République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira, Bejaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de master en Informatique

Option : Administration et sécurité des réseaux

Thème

Gestion des clés dans les réseaux véhiculaires

Réalisé par :

M^lle^, ABBAS Sonia

M^lle^, IBACHIRENE Melissa

Encadré par :

M. NAFI Mohammed

Devant le jury composé de :

Président : M.BAADACHE Abderahmane

Examinateur : M.ALOUI Abdelouhab

Examinatrice : M^me^.CHERIFI Feriel

Promotion : 2016/2017

Remerciements

En guise de remerciements, nous tenons à féliciter toutes les personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire et à sa réussite. Nous tenons également à remercier chaleureusement ***M.NAFI MOHAMMED****, qui, en tant qu'encadrant, nous a été d'une aide précieuse et s'est montré toujours présent pour nous tout au long de la réalisation de ce mémoire. Nos remerciements vont également à l'ensemble du jury pour avoir accepté de juger notre travail. Enfin, nous adressons nos plus sincères remerciements à nos parents et ami(e)s, pour leur soutien et encouragements au cours de cette année universitaire. Merci à tous et à toutes.*

Dédicaces

A nous.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACK : Acquittement.

CA : Certificate Authority.

CVIS : Cooperative Vehicle-Infrastructure Systèms.

C2C-CC : CAR 2 CAR Communication Consortium.

DoS : Denial of Service.

EVITA : E-Safety Vehicle Intrusion Protected Applications.

GeoNet : Geographic addressing and routing for vehicular communications.

GPS : Global Positioning System.

IHM : Interface Homme-Machine.

ID : Identifiant.

IP : Internet Protocol.

INRIA : Institut national de recherche en informatique et en automatique.

LG : Leader de Groupe.

MANET : Mobile Ad-hoc NETwork.

MAC : Message Authentification Code.

MIMA : Man In Middle Attack.

NOW : Network On Wheels.

OBU : On-Board Unit.

PU : Principal User.

RSA : Rivest, Shamir, Adleman.

RSU : Road Side Unit.

SAVECOM : Secure Vehicle Communication.

SSK : Send Session Key.

STI : Système de Transport Intelligent.

SU : Secondary User.

TA : Trusted authority.

TPD : Tamper proof device.

TPM : Trusted platform module.

VANET : Vehicular Ad hoc Networks.

V2V : Véhicule à Véhicule.

V2I : Véhicule à Infrastructure.

Introduction générale

Les réseaux VANETs ne sont qu'une application des réseaux Ad Hoc mobiles(MANET). Ils constituent le noyau d'un Système de Transport Intelligent(STI) ayant comme objectif principal l'amélioration de la sécurité routière . En effet, grâce à des capteurs installés au sein de véhicules, ou bien situés au bord des routes et des centres de contrôle, les communications véhiculaires permettront aux conducteurs d'être avertis suffisamment tôt de dangers éventuels.

Les VANETs ont été conçus pour apporter un certain nombre d'avantages, tel que : la réduction des accidents de la circulation sur les routes, du confort de conduit et de voyage pour les conducteurs et les passagers, des moyens de paiement facile pour certains services tel les parking, du gaz, etc. Ces réseaux implémentent aussi des applications de sureté, de maintenance et de confort comme l'accès à une connexion Internet, les jeux en ligne et en réseau, les téléchargements audio et vidéo [20]. Toutes ces applications font appel à l'échange des messages comme les messages d'urgences, les avertissements sur les incidents survenus, sur les conditions de la route à des instants précis, et les informations d'aide à la conduite. Tous ces échanges font intervenir des données informatiques et le contenu des messages peut influer sur le comportement des conducteurs et ainsi changer la topologie du réseau. Ceci implique donc un risque de danger d'attaque par des usagers malveillants qui peuvent trafiquer les messages échangés sur le réseau [21]. Quelques attaques que l'on peut observer sur les VANETs sont : des attaques de blocage de la circulation, attaque de rejeux, attaque de mensonge sur les informations transmises, les attaques de déni de service, les attaques de mascarade, attaque de vol d'identité, attaque d'illusion, attaque sur les équipements de communication,...etc. [22].

