vérifications autonomes et capteurs coopératifs.

1. Les capteurs de vérifications autonomes comprennent :

— ART (*Acceptance Range Threshold*): il consiste à vérifier si la position géographique annoncée se situe sur sa zone radio suivant un seuil prédéfini.

— MGT (Mobility Grade *Threshold*): il consiste à vérifier si les positions géographiques annoncées ne violent pas les conditions physiques telles la vitesse et l'accélération maximales.

— MDT (*Maximum Density Threshold*): il consiste à vérifier si le nombre de véhicules dans une zone géographique n'excède pas un seuil défini suivant la superficie de cette zone.

— Vérification de la carte digitale : puisqu'il est facile d'intégrer dans les OBUs de véhicules des cartes digitales, il est facile de vérifier si la position géographique annoncée est concordante avec le plan routier indiqué par la carte.

— Vérification des paquets interceptés de voisins: elle consiste à vérifier les nœuds sources et de destinations dans les paquets interceptés afin de détecter s'il y a inconsistance avec les positions géographiques annoncées suivant la technique du capteur ART.

2. Les capteurs de vérification coopératifs : ils emploient la technique du capteur ART sur les nœuds voisins soit en demandant explicitement les informations géographiques ou topologiques des voisins (approche réactive), ou en s'échangeant ces informations implicitement, de manière périodique (approche proactive).

3.3 La révocation de certificats

3.3.1 Les LRCs

Les certificats ont une durée de validité durant laquelle les nœuds sont considérés comme des membres légitimes. Malheureusement, les nœuds pourraient être contrôlés par des entités malveillantes, ce qui nécessite d'annuler la validité de leurs certificats. Une approche commune pour cette opération est de distribuer une LRC (Liste de Révocation de Certificat ou CRL « *Certificate revocation list* ») à tous les membres du réseau. Cette liste indique aux nœuds les certificats à négliger, et peuvent donc minimiser les capacités des attaquants qui contrôlent les clés privées correspondantes. Une implémentation de LRC a été proposée par Ardelean [53] (cf. Figure 3.2) dans laquelle la LRC est divisée en N parties où m ($m < N$) parties est suffisant pour reconstruire le LRC.

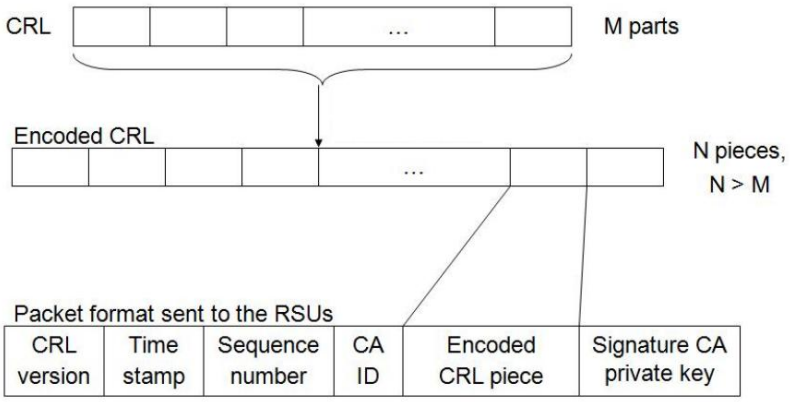


Figure 3.2 : L'encodage du LRC [53]

D'autres techniques peuvent être utilisées pour coder les LRCs, telle la technique proposée par Raya et al. [54]qui consiste à utiliser un codage probabiliste[55] afin de réduire leur taille. Suivant Haas et al. [56] un tel codage peut inclure 25 millions d'entrées dans une LRC de 32 Mb en considérant que chaque certificat est identifiable avec un condensé de 16 octets.

3.3.2 La distribution de certificats

De nombreux travaux de recherches ont traité de la problématique de distribution de certificats[57][53][58]. Ardelean et al. [53] qui supposent que les véhicules téléchargent la dernière LRC lorsqu'ils sont en mesure de communiquer avec les RSUs (cf. Figure 3.3) qui sont connectés directement à un système spécifique pour la distribution de certificats.

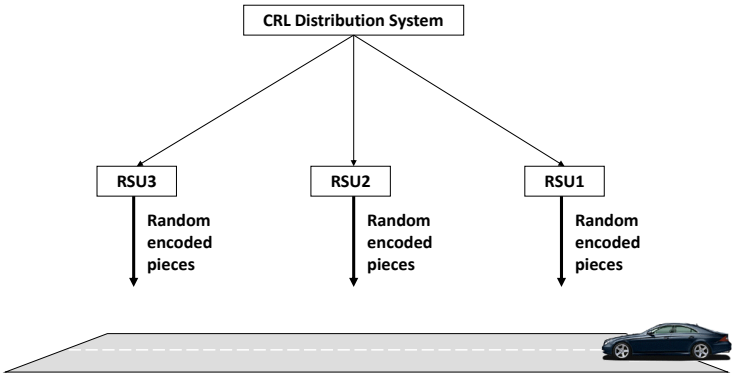


Figure 3.3 : Un système simple de distribution de certificats [53]

Raya dans [54] propose plusieurs approches de distribution de certificats, parmi lesquelles, celle qui consiste à employer les ondes radio FM pour transmettre les données de révocation (cf. Figure 3.4). En effet, elles peuvent être exploitées afin de transmettre un message sécurisé aux TPDs qui doit supprimer toutes les clés cryptographiques des nœuds exclus.

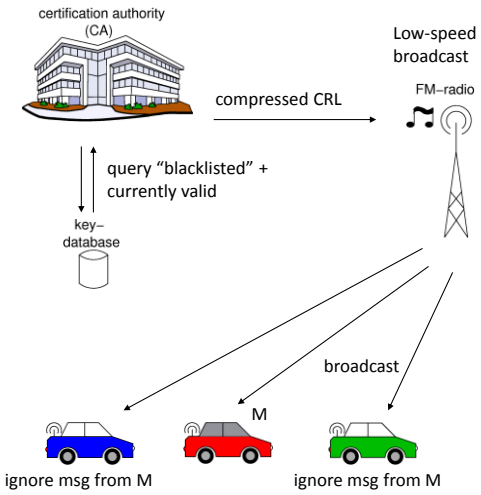


Figure 3.4 : La révocation en utilisant les ondes FM dans les VANETs [54]

3.4 La révocation de nœuds malveillants

La révocation des nœuds consiste à marquer ou à considérer leurs clés cryptographiques invalides : Soit via la réception des LRCs, dans ce cas la révocation est dite globale ou centralisée[59], soit via la dissémination des messages de révocation dans une zone géographique limitée. Cette catégorie d'approches de révocation est appelée révocation locale ou aussi révocation distribuée[60] car la décision de révocation est prise par un ensemble de nœuds qui coopèrent à travers l'échange des messages d'accusation[61]. La réception d'un ensemble de messages d'accusation vérifiant la condition de révocation mène à ajouter l'identifiant de ce nœud à la liste noire.

La révocation locale est indispensable car elle permet aux nouveaux nœuds voisins d'éviter rapidement les nœuds malveillants. En effet, les nœuds emploient le mécanisme de Watchdog qui a été proposé par Marti et al.[62] afin de contrôler les activités de nœuds malveillants en utilisant un IDS (*Intrusion detection system*) similaire à [63][64][65] pour les détecter et avertir les nœuds voisins via les messages d'accusation.

Le mécanisme de Watchdog consiste à activer le mode indiscriminé (en anglais est appelé « *Promiscuous mode* ») qui permet aux nœuds de capturer les paquets qui ne leur sont pas destinés. Donc, il est possible de les analyser et de détecter les activités malveillantes[66].

Les messages d'accusation doivent aussi être transmis à l'AC afin qu'elle puisse détecter les nœuds malveillants : par exemple en recevant un nombre important d'accusations qui excède un seuil prédéfini[67], l'AC doit ajouter l'identifiant du nœud accusé à la LRC. Dans le cas où un système de révocation nécessite la communication

La Figure 3.5, illustre un message d'accusation contre un véhicule M, échangé entre les véhicules A, B et C ; ce message contenant les signatures des nœuds accusateurs, est envoyé à l'AC qui peut inclure l'identifiant de M dans la prochaine LRC s'il y a un nombre suffisant de messages d'accusation contre lui.

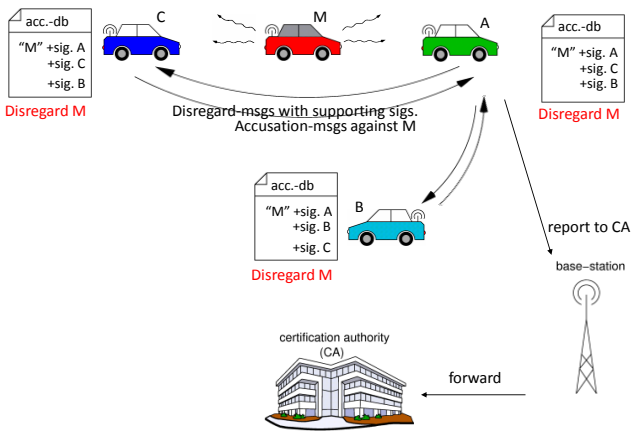


Figure 3.5 : Signalisation d'accusations vers l'AC [68]

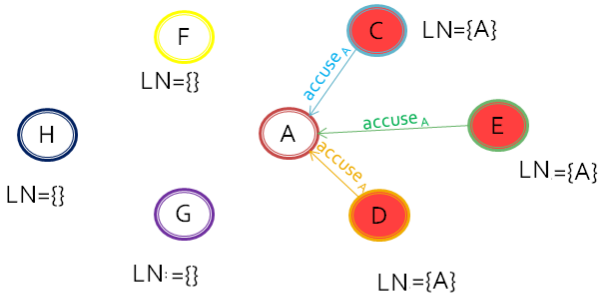
3.5 Les techniques de révocation existant dans les MANETs

Dans la littérature, il existe plusieurs systèmes de révocation de nœuds malveillants pour les réseaux MANET[69]. Ces solutions ont été modifiées et adaptées, par la suite, pour concevoir des systèmes de révocation pour les réseaux VANETs. Dans cette section, nous présentons quelques solutions proposées dans les MANETs. Ensuite, nous proposons un nouveau système de révocation pour les réseaux MANET.

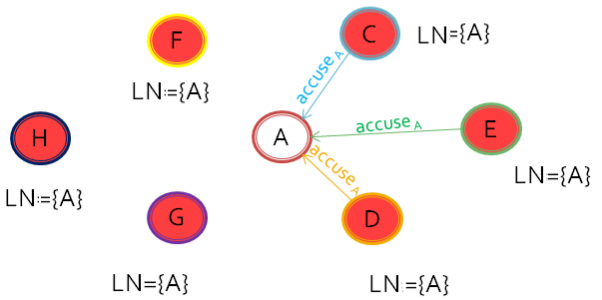
3.5.1 Le système de révocation de Chan

Parmi les premières solutions de révocation, il y a celle proposée par Chan et al. [70] qui est basée sur la cryptographie symétrique. Dans cette solution, un nœud diffuse une seule fois un message d'accusation aux voisins à n sauts, ce qui signifie que la mobilité n'a pas été prise en compte. De plus, chaque nœud accusé par n autres nœuds (au minimum), doit être ajouté à la liste noire.

Dans ce système, chaque paire de nœuds partage une clé utilisée pour authentifier les messages. En plus, chaque nœud doit au début générer une clé secrète de révocation. Cette dernière doit être divisée en n portions en utilisant le mécanisme de partage de clé secrète de Shamir [70]. Ensuite, chaque portion est envoyée à un voisin. Cette portion sera diffusée dans un message d'alerte par un nœud voisin lorsqu'il pense que le nœud qui partage avec lui cette portion a un comportement malveillant (cf. Figure 3.6). Donc, chaque nœud est capable de construire la clé de révocation d'un nœud malveillant s'il peut obtenir k de n (k ≤ n) portions de cette clé. Il faut noter que cette dernière doit être diffusée à travers le réseau comme une preuve de la révocation de ce nœud.



Phase 1: les noeuds C,D et E ajoutent A à leurs listes noires (LN) et partagent leurs portions de la clé secrète avec les autres noeuds F,G et H



Phase 2: Les noeuds F,G et H construisent la clé secrète de A et ajoutent A à leurs listes noires

Figure 3.6 : Système de révocation de Chan

Cette solution est simple et facile à implémenter, mais en présence de k nœuds malveillants en coalition tous les nœuds peuvent être exclus du réseau. De plus, la gestion des arbres d'hachage utilisés pour l'authentification des messages d'alerte nécessite une consommation élevée de la bande passante.

3.5.2 La révocation par détection et attaque suicide

La révocation des nœuds malveillants sera plus facile lorsqu'un seul nœud est capable de faire la décision de révocation. Dans le système de révocation par l'attaque suicide proposé par Clulow et al. [71][72] qui est inspiré du comportement des abeilles, lorsqu'un nœud A qui utilise des mécanismes de détection d'intrusion détecte un comportement malveillant d'un autre nœud M, A doit diffuser aux autres nœuds un message d'alerte " Suicide " qui contient l'identifiant des deux nœuds A et M, le message doit être signé par sa propre clé privée. N'importe quel nœud recevant le message doit ajouter les deux identifiants de A et M à la liste noire (cf. Figure 3.7). Il est clair que le fait de sacrifier de futures participations dans le réseau est une preuve de la véracité de ce message.

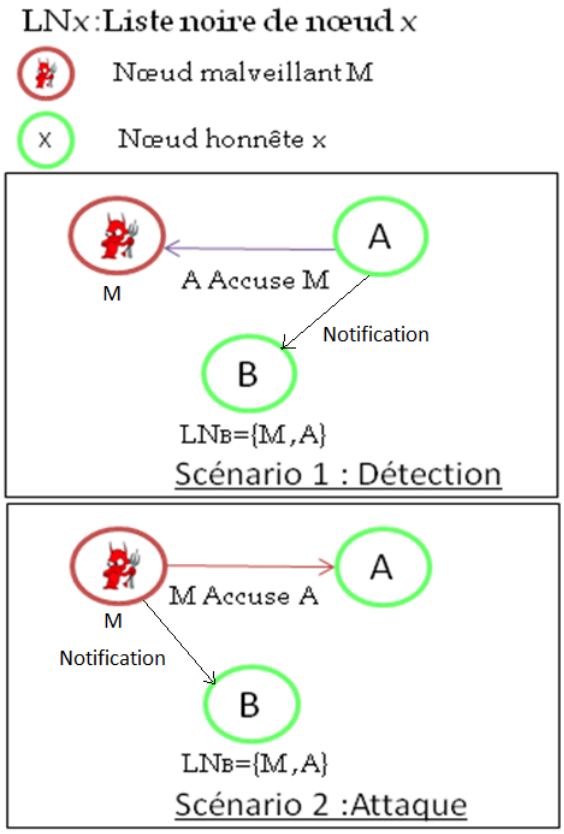


Figure 3.7 : La révocation par détection et attaque suicide

Dans le cas de la diffusion de plusieurs messages d'accusation simultanés accusant le même nœud, ceux ayant reçu ces messages ne doivent considérer que le dernier message reçu, et éliminer les anciens accusateurs de leurs listes noires.

3.5.3 Le système de révocation de Crépeau

Crépeau et al. [73] ont proposé un système de révocation qui prend en considération le contexte d'évolution des accusateurs. Il consiste à calculer le taux d'accusation Q d'un nœud qui sera révoqué si la valeur du taux dépasse un seuil prédéfini. Pour le calculer, les paramètres suivants sont nécessaires :

- A_i : le nombre des accusations contre le nœud i
- α_i: le nombre des accusations additionnelles émises par i.
- L'indice de comportement du nœud i (β_i) : l'indice de comportement du nœud i (β_i) a une valeur comprise entre 0 et 1. Il s'agit d'une mesure de comportement du nœud par rapport aux autres nœuds, et il est calculé de la manière suivante :

$$\beta_i = 1 - \lambda A_i$$

où $\lambda = \frac{1}{2N-3}$, où N est le nombre des nœuds dans le réseau.

- Le poids d'une accusation d'un nœud i (ω_i) : Le poids d'une accusation d'un nœud dépend de l'indice du comportement (β_i) et du nombre des accusations additionnelles du nœud i (α_i). ω_i est un nombre tel que $0 \leq \omega_i \leq 1$, il est calculé de la manière suivante:

$$\omega_i = \beta_i - \lambda\alpha_i$$

- Q_j le taux d'accusation du nœud j peut être calculé de la manière suivante :

$$Q_j = \frac{1}{N}\sum_{i=1}^{N} \sigma_{ij}\ \omega_i$$

Où $\sigma_{ij} = 1$ si le nœud i accuse le nœud j, ou $\sigma_{ij} = 0$ dans le cas contraire.

Le problème majeur de cette solution est toujours la présence d'un certain nombre d'attaquants qui pourraient causer la révocation de tous les nœuds du réseau.

Suivant l'auteur de cette technique, ce système de révocation est robuste contre les attaques pour chaque nœud j, si la condition suivante est vérifiée :

$$k \geq \frac{2 + \sqrt{4 + 8NQ_j(2N-3)}}{4}$$

Où k est le nombre des nœuds honnêtes.

3.5.4 Notre système de révocation ARS

Dans cette section, nous présentons notre système de révocation pour les réseaux MANETs ARS (Adaptive Revocation Scheme).

A. Description d'ARS

La plupart des systèmes de révocation existants sont basés sur un seuil prédéfini. Une configuration appropriée des nœuds malveillants peut conduire à révoquer tous les nœuds du réseau. De plus, l'augmentation de la valeur du seuil minimise les taux de détection, alors que la diminution de cette valeur conduit à la minimisation du nombre de messages d'accusation nécessaire à la vérification de la condition de révocation, d'une part, et à l'augmentation du nombre de nœuds faux-positifs (Des nœuds honnêtes qui sont révoqués par erreur), d'autre part. Un exemple d'approche de révocation qui minimise le seuil est la révocation par l'attaque suicide de Clulow et al. [71][72]. Dans cette approche un seul message d'accusation mène à la révocation de l'accusateur et de l'accusé. Cette approche, n'est pas préférable car aucun nœud ne veut sacrifier son existence dans le réseau. De plus, le réseau souffre de l'attaque des nœuds qui accusent et se déplacent afin de mettre en péril la disponibilité dans le réseau[74].

A cet effet, nous avons proposé le système hybride de révocation ARS[75] qui traite ce problème de manière rationnelle qui n'inflige aucune sanction aux nœuds accusateurs. En effet, l'objectif principal d'ARS est d'éviter l'épuisement des nœuds dans le réseau autant que possible afin qu'il soit possible d'assurer un certain niveau de disponibilité de service dans le réseau. Le principe de notre approche est de minimiser le nombre de nœuds révoqués autant que possible en rendant la condition de révocation plus difficile à satisfaire.

Supposons que $m \leq n/3$ où m est le nombre de nœuds malveillants et n le nombre de nœuds dans le réseau. Dans ARS, un nœud e est révoqué s'il y a un nœud a qui l'accuse et satisfait la condition suivante :

$$d(a) \leq d(e)$$

où $d(x)$ est la fonction de défiance qui est définie de la manière suivante :

$$d(x) = \alpha . A_x + \beta . B_x \qquad (3.1)$$

Avec A_x, B_x est le nombre d'accusations dans lesquelles x est respectivement accusateur et accusé. α et β sont deux nombres réels positifs. Il est clair que l'attribution d'une valeur élevée à α permet de réduire les chances d'accepter des accusations de nœuds qui émettent un nombre élevé d'accusations. Donc, elle augmente les risques de rejeter les accusations contre un grand ensemble de nœuds malveillants. Alors que l'augmentation de la valeur de β augmente les chances d'acceptation de n'importe quelle accusation, ce qui conduit à augmenter le taux de faux-positifs. Donc, les valeurs de α et β dépendent de l'application envisagée. Dans ce qui suit, nous considérons qu'ils ont la même pondération 1.

B. Analyse de sécurité

Nous avons vu que dans les autres systèmes de révocation certains ensembles de nœuds malveillants peuvent révoquer des nœuds autant qu'ils veulent. Dans cette section, nous allons voir à quel point ARS se défend contre les accusations falsifiées de nœuds malveillants.

Soit M l'ensemble de nœuds malveillants, et H l'ensemble de nœuds honnêtes, avec ($2|M|<|H|$). Suivant les valeurs de α et β adoptées, nous donnons les propriétés suivantes :

Propriétés 1 : *si un nœud malveillant m est accusé par plus de $2.|M|$ nœuds honnêtes, alors les accusations de m ne sont pas acceptées contre les nœuds honnêtes. De plus, n'importe quelle accusation contre m sera acceptée.*

Suivant la propriété 1, plus l'ensemble de nœuds malveillants est grand, plus un grand nombre de messages d'accusation est nécessaire, ce qui rend notre système adaptif. En effet, la révocation d'un nœud malveillant qui n'est pas en coalition avec d'autres nécessite un seul message d'accusation. Ce nombre de messages d'accusation peut être facilement atteint, ce qui rend le processus de révocation plus rapide. De plus, notre système est sûr s'il y a plus de $2.|M|$ nœuds honnêtes, ce qui signifie qu'un taux de nœuds honnêtes supérieur à 66,66% est nécessaire. Ceci est le taux minimum de nœuds honnêtes qui les rendrait capables de rejeter les messages d'accusation malveillants.

Propriété 2: *si un nœud malveillant m accuse plus de $2.|M|$ nœuds honnêtes, alors aucun message d'accusation de m n'est accepté, et n'importe quel message d'accusation contre m est accepté.*

Nous pouvons conclure d'après cette propriété que la falsification d'un grand nombre de messages d'accusation, conduit au rejet de ces accusations et à l'acceptation de n'importe quelle autre accusation contre les nœuds accusateurs.

Démonstration de la propriété 1 :

Soit $m \in M$ un nœud malveillant qui est accusé par plus de $2.|M|$ nœuds honnêtes.

Il existe deux cas :

Cas 1 : m accuse h, donc :

$$MIN|d(m)| = 2 \times |M| + 1 \qquad (3.2)$$

Cas 2 : m n'accuse pas h, donc :

$$MIN|d(m)| = 2 \times |M| \qquad (3.3)$$

le nombre maximum d'accusations contre un nœud honnête $h \in H$ est $|M|$ et le nombre maximum d'accusations émises par un nœud h est $|M|$. Donc, à partir de l'équation (3.1), nous avons :

$$MAX|d(h)| = 2 \times |M| \qquad (3.4)$$

A partir des équations (3.2) et (3.4), $\forall m \in M, h \in H, MAX|d(h)| < MIN|d(m)|$. Par conséquent, n'importe quel message d'accusation de m n'est pas accepté.

A partir des équations (3.3) et (3.4), $\forall m \in M, h \in H, MAX|d(h)| \leq MIN|d(m)|$. Par conséquent, n'importe quel message d'accusation contre m est accepté.

Démonstration de la propriété 2 :

Soit $m \in M$ un nœud malveillant qui accuse plus de $2.|M|$ nœuds honnêtes.

Soit h un nœud honnête, il y a deux cas :

Cas 1 : h accuse m, donc :

$$MIN|d(m)| = 2 \times |M| + 1 \qquad (3.5)$$

Cas 2 : h n'accuse pas m, donc :

$$MIN|d(m)| = 2 \times |M| \qquad (3.6)$$

Le nombre d'accusations contre un nœud honnête $h \in H$ est $|M|$ et le nombre maximum d'accusations émises par un nœud h est $|M|$. Donc, à partir de l'équation (3.1), nous avons :

$$MAX|d(h)| = 2 \times |M| \qquad (3.7)$$

A partir des équations (3.5) et (3.7), $\forall m \in M, h \in H, MAX|d(h)| < MIN|d(m)|$. Par conséquent n'importe quel message d'accusation de m est rejeté.

A partir des équations (3.6) et (3.7), $\forall m \in M, h \in H, MAX|d(h)| \leq MIN|d(m)|$. Par conséquent, n'importe quel message d'accusation contre m est accepté.

C. Résultats de simulation

Nous avons effectué les simulations en utilisant le simulateur NS2; les autres paramètres de simulation sont illustrés dans le tableau suivant :

Paramètre	Valeur
Portée d'antenne	250 m
Région de simulation	1500 m×1500 m
Modèle de mobilité	RWP (Randome Way Point)[76]
Fréquence de message d'accusation	Un message par seconde
Taux de nœuds malveillants	30%

Tableau 5: Paramètres de simulation d'ARS

La performance de notre système ARS est comparée à deux autres approches : un système de révocation simple à un seuil égal à 3 (3 accusations sont suffisantes pour révoquer un nœud), et le système de révocation par l'attaque suicide.

La Figure 3.8 montre le NRAM (*Number of required Accusation Messages*), qui est le nombre de messages requis pour la révocation d'un nœud, en terme de taux de nœuds honnêtes accusés. Nous remarquons que notre système surpasse le système de révocation simple, mais sa performance est inférieure à celle obtenue avec le système de révocation par l'attaque suicide qui donne de meilleurs résultats au détriment de sa vulnérabilité aux attaques.

Dans la même figure, nous remarquons aussi qu' avec un taux d'accusation supérieur à 25%, notre système adaptatif a réduit le NRAM, car il accepte les accusations contre les nœuds malveillants lorsqu'ils falsifient beaucoup d'accusations.

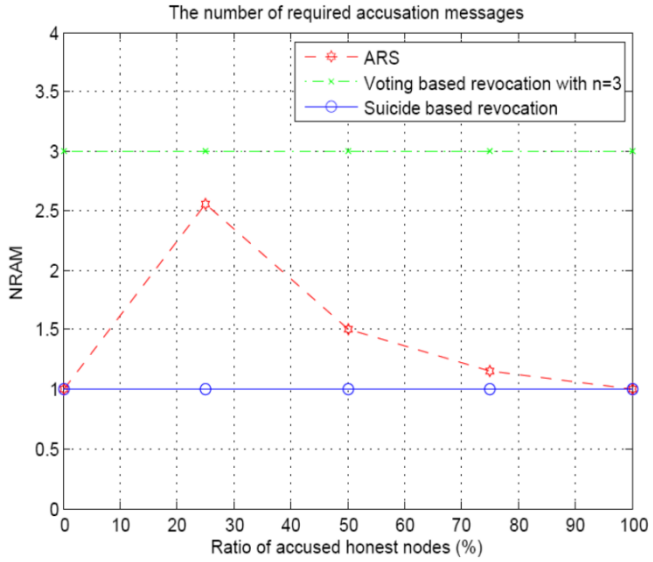


Figure 3.8 : NRAM en terme de taux nœuds honnêtes accusés

La Figure 3.9 montre le taux de faux-positifs en terme de taux d'accusation: nous remarquons que notre système ARS surpasse les autres systèmes de révocation au-delà du taux d'accusation 25%, car notre système refuse les accusations de nœuds malveillants et n'accepte pas les accusations falsifiées si elles sont nombreuses.

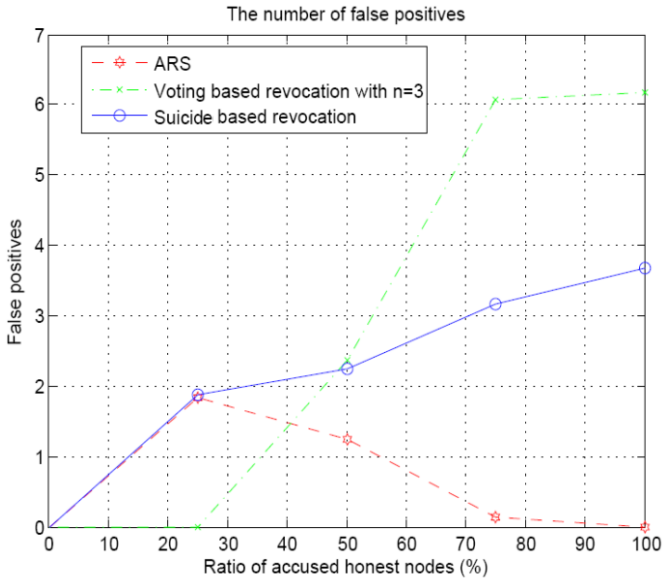


Figure 3.9 : Le taux de faux-positifs en terme de taux d'accusation

3.6 La révocation dans les VANETs

Les chercheurs ont proposé plusieurs systèmes de révocation qui sont une adaptation de ceux dans les MANETs. Dans ce qui suit, nous donnons quelques techniques existant dans la littérature.

3.6.1 Le système de révocation LEAVE

Le système de LEAVE (Local *Eviction of Attackers by Voting Evaluators*), est un système proposé par Raya et al.[77]. Ce système consiste à minimiser les poids des accusations des nœuds suivant le nombre d'accusateurs. Ces poids sont calculés de la manière suivante :

$$W_i = 1 - \frac{A_i}{P_i}$$

P_i est le nombre de voisins communs à l'évaluateur et au nœud évalué.