Dans un VANET les véhicules éhangent des messages et communiquent entre eux. Cette situation peut donner lieu à des attaques de sécurité internes ou bien externes qui peuvent avoir pour objectifs de rendre le réseau non-fonctionnel, de causer un accident.La préservation de la sécurité des informations échangées entre les véhicules est une nécessité cruciale pour les VANETs. Une communication doit passer par l'analyse du potentiel des menaces de sécurité et la conception d'une architecture robuste capable de faire face à ces menaces. Dans la littérature plusieurs approches basées sur la cryptographie symétrique et d'autres

asymétrique ont été proposées dont la plupart traite le sujet de gestion de clés.

La problématique de notre étude est de mettre en place un système de gestion de clés qui servira à une bonne communication sécurisée entre les véhicules.

Ce mémoire est organisé en quatre chapitres. Nous présentons dans le premier chapitre les réseaux véhiculaires ainsi que leurs caractéristiques spécifique. Nous détaillons plus précisément, le système de communication utilisé tout en présentant les entités communicantes, les architectures de communication possibles.

Dans le deuxième chapitre, nous nous focalisons sur la sécurité. Nous décrivons tout d'abord les services et les mécanismes qui peuvent être mis en œuvre afin de réaliser la sécurité ainsi que la classification des attaques menaçant ce type de réseaux. Nous étudions aussi la gestion de clés et les exigences des systèmes de gestion de clés dans les réseaux VANET.

Le troisième chapitre sera consacré à la présentation de quelques solutions qui ont été proposés pour adresser le problème de gestion de clés. Une comparaison sera effectuée entre les différentes techniques utilisées.

En effectuant cet état de l'art nous allons finir par déceler les manques et delà résulte notre contribution qui est spécialement conçue afin de pouvoir résoudre le problème de compromission de nœuds et des RSU. Nous conclurons par une conclusion générale résumant les points essentiels qui ont été abordés ainsi que des perspectives que nous souhaitons accomplir prochainement.

Chapitre 1

Introduction au Réseaux VANET

Introduction

L'objectif de ce chapitre est de présenter tout d'abord les réseaux ad hoc de manière générale, puis, d'appréhender la notion de réseau sans fil véhiculaire et de définir le contexte de ce mémoire. Nous présentons dans un premier temps les applications potentielles. Ensuite, nous décrivons les entités communicantes, les architectures de communication et les caractéristiques des réseaux véhiculaires. Nous analysons les technologies d'accès utilisables afin de déployer ces applications, avant de présenter les standards de communication véhiculaire.

1.1 Réseaux Ad Hoc

Les réseaux ad hoc sont des réseaux sans fil capables de s'organiser spontanément et de manière autonome dans l'environnement dans lequel ils sont déployés sans infrastructure définie préalablement. La tâche de la gestion du réseau est repartie sur l'ensemble d'entités communicantes par liaison sans-fil, ces entités sont souvent appelées « Nœuds ». Dans ces réseaux, les entités envisagées sont des terminaux légers et de taille réduite qui fonctionnent sur batterie, donc elles ont des capacités de traitement et de mémoire limitées [1].

Les réseaux ad hoc, dans leur configuration mobile, sont connus sous le nom de MANET *(Mobile Ad-hoc NETwork)*. La figure suivante illustre un exemple d'un réseau Ad Hoc.