A_i le nombre total des accusations contre le nœud i.

Le taux d'accusation est calculé comme suit :

$$Q_j = \frac{1}{P_j} \sum_{i=1}^{P_j} W_i . \delta_{i,j}$$

Où $\delta_{i,j}$=1 si le nœud i accuse le nœud j, $\delta_{i,j}$=0 dans le cas contraire.

La figure suivante montre l'organigramme qui montre le fonctionnement de cette technique :

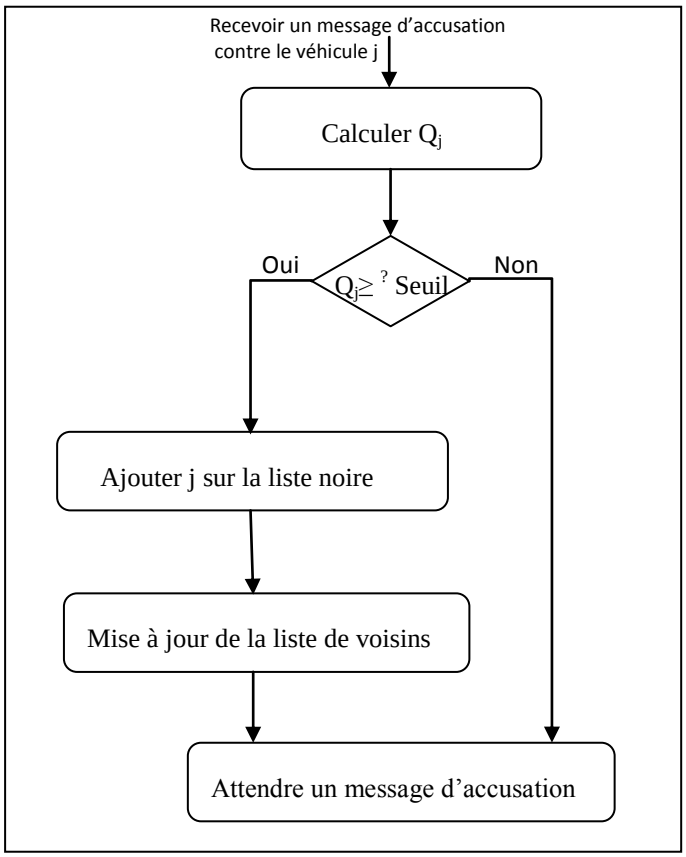


Figure 3.10 : L'organigramme de la technique de révocation de LEAVE

3.6.2 Le système Stinger

Ce système de révocation a été proposé par Moore et al. [74] : il consiste à adapter la stratégie de révocation par attaque suicide au réseau VANET. Dans Stinger, les nœuds qui émettent des messages Sting (c'est l'équivalent des messages d'accusation dans le système de révocation par attaque suicide) et les nœuds accusés sont pénalisés seulement pour une durée limitée afin de défendre aux attaques des accusations falsifiés.

La figure ci-dessous montre l'attaque des accusations falsifiées contre le système de révocation Stinger. Dans cette attaque, le nœud malveillant M provoque les nœuds honnêtes d'une région d'émettre des messages Sting afin de forcer la révocation des nœuds honnêtes (dans l'exemple, les identifiants de A et M sont ajoutés à la liste noire des nœuds B et C). Ensuite, le nœud malveillant M se déplace vers une autre région et répète le même scénario d'attaque afin de provoquer la révocation d'autres nœuds honnêtes. Mais, le mécanisme de révocation temporaire utilisé par Stinger permet de réduire l'impact de cette attaque.

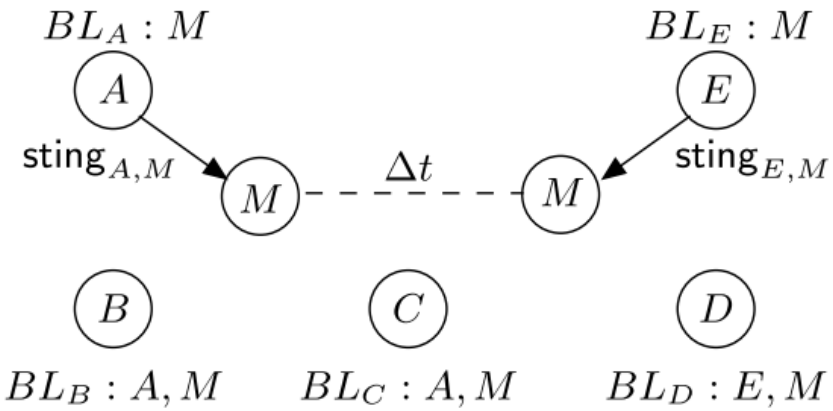


Figure 3.11: Attaque contre le système Stinger[74]

3.6.3 Le système SLEP

Le système de révocation SLEP[67] (Suicide-based Local Eviction Protocol) est une variante adaptée aux réseaux VANET de système du révocation par attaque suicide. Dans ce système, les deux nœuds accusateur et accusé sont ajoutés à la liste noire. Cependant, ce système dispose d'un mécanisme pour réduire le taux de faux-positifs. En effet, les auteurs ont introduit le mécanisme du backoff[78] afin d'éviter les accusations non nécessaires. Après la détection d'un comportement malveillant, les nœuds doivent attendre un délai aléatoire τ avant de diffuser le message d'accusation. Cela permet de réduire les chances d'avoir deux nœuds sur la liste noire à cause de leurs accusations par un seul nœud malveillant.

La Figure 3.12 montre le format de message de ce système, il contient les clés publiques de l'accusateur et de l'accusé, l'instant de l'accusation, la cause, et la signature numérique.

PID of accused node	PID of accuser	Time	Reason	Signature of accuser

Figure 3.12: Le format de message d'accusation de SLEP[67]

3.7 Etude comparative

L'analyse de performance d'une technique de révocation doit être effectuée suivant certains critères, la dégradation de l'un de ces critères peut influencer sur l'autre. Le tableau suivant résume les performances des techniques de révocation précédentes en termes de ces critères:

1. **Le traitement et l'overhead des messages d'accusation**: le nombre de cycles d'horloge et la bande passante consommée sont deux aspects importants afin d'étudier la performance. Trois possibilités pour ce critère : élevé, moyen et faible, elles sont données comme suit :

- **Elevé** : si le traitement des messages d'accusation nécessite un nombre élevé de cycles d'horloge, et ces messages épuisent excessivement la bande passante.
- **Moyen** : si seulement l'un des deux métriques : le traitement et la consommation de la bande passante est élevé.
- **Faible** : si les deux le traitement et la consommation de la bande passante sont faibles.

2. **NNMA (le Nombre Nécessaire de Messages d'Accusation pour la révocation)** : chaque technique de révocation a son propre approche pour ajouter un nœud malveillant sur la liste noire. Suivant cette approche, un certain nombre de message d'accusation est nécessaire pour révoquer un nœud.
3. **L'impact de l'attaque de FMA (Falsification de Messages d'Accusation)** : les nœuds malveillants en coalition peuvent falsifier les messages d'accusation afin de dégrader la performance en provoquant la révocation des nœuds honnêtes. L'impact est sévère si la stratégie ne dispose pas des moyens permettant aux nœuds honnêtes de réduire l'impact des messages d'accusation malveillants et il est faible s'il y a des forts mécanismes permettant de filtrer les messages d'accusation malveillants. Cependant, l'impact est moyen s'il existe des mécanismes permettant de réduire les poids associés aux messages d'accusation.
4. **Le mécanisme de pénalisation** : les techniques de révocation peuvent adopter deux différentes approches pour la sanction infligée à un nœud malveillant, l'identifiant des nœuds malveillants peut être marqué comme invalide de manière temporaire ou permanente.
5. **La stratégie de révocation** : la procédure nécessaire pour marquer un nœud malveillant est importante pour évaluer la performance d'une technique de révocation. Les nœuds peuvent être révoqués suivant les stratégies suivantes :
   - **Le Système de Vote (SV)**: il consiste à compter le taux des nœuds qui accuse un nœud malveillant et le révoquer si le taux dépasse un seuil prédéfini.
   - **Accusations pondérées**: c'est une variante de la stratégie précédente dans laquelle le taux d'accusation est la moyenne pondérée des accusations des nœuds.
   - **Attaque suicide** : c'est la variante la plus simple de révocation dans laquelle une seule accusation est suffisante pour éliminer le nœud accusateur et le nœud accusé.
6. **L'architecture de révocation** : L'architecture est centralisée si la révocation nécessite la communication avec une entité prédéfinie (l'autorité de certification via les RSUs, par exemple). L'architecture est décentralisée si un ou plusieurs nœuds peuvent révoquer un nœud sans l'intervention d'aucune entité prédéfinie.

	Overhead	NNMA	Impact de FMA	Mécanisme de pénalisation	Stratégie de révocation	Architecture
LEAVE[77]	Elevé	Elevé	Faible	Permanent	Accusations pondérées	Décentralisée
SLEP[67]	Faible	Bas	Moyen	Temporaire	Attaque Suicide	Décentralisée
Stinger[74]	Faible	Bas	Elevé	Temporaire	Attaque Suicide	Décentralisée
Qianhong et al.[79]	Moyen	Moyen	Moyen	Temporaire	SV	Centralisée

Tableau 6: Etude comparative des protocoles de révocation dans les VANETs

Le Tableau 6 présente une étude comparative entre les protocoles de révocation dans les VANETs. En ce qui concerne le système de révocation de LEAVE, il utilise la signature numérique pour chaque message d'accusation ce qui cause un overhead élevé pour le traitement et la bande passante consommée en cas d'attaque. L'avantage de LEAVE est l'utilisation d'un système de pondération très efficace contre la falsification des messages d'accusation. En effet, considérant le cas d'une observabilité très élevée (Les nœuds honnêtes accusent la plupart des nœuds malveillants) et un taux de nœuds malveillant égal à x, Raya et al. [77] ont montré que le système est protégé contre l'attaque de falsification de message pour un seuil inférieur x^2, alors que le seuil doit être supérieur à x si les nœuds honnêtes ne peuvent pas envoyer des messages d'accusation. D'autre part, le même mécanisme aura un impact négatif sur le taux de détection et le NNMA. En effet, les messages d'accusation falsifiés des nœuds malveillants réduisent les poids de messages d'accusation des nœuds honnêtes, et conséquent un NNMA élevé est nécessaire.

Le système de révocation Stinger nécessite peu de traitement pour faire une décision de révocation, car il basé sur le principe de l'attaque suicide. De plus, les nœuds diffusent les messages Sting que pour une durée limitée.

Le système de révocation de Qianhong et al. est un système de révocation basé sur le SV (plusieurs seuils sont possibles selon le contexte), donc le NNMA nécessaire est moyen et l'impact de FMA est moyen. L'overhead est moyen car les auteurs ont proposé des mécanismes de traitement par lôts pour réduire la complexité de calcul introduit par l'utilisation de la cryptographie bilinéaire[2][80][81].

[2] La cryptographie bilinéaire est une nouvelle approche qui permet de générer et de vérifier la signature numérique offline sans avoir besoin de certificats numériques[170][171].

Le système SLEP qui est une variante de système de révocation par attaque suicide pour les VANETs présente pratiquement la même performance de Stinger. Mais, vu que SLEP utilise le mécanisme de backoff, cela permet de réduire le taux de faux-positifs d'une part , et augmente le délai de détection d'autre part.

3.8 Conclusion

Dans ce chapitre, nous avons présenté les différentes techniques pour la détection et la révocation des nœuds malveillants. Les techniques de révocation sont centralisées si la station de base est nécessaire pour la révocation, et elles sont distribuées si les nœuds honnêtes collaborent pour exclure les nœuds malveillants. Nous avons aussi proposé un nouveau protocole ARS qui consiste à révoquer les nœuds de manière adaptative. En effet, le taux de faux-positifs et le taux de détection est dépendant du nombre de nœuds malveillants. Enfin, nous avons présenté une étude comparative entre les différentes techniques de révocation de nœuds malveillants.

Chapitre 4

Le système de révocation SDRP

4.1 Introduction

SDRP (*Secure Distributed Revocation Protocol*) est un système de révocation aux réseaux VANET que nous avons proposé et qui est conçu pour assurer le bon acheminement de données.

Dans cette section, nous commençons par donner une description exhaustive du modèle utilisé pour empêcher les attaques et rendre le processus de routage plus efficace. Ensuite, nous décrivons le modèle d'adversaire adopté, suivi de la description de SDRP et de l'analyse de sa performance.

4.2 Protocole de routage par la révocation

Dans les VANETs, les nœuds peuvent échanger des messages liés à la sécurité en utilisant un protocole de routage sécurisé similaire à celui présenté dans[82]. Mais, celà ne peut pas empêcher de sélectionner les nœuds malveillants comme relais. En outre, en raison de la grande mobilité des nœuds, le nœud relais sélectionné suivant la stratégie de routage, peut être différent pour chaque paquet à transmettre. Par conséquent, identifier tous les nœuds malveillants à la fois pourrait considérablement dégrader la performance du système. Pour cette raison, le protocole de routage doit coopérer avec le système de révocation, comme illustré dans l'algorithme suivant :

```
1: function Route(Neighborslist: Set of nodes, P:packet):
Boolean;
 2:  while Neighborslist ≠ Φ do
 3:   x=Select_candidate_node(Neighborslist);
 4:   Neighborslist=Neighborslist−{x};
 5:   if MALICIOUS(x)=false then
 6:     send(p);
 7:     return true;
 8:   end if
 9:  end while
10:  return false;
11: end function
12:
13:
14: function Malicious (x:node):Boolean;
15:  if x∈Blacklist then
16:    return true;
17:  end if
18:  if x is malicious then
19:    Blacklist=Blacklist∪{x};
20:    return true;
21:  end if
22:  return false;
23: end function
```

Algorithme du routage sécurisé [83]

Pour relayer un paquet, le module de routage doit sélectionner un nœud x parmi les voisins. Comme certains messages sont liés aux applications temps réel (par exemple, les messages liés à la sécurité routière), le paquet peut être transmis à x avant l'évaluation. Ensuite, le SDRP doit évaluer x et décider s'il est malveillant ou non. Si x est considéré comme honnête, la transmission du paquet est considérée correcte. Sinon, le module de routage doit choisir un autre nœud candidat qui retransmettrait le paquet. Le système sécurisé doit être capable de détecter la plupart des attaques contre le processus de routage à travers des mécanismes de détection d'intrusion et de vérification de position (voir section 3.2) qui permettent de contrôler la stratégie d'acheminement de paquets. En effet, les nœuds peuvent injecter, modifier ou voire même empêcher l'acheminement de paquets.

4.3 Le modèle d'adversaire

L'objectif principal de notre système proposé est d'exclure les nœuds malveillants de l'opération de routage dans les VANETs. Les nœuds malveillants peuvent être considérés comme nœuds contrôlés par des entités égoïstes ou malveillantes, ou des nœuds ayant des équipements défaillants. Dans le système SDRP, nous considérons le pire des cas de nœuds malveillants, qui sont définis comme des nœuds compromis contrôlés par des attaquants malveillants en coalition. Nous supposons que ces nœuds malveillants sont en mesure de communiquer entre eux, ce qui

signifie qu'ils sont capables de coordonner leurs attaques pour empêcher l'acheminement de messages vers leurs destinations. Ces attaques peuvent être classées en deux catégories principales: les attaques contre le protocole de routage et les attaques visant à exclure un grand nombre de nœuds honnêtes du réseau, et donc à réduire les chances de transmettre correctement les messages de sécurité.

4.4 Une vue d'ensemble du système

Notre système comprend trois modules : MDM (*Misbehaviour Detection Module*),APM (*Accusation Processing Module*) et NAM (*Neighbors' Advertiser Module*).

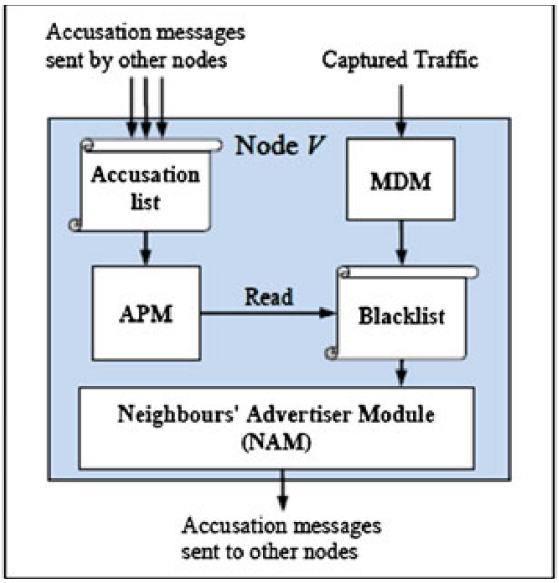


Figure 4.1 : Vue d'ensemble de SDRP [83]

La Figure 4.1 montre ces modules et leurs interactions. Le MDM consiste à utiliser un système de détection d'intrusion qui analyse les activités de tous les nœuds dans sa zone radio permettant ainsi de détecter les nœuds malveillants en utilisant le mode indiscriminé[62]. Il permet d'éviter les nœuds relais malveillants en utilisant une base de données de signatures d'attaque. Dans le cas ou un nœud malveillant M est détecté, ce module doit l'ajouter sur la liste noire. Donc, les messages de M seront ignorés par le nœud vérificateur e, et par conséquent il ne sera plus sélectionné comme relais. Afin d'avertir les nouveaux voisins, le nœud e doit utiliser le NAM qui doit périodiquement réémettre un message d'accusation signé qui inclut les identifiants de tous les nœuds détectés. Suivant le contenu de ces messages, tous les nœuds voisins récepteurs doivent mettre à jour le contenu de leurs listes d'accusations. Ces dernières joueront un rôle primordial, car les APMs les utilisent pour calculer le taux d'accusation qui entraîne la révocation du nœud évalué s'il dépasse un certain seuil.

4.5 Méthode de révocation

La plupart des solutions de révocation existantes utilisent tous les messages d'accusation émis contre un nœud pour calculer le taux d'accusation. Dans notre solution, nous ne les utilisons pas tous, nécessairement, parce qu'une partie d'entre eux pourrait être émise par des nœuds malveillants. Par conséquent, nous avons développé une nouvelle fonction, appelée Rev, qui est utilisée pour détecter et filtrer les messages d'accusation des nœuds malveillants et de les exclure du calcul du taux d'accusation. Un message d'accusation est considéré comme suspect si la fonction attribue au nœud accusateur une valeur inférieure à celle attribuée au nœud accusé.

A. La fonction de filtrage

Avant de définir la fonction de filtrage, nous devons être en mesure de faire la distinction entre les accusations d'un nœud malveillant et de celle d'un nœud honnête. A cet effet, nous avons considéré deux situations:

1) Le nombre de nœuds malveillants n'est pas suffisant pour révoquer un nœud honnête.
2) Le nombre de nœuds malveillants est suffisant pour révoquer n'importe quel nœud voisin.

Dans le premier cas, les nœuds malveillants ne sont pas en mesure de révoquer tous les nœuds honnêtes en falsifiant les accusations; ils sont seulement en mesure de lancer des attaques ordinaires qui peuvent être détectées par le MDM telles que la suppression des paquets à transmettre. Pour détecter les attaques en coalition dans ce cas, nous définissons la fonction de similarité inspirée du caractère humain, qui considère une personne semblable à une autre si elles ont des comportements similaires. Soit c le nœud relai candidat et $N_{c,e}$ l'ensemble de voisins commun à c et le nœud évaluateur e (nœud exécutant la procédure de vérification), et A_x l'ensemble des nœuds accusés par le nœud x et E l'ensemble des accusations telles que $(x, y) \in E$ signifie que y est accusé par x ; donc, la similarité entre deux nœuds peut être exprimée de la manière suivante :

$$\boldsymbol{SIM}(\boldsymbol{x}, \boldsymbol{y}) = \left|\boldsymbol{A_x} \cap \boldsymbol{A_y}\right| + \left|\overline{\boldsymbol{A_x}} \cap \overline{\boldsymbol{A_y}}\right| \qquad (4.1)$$

où

$A_x = \{y \in N_{c,e} \,/(x, y) \in E \ \}$

$\overline{A_x} = \{y \in N_{c,e} \,/(x, y) \notin E \ \}$

A partir de l'équation (4.1), il est clair qu'une similarité complète entre deux nœuds signifie qu'ils évaluent tous les nœuds voisins de la même manière. Pour rendre l'équation (4.1) plus pertinente, il est nécessaire que le nœud en cours d'évaluation doit avoir une grande similarité avec la plupart des nœuds, parce que les nœuds honnêtes en représentent la majorité. Par conséquent, en présence de plusieurs nœuds voisins, l'équation (4.1) peut être réécrite comme suit:

$$sim(x) = \frac{1}{\left|N_{c,e}\right|^2} \sum_{y \in N_{c,e} - \{x\}} \left|A_x \cap A_y\right| + \left|\overline{A_x} \cap \overline{A_y}\right| \qquad (4.2)$$

Dans le deuxième cas, le nombre de nœuds malveillants qui falsifient les accusations, est suffisant pour révoquer les nœuds voisins. La situation sera plus grave si les nœuds malveillants sont indétectables par le MDM. Donc, c'est le rôle de l'APM qui doit empêcher la révocation d'un grand nombre de nœuds honnêtes.

Maintenant, supposons qu'un nœud z accuse un nœud honnête et en même temps génère des accusations nombreuses. Donc, le nœud z doit être pénalisé en prenant son $|A_z|$ pour accroître la crédibilité du nœud x qu'il accuse (x est un nœud que nous mesurons sa crédibilité). Mais, lorsque le nœud x n'est pas accusé par z, nous prenons sa $|\overline{A_z}|$ (plus z accuse, plus il augmente la crédibilité des nœuds accusés). Par conséquent, nous définissons comme suit la fonction de la crédibilité $Cred(x)$ qui prend en compte deux cas : dans le premier cas, un nœud x en cours d'évaluation est supposé être accusé par un nœud z donné, et dans le deuxièmes cas, x n'est pas accusé $(z, x) \notin E$. L'expression de cette fonction peut être écrite de la manière suivante :

$$Cred(x) = \frac{1}{|N_{c,e}|^2}\left[\sum_{z \in N_{c,e}, (z,x) \in E} |A_z| + \sum_{z \in N_{c,e}, (z,x) \notin E} |\overline{A_z}|\right] \qquad (4.3)$$

Maintenant, il est clair que la fonction Sim donne un poids élevé aux messages d'accusation émis par les nœuds honnêtes et que la fonction $Cred$ rejette les messages d'accusation de nœuds malveillants en coalition. Nous définissons la fonction composite Rev, qui prend en compte à la fois les évaluations de Sim et $Cred$ comme suit:

$$Rev(x) = \alpha . Sim(x) + \beta . Cred(x) \qquad (4.4)$$

Où $\alpha + \beta = 1$

L'attribution d'une valeur supérieure à α conduit à un mode de révocation d'un nœud nécessitant peu de messages d'accusation, alors qu'une valeur plus élevée de β conduit à un mode de révocation avec un faible risque de faux-positifs. Par conséquent, la spécification des meilleures valeurs de α et β est en fin de compte liée à la stratégie d'attaque. Nous présentons dans ce qui suit une proposition indiquant comment faire face aux attaquants qui changent leurs stratégies d'attaques au cours du temps. Un mécanisme typique de défense contre ces attaquants nécessite de changer les valeurs de α et β en temps réel dans le but de maximiser la sécurité du système. Ceci peut être obtenu efficacement en contrôlant le taux de nœuds voisins sur la liste noire. Si ce rapport dépasse un seuil prédéfini (en fonction de la qualité de service requise), il est obligatoire de changer la valeur de β comme suit:

$$\beta = \left(\frac{|BL|}{Nb}\right)^{\theta} \qquad (4.5)$$

BL est l'ensemble des nœuds sur la liste noire, Nb le nombre de nœuds voisins et θ est supérieur à 1, si un taux de détection élevé est nécessaire, ou inférieur à 1 (et supérieur à zéro) si la minimisation du taux de faux-positifs est nécessaire.

B. Procédure de révocation

Dans cette section, nous décrivons comment un nœud est révoqué. Un nœud évaluateur e qui évalue un nœud candidat c sélectionné par le protocole de routage sécurisé, exécute la procédure de révocation suivant l'algorithme de la section 4.2. Soit L_C l'ensemble des nœuds accusateurs du nœud candidat c. La procédure de révocation consiste à calculer le taux d'accusation Q_C de ce dernier, si le taux dépasse un seuil prédéfini Th. Dans ce cas, le nœud candidat c est considéré comme malveillant ou compromis et doit donc être révoqué. Le calcul de Q_C est effectué grâce à l'utilisation de la fonction de révocation Rev qui doit être utilisée pour chaque nœud accusateur a appartenant à $N_{c,e}$, de telle manière que chaque élément a de L_C doit vérifier la condition suivante :

$$Rev(a) \geq Rev(c) \qquad (4.6)$$

Le taux d'accusation Q_C est défini comme suit :

$$Q_C = \frac{|L_C|}{N_{c,e}} \qquad (4.7)$$

L'algorithme suivant décrit la procédure de révocation :

```
1: v: Evaluator node
2: c: Evaluated node
3: Th: Revocation threshold
4: Qc: Accusation quotient of node c
5: Lc: List of accusers of c
6: function REVOCATION_PROCEDURE(v, c)
7:   Qc = ACCUSATION_QUOTIENT(c)
8:   if Qc > Th then
9:     revoke(c)
10:  end if
11: end function
12:
13:
14: function ACCUSATION_QUOTIENT(c):real
15:   Establish the list Lc of accusers of c
16:   for a ∈ Lc
17:     if a ∉ Nc, v ∨ (Rev(a) Rev(c)) then
18:       Lc = Lc − a
19:     end if
20:   end for
21:   Qc=|Lc|/|Nc,v|
22: end function
```

Algorithme de révocation [83]

4.6 Exemple de révocation par SDRP

Pour illustrer le fonctionnement de la procédure de révocation, nous prenons l'exemple suivant: considérons deux ensembles de nœuds dénotés par l'Ensemble1 et l'Ensemble2. L'Ensemble1 comprend deux nœuds malveillants marqués, respectivement, 1 et 2, (cf. Figure 4.2), et l'Ensemble2 comprend des nœuds honnêtes. Chaque paire de nœuds de l'union de deux ensembles sont voisins. Nous remarquons que tous les nœuds de l'Ensemble1 génèrent des messages d'accusation contre tous les nœuds de l'Ensemble2. La Figure 4.2 représente le graphe d'accusation, où une flèche partant d'un nœud de l'Ensemble1 et arrivant à un autre de l'Ensemble2 représente une accusation. Supposons que le MDM de nœuds honnêtes ne peut pas détecter les activités malveillantes, et donc, ils ne génèrent aucun message d'accusation. Maintenant, considérons le scénario dans lequel le nœud 4 est un nœud candidat sélectionné par le protocole de routage, SDRP permet donc d'évaluer l'honnêteté du nœud 4 en utilisant la fonction de révocation. Il est à noter que l'accusation par un nœud x contre le nœud 4 ne sera pas acceptée que si $Rev(x) \geq Rev\ (4)$. Mais, tout d'abord, nous devons calculer les deux fonctions (Sim et $Cred$) constituant la fonction de révocation.

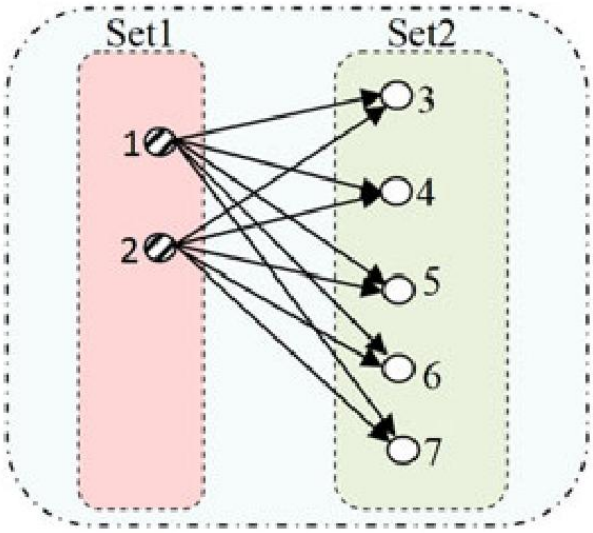


Figure 4.2 : Illustration du graphe d'accusation

1) **Le calcul de la similarité (la fonction Sim):** à partir du graphe d'accusation, en utilisant l'équation (4.2), le nœud 4 a gagné une valeur de similarité considérable en raison du fait qu'il a un comportement accusateur similaire à quatre nœuds qui représentent la majorité de ces derniers. Ce qui peut être exprimée par :

$$\begin{cases} A_4 = A_3 = A_5 = A_6 = A_7 = \emptyset \\ \overline{A_4} = \overline{A_3} = \overline{A_5} = \overline{A_6} = \overline{A_7} \end{cases}$$

2) **Le calcul de la crédibilité (la fonction $Cred$):** Puisque les nœuds 1 et 2 accusent la majorité des autres nœuds, la fonction de la crédibilité (voir l'équation (4.3)) attribue des valeurs

élevées aux nœuds accusés 3, 4, 5, 6 et 7. Ces valeurs augmentent la crédibilité par le nombre de messages d'accusation émis par le nœud 1 et le nœud 2.