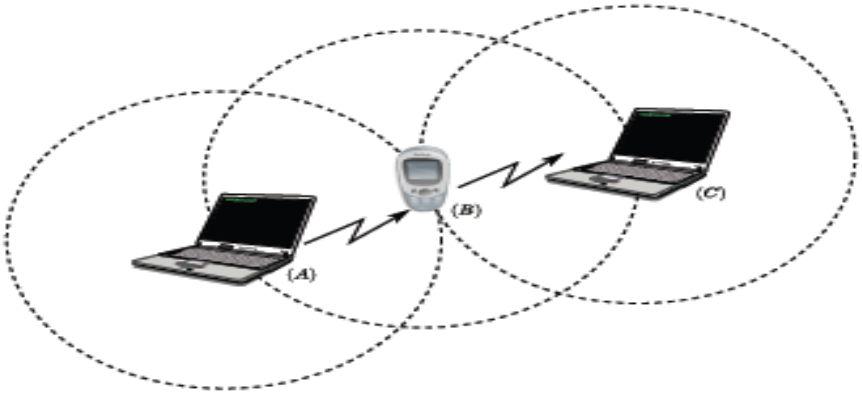

Figure 1.1 – Exemple de transmission d'un message dans un réseau ad hoc[1].

L'entité **A** veut communiquer avec **C**. Puisqu'elles sont hors de portée directe de transmission, **A** transmet son message vers **B**, qui à son tour le relaie vers **C** [1].

1.2 Réseaux ad hoc véhiculaires (VANET)

1.2.1 Définition

Les réseaux VANETs *(Vehicular Ad hoc Networks)* constituent une nouvelle forme de réseaux ad hoc mobiles (MANET). Par rapport à un réseau ad hoc classique, les réseaux VANET sont caractérisés par une forte mobilité des nœuds rendant la topologie du réseau fortement dynamique.

Pour la mise en place d'un tel réseau, certains équipements électroniques doivent être installés au sein de véhicules, tel : les dispositifs de perception de l'environnement (radars, caméras), un système de localisation GPS, et bien sûr une plateforme de traitement[2].

1.2.2 Caractéristiques des réseaux véhiculaires

Les réseaux VANETs peuvent être considérés comme une sous-classe des MANETs. La mobilité de leurs nœuds constitue la différence principale. Cette mobilité est souvent influencée par le comportement du conducteur et les contraintes de la mobilité comme la restriction de la vitesse routières.

Les principales caractéristiques de VANETs sont :

- **Capacité d'énergie et de stockage**

Contrairement au contexte des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les éléments du réseau VANET disposent suffisamment

d'énergie qui peut alimenter les différents équipements électroniques d'un véhicule intelligent. D'autant plus, les nœuds ont une capacité de traitement et de stockage de données suffisantes.

- **Environnement de communication**

Dans les réseaux véhiculaires, il est impératif de prendre en compte la grande diversité environnementale. Contrairement aux autres réseaux sans fil qui ont un environnement bien spécifique selon leur fonctionnement, les réseaux véhiculaires sont appelés à passer d'un environnement urbain caractérisé par de nombreux obstacles à la propagation des signaux, à un environnement rural ou autoroutier présentant des caractéristiques différentes.

- **Modèle de mobilité**

Les réseaux véhiculaires se distinguent également des réseaux sans fil ordinaires par un modèle de mobilité très dynamique dû à l'importante vitesse des nœuds qui réduit considérablement les durées de temps pendant lesquels les nœuds peuvent communiquer. En plus c'est difficile d'avoir un modèle de mobilité puisque les déplacements des nœuds sont liés à la volonté des conducteurs. D'autre part, on peut profiter de quelques exceptions pour construire une base d'infrastructure fondée sur des nœuds spécifiques que l'on connait bien, les routes que ces nœuds vont emprunter comme les bus de transports.

- **Sécurité et l'anonymat**

L'importance des informations échangées via les communications véhiculaires rend l'opération de sécurisation cruciale et constitue un prérequis au déploiement des VANETs.

- **Taille du réseau**

Sachant que les véhicules d'aujourd'hui et certainement de demain seront équipés majoritairement avec des interfaces de communications sans fil et vu la densité du pare automobile, on peut s'attendre à ce que la taille des réseaux véhiculaires, soit d'une tout autre ampleur. Ce qui fait de ce point une caractéristique majeur à prendre en considération dans la conception des différents protocoles de ces réseaux.

- **Modèle de communication**

Les réseaux véhiculaires ont été instauré principalement pour les applications liées à la sécurité routière et réduire les risques des accidents (ex. diffusion de messages d'alerte de collision). Dans ce type d'application, les communications se font presque exclusivement par diffusion successifs d'une source vers une ou plusieurs destinations. Le modèle de transmission en Broadcast on en Multicast est donc appelé à dominer largement dans les réseaux véhiculaires, ce qui risque d'avoir des conséquences importantes sur la charge du réseau et le modèle de sécurité à mettre en œuvre.

1.2.3 Applications offertes par les réseaux VANET

1. Applications de gestion du trafic routier

Les applications de gestion du trafic routier visent à optimiser le trafic routier et à prévenir la congestion. Grâce à la communication entre véhicules, ces derniers deviennent alors des capteurs de trafic. La granularité de l'information devient donc plus fine qu'avec la simple utilisation de bornes de comptage. Des exemples d'applications sont la coopération entre les véhicules afin de faciliter le passage des véhicules d'urgence, ou les itinéraires alternatifs. Ce dernier exemple est de plus en plus proposé par les systèmes de navigation actuels en cas d'embouteillage.

2. Applications de sécurité du trafic routier

Cette catégorie contient tous les services qui visent à améliorer la sécurité routière. Il s'agit d'améliorer le champ de vision du conducteur en lui proposant une aide à la conduite. Le conducteur pourra être informé qu'un véhicule vient de passer un feu rouge ou qu'un piéton est en train de traverser la route. Une application, qui est déjà déployée dans les véhicules haut de gamme, est le service SOS. En cas d'accident, lors du déclenchement de l'airbag (c'est-à-dire dans les dix millisecondes qui suivent la collision), un message est émis afin de prévenir le centre de secours le plus proche. Ce service permet d'économiser de précieuses minutes dans le processus d'arrivée des secours.

Dans cette catégorie, on retrouve les applications qui utilisent les informations des autres véhicules : l'alerte d'état de la route (verglas, obstacle), l'aide au dépassement (calcul des distances, vérification de l'angle mort), l'alerte de freinage ou de collision en amont du trajet. On remarque donc que les applications de sécurité du trafic routier ont un rôle majeur dans la réduction du nombre d'accidents.

Le service d'alerte de danger local permet à chaque véhicule de diffuser un message d'alerte afin de prévenir les véhicules arrivant dans la zone de danger. Cette application a donc de fortes contraintes temporelles, car recevoir un message d'alerte en retard met à mal le bien fondé de cette application et peut engendrer de graves conséquences comme les accidents. Nous distinguons deux types d'alerte en fonction de la gravite de l'alerte :

1. **Le cas d'un accident :** Ce service avertit les véhicules se dirigeant vers le lieu de l'accident que les conditions de circulation sont modifiées et qu'il est nécessaire de redoubler de vigilance. Il est nécessaire, également, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission.

2. **Le cas de ralentissement anormal (embouteillage, travaux, intempéries,...etc.) :** Ce service permet d'avertir les automobilistes de situations de circulation particulières. L'information, quelle que soit la nature des difficultés de circulation, renseigne l'automobiliste de la menace et qu'il est nécessaire de ralentir. Le message d'alerte est émis par un véhicule détectant les difficultés de circulation (freinage important, déclenchement des feux de détresse, pluie par exemple). Un véhicule banalisé effectuant des travaux peut également être à l'origine du message d'alerte. Comme pour le message d'alerte informant d'un accident, le message d'alerte informant d'un ralentissement doit être transmis aux autres véhicules de façon efficace et rapide.

3. Applications de confort

Cette catégorie comporte toutes les applications qui participent au confort du conducteur et qui ne relèvent pas de la gestion du trafic ni de la sécurité routière. Ces applications se présentent donc en tant que services fournis au conducteur.

Parmi ces applications, citons les panneaux d'annonces locales : d'ordre commercial comme les offres de restaurants, la présence de stations-service à proximité, ou culturel comme des informations touristiques relatives à la localisation du véhicule.