Après le calcul de la fonction Sim et la fonction $Cred$, la fonction Rev attribue aux noeuds 1 et 2 des valeurs inférieures à celles des autres. Ce qui mène à rejeter les accusations des nœuds malveillants 1 et 2.

4.7 Analyse de complexité de SDRP

L'analyse de complexité de n'importe quel algorithme est importante, car elle fournit des estimations de ressource nécessaire et de temps de réponse. Considérons un nœud évaluateur e et un nœud candidat c, en utilisant les équations (4.2) et (4.3) (voir section 4.5), nous pouvons vérifier que la complexité de Sim et $Cred$ est $\mathcal{O}(n)$, où n est le nombre de voisins communs à e et c, et par conséquent la complexité de la fonction Rev qui est la somme pondérée de Sim et $Cred$ est également $\mathcal{O}(n)$. De plus, la fonction de révocation (voir l'algorithme de révocation précédent) exécutée par le nœud évaluateur e pour chaque nœud accusateur du nœud c appartenant à $N_{e,c}$ est $\mathcal{O}(n^2)$.

4.8 Evaluation de performance de SDRP

A. Environnement de simulation

Dans cette section, nous décrivons et analysons les résultats de performance obtenus par les différents scénarios de simulations de SDRP. Nous avons effectué toutes les simulations en utilisant le simulateur NS2. Tous les paramètres utilisés dans les simulations sont résumés dans le tableau suivant :

Paramètre	Valeur
La portée d'antenne	300 m
La couche MAC	802.11P
Modèle de mobilité	Freeway
Caractéristiques de l'autoroute	5 km longueur (3voies/Direction)
Nombre de nœuds	300
Durée de simulation	15 mn
Fréquence de messages d'accusation	1 message/s
Taux de nœuds malveillants	30%
Valeur de α et β	0,5 - 0,5
Seuil de révocation	0,25 - 0,5

Tableau 7 : Paramètres de simulation de SDRP

Pour évaluer l'efficacité de SDRP, nous avons considéré les deux métriques suivantes:

1. Le taux d'acheminement de paquets PDR (*Packet delivery ratio)*: il représente la proportion des paquets de données reçus par les nœuds destinataires.
2. Le délai de bout en bout EED (End-to-End Delay): il représente le temps moyen d'acheminement de paquets de bout en bout.

Les paquets dans le réseau sont acheminés suivant la stratégie gloutonne géographique, c'est-à-dire les relais sélectionnés sont ceux les plus proches de la destination. Nous supposons que les nœuds honnêtes sont capables de générer un message d'accusation contre un nœud malveillant voisin avec une probabilité uniforme égale à 0,8. Pour avoir une bonne idée sur la performance du réseau, nous avons considéré deux scénarios d'attaques de nœuds malveillants :

1. Scénario d'attaques isolées: dans ce scénario, chaque nœud malveillant envoie des messages d'accusation falsifiés contre ses voisins, indépendamment des autres nœuds malveillants.
2. Scénario d'une attaque coordonnée: dans ce scénario, les attaquants ne devraient pas accuser un nombre élevé de nœuds afin d'éviter d'être détectés et révoqués facilement, mais ils ont tendance à coordonner leurs attaques et accusent seulement un ensemble spécifique de nœuds honnêtes.

B. Résultats de simulation

a. Le taux d'acheminement de paquets

1. Tout d'abord, nous évaluons le PDR en changeant la proportion des nœuds accusés dans le cas d'attaques isolées. La Figure 4.3 montre que sans SDRP, le PDR diminue à moins de 10% pour une proportion de nœuds malveillants qui ne dépasse pas 10%, et atteint 0% au-delà 25% de nœuds malveillants. Mais, avec l'utilisation de SDRP, le PDR atteint 85% en présence de 10% de nœuds malveillants et dépasse toujours 38%, même en présence de 30% de nœuds malveillants dans le réseau.
2. Deuxièmement, nous considérons une attaque coordonnée dans laquelle nous changeons la proportion de nœuds honnêtes accusés par les nœuds malveillants qui sont en coalition, et nous mesurons le PDR dans ce cas en ajustant le rapport de nœuds accusés.

   Les résultats de simulation présentés dans la Figure 4.4 montrent que, en présence de 30% des nœuds malveillants en coalition, le PDR décroit pour un taux des nœuds accusés allant de 0% à 50%, puis il augmente à nouveau pour un pourcentage des nœuds accusés supérieur à 50%. Celà est dû au fait que l'APM a pu détecter la plupart des nœuds malveillants et de les révoquer car il y a une minorité de nœuds malveillants qui accusent les nœuds honnêtes qui

constituent la majorité dans le réseau. Il est aussi à noter que SDRP a donné des taux de détection considérables en présence d'un taux inférieur à 30% de nœuds malveillants.

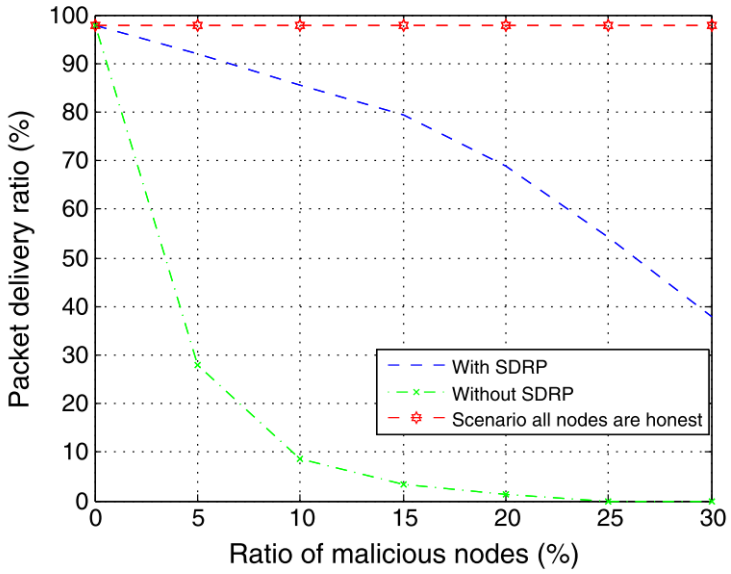


Figure 4.3 : L'impact de taux des nœuds malveillants sur le PDR

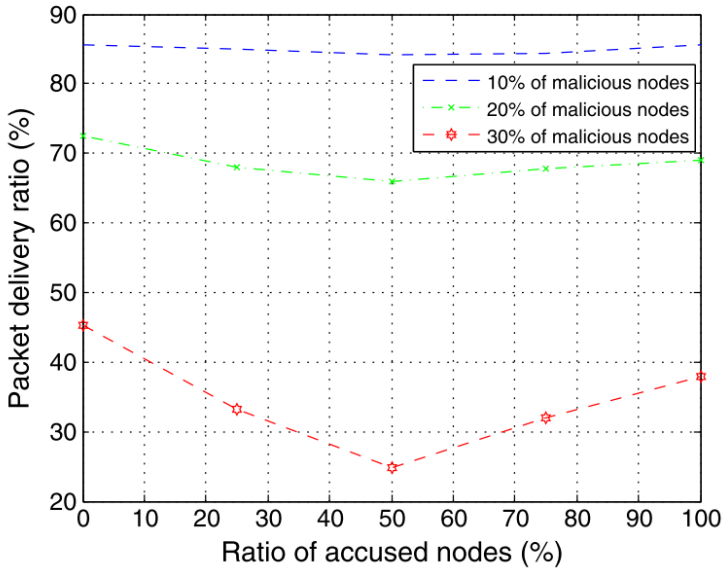


Figure 4.4 : L'impact de taux des nœuds accusés sur le PDR

b. Le délai d'acheminement de paquets de bout en bout

1. La Figure 4.5 montre que l'EED augmente avec l'augmentation du taux de nœuds malveillants qui éliminent les paquets qu'ils sont censés acheminer (Scénario d'attaque isolée). Ceci est principalement dû au fait que l'augmentation du taux de nœuds malveillants réduit la probabilité de trouver un nœud relai honnête proche de la destination (suivant la stratégie de routage géographique gloutonne); ce qui augmente donc le nombre de sauts nécessaires à l'acheminement des paquets et l'EED correspondant.
2. Dans le scénario d'attaque coordonnée, la Figure 4.6 montre que les nœuds malveillants sont capables de diminuer la performance du système de révocation (augmenter considérablement le délai d'acheminement de bout-en-bout) s'ils ne falsifient pas un grand nombre de messages d'accusation contre les nœuds honnêtes. Pour une proportion de nœuds accusés variant de 0% à 50%, l'EED augmente toujours. Mais, pour un taux supérieur à 50%, il diminue grâce au module APM, qui exécute la procédure de révocation et empêche les attaques DoS. Dans la même figure, nous remarquons également que le taux de nœuds malveillants peut considérablement augmenter l'EED: Par exemple, en présence de 30% de nœuds malveillants il augmente de 0,067 s à 0,1 s.

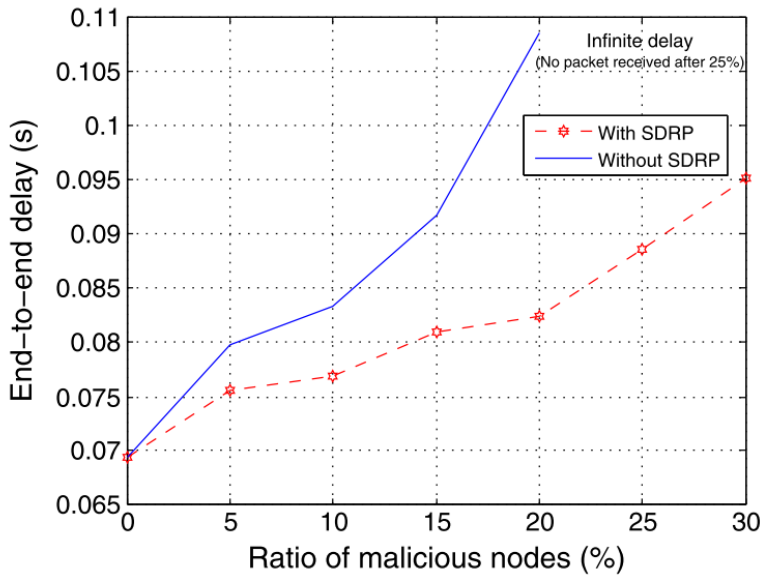


Figure 4.5 : L'impact de taux de nœuds malveillants sur l'EED

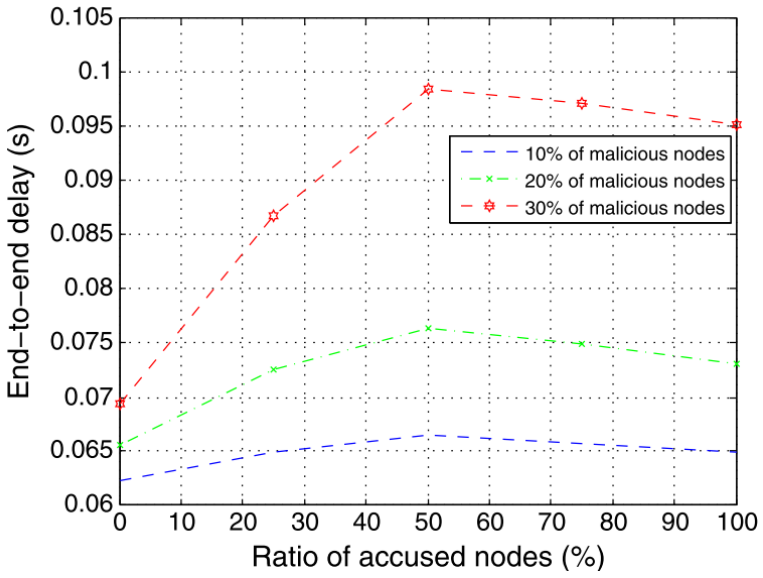


Figure 4.6 : L'impact de taux des nœuds accusés sur l'EED

c. L'impact des facteurs de pondération

Dans les scénarios de simulation précédents, nous avons mis les valeurs de α et β à 0,5. Maintenant, nous analysons l'impact de changement de leurs valeurs sur la performance du système.

Nous avons déjà proposé une méthode pour ajuster les valeurs de α et β de façon adaptative (voir équation (4.5)). Pour déterminer l'impact d'un choix spécifique de valeurs des facteurs de pondération sur la performance, nous avons considéré les deux métriques suivantes :

- Le taux de détection DR (*Detection rate*) : il indique le pourcentage de nœuds compromis détectés.
- Le taux de faux-positifs FPR (*false positive rate*) : il indique le pourcentage de nœuds honnêtes qui sont considérés à tort comme des nœuds compromis.

Nous avons changé les valeurs de α et β comme illustré dans le tableau suivant :

α	β	Taux de détection %	Taux de faux-positifs %
0	1	5,41	0
0,25	0,75	39,42	0,01
0,5	0,5	86,71	0,14
0,75	0,25	95,38	7,98
1	0	99,89	33,27

Tableau 8 : L'impact de changement de α et β sur la performance de SDRP

Nous remarquons que les taux de détection augmentent avec l'augmentation de α (ou diminution de β) car la fonction Sim a plus de poids que la fonction $Cred$. Alors que β réduit le taux de faux-positifs, à cause du poids élevé associé à la fonction $Cred$.

d. Comparaison avec d'autres systèmes de révocation

Pour mieux évaluer l'efficacité de SDRP, nous avons choisi de comparer sa performance avec d'autres systèmes proposés. Nous avons considéré le système de révocation de Crépeau (voir section 3.5.3) et LEAVE (voir section 3.6.1).

Pour une comparaison équitable entre ces protocoles, nous avons examiné deux scénarios selon les hypothèses suivantes:

- Un nœud honnête accuse un nœud malveillant si ce dernier est un nœud voisin pour une période plus longue qu'une période de temps spécifique dénotée MTD (*Minimum Time for Detection*).
- Dans le calcul de DR (*Detection rate*), nous ne considérons que les détections effectuées par l'APM, c'est à dire seulement les nœuds qui sont jugés malveillants par l'APM.

Les résultats illustrés dans la Figure 4.7 montrent que la performance de notre système SDRP surpasse le système de Crépeau et de LEAVE en terme de DR. Nous remarquons que le DR diminue à l'augmentation de MTD. Ceci est expliqué par le fait que le MTD est court, les nœuds honnêtes n'émettent pas suffisamment de messages d'accusation qui sont nécessaires pour la détection de nœuds malveillants. De plus, la détection de nœuds malveillants avec des valeurs élevées de MTD nécessite la présence d'un nombre élevé de voisins détectant les activités malveillantes des nœuds compromis.

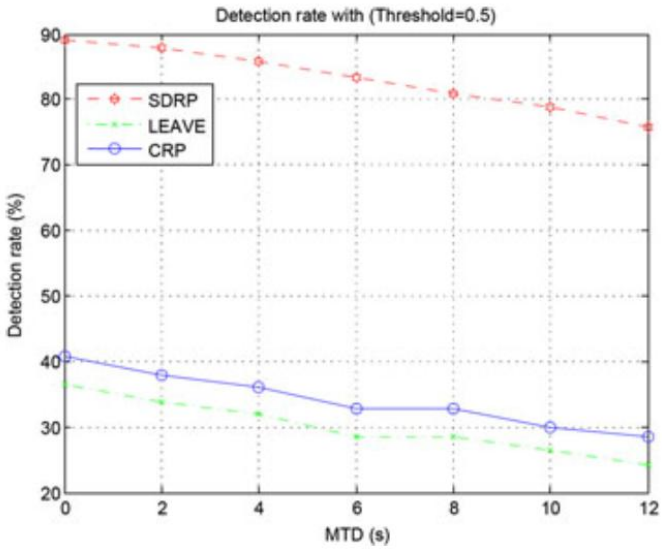


Figure 4.7 : Taux de détection en terme de MTD(Seuil= 0,5)

En comparaison avec les résultats ci-dessus, la Figure 4.8 montre que la supériorité du SDRP est maintenue, par rapport aux autres systèmes de révocation, en diminuant la valeur du seuil qui augmente plus le DR du SDRP. Cependant, nous remarquons que lorsque le MTD = 0 (le cas où chaque nœud honnête accuse tous les nœuds malveillants voisins à n'importe quel moment) il ne conduit pas nécessairement à un DR de 100%. Celà est dû à des situations dans lesquelles les nœuds malveillants constituent une majorité locale.

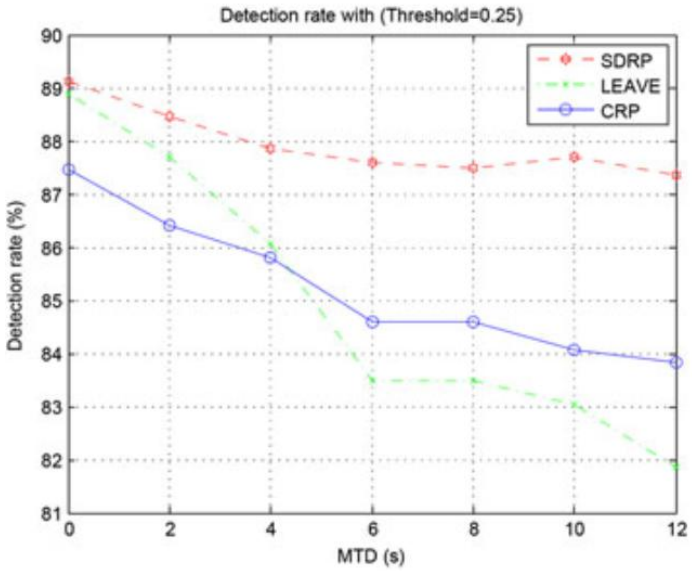


Figure 4.8 : Taux de détection en terme de MTD (Seuil =0,25)

En ce qui concerne le taux de faux-positifs, les résultats illustrés dans la Figure 4.9 montrent que pour un seuil égal à 0,5, l'augmentation de la valeur de MTD a augmenté le poids des nœuds malveillants (à cause des retards de détection des MDMs). Dans la même figure, malgré que LEAVE a donné le meilleur FPR (False positive rate)au détriment d'un faible taux de détection, notre système SDRP donne des taux de faux-positifs acceptables.

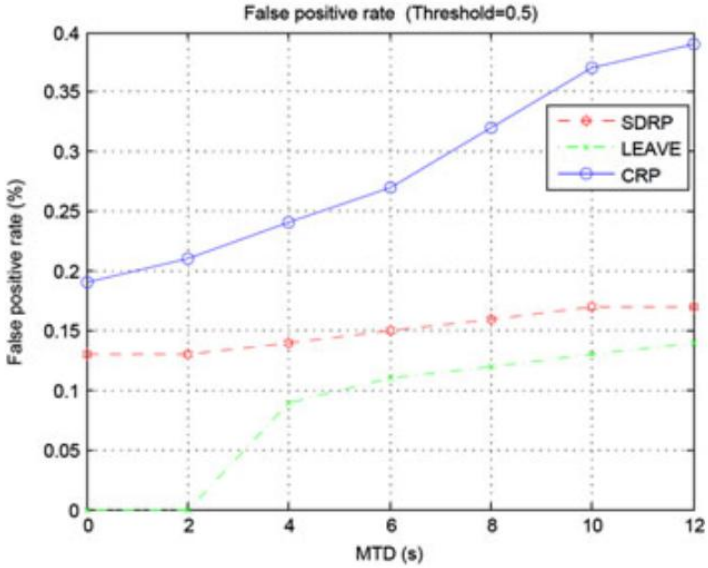


Figure 4.9 : Le taux de faux-positifs en terme de MTD (Seuil=0,5)

La Figure 4.10 montre que avec (MTD> 6), SDRP surpasse les autres systèmes de révocation en raison du dépassement du seuil de révocation à cause des messages d'accusation falsifiés.

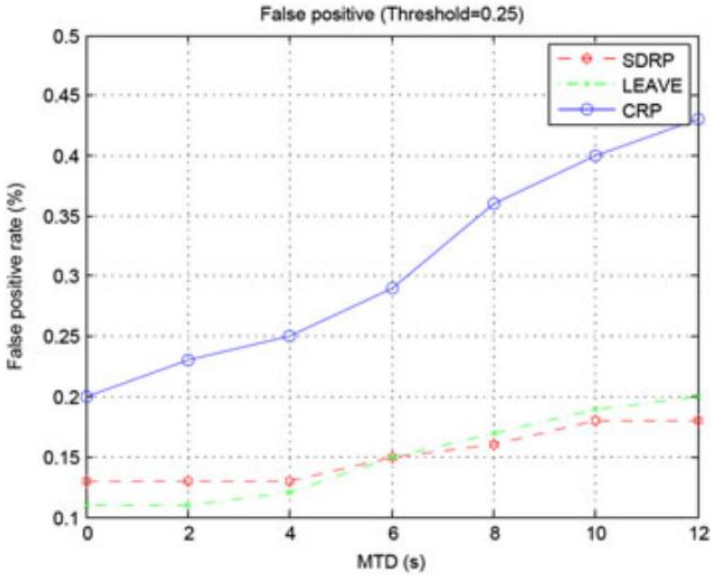


Figure 4.10 : Le taux de faux-positifs en terme de MTD (Seuil=0,25)

4.9 Conclusion

Les nœuds malveillants peuvent attaquer les réseaux VANET et causer leur dysfonctionnement. En effet, ils disposent de certificats légitimes générés par L'AC, et par conséquent ils peuvent commettre les actions appropriées pour attaquer ces réseaux facilement. Donc, la détection et la révocation des certificats de ces nœuds malveillants est essentielle pour le bon fonctionnement de ces réseaux. A cet effet, nous avons proposé des systèmes de révocations pour améliorer la protection contre les nœuds malveillants. Nous avons évalué et étudié la performance de nos propositions à travers la démonstration mathématique de certaines propriétés qui les caractérisent. De plus, les résultats de simulation obtenus montrent leur efficacité par rapport aux autres systèmes de révocation existants.

Chapitre 5

Le changement de pseudonymes dans les VANETs

5.1 Introduction

Dans les réseaux VANET, les applications liées à la sécurité nécessitent l'authentification des messages et de leurs origines. Cependant, la vie privée des propriétaires et des conducteurs de véhicules doit être aussi envisagées, car les VANETs ne seront plus acceptés s'ils ne préservent pas la vie privée des personnes qui les utilisent. Donc, les communications véhiculaires doivent être anonymes. La solution de l'utilisation pseudonymes est la plus acceptée dans la littérature, afin de préserver la vie privée dans les VANETs [84]. Cette solution consiste à utiliser un identifiant à court terme au lieu de l'identifiant principal de véhicule. Ainsi, elle peut satisfaire à la fois les exigences de la sécurité et de confidentialité dans une certaine mesure. En effet, les identités des attaquants qui causent le disfonctionnement de système doivent être identifiées aux fins de révocation et de poursuites juridiques. Ainsi, il est indispensable d'avoir aussi la possibilité de corréler la vraie identité à celle utilisée dans les VANETs. Cette exigence est connue sous le nom de la vie privée conditionnelle « *Conditional privacy* ». Donc, le problème de la gestion d'identité est un problème complexe vue la présence des contraintes sociales, juridiques, économiques et autres liées à la sécurité routière.

Un grand nombre de travaux de recherche a été effectué pour résoudre les problèmes liés à ce sujet. Dans ce chapitre, nous décrivons l'opération courante d'identification de véhicule, puis nous présentons la problématique de la vie privée dans les VANETs. Enfin, nous décrivons la solution de pseudonymat.

5.2 L'identité dans les VANETs

L'identité d'une entité donnée est un attribut qui l'identifie de manière unique. La gestion de l'identité a été étudiée dans plusieurs travaux de recherche. Parmi les travaux les plus importants, celui proposé par Papadimitratos et al.[85].

Traditionnellement, les numéros de plaques d'immatriculation ont été utilisés comme identifiant principal pour un véhicule donné. Les autorités de transport en ont fait leurs processus administratifs. Par exemple, si un certain conducteur dépasse la limite de vitesse autorisée, il sera poursuivi par les autorités. Pour l'identifier, les autorités utilisent le document de véhicule. Habituellement, on suppose que le conducteur est le propriétaire du véhicule. Cependant, ce n'est pas toujours le cas. En effet, la plaque d'immatriculation est une plaque fixée sur un véhicule à des fins d'identification, elle permet de faire la liaison de manière unique entre un véhicule et son propriétaire et non son conducteur.

Les plaques d'immatriculation en Algérie (cf. Figure 5.1) comprennent respectivement les quatre champs suivants : les cinq premiers chiffres correspondent à un numéro spécifique (il permet d'identifier le véhicule de manière unique en considérant les autres champs), le chiffre suivant au type de véhicule, les deux suivants à l'année de mise en circulation, et les deux derniers au code de Wilaya.

La relation entre un véhicule et un conducteur n'est pas une relation un à un. Une personne peut posséder ou conduire plusieurs véhicules, comme un véhicule peut être conduit par plusieurs personnes. L'exemple de cette relation est dans les bus publics qui sont conduits par plusieurs conducteurs dans une journée donnée.

Figure 5.1 : La relation entre un matricule, le propriétaire et le conducteur

Dans les VANETs, tous les identifiants qui sont utilisés dans le système d'identification actuel devraient maintenir son rôle. La plaque d'immatriculation, le permis de conduire et le véhicule lui-même sont tous des éléments d'identification dans les VANETs émergents. Les fabricants de véhicules attribuent un numéro d'identification du véhicule unique VIN (*Vehicle Identification Number*) qui est en relief sur le châssis, et celà peut servir d'identifiant avec des attributs tels que le fabricant, la date de production, le modèle et la couleur.

Dans les VANETs, un identifiant de véhicule (souvent abrégé VID pour «*Vehicle IDentifier*») peut être considéré comme un certificat signé qui permet d'authentifier sans ambiguïté un véhicule. Le VID est un identificateur de longue durée supposé être pré-installé dans l'OBU d'un véhicule. Le VID pourrait être délivré avec l'immatriculation du véhicule et de la plaque d'immatriculation par une autorité d'immatriculation du véhicule, tel le service d'immatriculation.

5.3 Les risques de la vie privée dans les VANETs

L'échange périodique des messages beacons est indispensable dans les VANETs, car il jouera un rôle essentiel pour augmenter la prise de conscience contextuelle des véhicules. Malheureusement, ces messages beacons contiennent des informations concernant l'identité et la position géographique des nœuds, et d'autres informations qui mettent en péril la vie privée des utilisateurs. En effet, des profils des activités personnelles des utilisateurs de VANETs peuvent être établis contenant des informations personnelles telle la trajectoire parcourue. Ce dernier scénario est connu dans la littérature sous le nom de « *Big brother scenario* » (cf. Figure 5.2)[86].

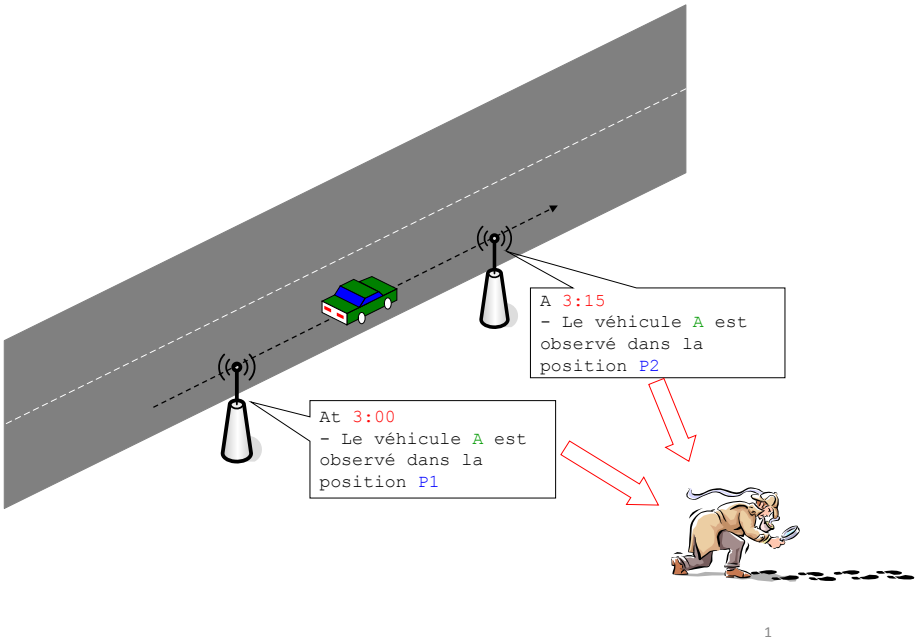


Figure 5.2 : Le syndrome Big Brother

5.4 Limite de la vie privée dans les VANETs

Westin [87] a défini la vie privée comme le droit des individus « de contrôler, éditer, gérer, supprimer des informations qui les concernent, et décident quand, comment et à quel point ces informations peuvent être communiquées aux autres ».

Dans le contexte des routes publiques, la préservation de la vie privée des utilisateurs est limitée par les plaques d'immatriculation qui peuvent être utilisées pour identifier les véhicules de manière unique.

De plus, la technologie ALPR « *Automatic Licence Plate Reader* »[88] a fourni un système pour lire automatiquement les plaques d'immatriculation. En effet, les ALPRs sont utilisés pour prendre des photos numériques des plaques d'immatriculation des véhicules afin de reconnaître les numéros correspondants et les enregistrer. Ils utilisent un logiciel de détection de plaques d'immatriculations optiques qui permet de rechercher et de reconnaître leur présence au moyen d'une caméra ALPR. Une fois le système ALPR a reconnu la présence d'une plaque d'immatriculation, le numéro correspondant est automatiquement extrait grâce aux techniques de reconnaissance optique de caractères.

Figure 5.3 : Atalaya'Compact ALPR[89]

La Figure 5.3 illustre un système ALPR très évolué. Ce système est capable de reconnaitre les plaques d'immatriculation de voitures roulant à une grande vitesse même dans des mauvaises conditions climatiques.

Ce système utilise la technologie GPS pour enregistrer la date et l'heure, ainsi que l'emplacement relatif de toutes les images captées. Par conséquent, l'ALPR permet de suivre les véhicules, et peut révéler des détails personnels tels: vos visites médicales auprès d'un médecin, si vous visitez un lieu de culte ou non,..etc.[90]. Donc, même sans communications véhiculaires, la vie privée des utilisateurs reste limitée, vue la présence des systèmes installés par diverses forces de police qui contrôlent les plaques d'immatriculation visibles.

En raison de la nature de diffusion d'une grande partie des communications véhiculaires, les attaquants ont un autre moyen pour avoir accès aux informations liées à la vie privée des utilisateurs.

Dans le contexte de réseaux de véhicules, la vie privée d'un utilisateur est protégée lorsqu'il sera capable de contrôler les informations transmises par l'OBU (même en cas de renvoi d'information), et la durée de vie de ces informations. L'anonymat est une méthode usuelle pour protéger la vie privée des individus[91]. Pfitzmann et Kohntropp [92] définissent l'anonymat

comme « l'état de ne pas être identifiable au sein d'un ensemble de sujets», qui peut être fourni dans les systèmes de communication basés sur les pseudonymes.

5.5 Les pseudonymes pour assurer la vie privée dans les VANETs

Les pseudonymes numériques ont été initialement introduits par Chaum[93] dans le but de fournir l'anonymat aux transactions électroniques à travers une clé publique utilisée pour vérifier les signatures effectuées par l'entité anonyme qui possède la clé privée correspondante[93]. Pfitzmann et Hansen [94] ont généralisé cette notion. Ils définissent un pseudonyme numérique comme une chaîne de bits qui est l'identifiant unique (au moins avec une très forte probabilité). Elle peut être utilisée pour authentifier les messages de son titulaire. A partir de ces deux définitions, nous pouvons conclure qu'un pseudonyme, ou les informations liées à ce dernier, doivent être utilisables pour l'authentification, mais ne doivent contenir aucune information personnelle qui pourrait être liée à l'identité réelle du titulaire du pseudonyme. Ainsi, un pseudonyme permet l'authentification d'une entité spécifique sans connaître sa vraie identité. Par conséquent, toutes les actions authentifiées avec le même pseudonyme sont considérées d'une origine unique[95]. Ceci présente l'avantage de permettre une communication bidirectionnelle, ce qui n'est pas réalisable avec les approches entièrement anonymes. Toutefois, le titulaire peut utiliser un ensemble de pseudonymes pour assurer son anonymat. Une entité dans un réseau peut soit changer les pseudonymes au cours du temps pour éviter de faire la corrélation entre les actions effectuées dans une longue durée, soit utiliser des pseudonymes différents pour différents contextes [94]. Dans un cas extrême, un pseudonyme différent pourrait être utilisé pour chaque action.

Bohli et Pashalidis[96] montrent que l'utilisation d'un système de pseudonymes ne révèle que la liaison entre le pseudonyme et les actions associées. De plus, un adversaire ne peut pas déduire la taille de l'ensemble des utilisateurs.

5.6 Classification des systèmes de pseudonymes

En examinant les mécanismes cryptographiques utilisés pour la réalisation des systèmes de pseudonymes, quatre grandes catégories peuvent être distinguées dans les VANETs :

- **Les systèmes basés sur la cryptographie asymétrique**: dans cette catégorie, les pseudonymes sont généralement représentés par des clés publiques[97]. Pour faciliter la vérification des messages reçus par les véhicules, un certificat de pseudonyme doit être envoyé conjointement avec le message.
- **Les systèmes basés sur la cryptographie basée sur l'identité** : ils permettent d'atteindre les mêmes objectifs, mais ils ne nécessitent pas de certificats à clés publiques explicites. Celà permet, d'une part, d'éviter d'échanger des informations cryptographiques de taille importante, mais introduit de nouveaux défis pour la génération de pseudonymes d'autre part[98].

- **Les systèmes de pseudonymes basés sur les signatures de groupe** : ils introduisent une clé privée pour un groupe de véhicules, qui permet à une entité d'un groupe de générer une signature au nom de celui-ci, c'est à dire, que la signature peut être vérifiée à l'aide d'une clé publique correspondante. Malgré que ces systèmes offrent, généralement, l'anonymat aux signataires au sein du groupe[99] et réduisent la nécessité de changements de pseudonyme, ils posent de nouveaux défis pour la résolution de pseudonyme et la révocation.
- **Les systèmes basés sur la cryptographie symétrique**: ils sont attrayants en raison de leur efficacité de calcul. Dans ces systèmes, un récepteur doit connaître la clé secrète (partagée entre l'émetteur et le récepteur) pour être en mesure d'authentifier l'émetteur.

5.7 La vie privée descendante et ascendante

On dit qu'un système de pseudonymes assure une vie privée descendante (en anglais « *Backward privacy* »), s'il est difficile à n'importe quelle entité de déduire sa vraie identité (ou la possibilité de déduire les anciens pseudonymes utilisés) même après la révocation de son certificat[100]. Tandis que la vie privée ascendante (en anglais « *Forward Privacy* »), concerne la possibilité de retrouver la liaison entre les pseudonymes après la révocation du certificat correspondant à un pseudonyme utilisé auparavant.

5.8 Le pseudonymat conditionnel

Si la responsabilité est une caractéristique souhaitée, la partie secrète du pseudonyme (l'information qui permet de déduire de manière unique la vraie identité) ne doit être connue que par son titulaire. Ce dernier la partage seulement avec un tiers de confiance qui peut être une base de données consultable seulement après une autorisation judiciaire. Cette caractéristique permet de satisfaire l'objectif de la non répudiation[101]. Elle est connue sous le nom de pseudonymat conditionnel (ou parfois l'anonymat conditionnel)[102]. Donc, le pseudonymat est garanti seulement pour le fonctionnement normal des VANETs, sauf sous certaines conditions dans lesquelles (la suspicion de présence d'un comportement malveillant) une autorité spécifique, ou un ensemble d'autorités, pourrait déterminer les identités correspondantes. Cette dernière opération est appelée la résolution de pseudonymes.

Un exemple d'une approche simple qui assure cette propriété est présenté par Kilian et al.[103] . Ils ont fourni une approche simple pour le pseudonymat conditionnel qui consiste à utiliser un système d'entrepôt des identités dans lequel une autorité qui le gère est responsable de la génération des pseudonymes qui seront utilisés par un nœud.

Après l'authentification de l'identité d'un nœud, l'autorité lui génère un ensemble de pseudonymes et conserve les informations qui permettent de mapper, en cas de conflit, les pseudonymes générés à l'identité du nœud. L'inconvénient majeur de cette approche est qu'elle

n'a pas traité comment empêcher les résolutions de pseudonymes non autorisées par l'autorité qui gère le mappage.

5.9 Le modèle d'adversaire

Les attaques contre les systèmes de pseudonymes ciblent l'anonymat du système de pseudonymes et le rend vulnérable.

Wernke et al. [104] ont classé les attaques contre la vie privée dans les catégories suivantes :

1. **Attaque de position unique** : dans cette attaque, l'entité malveillante essaye de localiser la position ou déterminer l'identité d'un nœud en analysant le contenu d'une requête.
2. **Attaque de positions multiples** : dans cette attaque, l'entité malveillante essaye de corréler les différents pseudonymes et d'établir le chemin complet parcouru par un nœud (cf. Figure 5.4).
3. **Attaque à base de contexte** : elle consiste à utiliser des informations personnelles concernant la victime comme des contrats signés avec des entreprises spécifiques, ses préférences et ses intérêts pour faire la corrélation spatiotemporelle et établir un profil d'activité de l'utilisateur. Une autre attaque qui est classée dans cette catégorie est l'identification de l'empreinte radio d'un nœud[84].
4. **Attaque à travers d'un tiers de confiance compromis** : si un attaquant parvient à compromettre un tiers de confiance, il peut accéder aux informations qui lui permettent de mettre la vie privée des utilisateurs des VANETs en péril.

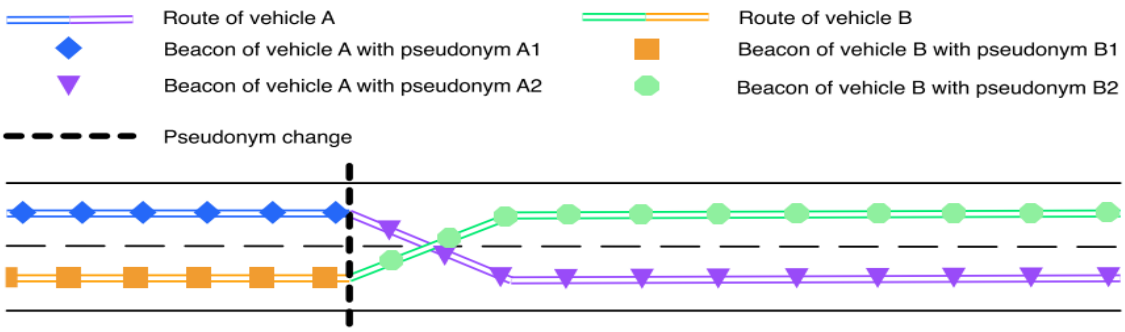


Figure 5.4 : La traque d'un véhicule [105]

Un réseau véhiculaire est un système distribué complexe où un adversaire peut effectuer différents types d'attaques selon ses capacités. En se basant sur les dimensions de la classification d'attaques dans [68], nous décrivons le modèle d'attaquant comme suit :

- **Global ou Local** : cette dimension définit le rayon d'action de l'adversaire. Un adversaire local a un nombre limité de stations qui écoutent le trafic du réseau. Par exemple, les stations d'écoute déployées aux intersections de la route peuvent écouter le communications des nœuds entrants et sortants de l'intersection[106]. Un attaquant global peut suivre les chemins de n'importe quel véhicule, en écoutant leurs messages diffusés, dans la région de ses intérêts[107][108]. Il peut exploiter des infrastructures déployées (RSUs par exemple) aux bords des routes. Cet attaquant peut avoir intérêt à avoir une idée sur le modèle de mobilité afin de personnaliser des annonces publicitaires ou réaliser des techniques de datamining[109]. Donc, l'attaquant peut être un gouvernement ou de grandes entreprises comme les opérateurs de télécommunication.
- **Actif ou Passif** : un adversaire passif n'injecte ni ne modifie des messages, mais il collecte des pseudonymes à des points stratégiques (comme les intersections) où il dispose d'une station d'écoute. Les activités malveillantes d'un adversaire actif dépendent du mécanisme d'utilisation et du changement de pseudonyme. Cet adversaire pourrait bloquer le changement de pseudonyme, forcer son changement, ou perturber sa gestion. Il existe une variante d'attaque active très connue appelée l'attaque d'épuisement de pseudonymes, où un attaquant vise à forcer leurs changements, de manière répétitive, jusqu'à ce que l'ensemble des pseudonymes de véhicule ciblé soit épuisé. Dans cette situation, la victime doit contacter l'autorité pour acquérir de nouveaux pseudonymes.
- **Interne ou Externe** : un attaquant interne est authentifié dans le réseau et peut avoir, par conséquent, plus de capacité pour écouter et analyser le trafic, alors que l'attaquant externe a plus de difficultés à analyser les messages qui sont éventuellement chiffrés. Donc, l'attaquant interne a plus de chance de corréler les différents pseudonymes utilisés par un seul nœud.

5.10 Les exigences de pseudonymat dans les VANETs

Les attaques éventuelles définissent les exigences qui doivent être pris en compte par un système de pseudonymes. L'exigence de la vie privé principal est de rester intraçable et anonyme. Néanmoins, une balance doit être établie entre les exigences de la sécurité et celles de la vie privée. Dans ce contexte, Schaub et al. [110]ont défini les exigences suivantes :

- **La divulgation minimale :** la quantité d'informations à révéler dans une communication doit être minimale. Par exemple : Pas plus que les informations nécessaires pour une communication V2X (V2I, V2V ou V2P).
- **L'anonymat conditionnel :** un émetteur d'un message doit être anonyme parmi un ensemble d'émetteurs éventuels. Cet ensemble est appelé l'ensemble d'anonymat du message. Comme l'identité du conducteur doit être résolue en cas de conflit, l'anonymat est conditionnel dans les VANETs.

- **La non-corrélation :** elle nécessite que la relation entre deux pseudonymes de la même entité physique dans le réseau ne doit pas être trouvée.
- **L'autorité de résolution distribuée :** l'aptitude de résolution d'identité doit être distribuée à plusieurs autorités de telle manière que la coopération entre plusieurs d'entre elles soit nécessaire pour corréler les pseudonymes d'un individu.
- **La résolution parfaite :** une opération de résolution de pseudonymes pour une entité x ne doit pas mener à (ou augmenter les chances de) révéler la vraie identité des nœuds qui sont pas en question.

Nous donnons ci-après les caractéristiques qui doivent être satisfaites par un pseudonyme pour protéger la vie privée :

1. **La limitation de durée de vie** : afin d'empêcher la traque, un pseudonyme doit avoir une durée de vie limitée. Cette caractéristique peut être garantie à l'aide du certificat qui accompagne le pseudonyme.
2. **L'unicité** : afin d'éviter qu'une identité à court terme soit utilisée par plusieurs véhicules, chaque pseudonyme doit être unique. Cette caractéristique est garantie par le système cryptographique de base qui est utilisé pour générer les pseudonymes.
3. **La disponibilité** : un nouveau pseudonyme doit être toujours disponible pour un éventuel changement de pseudonyme. Cette caractéristique peut être garantie en stockant un très grand nombre de pseudonymes dans l'OBU.
4. **Le verrouillage de changement de pseudonyme** : cette caractéristique est nécessaire pour empêcher des attaques comme l'épuisement de pseudonymes.
5. **L'abandon des anciens identifiants** : une fois, un nouveau pseudonyme est utilisé, n'importe quel ancien identifiant au niveau de la pile protocolaire doit être aussi changé afin d'empêcher la traque. Par exemple : les identifiants utilisés le standard ETSI[111],sont dérivés du pseudonymes.

5.11 Le cycle de vie abstrait d'un pseudonyme

Vu les nombreuses exigences de la vie privée dans les VANETs, un nombre important de systèmes de changement de pseudonyme ont été proposés. Ces systèmes paraissent divergents à première vue. Néanmoins, comme ces systèmes sont tous soumis aux caractéristiques de l'environnement véhiculaire, celà nous mène à avoir un cycle de vie abstrait (cf. Figure 5.5) similaire à la plupart des approches des pseudonymes dans les réseaux véhiculaires. L'objectif principal d'un pseudonyme est d'authentifier l'émetteur s'il est valide. Celà peut être achevé en certifiant l'émetteur en tant que véhicule, ou implicitement en assurant que les seuls véhicules valides peuvent faire certaines actions comme la signature de groupe.

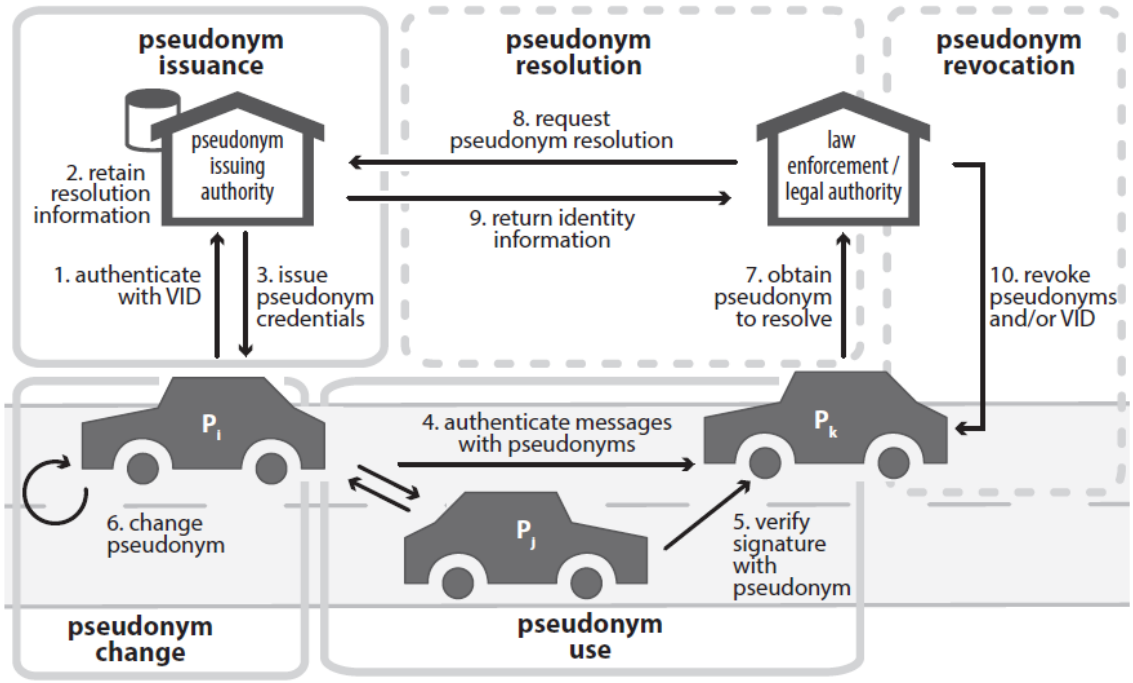


Figure 5.5 : Le cycle de vie abstrait d'un pseudonyme[112]

Dans les réseaux véhiculaires, les pseudonymes passent par un cycle de vie abstrait commun résultant des exigences précédentes. Avec certains systèmes d'authentification de pseudonymes spécifiques, une partie des phases du cycle de vie peuvent s'écarter de notre modèle de cycle de vie abstrait. Cependant, les phases décrites ci-après peuvent être trouvées dans presque tous les systèmes d'authentification de pseudonymes.

Un cycle de vie abstrait d'un pseudonyme comporte les phases suivantes: la génération et l'émission, l'utilisation, le changement, la résolution et la révocation. La phase de génération et d'émission de pseudonyme doit prendre en compte, à l'avance, celle de la résolution de pseudonyme. Les autres phases aussi dépendent intrinsèquement des mesures prises dans le processus de génération et d'émission de pseudonyme pour qu'elles soient efficaces. L'utilisation de pseudonyme et son changement s'influencent mutuellement et dépendent aussi de la manière de génération ou d'obtention des pseudonymes par les véhicules. Certaines phases sont également en option : par exemple, les systèmes ne considèrent pas tous la résolution de pseudonyme ou la révocation. Dans ce qui suit, nous définissons et discutons chaque phase et soulignons leurs défis spécifiques.

5.11.1 Génération et émission de Pseudonyme

Presque tous les systèmes d'authentification de pseudonymes pour les communications véhiculaires supposent qu'un véhicule possède un identifiant numérique unique. Bien que le VID est nécessaire pour l'émission de pseudonymes par la plupart des systèmes proposés, la

génération de VID lui-même n'est généralement pas considérée comme faisant partie du système de pseudonymes ou du cycle de vie de pseudonymes, parce qu'ils sont des processus séparables.

Dans le processus d'émission de pseudonymes, le VID est utilisé pour authentifier l'OBU du véhicule pour s'assurer que seuls les véhicules valides peuvent obtenir des pseudonymes et peuvent donc participer aux communications véhiculaires. Pour la génération de pseudonymes, deux approches principales peuvent être distinguées: la génération par un tiers de confiance et l'auto-génération.

1. La première approche est celle adoptée par la plupart des systèmes dans lesquelles les pseudonymes sont générés par une autorité spécifique PIA «*Pseudonyme Issuing Authority*». Suivant le système, cette entité peut être composée de plusieurs sous-entités : l'AC « Autorité de Certification) et le PP (*Pseudonyme Provider*), ou seulement l'AC. L'architecture de sécurité de ETSI[111] se réfère à eux comme les autorités d'enregistrement et d'autorisation. Le rôle de l'autorité d'émission de pseudonymes est généralement affecté aux infrastructures gérées par les ACs et les PPs, ou par les RSUs. Dans les deux cas, l'autorité émettrice d'un pseudonyme authentifie le véhicule avec son VID, et vérifie l'admissibilité du véhicule pour obtenir des pseudonymes (si le VID du véhicule est valide et n'a pas été révoqué).

   L'autorité du certificat émetteur peut garder des informations permettant de faire le mappage entre le pseudonyme et son identité correspondante afin de pouvoir faire la résolution de pseudonymes plus tard. Il faut noter que l'opération de mappage est une application surjective dont l'ensemble de départ est l'ensemble de pseudonymes et celui d'arrivée est l'ensemble des identités de véhicules. L'opération de mappage consiste en un tableau ou des paramètres secrets qui permettent de vérifier la relation entre l'identité et ses antécédents.

   L'aptitude de l'autorité à faire la résolution signifie qu'elle est digne de confiance. De plus, les infrastructures utilisées par cette autorité doivent être protégées contre les attaques afin d'empêcher l'accès non autorisé à ces informations critiques pour la vie privée.

   Les pseudonymes ont généralement une période de validité[113]. Cette caractéristique permet d'une part d'avoir un gaspillage de pseudonymes, et de limiter le nombre de pseudonymes disponibles à un véhicule à un moment donné dans le but de prévenir les attaques Sybil, d'autre part. Par exemple, un conducteur égoïste peut tricher et utiliser plusieurs pseudonymes à la fois afin de convaincre d'autres conducteurs que la route est congestionnée et par conséquent lui céder le passage[114].

   Comme un pseudonyme a une période de validité limitée et ne peut pas être réutilisé après son changement, certaines approches favorisent le pré-chargement d'un grand nombre de pseudonymes suffisant pour deux ans (Par exemple, pendant l'opération d'inspection de véhicules)[115].

D'autres approches adoptent les recharges occasionnelles de pseudonymes à cause de la connectivité intermittente avec l'autorité émettrice de pseudonymes[116]. La fréquence de recharge de pseudonymes dépend du taux de changement et de la période de validité de pseudonymes.

Raya et Hubaux dans [19] propose le changement de pseudonyme à chaque minute de conduite. Ils estiment que la durée de conduite moyenne est de deux heures par jour. Ce qui résulte en 43800 pseudonymes par an et nécessite 7 méga octets de mémoire de stockage en considérant un pseudonyme de 153 octets.

2. Contrairement à l'approche de génération par un tiers de confiance, l'approche d'auto-génération de pseudonymes[117] a l'avantage que l'OBU d'un véhicule est plus autonome et peut générer les pseudonymes dont il aura besoin, et par conséquent il est possible de minimiser la capacité de stockage nécessaire pour le pseudonyme pool (l'ensemble de pseudonymes disponibles dans un OBU) . Cependant, les attaques Sybil sont généralement plus difficiles à éviter dans ces systèmes en raison du niveau d'autonomie.

5.11.2 L'utilisation de pseudonyme

Une fois qu'un véhicule a obtenu des pseudonymes, il peut communiquer avec d'autres véhicules ou infrastructures. L'utilisation de pseudonyme comporte deux étapes: l'authentification des messages émis et la vérification des messages reçus.

Il faut noter que l'authentification avec pseudonymes n'empêche pas les attaques, donc des opérations complémentaires sont nécessaires. Le standard 1609.2 n'a pas spécifié ces opérations complémentaires vue la complexité du problème qui reste un grand sujet de recherche.

Généralement, les systèmes d'authentification de pseudonymes utilisent soit des signatures asymétriques soit le code d'authentification de messages. L'authentification d'un message nécessite la vérification de validité d'un pseudonyme. Un pseudonyme valide doit être généré soit par une autorité digne de confiance vérifiable avec un certificat qui l'accompagne soit de manière autonome et peut être authentifié avec des paramètres secrets. Les vérifications de validité en ligne ne sont pas considérées faisables à cause de la connectivité intermittente avec les RSUs, la bande passante contraignante, et la contrainte de temps réel des applications des VANETs[118].

Nous avons vu dans le chapitre 2 que l'authentification des messages beacons est un problème dans les scénarios à haute densité de nœuds qui nécessite beaucoup de travail ; la problématique sera plus grave en considérant le changement d'un pseudonyme car ce dernier est généralement effectué simultanément par un ensemble de véhicules voisins, ce qui rend la situation plus difficile.

Les pseudonymes seront efficaces, si et seulement s'ils sont protégés contre l'extraction non autorisée. Donc, ils doivent être protégés avec des HSMs ou des TPDs[119]. La protection matérielle peut aussi être envisagée pour empêcher l'attaque Sybil qui consiste à utiliser plusieurs pseudonymes simultanément.

5.11.3 Le changement de pseudonyme

Les actions effectuées sous un pseudonyme peuvent être liées les unes aux autres, en raison des caractéristiques mentionnées des pseudonymes. Ainsi, les actions effectuées sous différents pseudonymes peuvent être un indicateur pour retrouver la liaison entre deux pseudonymes. Donc, le changement d'un pseudonyme touche pratiquement toute la pile protocolaire[120]. Les identifiants du réseau telles les adresses IP et MAC, doivent tous être modifiés simultanément afin d'éviter que la liaison entre l'ancien et le nouveau pseudonyme ne soit pas triviale.

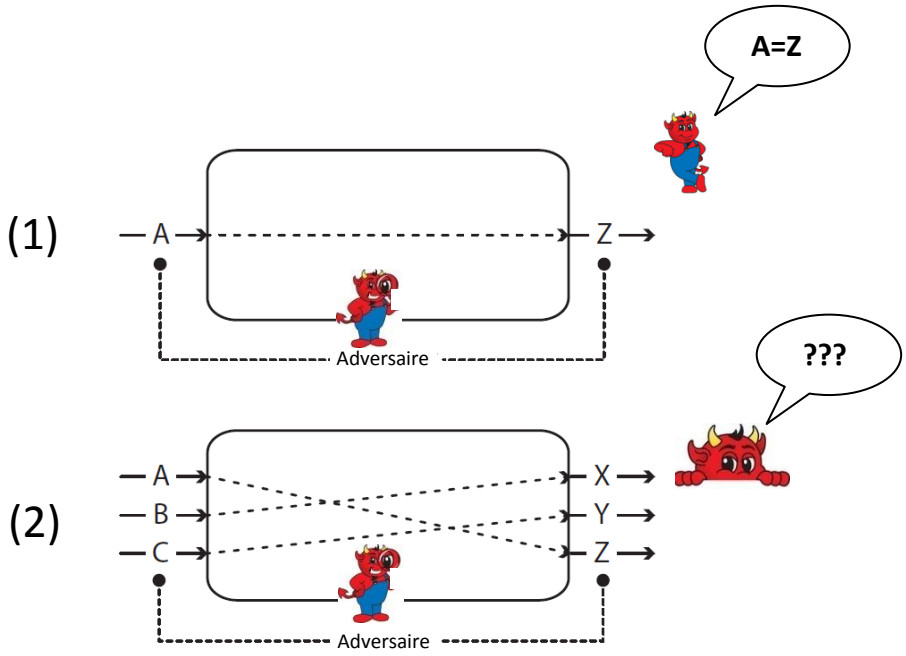


Figure 5.6 : Le contexte de changement de pseudonyme

Un autre aspect important est la nécessité d'avoir des véhicules voisins lors de changement de pseudonyme. Comme le montre la Figure 5.6, en surveillant un endroit stratégique avant et après le changement de pseudonymes, il est facile pour un observateur de savoir la relation entre deux pseudonymes consécutifs utilisés par un nœud lorsque ce dernier change son pseudonyme tout seul à un moment donné. Alors que dans le deuxième cas dans lequel plusieurs nœuds changent leurs pseudonymes simultanément, un éventuel observateur peut, dans une certaine mesure, éprouver une confusion.