Il y a aussi des services télématiques comme le péage à distance sur autoroute, le paiement automatique dans les stations-service (ce qui peut faciliter la vie des handicapes). Un autre type d'application de confort est la communication à vocation de divertissement. Une offre de connexion Internet a bord avec vidéo à la demande en est un parfait exemple.

A toutes ces applications s'ajoutent aussi les communications point à point entre deux conducteurs qui voyagent ensemble. Ils peuvent ainsi s'échanger des messages ou partager des données (vidéo, musique, itinéraire, jeux en réseau). La vie des usagers pourra aussi être facilitée par le contrôle à distance de véhicule de manière électronique (vérification du permis de conduire, contrôle technique, plaque d'immatriculation) pour les services compétents (police, douane, gendarmerie).

1.2.4 Messagerie et architectures des réseaux véhiculaires

Un réseau véhiculaire est un ensemble d'entités communicantes organisées selon une architecture de communication. Ces entités embarquées peuvent rencontrer différents environnements (urbain, périurbain, autoroutier), ayant leurs contraintes propres. Comme le montre la figure suivante.

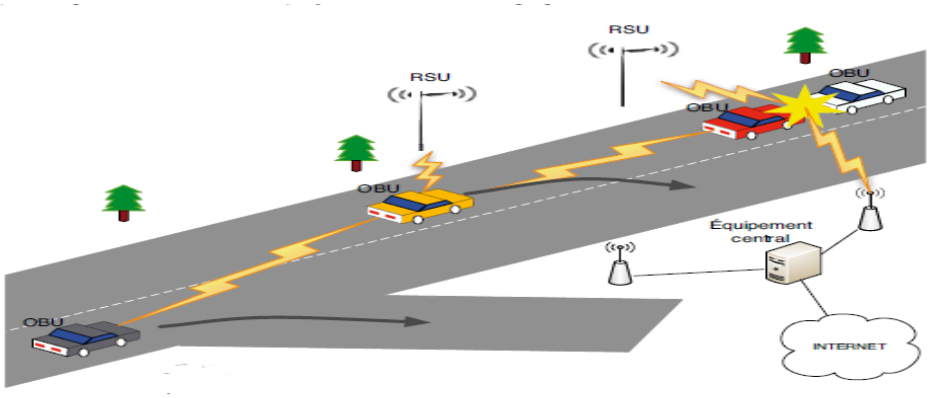

Figure 1.2 – Exemple d'un réseau véhiculaire[23].

1. Entités communicantes

Il existe quatre entités communicantes dans un réseau véhiculaire.

- **Les équipements personnels :** Sont les équipements qui peuvent être apportés par l'utilisateur à l'intérieur de son véhicule. Cela peut être un téléphone, un ordinateur portable ou encore un GPS autonome. Ces équipements peuvent interagir avec le véhicule. De nos jours, en activant l'interface Bluetooth du téléphone portable, on peut utiliser son téléphone par commande vocale (en utilisant les microphones intégrés au véhicule) ou par le biais de *l'interface Homme-Machine* (IHM) du véhicule.
- **Les véhicules modernes :** Sont équipés d'un ensemble de processeurs connectés à une plateforme centrale de calcul qui dispose d'interfaces filaires et sans fil. Les véhicules intelligents sont des véhicules équipés d'une unité nommée *On-Board Unit* (OBU). Cette unité peut enregistrer, calculer, localiser et envoyer des messages sur une interface réseau.

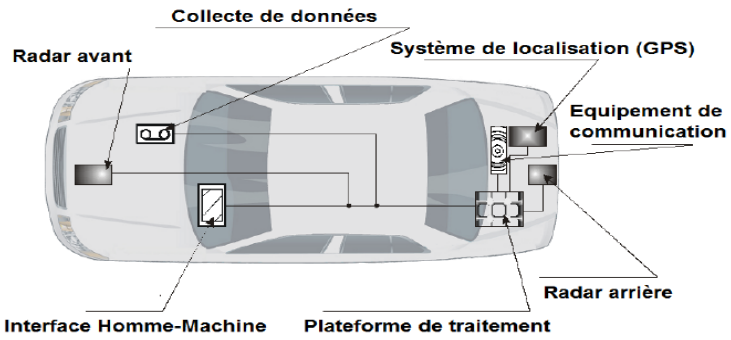

Figure 1.3 – Véhicule intelligent[24].