Les pseudonymes ont une durée de vie limitée volontairement pour entraver leur identification. Lorsqu'un pseudonyme expire, l'OBU charge un nouveau pseudonyme de son pseudonyme pool ou demande de nouveaux pseudonymes, s'il est en mesure de communiquer avec l'AC et le nombre de pseudonymes est inferieur à un seuil à déterminer. Généralement, les pseudonymes sont remplacés selon le contexte de véhicule pendant la conduite. La stratégie employée est fondamentale pour prévenir l'identification de pseudonymes changés.

Le sujet de changement de pseudonyme est un sujet de recherche actif dans lequel les travaux traitent comment, où et dans quelle situation le changement d'un pseudonyme est efficace[121][122][123]. N'importe quelle proposition pour la vie privée dans les VANETs, ne doit entraver le fonctionnement d'une application liée à la sécurité routière[124].

La Figure 5.7 illustre un algorithme général pour le changement de pseudonyme dans les VANETs. Dans cet algorithme, les nœuds prennent en considération leurs contextes (tels le nombre de voisins, leurs directions et leurs vitesses) et peuvent collaborer afin de décider le meilleur moment de changer leurs pseudonymes.

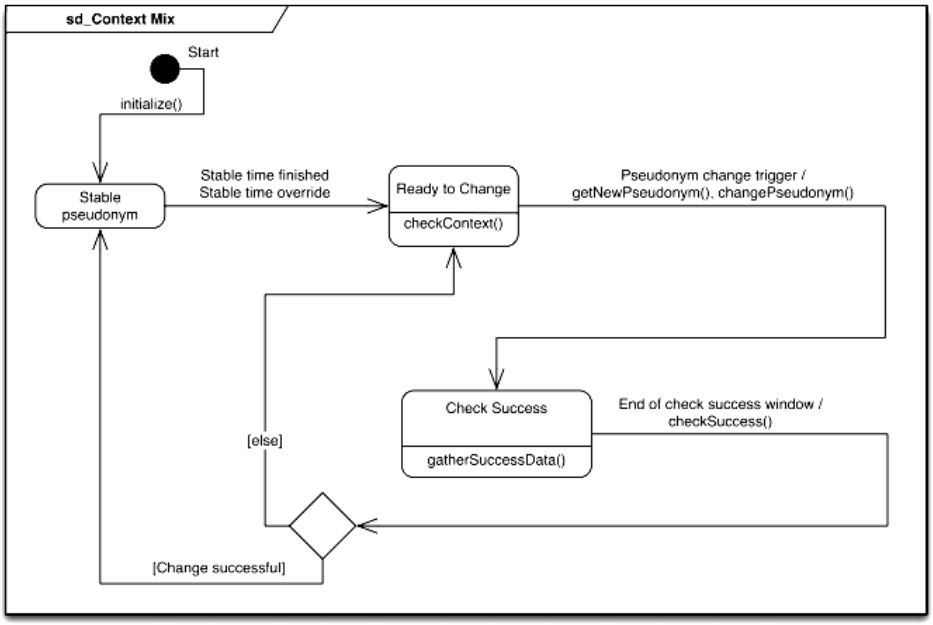


Figure 5.7 : Un algorithme général pour le changement de pseudonyme [84]

Suivant cet algorithme, le processus de gestion d'un pseudonyme comprend trois phases :

- **La phase « *stable pseudonym*»** : cette phase est une période dans laquelle le véhicule ne change pas son pseudonyme et reste dans cette phase jusqu'à avoir un déclencheur[3] (ou « *Trigger* » en anglais) pour passer à la phase de prédisposition.
- **La phase prédisposition** : dans cette phase, le véhicule vérifie son contexte pour choisir le bon moment de changement de pseudonyme, certaines techniques peuvent être utilisées pour créer la confusion et renforcer la vie privée dans cette phase[125].
- **La phase de vérification de succès de changement de pseudonyme** : dans cette phase, un véhicule vérifie si le changement de pseudonyme est effectué dans de bonnes conditions.

[3] Il se peut qu'il soit l'événement TimeOut déclenché par un éventuel Timer qui définit la durée minimale dans laquelle le pseudonyme d'un nœud ne peut pas être changé (verrouiller le changement de pseudonyme)

Il se peut qu'il y ait eu des véhicules voisins malveillants qui ont effectué des actions minimisant le niveau d'anonymat de leurs nouveaux pseudonymes (Par exemple, s'ils ne changent pas leurs pseudonymes ou ne suivent pas les règles nécessaires pour cette opération).

5.11.4 La résolution de pseudonyme

Pour améliorer la vie privée des utilisateurs des VANETs, il existe des propositions[126][127][128] qui comprennent la séparation des autorités de résolution de pseudonyme afin de distribuer le rôle entre eux. En effet, ils ont employé les systèmes de partage de secret[129] pour exiger la coopération entre plusieurs autorités.

Malgré que les chercheurs ont proposé des solutions techniques au problème de résolution de pseudonyme, les implications juridiques et sociales de cette opération ne peuvent pas être déterminées, sachant que, spécialement en Europe, la légalité et la nécessité de l'anonymat conditionnel dans les futurs réseaux de véhicules ont été très débattues ces dernières années. Ainsi, à ce stade, il reste difficile à savoir si ces réseaux adoptent la résolution de pseudonyme ou non[130].

Dans le cas où il y a une interférence avec les applications liées à la sécurité routière, la proposition doit fournir une description complète pour résoudre le problème.

5.11.5 La révocation de pseudonyme (facultatif)

Les nœuds ayant un comportement malveillant doivent être révoqués à partir du réseau de véhicules pour assurer son bon fonctionnement. De manière générale, la révocation des véhicules anonymes consiste à révoquer leurs identifiants à court terme, c'est-à-dire leurs pseudonymes, leurs VIDs, ou voire même les deux. Si des pseudonymes spécifiques, seulement, ont été révoqués, il faut prendre en considération que le véhicule correspondant peut posséder d'autres pseudonymes qui peuvent être utilisés pour de futures communications. Si tous les pseudonymes d'un nœud donné doivent être révoqués, les informations nécessaires permettant d'identifier tous ses pseudonymes doivent être mises en œuvre. Cette possibilité va considérablement affaiblir la vie privée fournie par des pseudonymes.

5.12 Les travaux de recherche existant pour les systèmes de pseudonyme

Les communications basées sur les pseudonymes peuvent être obtenues avec des systèmes traditionnels de la cryptographie à clé publique en équipant les véhicules d'un ensemble de certificats de clés publiques et de paires de clés correspondantes. Ces certificats de clés publiques ne contiennent aucune information d'identification et sont utilisés comme pseudonymes non identifiables. Les véhicules signent les messages avec la clé secrète du pseudonyme actif et rattachent au message la signature résultante, ainsi que le certificat de pseudonyme correspondant. Les récepteurs peuvent vérifier la signature du message en se basant sur le certificat de pseudonyme, mais sans être en mesure de déterminer le VID de l'émetteur.

Les premières propositions, pour assurer la vie privée dans les réseaux de véhicules, ont été basées sur la cryptographie asymétrique [131][132][133]. Ensuite, cette approche a été adoptée par la norme l'IEEE 1609.2v2 [30], et le Consortium Car-to-Car.

Le problème des PKIs traditionnels est que les véhicules doivent, périodiquement, acquérir de nouveaux pseudonymes certifiés. C'est pour cette raison, Zeng [134] a proposé l'approche PKI+ qui permet aux utilisateurs de générer, eux-mêmes, des pseudonymes certifiés par l'AC, réduisant ainsi la charge sur le canal. Armknecht et al. [135] ont appliqué cette approche aux communications V2X, ce qui résulte en un système ayant des phases de génération et de révocation spécifiques. Par la suite, des techniques basées sur les structures de données probabilistes[136] ont été proposé pour rendre l'opération de corrélation des pseudonymes plus difficile.

En ce qui concerne l'émission de pseudonyme, le PKI+ ne distribue pas des pseudonymes aux véhicules. Par contre, les véhicules génèrent leurs propres pseudonymes à partir de leurs propres clés principales. Celles-ci sont choisies par les propriétaires de véhicules et certifiées par l'AC.

PKI+ emploie la cryptographie à couplage[4] pour la génération de pseudonymes et l'authentification des messages[134]. Comme le PKI+ permet aux véhicules de générer leurs propres pseudonymes, il n'est pas nécessaire d'avoir des PPs dans le système. Si l'identité d'un véhicule doit être résolue, l'AC peut identifier le propriétaire du certificat de pseudonyme.

Quand une clé doit être révoquée, l'AC publie les paramètres systèmes mis à jour. Tous les nœuds doivent ainsi mettre à jour leurs clés afin de continuer à participer dans le réseau véhiculaire. Les paramètres sont choisis de telle sorte que le véhicule à exclure du réseau, soit incapable de mettre à jour sa clé principale.

Dans une approche différente, Calandriello et al. [137] combinent le PKI conventionnel avec un système de signature de groupe pour éviter la nécessité de rechargement de pseudonymes. Chaque véhicule possède sa propre clé privée dans un système de signature de groupe avec une clé publique de groupe commun. Un véhicule utilise sa clé privée de groupe pour signer des clés publiques qui lui servent comme pseudonymes. Donc, pour qu'un véhicule puisse vérifier une signature de message, il doit, tout d'abord, vérifier que la clé publique est signée par un membre légitime au sein du groupe. Ensuite, il peut vérifier la signature de groupe sans avoir une idée sur l'identité de l'émetteur.

Plusieurs approches ont été proposées pour défendre contre les résolutions de pseudonymes non justifiées. Elles se basent sur la séparation de rôles entre l'AC, le PP et l'autorité d'enregistrement de pseudonyme RA (*Registration Authority*). Par example, le CAMP (*Crash Avoidance Partnership*) et l'USDOT (*U.S. Department of Transportation*) ont proposé de restreindre les capacités des ACs

[4] La cryptographie à couplage consiste à utiliser une application mathématique vérifiant certaines propriétés afin de diminuer la complexité des problèmes mathématiques

pour lier les pseudonymes. En effet, les RAs enregistrent les demandes de pseudonymes et effectuent le brouillage des requêtes de pseudonymes envoyés aux ACs. L'AC utilise les paramètres secrets de deux entités LA1 et LA2 (des autorités d'identification) pour générer les pseudonymes, sans avoir une idée sur les véhicules auxquels ils sont destinés. Enfin, le RA envoie les pseudonymes aux OBUs après leur compression et leur chiffrement. Donc, la résolution de pseudonymes est une opération complexe qui nécessite la coopération des quatre autorités précédentes[115].

D'autres approches emploient les primitives cryptographiques pour exiger la coopération entre les autorités afin qu'elles puissent effectuer une résolution d'un pseudonyme. Fischer et al. [126] proposent le protocole SRAAC, qui est un protocole pour la génération de pseudonymes qui utilise la signature aveugle[5] et les mécanismes de partage de secret afin de créer les pseudonymes. En effet, pour la création d'un pseudonyme, un véhicule envoie sa clé publique, divisée en portions par le mécanisme de partage de secret, à signer à *n* différentes ACs (une portion différente pour chaque AC). Ensuite, le véhicule peut reconstruire un pseudonyme signé à partir des différentes portions partiellement signées par les différentes ACs. Pour la résolution de pseudonymes, au minimum k(inferieurs ou égale à *n)* autorités doivent échanger leurs portions pour reconstruire le secret. Donc, ce système de pseudonymes est sûr au maximum contre *k*-1 autorités malhonnêtes, ce qui est difficile à avoir.

5.13 Stratégies de changement de pseudonyme

Un paramètre important pour les changements de pseudonyme est le taux de changement[138]. En effet, il influe sur la communication, le calcul, la capacité de mémoire de stockage nécessaire et le niveau de la vie privée. De plus, un changement de pseudonyme simple n'est pas suffisant pour éviter la traque[107].

Un certain nombre de différentes stratégies de changement de pseudonyme ont été proposées, nous citons entre autres :

1. **Le changement périodique**: dans cette stratégie, un véhicule change de pseudonyme à chaque intervalle de temps prédéfini (cf. Figure 5.8). Eckhoff et al. [138] ont proposé une extension (appelée « *time-slotted pseudonym* ») pour cette stratégie afin d'avoir la possibilité de changer de pseudonyme même en absence de PP. Leur proposition permet d'éviter de stocker une très grande quantité de pseudonymes, grâce à leur réutilisation périodique. De plus, ils ont défini la quantité maximale de pseudonymes à stocker. Malheureusement, leur solution est inefficace une fois que l'attaquant ait connu la période utilisée des pseudonymes[139].

[5] La signature aveugle est une signature effectuée sur une information qui a été masquée avant d'être signée

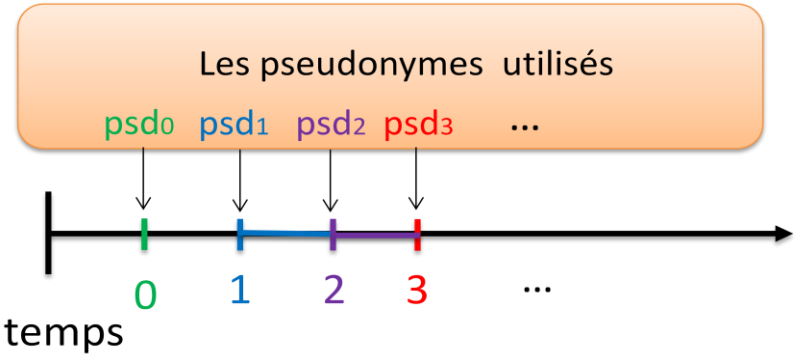


Figure 5.8 : Le changement périodique

2. **Le changement aléatoire**: afin de résoudre le problème de la période fixe de changement de pseudonyme, les véhicules peuvent changer les leurs selon une période aléatoire (cf. Figure 5.9) [140]. En conséquence, un adversaire ne peut pas prédire le prochain changement de pseudonyme. Toutefois, la traque est toujours possible si peu de véhicules changent leurs pseudonymes à un moment précis, parce que tous les autres voisins gardent leurs identités. De plus, une analyse de longue durée permet d'identifier les véhicules qui réutilisent leurs pseudonymes[139].

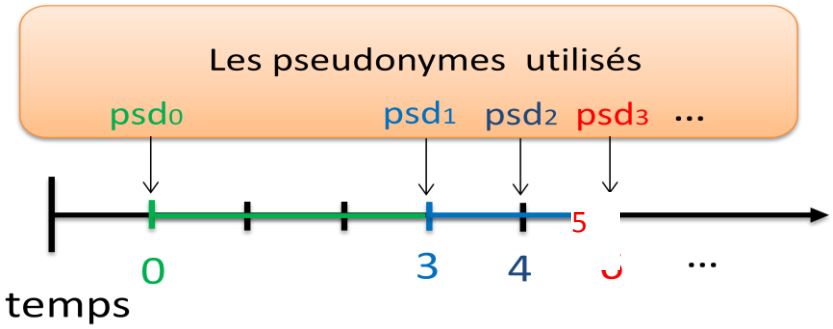


Figure 5.9 : Le changement aléatoire

3. **La période de silence entre le changement**: dans le système de changement AMOEBA[108] et son prédécesseur CARAVAN [141], un véhicule n'accède pas au canal pour une certaine période (appelée « période de silence ») avant de changer son pseudonyme. La période de silence rend les attaques difficiles contre la vie privée. En effet, si un véhicule utilise la stratégie de période de silence dans une intersection, il sera difficile de prévenir son mouvement. La stratégie de période de silence consiste à faire un compromis entre la vie privée et la sécurité routière.
4. **Le changement autonome**: dans cette stratégie, les véhicules déterminent indépendamment où et quand changer leurs pseudonymes. Les deux protocoles Swing et Swap qui ont été proposé par Li et al. [142] adoptent cette stratégie. Dans Swing, les véhicules changent leurs pseudonymes lors du changement de vitesse et de direction.

Ainsi, un adversaire ne peut pas utiliser la prévisibilité de mouvement de nœuds pour établir une corrélation entre leurs emplacements avant et après le changement de pseudonymes. Une amélioration de cette stratégie a été proposée par Eichler [143] dans laquelle la période de silence est ajustée suivant le degré de mobilité de véhicules. Dans SWAP, chaque paire de véhicules échangent leurs pseudonymes, entre eux, lors de changement de pseudonyme avec une probabilité de certitude 0,5, puis entrent dans une période de silence aléatoire. Donc, ils sont indiscernables pour les autres véhicules. Dans un autre protocole appelé SLOW, si la vitesse d'un véhicule descend en dessous de 30 km/h, il entre dans une période de silence et change son pseudonyme[144].

5. **Le changement basé sur la densité (La stratégie CROWD)**: dans cette stratégie, le changement de pseudonyme dépend du nombre de voisins courant. Par conséquent, un véhicule peut éviter le changement inefficace de pseudonyme (lorsque le véhicule est isolé par exemple). Suivant Chaurasia et al. [145][146], le changement de pseudonyme doit être effectué si la taille de l'ensemble de véhicules voisins est supérieure à un seuil à déterminer.
6. **Le changement collaboratif (synchrone)**: lors du changement de pseudonymes, lorsqu'un véhicule change seul de pseudonymes, il tombe facilement victime d'attaques de traque. Une meilleure stratégie est de changer son pseudonyme simultanément avec ses voisins. A cet effet, le véhicule diffuse un message aux voisins pour les informer qu'il est dans l'état de prédisposition [138]. Cette stratégie crée une Mix-zone où les véhicules, dans la même zone, changent leurs pseudonymes simultanément[147]. La Mix-zone a été initialement conçue pour permettre aux entités mobiles de changer leurs pseudonymes dans une zone déterminée. Buttyan et al. [148] utilisent l'approche de Mix-zone pour éviter la traque à travers les changements de pseudonyme. Lu et al.[149] suggèrent de placer des Mix-zones dans les SPs « Social Spots » (par exemple feu de circulation, stationnement,..etc) pour augmenter le nombre de véhicules changeant leurs pseudonymes simultanément. L'inconvénient de cette approche est la faible protection de la vie privée dans des scénarios de faible densité de véhicules[150].

   Buttyan et al. [148] analysent l'efficacité des Mix-zones et concluent que la fréquence optimale de changement de pseudonyme dépend des caractéristiques de la Mix-zone (taille, emplacement, nombre de points d'entrée), qui sont difficiles à déterminer en pratique. Ils montrent que le changement de pseudonymes dans des Mix-zones entre les RSUs ne suffit pas pour protéger la vie privée si un éventuel attaquant surveille plus de 50% des intersections du réseau routier. Freudiger et al. [151] proposent les Mix-zones cryptographiques appelées CMIX. Le protocole CMIX utilise la cryptographie symétrique conventionnelle pour distribuer les clés symétriques afin d'établir une Mix-zone cryptographique qui se situe sous la zone radio d'un RSU. Dans cette zone, les véhicules cryptent tous les messages échangés avec la même clé symétrique fournie par le RSU.

Intuitivement, un adversaire ne peut pas distinguer parmi les véhicules ceux qui utilisent la même clé.

Dans une approche similaire, Wasef et Shen [152] présentent un système pour changement de pseudonymes pendant des périodes (aléatoires) dans lesquelles les véhicules voisins chiffrent les messages échangés avec des clés de groupe symétriques. Encore une fois, un attaquant peut être facilement un membre d'un groupe et peut ainsi observer le changement de pseudonyme [105]. Gerlach et Guttler [84][153] proposent une variante de Mix-zone où les véhicules changent leurs pseudonymes lors de la détection d'un contexte approprié. Ce dernier est déterminé suivant le nombre de voisins, leur vitesse et leur direction. A cet effet, les valeurs de seuils nécessaires sont définies soit par l'application ou par l'utilisateur lui même.

Freudiger et al. [154] ont introduit un modèle de la vie privée dans les VANETs pour mesurer le degré d'anonymat et pour définir les meilleures stratégies de changement de pseudonyme, définissant ainsi une stratégie pseudogame (basée sur la théorie de jeu) dans laquelle les véhicules sont les joueurs.

Malgré qu'il y a de nombreuses stratégies proposées pour le changement de pseudonyme, on ne peut pas savoir laquelle est la plus efficace en pratique. Néanmoins, suivant les droits législatifs et les objectifs définis de l'anonymat ou suivant des métriques bien définies telles la vitesse de traitement, la taille de messages échangés, la capacité de stockage nécessaire, le degré d'anonymat voulu, la complexité de résolution de pseudonymes, on peut déterminer celle qui convient le mieux.

5.14 Systèmes de révocation de pseudonyme

Vu la nature décentralisée des réseaux véhiculaires et leur taille, la distribution de la dernière information de révocation constitue un défi majeur pour un changement de pseudonyme et une révocation efficaces[77]. Dans ce qui suit, nous donnons une classification de système de révocation de pseudonymes dans les VANETs :

5.14.1 La révocation passive

Dans cette catégorie, la révocation du pseudonyme est limitée à la révocation de VID pour des raisons de scalabilité. Si l'identité à long terme est révoquée, aucun nouveau pseudonyme ne peut être obtenu. Ainsi, selon [155][156] la distribution de LRC aux OBUs n'est pas pratique, à cause de la fréquence élevée des messages et la taille de LRC qui peut être éventuellement élevée. D'autre part, en révoquant seulement le VID, le véhicule correspondant peut continuer à participer dans le réseau jusqu'à ce que tous ses pseudonymes soient expirés (cette approche de révocation globale est connue sous le nom de la révocation passive)[157]. Une solution à ce problème est de réduire efficacement la durée de vie des pseudonymes à des intervalles très courts[158]. Il en résulte donc l'augmentation de la fréquence des recharges de pseudonymes.

Cette approche générale soulève des défis tels que le changement de pseudonyme, son rechargement, et la protection de la vie privée contre les émetteurs de pseudonymes malhonnêtes.

5.14.2 Auto-révocation

Cette catégorie des protocoles de révocation[77][159][160] consiste à envoyer les notifications du comportement malveillant détecté par les véhicules voisins du nœud malveillant à l'autorité de révocation (cf. Figure 5.10). Ensuite, cette dernière envoie un message OSR (*Order of Self-Revocation*) au TPD du véhicule malveillant détecté (le véhicule malveillant est en couleur noir dans la figure ci-dessous) en mode géocast [161] chaque T_{repeat} secondes jusqu'à ce que le TPD du nœud malveillant confirme la suppression de tous les pseudonymes stockés. Il faut noter que le rayon de la région géocast est incrémenté à chaque itération pour augmenter les chances que le TPD du véhicule malveillant reçoit le message OSR.

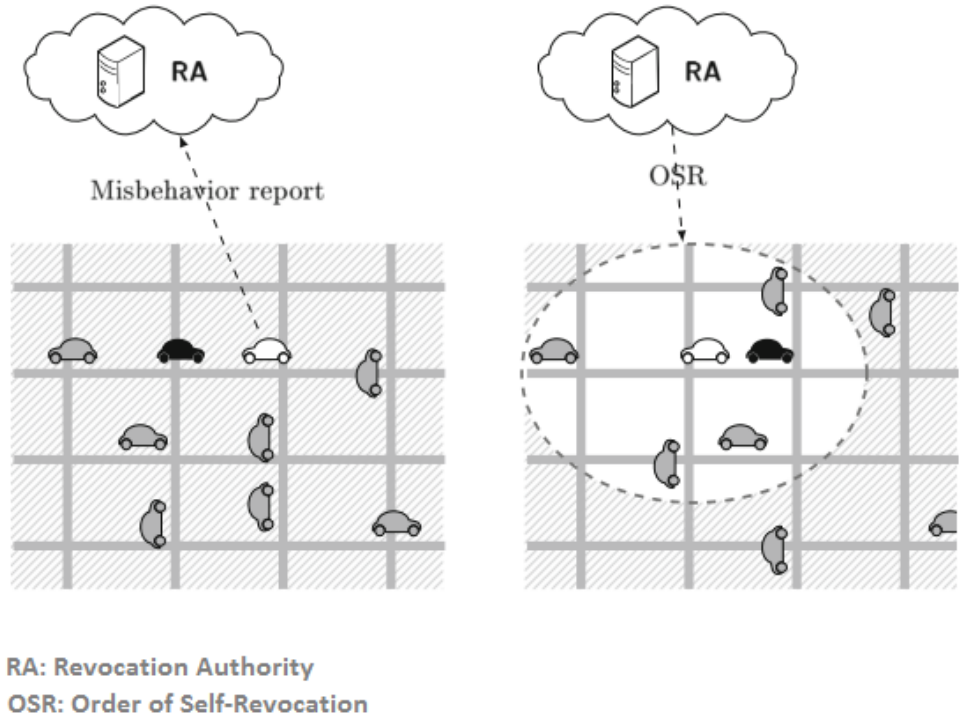


Figure 5.10 : Le protocole de révocation REWIRE[160]

5.14.3 La révocation de pseudonyme basée sur le seuil

Les techniques de révocation de cette catégorie sont généralement basées sur les systèmes de vote que nous avons déjà présentés dans le chapitre précédent. Elles sont nécessaires pour avoir l'aspect distribué du mécanisme de révocation. En effet, il existe d'autres techniques basées sur les systèmes de réputation [162][163], mais le processus de révocation est centralisé.

Sans doute ces techniques sont plus rapides, mais elles présentent des problèmes liés à l'utilisation du concept de l'anonymat. En effet, les chercheurs qui ont développé ces techniques n'ont pas pris en compte le cycle de vie de pseudonymes qui a un grand impact sur leurs techniques. Donc, il est nécessaire d'avoir une nouvelle étude sur l'impact d'anonymat sur cette catégorie. De plus, des nouveaux mécanismes doivent être conçus pour les rendre efficaces.

5.14.4 L'approche de preuve de non-révocation

Cette approche a été proposée par Gañán et al. [164] en présentant la technique EPA (Efficient and Privacy-Aware revocation mechanism for vehicular ad hoc networks) afin de minimiser le taux de faux-positifs.

L'idée principale de l'EPA repose sur l'utilisation de preuves de validité du pseudonyme au lieu de forcer les véhicules à télécharger grandes listes de révocation. Donc, cette approche permet à chaque nœud de prouver que son pseudonyme n'a pas été révoqué récemment. Ces preuves peuvent être obtenues par l'AC en construisant un MHT (Merkle Hash Tree) qui peut être obtenu à partir de la liste des nœuds révoqués. Donc, les traces des informations de révocation peuvent être représentées en un seul champ (la racine de MHT). A chaque fois, un nœud voulant obtenir des informations qui lui permet de prouver son existence dans le réseau, il doit communiquer de manière sécurisée avec un RSU. Ce dernier doit utiliser le MHT afin de vérifier la validité (non-révocation) de ce nœud avant de transmettre les données de certification nécessaires (cf. Figure 5.11). L'inconvénient de cette approche est que les nœuds doivent, de temps en temps, trouver un moyen pour communiquer avec les RSU. Donc, il est difficile de définir la durée d'expiration de preuves de non révocation.