- **Les entités de bord de route :** Sont appelées *Road-Side Unit* (RSU). Ces unités peuvent informer les véhicules à proximité en diffusant les conditions de trafic, météorologiques ou spécifiques à la route (vitesse maximale, autorisation de dépassement,...etc.). Les RSU peuvent aussi jouer le rôle de station de base en relayant l'information envoyée par un véhicule.
- **L'équipement central :** Se situe du côté « Serveur ». Il est transparent pour l'utilisateur. Cet équipement central pourra être un serveur de stockage, un point d'entrée à un réseau filaire (Internet) ou un serveur de transaction (télépéage par exemple).

2. Types de messages

Les entités formant un réseau véhiculaire vont générer et s'échanger des messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer ou recevoir un message de contrôle, d'alerte ou autres.

a. **Message de contrôle :** Ce type de message fournit des informations sur l'état du réseau routier(trafic, travaux, météo). Il est généré à intervalle régulier, conventionnellement, chaque véhicule émet un message de contrôle toutes les 100 ms. Ce message, appelé aussi *« Beacon »*, contient la position, la vitesse, la direction et l'itinéraire du véhicule émetteur. Grâce aux messages de contrôle, chaque véhicule se crée une vue locale de son voisinage. Le véhicule peut aussi prédire et anticiper des situations accidentogénes ou de congestion. Le message de contrôle est l'équivalent du message *HELLO* des protocoles de routage. Chaque véhicule se fait donc connaitre de son voisinage direct. Bien entendu, les messages de contrôle ne sont pas transférés et utilisent une diffusion à un saut.

b. **Message d'alerte :** Le message d'alerte est généré lorsqu'un évènement est détecté. Cela peut être la détection d'un accident, d'un obstacle ou la réception d'un autre message d'alerte. Ce dernier doit être émis à intervalle régulier afin d'assurer la pérennité de l'alerte. Ainsi le ou les véhicules désignés pour la retransmission des messages émettront des alertes à instants réguliers. Les messages d'alerte doivent donc être de taille réduite pour être transmis le plus rapidement possible. Les messages contiennent en particulier les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

c. **Autres messages :** Ce type de message contient tous les messages qui ne sont ni messages d'alerte ni de contrôle. Ces messages ne sont généralement pas répétés à intervalle régulier. En effet, cela peut être par exemple un message de transaction financière ou l'envoi de courrier électronique. Tous les messages reçus seront stockés dans un « cache des messages récemment reçus ». Chaque message se verra associer une durée de vie dans le cache.

3. Architectures de communication

Les systèmes de gestion de trafic « conventionnels » sont basés sur des infrastructures centralisées ou des caméras et des capteurs implantés sur la route collectant des informations sur la densité et l'état du trafic. Ces informations sont transmises à une unité centrale pour les traiter et prendre les décisions adéquates. De tels systèmes exhibent un coût de déploiement assez important et se caractérisent par un temps de réaction de l'ordre de la minute pour le traitement et le transfert des informations.

Dans un contexte òu le délai de transmission de l'information est vital et revêt une importance majeure dans ce type de systèmes, ce délai est un véritable frein. De plus, les équipements mis en place sur les routes nécessitent une maintenance périodique et chère. Par conséquent, pour déployer un tel système à large échelle, un important investissement dans l'infrastructure de communication et de capteurs est nécessaire.