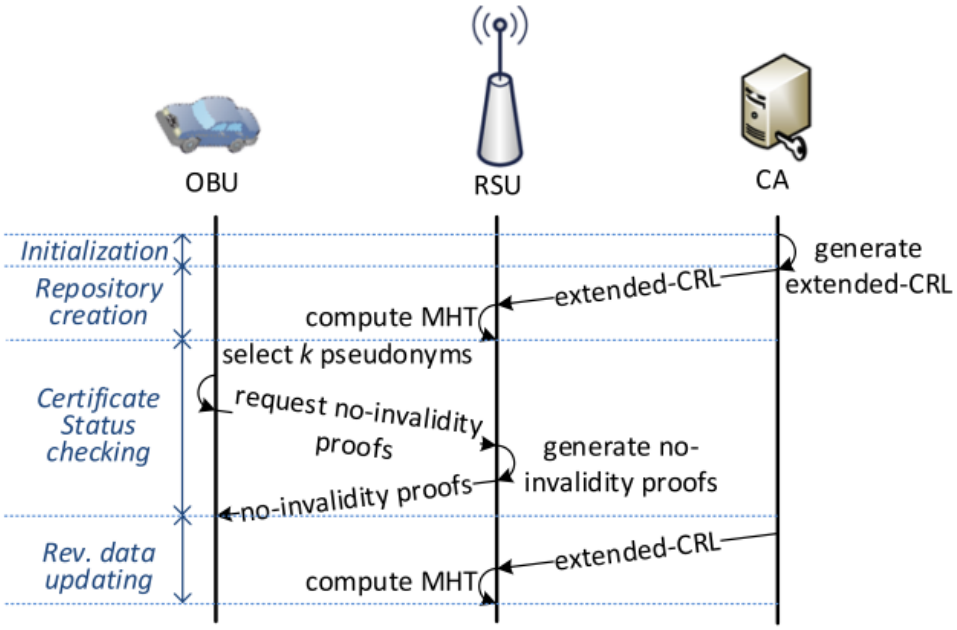


Figure 5.11: Les étapes de la technique de révocation de l'EPA [164]

5.15 Conclusion

L'anonymat des utilisateurs des futurs réseaux véhiculaires doit être intensivement étudié et analysé afin que les systèmes développés au dessus de ces réseaux ne violent pas leur vie privée. Le pseudonymat est l'approche la plus acceptée dans la communauté de recherche pour traiter de ce problème. Néanmoins, il y a toujours des défis techniques, économiques et juridiques qui confrontent les concepteurs. En effet, une solution envisagée en Algérie pourrait être infaisable pour l'Europe à cause de différentes orientations politiques et capacités économiques.

Chapitre 6

Notre système de révocation de pseudonymes dans les VANETs

6.1 Introduction

Nous avons vu dans le chapitre précédent que les chercheurs ont montré que la révocation globale doit être passive, ce qui signifie que les nœuds malveillants détectés peuvent participer dans le réseau et peuvent donc causer le disfonctionnement du système jusqu'à ce que leurs pseudonymes soient invalides. Pendant cet intervalle, le système est vulnérable aux attaques de nœuds malveillants. Donc, il est indispensable de protéger le système pendant cet intervalle de temps.

Dans ce chapitre, nous proposons l'utilisation de la révocation locale afin de faire face aux attaques de nœuds malveillants. Nous commençons par une description de la communauté d'accusation et les problèmes qui lui sont liés, puis nous présentons deux nouveaux mécanismes DAPM (*Duplicate Accusations Prevention Mechanism*) et IRM (*Instantaneous Revocation Mechanism*) pour résoudre ces problèmes. Ensuite, nous donnons une description de notre système EPRV (*Efficient Pseudonym Revocation in VANETs*) qui implémente ces deux mécanismes, et enfin nous analyserons la performance de notre système à travers les résultats de simulation obtenus.

6.2 La communauté d'accusation

La performance de tout système de révocation est étroitement dépendante de la Communauté d'ACcusation (CAC). Deux aspects principaux affectent l'ensemble des accusateurs: l'ampleur du réseau, et son modèle de mobilité. Le choix effectué ne devrait pas surcharger le réseau par des messages de contrôle (par exemple des messages d'accusation). Un nœud évaluateur (dénoté e) peut prendre l'avis de tous les membres du réseau dans le cas des petits réseaux sans fil (en utilisant des messages multi-sauts d'accusation), ou il peut être intéressé par l'opinion des voisins à n-saut pour les réseaux MANET qui sont généralement de taille moyenne. Dans les réseaux à haute densité et dynamiques, l'évaluateur peut se contenter de prendre l'opinion des voisins à un saut afin de réduire le nombre de messages d'accusation.

Dans certains systèmes des VANETs, la CAC du nœud évaluateur e (nous dénotons cette communauté par CAC_e) comprend seulement ses voisins communs avec le nœud vérifié v [83][77]. En fait, la meilleure CAC, sans tenir compte de la complexité, est d'inclure tous les participants du réseau ayant un temps d'interaction avec le nœud vérifié v au pseudonyme actuel. Cette information est difficile à obtenir à cause de l'overhead accompagné, en particulier, si les accusateurs envisagés (les accusateurs récemment rencontrés) sont devenus lointains à cause de la haute mobilité de nœuds. Pour avoir une idée sur les coûts à supporter, nous supposons que la durée de vie moyenne d'un pseudonyme est d'environ 1 mn, comme dans [54][67]. Au cours de cette période de temps, le véhicule pourrait parcourir une distance d'environ 2 kilomètres. Celà signifie que le vérificateur aura besoin de l'avis de véhicules sur 4 kilomètres de distance (en considérant le cas de deux véhicules qui roulent dans deux sens opposés). Considérant les messages de contrôle nécessaires à la sécurisation de la procédure, l'opération complète entraîne un énorme overhead.

6.3 Nouvelles Solutions pour les problèmes de révocation dans les VANETs

Dans cette section, nous présentons deux nouveaux mécanismes DAPM et ARM pour résoudre quelques problèmes de révocation dans les VANETs. Mais, avant de décrire ces deux nouveaux mécanismes, nous devons considérer les problèmes de révocation dans les cas suivants:

a. Considérons plusieurs accusations avec un seul accusateur et un seul accusé: ce cas aura lieu si le véhicule accusateur émet deux messages d'accusation sous des pseudonymes différents.

b. La condition de révocation est vérifiée contre un nœud y à un instant de temps t, mais le système de révocation ne le révoque pas.

6.3.1 DAPM

DAPM (Duplicate Accusations Prevention Mechanism) est un mécanisme qui permet d'éviter d'avoir plusieurs accusations avec un seul accusateur et un seul accusé (cas a).

Pour résoudre ce problème, nous devons identifier l'origine de ce problème via un exemple illustratif.

Considérons le cas d'un nœud malveillant qui profite de la possibilité de changer le pseudonyme afin d'émettre des accusations falsifiées sous différents pseudonymes [165], et causer ainsi ce que nous appelons une succession d'accusations falsifiées. Cette attaque est légèrement différente de l'attaque Sybil. Cette dernière dans le contexte de changement de pseudonyme, consiste à émettre simultanément plusieurs messages d'accusation falsifiés et autant quelle le veut, sous plusieurs pseudonymes. Alors que le cas de la succession d'accusations falsifiées, celles-ci sont émises sous différents pseudonymes dans des périodes de temps plus courtes. Dans le cas d'un nœud honnête, un pseudonyme devrait être changé dans une durée moyenne d'une minute, alors que cette durée est beaucoup moins dans le cas des nœuds malveillants, qui peuvent changer à des périodes de temps moindres. Donc, corréler les pseudonymes dans le cas d'une succession d'accusations est un peu plus difficile que dans celui des attaques Sybil (il existe des systèmes pour détecter les attaques Sybil [52]).

Pour faire face à l'attaque de succession d'accusations falsifiées, nous avons proposé un nouveau mécanisme qu'on a appelé DAPM (Duplicate Accusations Prevention Mechanism). Le principe de DAPM est comme suit :

- Chaque nœud doit gérer une liste d'accusations sur laquelle il ajoute des informations concernant les nœuds accusés et accusateurs.
- A chaque fois un nœud x quitte la CAC (le nœud évaluateur e ne reçoit aucun message hello provenant du nœud x), toute les accusations, dans laquelle x est un nœud accusé ou un accusateur, doivent être supprimées.

Il faut noter que les contre-mesures précédents sont obligatoires afin d'éviter le problème de plusieurs accusations avec un seul accusateur et un seul accusé (voir cas a). De plus, les nœuds malveillants peuvent modifier leurs pseudonymes sans suivre les règles de la procédure de changement de pseudonyme. Par conséquent, il est impossible de voir si le nœud a physiquement quitté la CAC ou tout simplement, il a changé son pseudonyme. Donc, il est préférable de supprimer toutes les accusations de ces nœuds.

6.3.2 IRM

Le mécanisme IRM (*Instantaneous Revocation Mechanism*) assure la révocation des véhicules dès que la condition de révocation soit satisfaite.

Malheureusement, les protocoles de révocation existant vérifient la révocabilité d'un nœud qu'après la réception d'un message d'accusation qu'il accuse[166]. Malgré que la condition de révocation est satisfaite.

Pour bien clarifier la situation, nous avons considéré deux scénarios :

1. Scénario1

Dans ce scénario, nous sommes seulement intéressés par l'élimination d'un nœud de la CAC. Supposons que le nœud éliminé n'a émis aucune accusation et le nœud évaluateur e n'a pas reçu d'accusations contre ce nœud. Considérons le système de révocation SDRP (on peut choisir d'autres techniques [77][75]).

Pour illustrer la situation, considérons la Figure 6.1 qui montre le graphe d'accusation d'un évaluateur e avant que le nœud 5 quitte la CAC (avant l'instant t) et après qu'il l'ait quitté (après l'instant t). Il faut noter qu'un arc partant d'un nœud x vers un nœud y signifie que x accuse y.

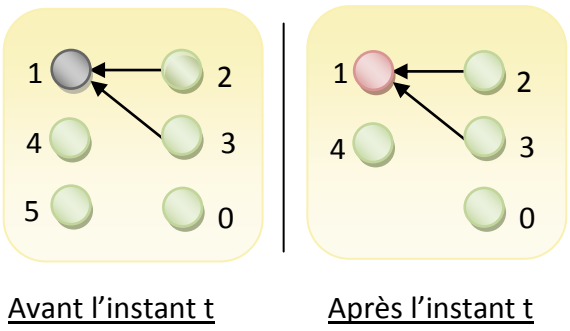


Figure 6.1 : Graphe d'accusation de scénario 1

Supposons qu'on veut vérifier le nœud 1 en utilisant un seuil Th égal à 0,5 :

Avant l'instant t :

- La taille de CAC est 5.
- Le nœud 1 n'accuse aucun nœud.
- Le nombre d'accusateur du nœud 1 est deux.

Donc, le valeur maximale du taux d'accusation $(Q_1) = \frac{2}{5} < Th$, et par conséquent la condition de révocation du nœud n'est pas vérifiée.

Après l'instant t, le nœud 5 n'est plus un membre de la CAC. Nous pouvons ainsi vérifier qu'aucune accusation n'est éliminée par la fonction de filtrage de SDRP. Donc, le nouveau taux d'accusation du nœud 1 est:

$$Q_1 = \frac{2}{4} = Th$$

Nous pouvons remarquer que, dans ce cas, le nœud 1 peut être révoqué, car la condition nécessaire est vérifiée après qu'un seul nœud neutre ait quitté la CAC. Il faut noter que les protocoles de révocation existants ne vérifient plus la condition de révocation si un nœud quitte la CAC.

2. Scénario2

Dans ce scenario, un nœud quitte la CAC après avoir généré des accusations: toutes les accusations dans lesquelles ce nœud est impliqué doivent être supprimées de la liste d'accusations. Cette situation pourrait satisfaire la condition de révocation contre certains nœuds.

Pour mieux illustrer la situation, considérons la Figure 6.2 dans laquelle les nœuds utilisent le protocole LEAVE décrit dans le chapitre 3, avec un seuil égal à 0,5.

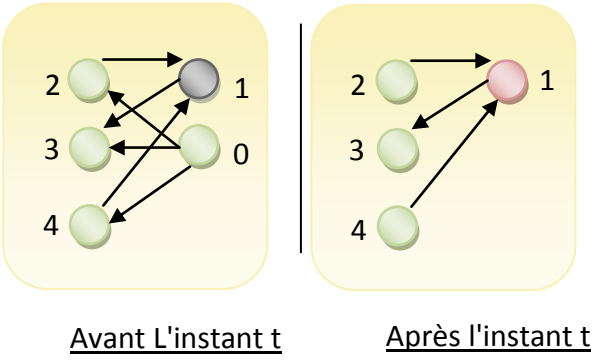


Figure 6.2 : Graphe d'accusation de scénario 2

Considérons les accusations avant et après instant t où le nœud 0 quitte la CAC. Dans ce qui suit, nous montrons les valeurs des taux d'accusation dans les deux instants.

Avant l'instant t, le poids d'accusation des nœuds 2 et 4 (accusateurs du nœud 1) et la valeur du taux d'accusation du nœud 1 peut être calculée comme suit :

— $W_2 = 1 - \frac{1}{4} = \frac{3}{4}$

— $W_4 = 1 - \frac{1}{4} = \frac{3}{4}$

— $Q_1 = \frac{1}{4}\left(\frac{3}{4} + \frac{3}{4}\right) = \frac{6}{16} < 0.5$

Dans ce cas la condition de révocation n'est pas vérifiée.

Après l'instant t, les valeurs précédentes peuvent être calculées comme suit :

— $W_2 = 1 - 0 = 1$
— $W_4 = 1 - 0 = 1$
— $Q_1 = \frac{1}{3}(1 + 1) = \frac{2}{3} > 0.5$

Donc, la condition de révocation est vérifiée et le nœud 1 doit être exclu.

Encore une fois, nous remarquons qu'un nœud doit attendre d'autres messages d'accusation (ce qui n'est pas toujours le cas) pour révoquer un autre nœud, alors que celui-ci pouvait être révoqué plus tôt. Ce qui met en évidence la nécessité d'amélioration des mécanismes de révocation existants pour avoir plus de performance dans un environnement hostile comme VANET.

Pour résoudre le problème précédent, nous avons considéré un nouveau mécanisme IRM. A la différence des autres systèmes de révocation, ce mécanisme consiste à vérifier tous les membres de la CAC à chaque fois le contenu de la liste d'accusations change. Cette stratégie engendre un traitement supplémentaire, mais il assure une détection plus rapide (les nœuds hostiles seront détectés dès que la condition de la révocation soit satisfaite).

Si la complexité de la technique de révocation utilisée est très élevée, des optimisations adaptées à la technique utilisée peuvent être envisagées. Par exemple, on vérifie seulement un sous-ensemble de la CAC.

Dans la section suivante, nous présentons notre nouveau système de révocation EPRV qui implémente les deux mécanismes précédents DAPM et IRM afin d'améliorer la performance de révocation de malveillants dans les VANETs.

6.4 Notre nouveau système de révocation de pseudonyme (EPRV)

Vue la contrainte temps réel des VANETs et la nécessité de mécanismes efficaces de révocation des nœuds, nous proposons un système nommé EPRV (*Efficient Pseudonym Revocation in VANETs*) dans lequel un nœud est révoqué une fois la condition de révocation est vérifiée (Le mécanisme IRM est utilisé). Ce qui augmente le taux de détection et améliore significativement les délais de révocation. Donc, notre système permet d'exclure les nœuds malveillants le plus tôt possible. De plus notre système EPRV implémente le mécanisme DAPM afin de faire face aux accusations falsifiées. Dans cette section, nous donnons les hypothèses de base, le modèle d'adversaire, et une vue d'ensemble de l'architecture de notre système suivie d'une description détaillée de chaque module.

6.4.1 Les hypothèses de base

Nous supposons un réseau véhiculaire qui utilise un système de pseudonymes basé sur la cryptographie asymétrique. Donc, les véhicules disposent d'un nombre limité de pseudonymes valides pour une courte durée. Ainsi, ils utilisent un système de changement de pseudonymes coopératif de PAN et al. [167], dans lequel les nœuds changent leurs pseudonymes s'il y a k véhicules voisins désirant changer leurs pseudonymes.

Nous supposons aussi que les véhicules utilisent un IDS autonome pour contrôler les activités des nœuds via les paquets captés et envoient des messages d'accusation pour notifier les nœuds voisins s'ils détectent un nœud malveillant. L'IDS utilisent des techniques similaires à celles décrites dans [148][144][168] afin d'avoir la possibilité de détecter le changement inapproprié de pseudonyme en corrélant l'ancien et le nouveau pseudonyme du nœud correspondant. Celà est utile pour les véhicules malveillants qui ne suivent pas les règles de changement de pseudonymes.

6.4.2 Le modèle d'adversaire

Nous supposons un adversaire qui contrôle des nœuds malveillants en coalition (qui constituent une minorité de nœuds dans le système). Ces derniers peuvent falsifier des messages d'accusation afin d'attaquer le système de révocation. De plus, les attaquants peuvent changer leurs pseudonymes à n'importe quel moment et de manière imprévisible. Donc, ils peuvent changer leurs pseudonymes à des intervalles très courts afin de causer l'attaque de succession d'accusations. Avec une telle capacité, les attaquants pourraient multiplier leurs impacts sur le système de révocation plusieurs fois, ce qui mène à dégrader considérablement la performance du système.

6.4.3 Une vue d'ensemble de l'architecture de notre système

Dans cette section, nous proposons une architecture pour améliorer les techniques de révocation de pseudonymes. Notre système comprend trois modules principaux (cf. Figure 6.3): AIDAM (*Autonomous Intrusion Detection and Advertisement Module*), le ALM (Accusation List Manager) et le RDM (Revocation Decision Maker).

1) L'AIDAM comprend deux sous-modules: un IDS (*Intrusion Detection System*) et une unité d'avertissement. Le premier sous-module détecte de manière autonome les activités malveillantes, tandis que le second est chargé de générer des messages d'accusation pour avertir les nouveaux nœuds voisins de nœuds malveillants.
2) Le module ALM gère la liste d'accusations et permet d'éviter des attaques telle la succession d'accusations. Donc, ce module fournit des mécanismes d'auto-défense pour résister aux attaques et éviter les problèmes présentés dans la section 6.3.
3) Le RDM ajoute le pseudonyme d'un nœud sur la liste noire, dès que la condition de révocation est vérifiée.

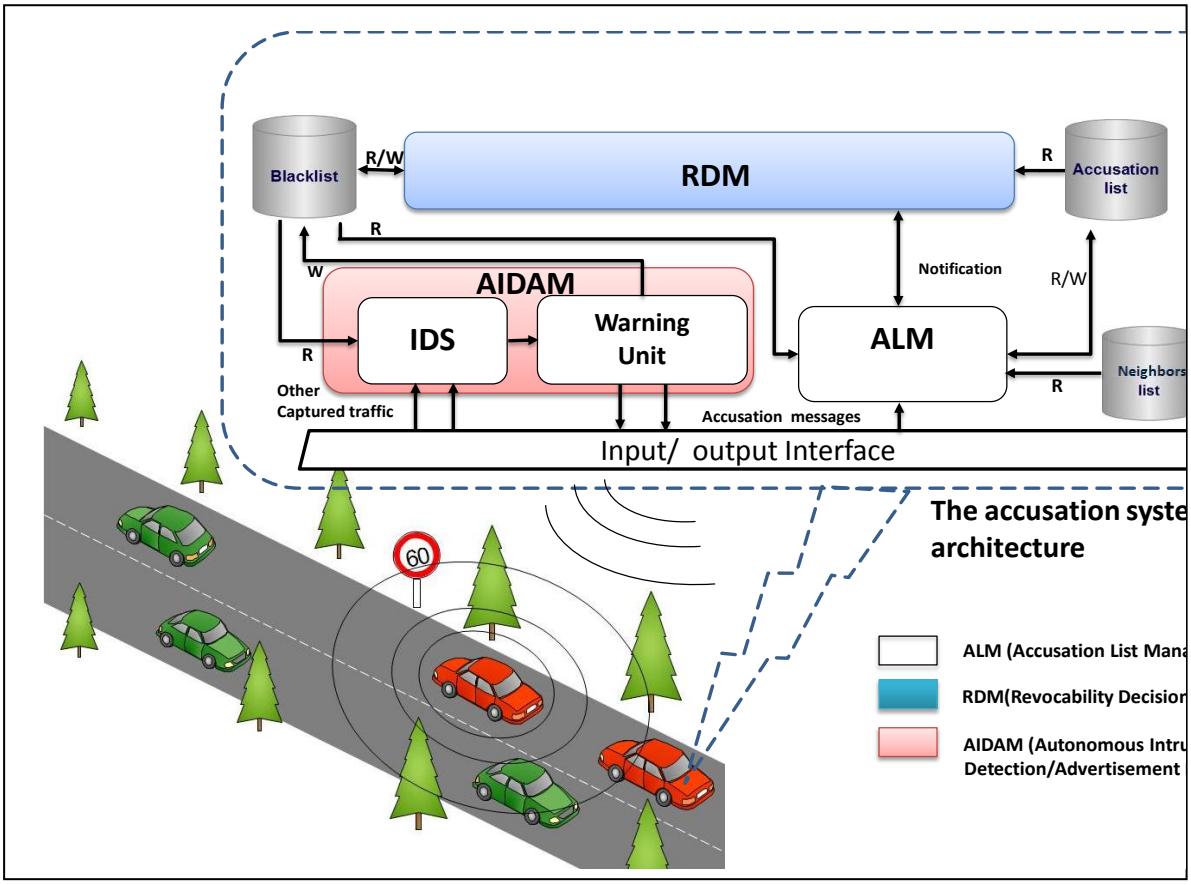


Figure 6.3 : L'architecture de notre système

6.4.4 L'AIDAM

Dans notre système, nous supposons la présence d'un'IDS similaire à celui utilisé dans [83][77][75][46]. Ce dernier est indispensable dans n'importe quel système de révocation pour détecter les nœuds malveillants et les ajouter sur la liste noire même si le temps d'interaction avec eux est très court.

Les accusations contre les nœuds malveillants sont incluses dans un seul message d'accusation à la manière de SDRP ou elles peuvent être compressées en utilisant les filtres bloom [169] d'une taille m bits (cf. Figure 6.4).

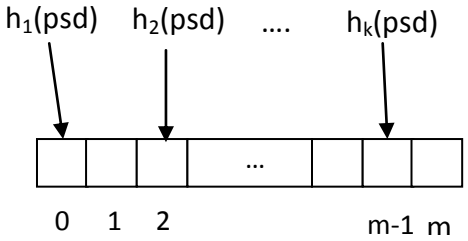


Figure 6.4 : Illustration du mécanisme du filtre bloom

Soit B un vecteur de m bits, pour compresser les accusations dans un filtre bloom, nous devons suivre les étapes suivantes:

1. Le nœud émetteur s met la valeur de tous les éléments (les bits) du B à zéro ;
2. Puis, s utilise k fonctions de hachage h_i dont les valeurs de sortie sont comprises entre 0 et $m-1$. Ces fonctions sont appliquées pour hacher les pseudonymes des nœuds accusés.
3. Enfin, il met la valeur 1 pour chaque élément du B ayant un index égal à $h_i(psd)$, avec psd est le pseudonyme du nœud malveillant et $0 \leq i < m$.

Après avoir effectué les étapes précédentes, le nœud s peut diffuser le message d'accusation, et n'importe quel nœud voisin recevant ce message doit ajouter son accusation contre un nœud a, si la condition suivante est vérifiée :

$$\sum_{i=1}^{k} B\left(h_i(psd_a)\right) = k$$

Le taux du faux-positifs introduit par les filtres de bloom est donné [169] par :

$$\left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^k \approx \left(1 - e^{kn/m}\right)^k \qquad (6.1)$$

Avec n est la taille de la CAC.

Pour avoir le taux de faux-positifs minimal, l'équation suivante doit être vérifiée:

$$k = (ln2).\left(\frac{m}{n}\right) \qquad (6.2)$$

Aux fins d'illustration, si la taille du filtre bloom m est 60 octets et n=120, nous devons choisir k=3 pour avoir un taux de faux-positifs minimal égal à 0,42% (voir équation 6.1).

6.4.5 ALM

Ce module gère la liste d'accusations et implémente les fonctions de base des deux mécanismes DAPM et IRM. Il doit supprimer chaque accusation (x, y) si x ou y a quitté la CAC (voir 6.3.1 pour la description du mécanisme DAPM). Trois scénarios sont possibles pour ce cas :

- x ou y n'est pas sous la portée de transmission du nœud vérificateur.
- x ou y a changé son pseudonyme.
- x ou y est inclus dans la liste noire.

Chaque fois qu'un changement se produit sur la liste d'accusations, L'ALM informe le RDM qui vérifie la révocabilité des nœuds accusés (cette action est requise pour l'implémentation du mécanisme IRM voir section 6.3.2).

Dans les VANETs, la topologie est très dynamique, et des véhicules peuvent rejoindre et quitter la CAC (cet opération pourrait avoir lieu de manière répétitive) pour de courtes durées. Ce qui mène à changer fréquemment le contenu de la liste d'accusations, et ainsi causait un traitement extrême à cause des vérifications inutiles de nœuds. Pour bien illustrer la situation, considérons la Figure 6.5 qui montre un véhicule V malveillant falsifiant les accusations sous un seul pseudonyme. Les véhicules qui le croisent sont obligés de procéder à des traitements inutiles à cause des accusations falsifiées de V.

Un véhicule malveillant qui lance une succession d'accusations peut nuire à ses voisins de manière similaire dans n'importe quelle zone.

Pour résoudre ce problème, nous proposons que chaque fois qu'une accusation est retirée de la liste d'accusations (en raison de la suppression d'un nœud v de l'ensemble des voisins), ce module doit solliciter d'analyser la révocabilité de nœuds si et seulement si:

$t - t' > P$

Avec t le temps courant, t' est l'instant de rejoindre la CAC, respectivement, et P est un seuil qui spécifie la durée minimum dans laquelle le nœud doit figurer dans la table de voisins.

Des valeurs minimes pour P augmentent les chances de détecter les nœuds malveillants plus rapidement, mais au détriment des éventuelles attaques décrites précédemment.

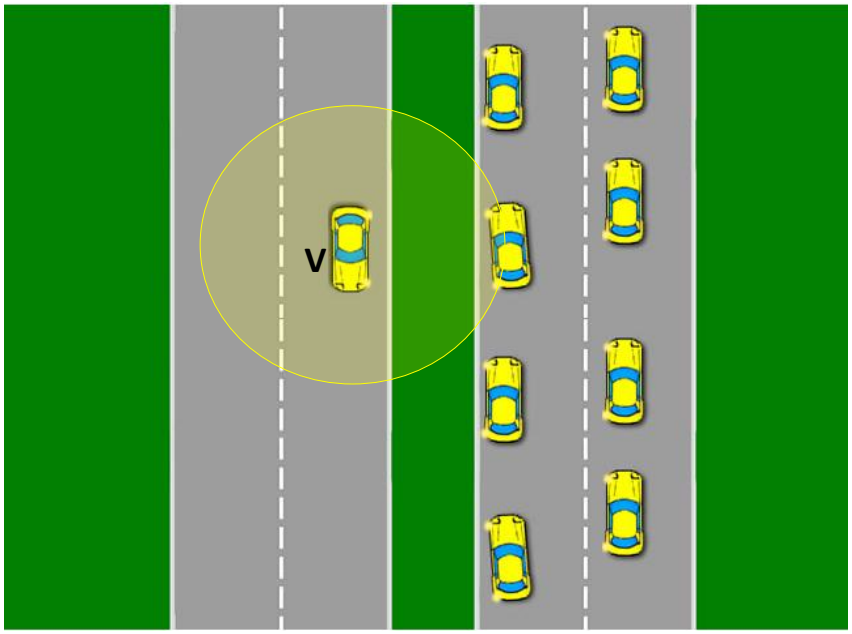


Figure 6.5 : Scenario d'accusations inutiles

L'algorithme exécuté par ce module est illustré ci-après :

Algorithme 1

```
1.  On_Receive_accusation_message(accuser:node,accused:node)
2.  Begin
3.    If (accuser∉ Blacklist AND accuser ∈ CAC  AND
          accused∉ Blacklist AND accused ∈ CAC AND
          (t − t′ ≥ P) )
        Begin
4.       Accusation_list.add (accuser,accused,now);
5.       Notify_RDM();
6.      End;
7.    End.

8.  On_Leaving_neighbors (leaving_node: node)
9.  Var
10. Flag: Boolean;
11. Begin
12.   For each accusation∈ Accusation_list  do
13.    Begin
14.    Flag=false;
15.      If  ((accusation.accuser=leaving node) OR
             (accusation.accused=leaving node)) Then
16.          Begin
17.           Accusation_list .remove(accusation.accuser,
              accusation.accused);   // IRM
18.           Flag=true;
19.          End;
20.    End;
21.          If  (Flag) then          // liste d'accusations modifiée
22.             Notify_RDM ();
23. End.
```

6.4.6 RDM

Ce module a le dernier mot si un nœud doit être révoqué ou non. Chaque fois qu'un nœud est soumis à une évaluation de révocation, ce module prend une décision sur le nœud à vérifier sur la base du contenu de la liste d'accusations et la procédure de révocation prédéfinie.

L'algorithme 2 montre l'algorithme de révocation exécuté par ce module. Il illustre le cas du protocole LEAVE.

Ce module vérifie tous les nœuds accusés chaque fois que la liste d'accusations change, afin d'assurer que les nœuds malveillants soient révoqués lorsque la condition de révocation est satisfaite (cette action est requise pour l'implémentation du mécanisme IRM voir section 6.3.2). De cette manière, l'ALM et le RDM coopère pour assurer une révocation rapide de nœuds malveillants.

Algorithme 2

```
1.  Revoke (): Integer;
2.  Flag: Boolean;
3.  Begin
4.  Flag=False
5.    Q=0;
6.  For each x ∈ CAC and (x,verified)∈ Accusation_list do
7.    Begin
8.       W=1-Nb_accuser(Accusation_list.x)/ |CAC| ;
                        // W is the weight of the accuser
9.        Q=Q+W ;
10.   End;;
11.  Q=Q/|CAC| ;  // LEAVE accusation quotient
12.  If (Q≥ th) then
13.   Begin
14.      Add_to_blacklist(verified);
15.      Notify_ALM (verified);
16.      Flag=true;
17.    End;
18.   If (flag) then
19.     Return 1;
20.   Else
21.      Return 0;
22. END.
```

6.5 Evaluation de la performance de notre système

Dans cette section, nous évaluons notre proposition EPRV à travers les simulations. Nous commençons par la description de l'environnement de simulation, ensuite nous donnons et analysons les résultats obtenus.

6.5.1 Environnement de simulation

Pour évaluer la performance de notre système, nous l'avons considéré avec le protocole de révocation LEAVE (avec un seuil égal à 0,5 qui est la valeur recommandée par les auteurs de l'article de cette approche), qui est le plus connu. Les nœuds honnêtes changent leurs pseudonymes de manière normale. Chaque nœud honnête effectue un verrouillage de changement de pseudonyme pour 45 s après chaque changement de pseudonyme afin d'éviter les problèmes qui en découlent, ensuite il peut collaborer avec les autres nœuds pour changer le pseudonyme suivant l'approche CPN [167], avec le paramètre k=3, ce qui signifie qu'un nœud honnête change son pseudonyme s'il y a 3 nœuds voulant changer les leurs.

L'attaquant est supposé capable de changer son pseudonyme sans suivre les démarches dictées par la technique de changement de pseudonyme CPN. Donc, il est capable de causer l'attaque de succession d'accusations, avec une durée de vie de pseudonyme distribuée de manière uniforme dans l'intervalle $[DM \times 0{,}5, DM \times 1{,}5]$ où DM est la durée de vie moyenne de changement de pseudonyme pour un nœud malveillant. Afin que les nœuds malveillants causent une attaque de

succession d'accusations, la valeur de DM doit être petite. De plus, n'importe quel nœud malveillant falsifie une accusation contre un nœud honnête une fois qu'il devient son voisin, alors qu'un nœud honnête accuse un autre malveillant si le temps d'interaction entre eux (l'un est dans la portée de l'autre) est de deux secondes. Il faut noter que les accusations de nœuds placés sur la liste noire sont supprimées de la liste d'accusations et toutes ses futures accusations sont ignorées. En outre, nous supposons que la valeur par défaut PLink (la probabilité de corréler les pseudonymes consécutifs d'un nœud malveillant), est égal à 0.

Le simulateur utilisé est le NS2, et les fichiers traces de mobilité utilisés avec ce simulateur sont générés avec l'outil SUMO en considérant la carte du centre ville de Laghouat (cf.

Figure 6.6).

Figure 6.6 : La zone considérée pour les fichiers traces

Les simulations sont amenées en considérant les paramètres suivants :

Paramètre	Valeur
Portée d'antenne	300 m
Couche MAC	802.11P
Région de simulation	2000m×1500m
Nombre de nœuds	300
Durée de simulation	15 mn
Seuil d'accusation	0,5

Tableau 9 : Les paramètres de simulation permanents

Les paramètres de simulation variables ayant des valeurs par défaut sont illustrés dans le tableau suivant :

Paramètre	Valeur par défaut
Nombre de messages d'accusation par seconde	0,5 HZ
Taux de nœuds malveillants	20%
P	0 s
DM	2 s
PLink	0
Taux de falsification	100 %

Tableau 10 : Les valeurs par défaut de paramètres variables

6.5.2 Résultats de simulations

Dans cette section, nous donnons et analysons les résultats de simulations obtenus.

La Figure 6.7 montre le taux de détection des nœuds malveillants en terme de DM (La durée de vie moyenne de pseudonymes des nœuds malveillants). +EPRV et -EPRV dénotent, respectivement, les résultats de simulation avec et sans notre amélioration de système de révocation. Nous remarquons que les pseudonymes avec une durée de vie courte dégradent la performance en terme de taux de détection, car l'augmentation de durée de vie de pseudonymes des nœuds malveillants donne plus de chance pour les détecter. De plus, la performance se stabilise au-delà de la valeur 10 pour les DMs, malgré qu'elle soit beaucoup plus inférieure par rapport à la durée de vie moyenne de pseudonymes de nœuds honnêtes, car le nombre d'accusations, après cette valeur, n'est pas suffisant pour dépasser le seuil de révocation.

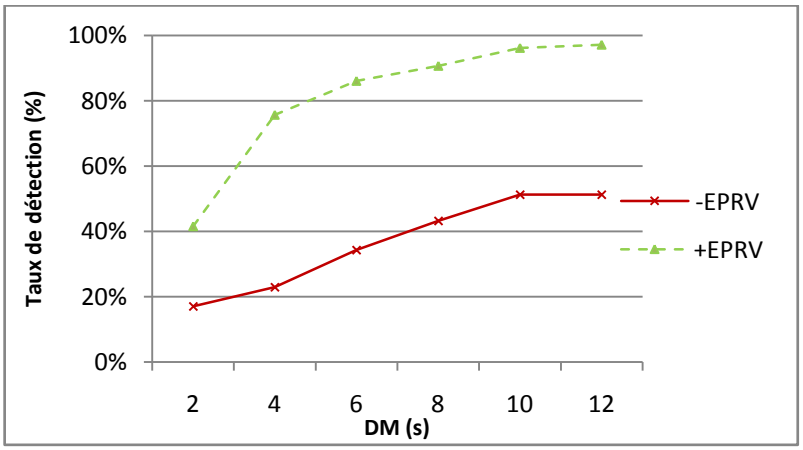


Figure 6.7 : Taux de détection de noeuds malveillants en terme de DM

Dans la même figure, nous remarquons aussi que les taux de détection obtenus avec +EPRV surpassent largement ceux de –EPRV, car notre approche contient des mécanismes pour ne considérer une accusation entre deux participants du réseau, qu'une seule fois.

La Figure 6.8 montre le taux de détection de nœuds malveillants, obtenu par notre système, en terme de PLink. Nous remarquons que l'augmentation de PLink augmente le taux de détection, car l'aptitude à corréler les pseudonymes de nœuds malveillants intrinsèquement, augmente le taux de détection et soulage le système des accusations falsifiées de nœuds malveillants. Dans la même figure, nous remarquons ainsi que le taux de détection a augmenté de manière considérable pour un PLink allant de 0,2 à 0,3, car les accusations éliminées dans cet intervalle a entraîné un dépassement du seuil de révocation.

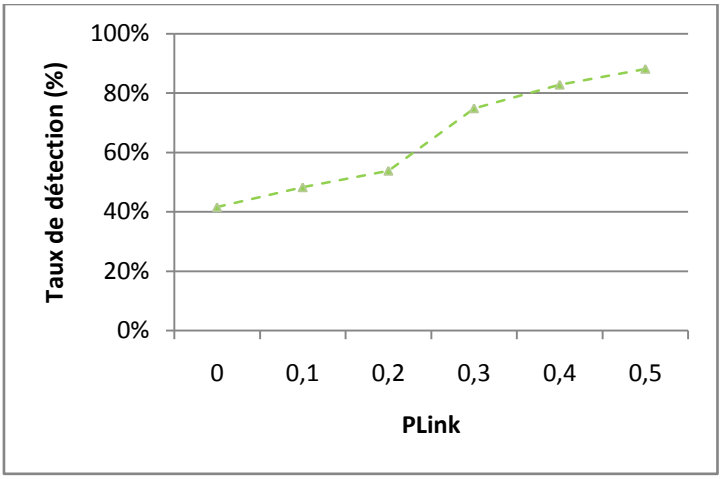


Figure 6.8 : Taux de détection de nœuds malveillants en en terme de PLink

La Figure 6.9 montre le taux de faux-positifs en termes de DMs. Le faux-positifs représente un pseudonyme d'un nœud honnête qui a été ajouté sur la liste noire. Nous remarquons que le taux de faux-positifs augmente avec l'augmentation de DM, car les accusations malveillantes ont plus de chance à dépasser le seuil du protocole de révocation, et causent la révocation de pseudonyme de nœuds honnêtes. Dans la même figure, nous remarquons aussi que notre approche a largement minimisé le taux de faux-positifs de l'approche originale, car notre système dispose d'un mécanisme qui empêche les accusations multiples.

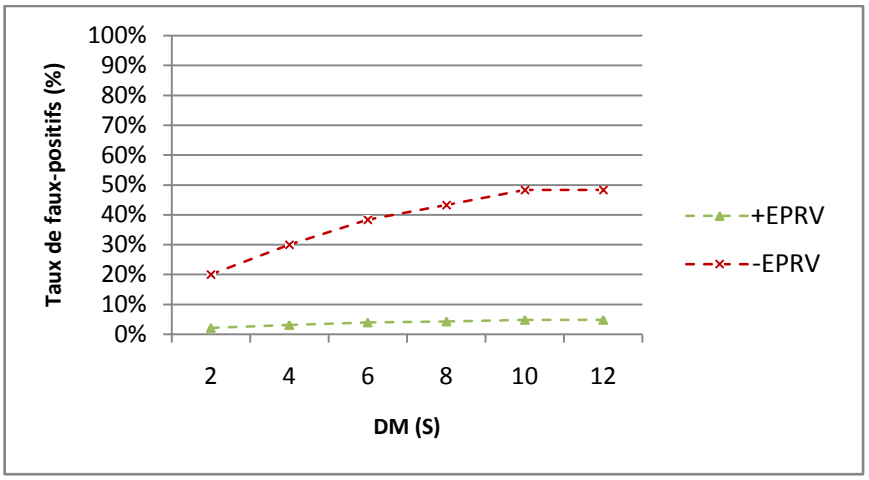


Figure 6.9 : Taux de faux-positifs en terme de DM

La Figure 6.10 montre le taux de faux-positifs en termes de taux de nœuds honnêtes (qui sont accusés par les nœuds malveillants en coalition). Dans la simulation, les nœuds honnêtes victimes d'attaque sont choisis de manière aléatoire afin d'avoir plus de chance qu'ils soient distribués à travers l'environnement de simulation. Nous remarquons que +EPRV a toujours donné les meilleurs résultats par rapport à la variante -EPRV. Le taux de faux-positifs de cette dernière augmente de manière considérable à l'augmentation du taux de falsification d'accusation.

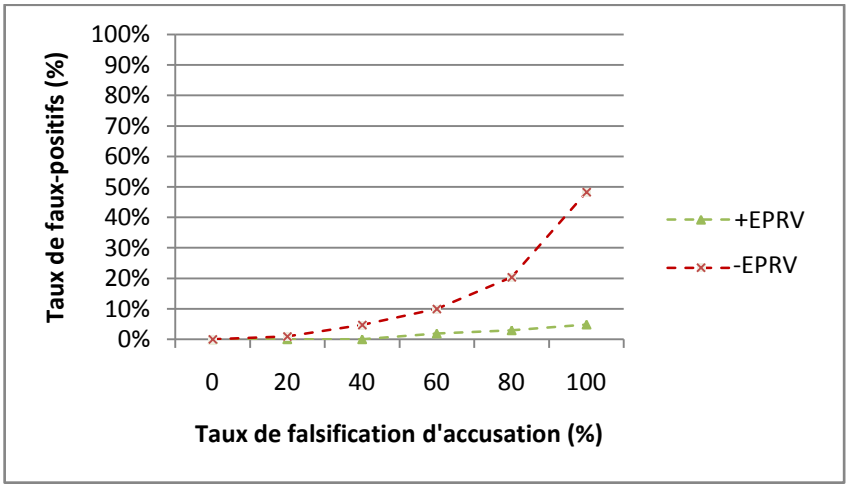


Figure 6.10 : Taux de faux-positifs en terme de taux de falsification d'accusation

La Figure 6.11 montre les délais de détection moyens de nœuds malveillants en terme de la durée de vie moyenne de leurs pseudonymes. Nous remarquons que l'augmentation de la durée de vie des pseudonymes de nœuds malveillants augmente les délais moyens de leur détection, car les nœuds détectés sont intrinsèquement détectés dans de courts délais.

Nous remarquons aussi que notre approche +EPRV a présenté les meilleurs délais de détection par rapport à la méthode originale de révocation LEAVE.

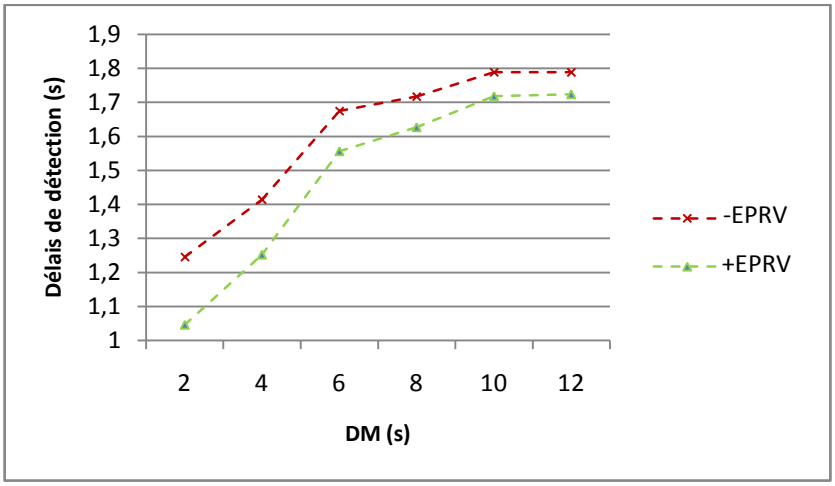


Figure 6.11 : Délais de détection moyens de noeuds malveillants

La Figure 6.12 montre le nombre moyen de nœuds vérifiés par seconde en terme de DM. Nous remarquons que l'augmentation des DMs augmente le taux de vérification, car avec de courtes DMs les pseudonymes des nœuds malveillants à ajouter sur la liste noire seront plus nombreux. Dans la même figure, nous remarquons aussi que notre approche +EPRV présente des taux de vérification plus élevés à ceux de l'approche originale, notamment, pour des courtes DMs.

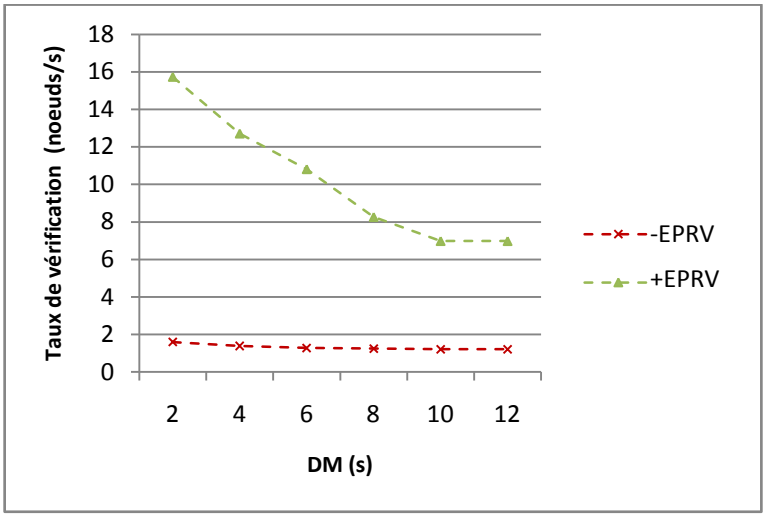


Figure 6.12 : Le nombre de vérification de nœuds moyen par seconde

La Figure 6.13 montre le taux de vérification en terme de valeur de P. Il faut noter que nous avons fixé la valeur de DM à 12 afin que le changement des valeurs de P soit significatif. Dans cette figure, nous remarquons que les taux de vérification diminuent avec l'augmentation de la valeur de P, car certaines accusations des nœuds qui ont une courte durée d'interaction avec les nœuds évaluateurs ne déclenchent pas les vérifications.

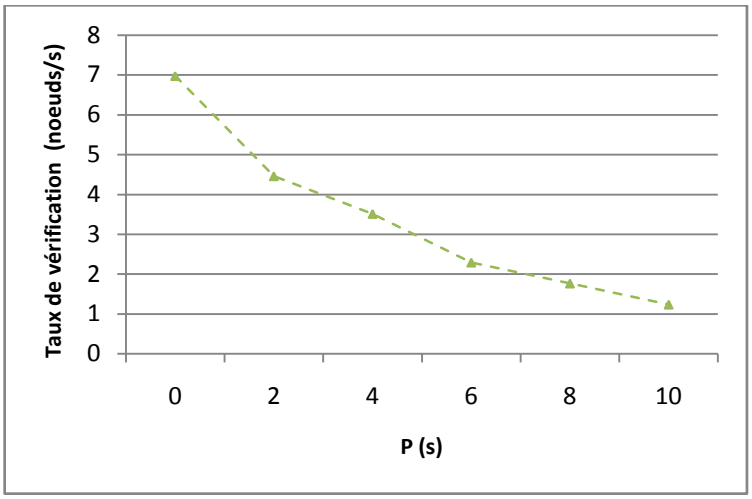


Figure 6.13 : Le taux de vérification en terme de la valeur de P

6.6 Analyse de la sécurité

Notre système garantit les propriétés suivantes :

1. **Propriété1 :** Soit $V(x)$ une fonction qui permet d'associer chaque pseudonyme x à son identité unique réelle. EPRV assure la propriété suivante :

   $\forall\, psd_1, psd_2 \in CAC: V(psd_1) \neq V(psd_2)$

   Conséquences: ALM supprime chaque accusation (x, y) si x ou y a quitté la CAC. Donc, la propriété1 assure que l'accusation d'un véhicule contre un autre est unique.

   Démonstration : il y a deux possibilités pour avoir deux pseudonymes pour une seule identité unique :

   -Cas1 (l'attaque Sybil): le nœud malveillant annonce deux pseudonymes différents psd_1et psd_2 simultanément. Vu que l'IDS de l'AIDAM détecte les positions falsifiées, les deux pseudonymes ne peuvent pas correspondre à deux positions différentes au même temps.

   -Cas2 (l'attaque de succession d'accusations falsifiées) : Dans ce cas le nœud malveillant fréquemment change son pseudonyme. Avant d'utiliser le nouveau pseudonyme, le nœud malveillant pourrait arrêter l'émission pendant une durée S_m (la période de silence). Supposant que les véhicules supprime un pseudonyme

psd de la liste de voisins si aucun beacon de psd n'a pas été reçu pendant une durée déterminée T_{out}. Dans ce cas, nous pouvons distinguer deux scénarios possibles:

-$T_{out} < S_m$: Dans ce scénario, l'ancien pseudonyme est certainement supprimé sur la liste de voisins. Donc, la CAC doit aussi supprimer ce pseudonyme.

-$T_{out} \geq S_m$: c'est le plus pire scénario. Le seul moyen pour rendre notre système sécurisé est de choisir des valeurs minimes pour T_{out}, de telle manière qu'il soit facile pour un IDS d'un nœud honnête de trouver la relation entre les deux pseudonymes consécutifs du nœud malveillant. L'inconvénient majeur de cette solution est la vulnérabilité aux attaques de brouillage du canal qui pourrait causer des modifications fréquentes sur la liste des voisins.

2- Propriété2 : Soit T un intervalle du temps et $P(psd, t)$ une fonction booléenne qui prend la valeur vrai si la condition de révocation est satisfaite à l'instant du temps t. EPRV assure la propriété suivante :

$$\forall\, psd \in ACC \wedge\ t \in T\colon\ P(psd, t) = true \Rightarrow\ psd \in Blacklist$$

Conséquences: A la différence des approches de révocation, EPRV détecte les nœuds malveillants dès que la condition de révocation est satisfaite, ce qui permet d'améliorer les délais et les taux de détection, et de minimiser les taux de faux-positifs.

Démonstration : Soit t un instant du temps et ε une valeur très petite de telle manière que la condition suivante est satisfaite :

$$P(psd, t) = true\ \wedge\ \ P(psd, t - \varepsilon) = false$$

La condition de révocation est essentiellement basée sur le contenu de la liste d'accusations. Donc, le contenu de cette liste avant et après t n'est pas le même, ce qui signifie qu'il y a un changement de son contenu et l'algorithme 2 doit être exécuté pour révoquer psd.

6.7 Conclusion

Vue la haute mobilité des nœuds et le changement fréquent de pseudonymes dans les VANETs, le contrôle de révocabilité des nœuds est indispensable à cause des contraintes de temps réels caractérisant ce type de réseaux. Dans ce chapitre, nous avons proposé un système pour contrôler de manière permanente la révocabilité de nœuds. Les résultats de simulation montrent que notre système améliore la performance de révocation locale dans les VANETs mais au détriment du coût de traitement.

Conclusion générale

Les réseaux VANET sont des réseaux ayant des applications prometteuses pour sauver la vie des personnes et assurer le confort des occupants de véhicules. Ces réseaux ne peuvent pas être déployés qu'après l'investigation et l'assurance de leur sécurité. Malheureusement, ces réseaux sont vulnérables aux attaques des entités malveillantes qui peuvent injecter des messages à des fins malveillantes.

L'authentification de l'origine de ces messages est un élément fondamental pour se défendre contre les attaquants. En effet, les nœuds incluent dans les messages échangés des signatures numériques qui permettent aux nœuds récepteurs de les authentifier.

La vérification de signatures numériques nécessite que le nœud vérificateur doit avoir une copie du certificat numérique du nœud signataire. Les différents travaux de recherche proposent le rattachement des certificats aux messages beacon. De cette manière, n'importe quel nœud possède les certificats de tous ses voisins à n'importe quel moment s'ils les rattachent à chaque message beacon diffusé. Le problème de cette approche est qu'elle nécessite des équipements spécifiques qui supportent cette complexité de traitement. Une autre approche est possible et consiste à omettre l'inclusion de certificats dans certains messages beacon qui permet aux nœuds de réduire le traitement et la bande passante consommée d'une part, et d'augmenter les chances des pertes cryptographiques, d'autre part. Ces dernières sont acceptables si elles ne causent pas une dégradation grave de la performance.

L'authentification n'empêche pas les attaques des nœuds qui sont sous le contrôle des entités malveillantes. En effet, ces nœuds peuvent être en coalition et emploient tous les moyens afin de monter des attaques dangereuses au niveau de toute la pile protocolaire.

Pour se défendre contre les nœuds malveillants, l'annulation de validité de leurs certificats numériques, au plus tôt, est indispensable pour éviter leurs attaques. A cet effet, les RSUs peuvent être utilisés pour distribuer la dernière liste de révocation de certificats. Cette opération n'empêche pas instantanément les attaques vue la nature centralisée de cette opération. Donc, le mécanisme de révocation locale est nécessaire pour exclure rapidement les nœuds malveillants.

La révocation locale est effectuée de manière décentralisée et ne nécessite pas l'intervention de l'AC. Elle peut être effectuée en contrôlant les activités des nœuds voisins et en échangeant des messages d'accusation contre ceux qui ont commis des activités malveillantes.

La révocation locale est vulnérable aux attaques de falsification de messages d'accusation. En effet, les nœuds malveillants peuvent employer des accusations afin de provoquer la révocation de nœuds honnêtes, en dégradant ainsi la performance du réseau.

ARS et SDRP sont deux systèmes de révocation que nous avons proposés pour résoudre ce problème. Nous avons analysé la performance d'ARS, et nous avons trouvé à travers la démonstration mathématique de certaines propriétés et l'évaluation des résultats de simulation qu'ARS présente de meilleurs résultats. En effet, dans ARS le nombre de messages d'accusation nécessaires pour la révocation de nœuds malveillants est adaptatif. Les nœuds peuvent être

révoqués avec peu de messages d'accusation, s'il n'y a pas de risque de mettre en péril la disponibilité dans le réseau. De plus, nous avons démontré qu'avec ARS, l'impact des nœuds malveillants sur la performance du système et sur la rapidité de leur révocation sont directement proportionnels à leur taux de présence dans le système.

SDRP est un nouveau système de révocation que nous avons proposé pour les VANETs. La particularité de ce système est qu'il est le premier système de révocation à la demande. SDRP coopère avec le protocole de routage afin d'éviter les nœuds relais malveillants rapidement. Les résultats de simulations montrent l'efficacité de SDRP et sa supériorité par rapport aux autres systèmes de révocation existants.

La protection de la vie privée des occupants de véhicules est obligatoire afin que les futurs réseaux véhiculaires prennent place chez les utilisateurs. L'approche la plus fiable pour assurer l'anonymat de véhicules est d'employer les pseudonymes. Ces derniers ont un cycle de vie spécifique comprenant les phases suivantes: la génération, l'émission, l'utilisation, la révocation et la résolution de pseudonymes. Ces phases peuvent coexister simultanément, ce qui pose des défis sans précèdent pour la révocation de ces pseudonymes. En effet, les véhicules malveillants possèdent suffisamment de pseudonymes à un moment donné et peuvent les changer sans suivre les démarches appropriées nécessaires à l'opération, et par conséquent ils peuvent causer une attaque de succession d'accusations qui leurs permet d'amplifier leur impact négatif sur la performance du système.

Pour adapter les systèmes de révocation locale existant aux réseaux véhiculaires employant le pseudonymat, et rendre la révocation de pseudonyme efficace, nous avons proposé un nouveau système dans lequel nous avons spécifié les démarches nécessaires pour améliorer la performance de révocation locale de pseudonymes. Les résultats de simulation ont montré que notre approche permet de détecter les nœuds malveillants de manière efficace même en présence d'attaques coordonnées de nœuds malveillants.

Comme extensions futures à notre travail nous proposons :

- La simulation de notre système de révocation de pseudonymes avec d'autres techniques de révocation locale.
- L'utilisation d'autres simulateurs pour évaluer la performance de notre système.
- La démonstration mathématique des autres propriétés des systèmes de révocation proposés.

References

[1] Department of Violence and Injury Prevention and Disability, “Injuries and violence: the facts,” Geneva,Switzerland, 2010.

[2] “L’automobile et la sécurité,” 2008. [Online]. Available: http://www.valeo.com/fr/communiques-presse/. [Accessed: 02-Apr-2016].

[3] A. M. Vegni, M. Biagi, and R. Cusani, *Smart Vehicles , Technologies and Main Applications in Vehicular Ad hoc Networks*. Rome, Italy: INTECH, 2013.

[4] S. Gillani, I. Khan, S. Qureshi, and A. Qayyum, “Vehicular Ad Hoc Network (VANET): Enabling Secure and Efficient Transportation System,” *Tech. J. Univ. Eng. Technol.*, vol. 13, 2008.

[5] U. S. D. of T. Federal Highway Administration, “Reducing Highway Fatalities.” [Online]. Available: http://safety.fhwa.dot.gov/facts/road factsheet.htm. [Accessed: 08-May-2016].

[6] M. K. Nasir, R. Md Noor, M. A. Kalam, and B. M. Masum, “Reduction of Fuel Consumption and Exhaust Pollutant Using Intelligent Transport Systems,” *Sci. World J.*, vol. 2014, pp. 1–13, 2014.

[7] European Conference of Ministers of Transport, *Gérer la congestion urbaine*. PARIS, FRANCE: OECD, 2010.

[8] G. Tasseron and K. Martens, “Urban parking space reservation through bottom-up information provision: An agent-based analysis,” *Comput. Environ. Urban Syst.*, vol. 64, no. July, pp. 30–41, Jul. 2017.

[9] A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, “Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications,” vol. 548, no. March, 2017, pp. 39–51.

[10] U. S. D. of Transportation, “ITS Research Initiatives.” [Online]. Available: https://ntl.bts.gov/lib/jpodocs/repts_te/14429_files/ch3.html. [Accessed: 02-Mar-2017].

[11] “ZXRIS 8900 Outdoor Road Side Unit.” [Online]. Available: http://wwwen.zte.com.cn/pub/en/products/wireless/rfid/microwave_band_products/201101/t20110104_198995.html. [Accessed: 04-Mar-2017].

[12] “Quand la voiture pilote.” [Online]. Available: http://www.cnewsmatin.fr/technologie/2014-02-05/quand-la-voiture-pilote-654902. [Accessed: 05-Apr-2017].

[13] E. Bergenheim, T. von Eichwald, G. Hallneus, and M. Erlingfors, “Pedestrian protection airbag,” US 20130200603 A1, 2013.

[14] “Honda demonstrates pedestrian and motorcycle safety technology.” [Online]. Available: http://motioncars.inquirer.net/13299/honda-demonstrates-pedestrian-and-motorcycle-safety-technology. [Accessed: 26-Mar-2016].

[15] M. JERBI, “Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections,” 2008.

[16] M. Fiore, J. Härri, F. Filali, and C. Bonnet, “Vehicular mobility simulation for VANETs,” in *Proceedings - Simulation Symposium*, 2007.

[17] R. S. Raw, M. Kumar, and N. Singh, “Security Challenges, Issues and Their Solutions for VANET,” *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 5, pp. 95–105, 2013.

[18] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Veh. Commun.*, vol. 7, pp. 7–20, 2017.

[19] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in *Proceedings of the 3rd {ACM} workshop on Security of ad hoc and sensor networks*, 2005, pp. 11–21.

[20] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2010.

[21] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” *Ad Hoc Networks*, vol. 61, pp. 33–50, Jun. 2017.

[22] G. Samara, W. A. H. Al-Salihy, and R. Sures, “Security Analysis of Vehicular Ad Hoc Nerworks (VANET),” in *2010 Second International Conference on Network Applications, Protocols and Services*, 2010, pp. 55–60.

[23] M. S. Al-kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs),” in *2012 6th International Conference on Signal Processing and Communication Systems*, 2012, pp. 1–9.

[24] M. Azees, P. Vijayakumar, and L. J. Deboarh, “EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 99, no. PP, pp. 1–10, 2017.

[25] M. L. Psiaki and T. E. Humphreys, “GPS Lies,” *IEEE Spectr.*, vol. 53, no. 8, pp. 26–53, 2016.

[26] “University of Texas students send yacht off-course with GPS exploit.” [Online]. Available: https://www.engadget.com/2013/07/30/university-of-texas-yacht-hack-experiment/. [Accessed: 02-Mar-2016].

[27] M. Franeková, P. Hole, E. Bubeníková, and A. Kanáliková, “Transport scenarios analysis within C2C communications focusing on security aspects,” in *IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2017, pp. 461–466.

[28] L. Buttyán and L. Csik, “Tamper resistant devices Tamper Proof Modules - Overview,” 2007.

[29] “1609 WG - Dedicated Short Range Communication Working Group.” [Online]. Available: https://standards.ieee.org/develop/wg/1609_WG.html. [Accessed: 20-Mar-2017].

[30] I. Transportation, S. Committee, I. Vehicular, and T. Society, *IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages IEEE Vehicular Technology Society*, vol. 2013, no. April. 2013.

[31] J. H. Zhang, M. Xu, and X. N. Su, “An Efficient and Provably Secure Digital Signature Scheme Based on Elliptic Curve,” *Int. J. Comput. Appl. Math.*, vol. 12, no. 1, pp. 45–52, 2017.

[32] M. E. Nowatkowski, “CERTIFICATE REVOCATION LIST DISTRIBUTION IN VEHICULAR AD HOC NETWORKS A Dissertation By Of the Requirements for the Degree,” Georgia Institute of Technology, 2010.

[33] ETSI (European Telecommunications Standards Institute), “ETSI TS 103 097 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats,” 2013.

[34] J. Kang, S. Ok, J. Y. Kim, and E. Kim, “Software Implementation of WAVE Security Algorithms,” *J. Korea Acad.*, vol. 15, no. 3, pp. 1691–1699, 2014.

[35] B. Lonc and P. Cincilla, “Cooperative ITS security framework: Standards and implementations progress in Europe,” in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2016, pp. 1–6.

[36] E. Schoch and F. Kargl, “On the efficiency of secure beaconing in VANETs,” in *Proceedings of the third ACM conference on Wireless network security - WiSec ’10*, 2010.

[37] N. Bißmeyer, S. Mauthofer, J. Petit, M. Lange, M. Moser, D. Estor, M. Sall, M. Feiri, R. Moalla, M. Lagana, and F. Kargl, “PREparing SEcuRe VEhicle-to-X Communication Systems,” V2X Security Architecture (PRESERVE Project), 2014.

[38] B. Karp and H. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” in *MobiCom ’00 Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000.

[39] D. Huang, Y. Yan, C. Su, and G. Xu, “Prediction-based geographic routing over VANETs,” *Rev. Tec. la Fac. Ing. Univ. del Zulia*, vol. 39, no. 2, pp. 157–164, 2016.

[40] “Ns-2, The Network Simulator.” [Online]. Available: http://www.isi.edu/nsnam/ns/. [Accessed: 06-Jan-2017].

[41] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and a. Lioy, “On the Performance of Secure Vehicular Communication Systems,” *IEEE Trans. Dependable Secur. Comput.*, vol. 8, no. 6, pp. 898–912, Nov. 2011.

[42] M. Feiri, J. Petit, and F. Kargl, “Evaluation of congestion-based certificate omission in VANETs,” *2012 IEEE Veh. Netw. Conf.*, pp. 101–108, Nov. 2012.

[43] L. Lamport, “Constructing Digital Signatures from One Way Function,” California, USA, 1979.

[44] R. C. Merkle, “SECRECY, AUTHENTICATION, AND PUBLIC KEY SYSTEMS,” Stanford University, 1979.

[45] H. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, “Flooding-resilient broadcast authentication for VANETs,” in *Proceedings of the 17th annual international conference on Mobile computing and networking MobiCom 11*, 2011.

[46] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, “Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems,” 2016.

[47] E. Pr, K. I. Kossonou, and S. Pour, “Etude d’un système de localisation 3-D haute précision basé sur les techniques de transmission Ultra Large Bande à basse consommation d ’ énergie pour les objets mobiles communicants,” Université de valenciennes et du hainaut-cambresis, 2014.

[48] O. J. Woodman and R. K. Harle, “Concurrent scheduling in the Active Bat location system,” in *8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2010, pp. 431–437.

[49] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, “The Cricket Location-Support

System," vol. 2000, no. August, 2000.

[50] H. Balakrishnan, T. Supervisor, and A. C. Smith, "The Cricket Indoor Location System," *Architecture*, vol. 16, no. 2001, p. 199, 2005.

[51] A. Fascista, G. Ciccarese, A. Coluccia, and G. Ricci, "A Localization Algorithm Based on V2I Communications and AOA Estimation," *IEEE Signal Process. Lett.*, vol. 24, no. 1, pp. 126–130, Jan. 2017.

[52] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Secur. Commun. Networks*, vol. 3, no. 4, pp. 289–302, Jul. 2010.

[53] P. Ardelean, "Implementation and Evaluation of Certificate Revocation List Distribution for Vehicular Ad-hoc Networks," EPFL, 2009.

[54] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing Vehicular Communications," *IEEE Wirel. Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[55] J. J. Haas, Y. C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 595–604, 2011.

[56] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking - VANET '09*, 2009, p. 89.

[57] B. Huang, J. Mo, Q. Lu, and W. Cheng, "Optimizing Propagation Network of Certificate Revocation in VANET with Meet-Table," in *Security, Privacy and Anonymity in Computation, Communication and Storage: SpaCCS 2016*, 2016, pp. 147–154.

[58] H.-S. Hong and H.-G. Kim, "A Regional Certificate Revocation List Distribution Method based on the Local Vehicle Location Registration for Vehicular Communications," *J. Korea Soc. Comput. Inf.*, vol. 21, no. 1, pp. 91–99, 2016.

[59] C. Caballero-Gil, J. Molina-Gil, J. Hernández-Serrano, O. León, and M. Soriano-Ibañez, "Providing k-anonymity and revocation in ubiquitous VANETs," *Ad Hoc Networks*, vol. 36, pp. 482–494, 2016.

[60] J. R. Singh, A. Kumar, D. Singh, and R. K. Dewang, "A Single-Hop Based Fast Certificate Revocation Protocol in VANET," in *2016 2nd International Conference on Computational Intelligence and Networks (CINE)*, 2016, pp. 23–28.

[61] C. I. Djamaludin, E. Foo, S. Camtepe, and P. Corke, "Revocation and update of trust in autonomous delay tolerant networks," *Comput. Secur.*, vol. 60, pp. 15–36, Jul. 2016.

[62] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. 6th Annu. Int. Conf. Mob. Comput. Netw. MobiCom 00*, vol. 1, pp. 255–265, 2000.

[63] M. N. Mejri and J. Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs," *IEEE Trans. Mob. Comput.*, vol. 16, no. 3, pp. 759–771, Mar. 2017.

[64] P. Maheshwaran and S. Rajagopal, "A scheme for detecting the types of misbehaviour and identifying the attacks using reputation mechanism in a mobile ad-hoc network," in *2016 International Conference on Communication and Electronics Systems (ICCES)*, 2016, pp. 1–6.

[65] H. Sedjelmaci, S. M. Senouci, and T. Bouali, "Predict and prevent from misbehaving

intruders in heterogeneous vehicular networks," *Veh. Commun.*, vol. 1, pp. 1–10, Dec. 2016.

[66] N. Rafique, M. A. Khan, N. A. Saqib, F. Bashir, C. Beard, and Z. Li, "Black Hole Prevention in VANETs Using Trust Management and Fuzzy Logic Analyzer," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 9, p. 1226, 2016.

[67] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems - MSWiM '09*, 2009, p. 106.

[68] M. Raya, M. Raya, J. Hubaux, and J. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, pp. 39–68, 2007.

[69] R. R. Pavithra and V. R. Nagarajan, "A survey on certificate revocation scheme using various approaches," *Indian J. Innov. Dev.*, vol. 5, no. 5, pp. 1–3, 2016.

[70] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings 19th International Conference on Data Engineering (Cat. No.03CH37405)*, 2003, pp. 197–213.

[71] J. Clulow and T. Moore, "Suicide for the common good," *ACM SIGOPS Oper. Syst. Rev.*, vol. 40, no. 3, pp. 18–21, 2006.

[72] T. Moore, J. Clulow, S. Nagaraja, and R. Anderson, "New strategies for revocation in ad-hoc networks," *Proc. 4th Eur. Conf. Secur. Priv. ad-hoc Sens. networks*, pp. 232–246, 2007.

[73] C. Crépeau and C. R. Davis, "A certificate revocation scheme for wireless ad hoc networks," *Proc. 1st ACM Work. Secur. ad hoc Sens. networks SASN 03*, p. 54, 2003.

[74] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, "Fast Exclusion of Errant Devices from Vehicular Networks," *2008 5th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks*, pp. 135–143, Jun. 2008.

[75] N. Chaib, N. Lagraa, M. Yagoubi, and A. Lakas, "Unthresholded adaptive revocation technique in mobile ad hoc networks," *Proc. 8h ACM Symp. QoS Secur. Wirel. Mob. networks - Q2SWinet '12*, p. 75, 2012.

[76] H. Koskinen, H. Koskinen, P. Lassila, P. Lassila, a Penttinen, a Penttinen, J. Virtamo, and J. Virtamo, "Random Waypoint Model in Wireless Networks," *Wirel. Networks*, pp. 1–55, 2005.

[77] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[78] Y. C. Tseng, S. Y. Ni, Y. S. Chen, and J. P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wirel. Networks*, vol. 8, no. 2–3, pp. 153–167, 2002.

[79] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[80] L. Wang, K. Chen, Y. Long, and H. Wang, "Cryptanalysis of a certificateless aggregate signature scheme," *Secur. Commun. Networks*, vol. 9, no. 22, 2016.

[81] J. Zhang, X. Zhao, and J. Mao, "Attack on Chen et al. 's certificateless aggregate signature

scheme," *Secur. Commun. Networks*, vol. 9, no. 1, pp. 54–59, Jan. 2016.

[82] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing," *Proc. 2008 IEEE Int. Conf. Veh. Electron. Safety, ICVES 2008*, pp. 346–353, 2008.

[83] N. Chaib, N. Lagraa, and M. B. Yagoubi, "SDRP : a secure distributed revocation protocol for vehicular environments," *Secur. Commun. NETWORKS Secur.*, vol. 9, no. 4, pp. 279–289, 2016.

[84] M. Gerlach and F. Güttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," *IEEE Veh. Technol. Conf.*, pp. 2521–2525, 2007.

[85] P. Papadimitratos, "Privacy and Identity Management for Vehicular Communication Systems : a Position Paper," in *Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[86] S. Zeng, Y. Chen, S. Tan, and M. He, "Concurrently deniable ring authentication and its application to LBS in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 844–856, 2017.

[87] R. Boguslaw and A. F. Westin, "Privacy and Freedom.," *Am. Sociol. Rev.*, vol. 33, no. 1, p. 173, 1968.

[88] B. Pechiammal and J. A. Renjith, "Survey on Effective Approach of Automatic License Plate Recognition (ALPR)," *Int. Res. J. Eng. Technol.*, vol. 04, no. 04, pp. 3477–3482, 2017.

[89] "Imagsa Technologies." [Online]. Available: http://www.roadtraffic-technology.com/contractors/detection/imagsa/imagsa1.html. [Accessed: 24-Apr-2017].

[90] A. Cavoukian and D. Ph, "SURVEILLANCE , THEN AND NOW : Securing Privacy in Public Spaces," no. June, 2013.

[91] T. B. Ptv, A. Kung, and M. K. Uber, "PRivacy Enabled Capability In Cooperative Systems and Safety Applications," 2009.

[92] A. Pfitzmann and M. Kohntopp, "Anonymity, Unobservability, and Pseudonymity ? A Proposal for Terminology," in *Designing Privacy Enhancing Technologies Technologies*, H. Federrath, Ed. Springer Berlin Heidelberg, 2001, pp. 1–9.

[93] D. Chaum, "Untraceable Electronic Mail , Return Addresses , and Digital Pseudonyms," *Commun. ACM*, vol. 24, no. 2, 1981.

[94] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization : Pseudonymity , and Identity Management," Dresden, Germany, 2010.

[95] E. C. Pons, G. Baldini, and D. Geneiatakis, "A wireless propagation analysis for the frequency of the pseudonym changes to support privacy in VANETs," Ispra, Italy, 2017.

[96] J.-M. Bohli and A. Pashalidis, "Relations among privacy notions," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–24, May 2011.

[97] L. M. S. Jaimes, K. Ullah, and E. dos Santos Moreira, "ARS: Anonymous reputation system for vehicular ad hoc networks," in *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, 2016, pp. 1–6.

[98] C. Wang, D. Shi, X. Xu, and J. Fang, "An anonymous data access scheme for VANET using pseudonym-based cryptography," *J. Ambient Intell. Humaniz. Comput.*, vol. 7, no. 1, pp. 63–

71, 2016.

[99] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, “Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs,” *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5460–5471, 2016.

[100] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, 2010.

[101] R. K üsters, T. Truderung, and A. Vogt, “Accountability,” in *Proceedings of the 17th ACM conference on Computer and communications security - CCS ’10*, 2010.

[102] M. Mungan, “Conditional Privacy Rights,” *J. Institutional Theor. Econ. JITE*, vol. 173, no. 1, pp. 114–131, Mar. 2017.

[103] J. Kilian and E. Petrank, “Identity Escrow,” *Adv. Cryptol. — CRYPTO ’98*, vol. 1462, pp. 169–185, 1998.

[104] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, “A classification of location privacy attacks and approaches,” *Pers. Ubiquitous Comput.*, vol. 18, pp. 163–175, 2014.

[105] F. Scheuer, K.-P. Fuchs, and H. Federrath, “A Safety-Preserving Mix Zone for VANETs,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6863 LNCS, 2011, pp. 37–48.

[106] M. Humbert, M. H. Manshaei, J. Freudiger, and J. P. Hubaux, “Tracking games in mobile networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6442 LNCS, pp. 38–57, 2010.

[107] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” *WONS 2010 - 7th Int. Conf. Wirel. On-demand Netw. Syst. Serv.*, pp. 176–183, 2010.

[108] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust location privacy scheme for VANET,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, 2007.

[109] Y. A. Al-Khassawneh and N. Salim, “On the Use of Data Mining Techniques in Vehicular Ad Hoc Network,” in *Advanced Machine Learning Technologies and Applications*, Springer, 2012, pp. 449–462.

[110] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” *Proc. - 12th IEEE Int. Conf. Comput. Sci. Eng. CSE 2009*, vol. 3, no. March, pp. 139–145, 2009.

[111] ETSI, “Intelligent Transport Systems (ITS): Security Services and Architecture,” sophia antipolis, 2010.

[112] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 228–255, Jan. 2015.

[113] H. Jin and P. Papadimitratos, “Proactive certificate validation for VANETs,” in *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, pp. 1–4.

[114] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” *Work. hot Top. networks*, no. 4, pp. 1–6, 2005.

[115] RITA - Intelligent Transportation Systems, “Security Credential Management System Design

Security system design for cooperative vehicle- to-vehicle crash avoidance applications using 5 . 9 GHz Dedicated Short Range Communications (DSRC) wireless communications," 2012.

[116] H. S. N. Bissmeyer, "A generic public key infrastructure for securing car-to-x communication," in *18th World Congress on Intelligent Transport Systems*, 2011.

[117] L. L. Wang, G. Z. Liu, L. j. Sun, and Y. W. Lin, "An Effective Pseudonym Generating Scheme for Privacy and Anonymity in VANETs," in *International Conference on Information System and Artificial Intelligence (ISAI)*, 2016, pp. 267–270.

[118] J. Song, Y. Zhuang, J. Pan, and L. Cai, "Certificateless secure upload for drive-thru internet," *IEEE Int. Conf. Commun.*, 2011.

[119] M. Wolf and T. Gendrullis, "Design, Implementation, and evaluation of a vehicular hardware security module," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7259 LNCS, pp. 302–318, 2012.

[120] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice," *IEEE Wirel. Commun. Netw. Conf. WCNC*, no. March, pp. 3402–3407, 2007.

[121] A. Boualouache, S. Senouci, and S. Moussaoui, "Towards an Efficient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, no. i, pp. 1–7.

[122] H. Artail and N. Abbani, "A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 106–119, 2016.

[123] A. Boualouache and S. Moussaoui, "TAPCS: Traffic-aware pseudonym changing strategy for VANETs," *Peer-to-Peer Netw. Appl.*, pp. 1–13, 2016.

[124] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting Location Privacy: Optimal Strategy against Localization Attacks," 2012.

[125] N. J. Aruna, M. D. Nandhini, and K. S. Ganesh, "Differential Privacy for preserving user Privacy on Selective Aggregation," *Int. J. Eng. Sci. Comput.*, vol. 7, no. 3, pp. 5350–5352, 2017.

[126] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (sraac)," *4th Work. Embed. Secur. Cars (ESCAR 2006)*, 2006.

[127] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2010, pp. 1 – 6.

[128] N. Bibmeyer, J. Petit, and K. M. Bayarou, "Copra: Conditional pseudonym resolution algorithm in VANETs," in *2013 10th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 2013, pp. 9–16.

[129] S. P. Mirashe and N. V Kalyankar, "Cloud Computing," *Commun. ACM*, vol. 51, no. 7, p. 9, Mar. 2010.

[130] E. Parliament, “European data protection supervisor,” *EN Off. J. Eur. Union*, vol. 47, no. 6, pp. 1–13, 2010.

[131] L. Gollan and C. Meinel, “Digital signatures for automobiles,” *Proc. Syst. Cybern. Informatics (SCI ’02)*, 2002.

[132] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, “Security Issues in a Future Vehicular Network,” *Symp. A Q. J. Mod. Foreign Lit.*, vol. 35, pp. 270–274, 2002.

[133] J. P. Hubaux, S. Čapkun, and J. Luo, “The security and privacy of smart vehicles,” *IEEE Secur. Priv.*, vol. 2, no. Ivc, pp. 49–55, 2004.

[134] K. Zeng, “Pseudonymous pki for ubiquitous computing,” *Public Key Infrastruct.*, vol. 4043, pp. 207–222, 2006.

[135] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, “4th Workshop on Mobile Ad-Hoc Networks (WMAN), Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication,” *4th Work. Mob. AdHoc Networks WMAN*, no. March, pp. 1–12, 2007.

[136] D. Smith, “Secure pseudonymisation for privacy-preserving probabilistic record linkage,” *J. Inf. Secur. Appl.*, vol. Online, Jan. 2017.

[137] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” *Proc. fourth ACM Int. Work. Veh. ad hoc networks VANET 07*, vol. 07, p. 19, 2007.

[138] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, “Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping,” *2010 IEEE Veh. Netw. Conf. VNC 2010*, pp. 174–181, 2010.

[139] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Grutese, W. Trappe, and I. Seskar, “Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study.,” *19th USENIX Secur. Symp.*, vol. 39, pp. 11–13, 2010.

[140] Y. Pan, J. Li, L. Feng, and B. Xu, “An analytical model for random changing pseudonyms scheme in VANETs,” *Proc. - 2011 Int. Conf. Netw. Comput. Inf. Secur. NCIS 2011*, vol. 2, pp. 141–145, 2011.

[141] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN : Providing Location Privacy for VANET,” in *Proc. of the Workshop on Embedded Security in Cars (ESCAR)*, 2005, pp. 1–15.

[142] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, “Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy,” *Wpes’06*, pp. 19–28, 2006.

[143] S. Eichler, “Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility,” *2007 IEEE Intell. Veh. Symp.*, pp. 541–546, 2007.

[144] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A Practical pseudonym changing scheme for location privacy in VANETs,” in *2009 IEEE Vehicular Networking Conference (VNC)*, 2009, pp. 1–8.

[145] B. K. Chaurasia and S. Verma, “Optimizing Pseudonym Updation for Anonymity in VANETS,” *2008 IEEE Asia-Pacific Serv. Comput. Conf.*, pp. 1633–1637, Dec. 2008.

[146] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar, “Pseudonym based mechanism for sustaining privacy in VANETs,” *2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009*, pp. 420–425, 2009.

[147] Q. A. Arain, Z. Deng, I. Memon, A. Zubedi, J. Jiao, A. Ashraf, and M. S. Khan, “Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks,” *China Commun.*, vol. 14, no. 4, pp. 89–100, Apr. 2017.

[148] L. Buttyán, T. Holczer, and I. Vajda, “On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs,” in *Security and Privacy in Ad-hoc and Sensor Networks*, vol. 4572, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 129–141.

[149] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, 2012.

[150] J. Liao and J. Li, “Effectively Changing Pseudonyms for Privacy Protection in VANETs,” *2009 10th Int. Symp. Pervasive Syst. Algorithms, Networks*, pp. 648–652, 2009.

[151] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-Zones for Location Privacy in Vehicular Networks,” *ACM Work. Wirel. Netw. Intell. Transp. Syst.*, 2007.

[152] A. Wasef and X. Shen, “REP: Location privacy for VANETs using random encryption periods,” *Mob. Networks Appl.*, vol. 15, pp. 172–185, 2010.

[153] M. Gerlach, “Assessing and Improving Privacy in VANETs,” *Proc. Fourth Work. Embed. Secur. Cars ESCAR*, 2006.

[154] J. Freudiger, M. H. Manshaei, J. Hubaux, and D. C. Parkes, “On Non-Cooperative Location Privacy : A Game-Theoretic Analysis Categories and Subject Descriptors,” in *the 16th ACM conference on Computer and communications security*, 2009, pp. 324–337.

[155] M. E. Nowatkowski and H. L. Owen, “Scalable certificate revocation list distribution in vehicular ad hoc networks,” *2010 IEEE Globecom Work. GC’10*, pp. 54–58, 2010.

[156] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, “Analysis of certificate revocation list distribution protocols for vehicular networks,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, 2010.

[157] F. Schaub, “Conditional Pseudonymity in Vehicular Ad Hoc Networks,” Ulm University, 2008.

[158] Z. Ma, F. Kargl, and M. Weber, “Pseudonym-on-demand: A new pseudonym refill strategy for vehicular communications,” *IEEE Veh. Technol. Conf.*, pp. 1–5, 2008.

[159] D. Förster, F. Kargl, and H. Löhr, “PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks,” *Ad Hoc Networks*, vol. 37, no. Special Issue on Advances in Vehicular Networks, pp. 122–132, Feb. 2016.

[160] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, “REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks,” in *Trust and Trustworthy Computing*, vol. 9229, Springer International Publishing, 2015, pp. 193–208.

[161] J. Timpner and L. Wolf, “Query-response geocast for vehicular crowd sensing,” *Ad Hoc Networks*, vol. 36, no. 2, pp. 435–449, 2016.

[162] J. Wang, Y. Zhang, Y. Wang, and X. Gu, “RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs,” *Int. J. Distrib. Sens. Networks*, vol. 2016, 2016.

[163] P. T. N. Diep and C. K. Yeo, “A trust-privacy framework in vehicular ad hoc networks (VANET),” in *Wireless Telecommunications Symposium (WTS)*, 2016, vol. 2016-May, pp. 1–7.

[164] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, “EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks,” *Pervasive Mob. Comput.*, vol. 21, pp. 75–91, Aug. 2015.

[165] B. Liu, J. T. Chiang, and Y. Hu, “Limits on Revocation in VANETs,” in *8th International Conference on Applied Cryptography and Network Security*, 2010.

[166] N. Chaib, N. Lagraa, and M. B. Yagoubi, “EPRV : Efficient Pseudonym Revocation in VANETs,” *Ad Hoc Sens. Wirel. Networks*, 2017.

[167] Y. Pan and J. Li, “Cooperative pseudonym change scheme based on the number of neighbors in VANETs,” *J. Netw. Comput. Appl.*, vol. 36, no. 6, pp. 1599–1609, Nov. 2013.

[168] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening privacy protection in VANETs,” *Proc. - 4th IEEE Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2008*, pp. 508–513, 2008.

[169] M. Mitzenmacher, “Compressed Bloom filters,” *IEEE/ACM Trans. Netw.*, vol. 10, no. 5, pp. 604–612, Oct. 2002.

[170] J. Camenisch and A. Lysyanskaya, “Signature Schemes and Anonymous Credentials from Bilinear Maps,” in *CRYPTO 2004: Advances in Cryptology*, vol. 3152, 2004, pp. 56–72.

[171] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” in *EUROCRYPT 2003: Advances in Cryptology*, 2003, pp. 416–432.

Glossaire

AC	Autorité de Certification
AIDAM	Autonomous Intrusion Detection/Advertisement Module
ALM	Accusation List Manager
ALPR	Automatic Licence Plate Reader
AoA	Angle of Arrival
APM	Accusation Processing Module)
ARS	Adaptive Revocation Scheme
ART	Acceptance Range Threshold
ASTM	American Society for Testing and Materials
CA	Certificate Authority
CAC	Communauté d'Accusation
CAMP	Crash Avoidance Partnership
CbCO	Congestion based Certificate Omission
CPL	Cryptographic Packet Loss
CRL	Certificate revocation list
DAPM	Duplicate Accusations Prevention Mechanism
DM	Durée de vie Moyenne de pseudonymes des noeuds malveillants
DoS	Denial of Service
DR	Detection rate
ECDSA	Elliptic curve digital signature algorithm
EED	End-to-End Delay
ELP	Electronic License Plate
EPRV	Efficient Pseudonym Revocation in VANETs
FMA	Falsification de Messages d'Accusation
FPR	False Positive Rate
IDS	Intrusion Detection system
IRM	Instantaneous Revocation Mechanism
LEAVE	Local Eviction of Attackers by Voting Evaluators
LRC	Liste de Révocation de Certificat
MANET	Mobile Ad-hoc NETworks
MDM	Misbehaviour Detection Module
MDT	Maximum Density Threshold
MGT	Mobility Grade Threshold
MTD	Minimum Time for Detection
MTS	Merkle Tree Signature
NAM	Neighbors' Advertiser Module
NbCO	Neighbor-based Certificate Omission
NHTSA	National Highway Traffic Safety Administration
NNMA	Nombre Nécessaire de Messages d'Accusation

NRAM	Number of required Accusation Messages
OBU	On Board Unit
OTS	One-Time Signature
PDR	Packet delivery ratio
PIA	Pseudonyme Issuing Authority
POoC	Periodic Omission of Certificates
PP	Pseudonyme Provider
RA	Registration Authority
RDM	Revocability Decision Manager
RSS	Received Signal Strength
RSU	Road Side Unit
RWP	Randome Way Point
SDRP	Secure Distributed Revocation Protocol
SS	Social Spot
STI	Système deTransport Intelligent
SV	Système de Vote
ToA	Time of Arrival
TPD	Tamper Proof Device
US FCC	United States Federal Communications Commission
USDOT	U.S. Department of Transportation
V2I	Communication de Véhicule à Infrastructure
V2P	Communication de Véhicule à Piéton
V2V	Communication Véhicule-à-Véhicule
VANET	Vehicular Ad hoc Network
VID	Vehicle IDentifier
VIN	Vehicle Identification Number
WAVE	Wireless Access for the Vehicular Environment
WRM	WAVE Resource Manager