Cependant, avec le développement rapide des technologies de communication sans fil, des systèmes de localisation et de collecte d'information par capteurs, une nouvelle architecture décentralisée (ou semi-centralisée) basée sur des communications véhicule-à-véhicule *(V2V, Vehicle to Vehicle)* suscite ces dernières années un réel intérêt auprès de la communauté scientifique, des constructeurs automobiles et des opérateurs Télécoms. Ce type d'architecture s'appuie sur un système distribué, autonome, et est formé par les véhicules eux-mêmes sans l'aide d'une infrastructure fixe pour le relayage des données et des messages. On parle dans ce cas d'un réseau ad hoc de véhicules *(VANET, Vehicular Ad hoc NETwork)*. Le VANET n'est autre qu'une application dédiée et spécifique des réseaux ad hoc mobiles conventionnels *(MANET, Mobile Ad hoc NETwork)*.

a. **Communication Véhicule à Véhicule (V2V) :** L'architecture de communication inter-véhicules (V2V ou IVC pour Inter Vehicle Communication) est composée uniquement d'OBU (véhicules légers, poids lourds, véhicules de secours,...etc.). Ils forment alors un réseau mobile sans avoir besoin d'un élément de coordination centralisé. Cette situation est plausible (et essentielle) si certains équipements RSU deviennent indisponibles (en panne ou hors de portée). Dans ce cas, le réseau doit continuer à fonctionner et les véhicules doivent alors collaborer pour assurer la disponibilité du service.

   Ce mode de fonctionnement est communément appelé « Ad Hoc » est utilisé par les VANETs. L'architecture V2V en mode Ad Hoc peut aussi être utilisée dans les scénarios de diffusion d'alerte (freinage d'urgence, collision, ralentissement,...etc.) ou pour la conduite coopérative. En effet, dans le cadre d'applications de sécurité routière, les réseaux à infrastructure montrent leurs limites, surtout en termes de délai. Prenons l'exemple d'un véhicule en difficulté sur la chaussée qui diffuse un message d'alerte. Il semble plus rapide d'envoyer l'information directement aux autres véhicules plutôt que de la faire transiter par une station de base.

Les services et les applications qui sont basées sur la simple communication inter-véhicule et n'impliquant pas d'infrastructure fonctionnent seulement dans le cas où un taux de pénétration suffisant de véhicules équipés a été atteint. En raison des longs cycles de vie des véhicules, un taux de pénétration approprié peut seulement être atteint après plusieurs années, même si toutes les voitures nouvellement produites ont été équipées en juste proportion. C'est pourquoi, les constructeurs automobiles doivent penser aux stratégies d'introduction graduelles du marché .

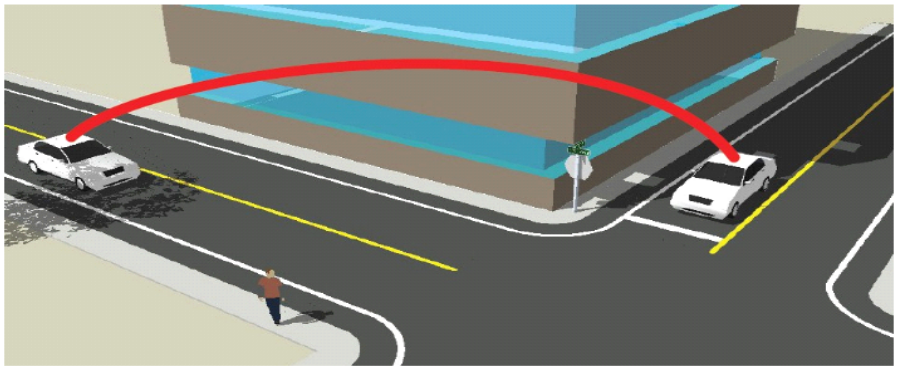

Figure 1.4 – Communication V2V.

b. **Communication Véhicule à Infrastructure (V2I) :** L'architecture Véhicule-vers-Infrastructure (V2I) est composée de RSU(road side units), auxquels les véhicules accèdent pour les applications de sécurité, de gestion et de confort. Les RSU sont administrés par un ou plusieurs organismes publics ou bien par des opérateurs autoroutiers. Un véhicule qui informe le service de voirie au sujet d'un obstacle est un exemple de communication V2I. Dans cet exemple, la communication est unidirectionnelle, du l'OBU vers la RSU.

Nous ne nous concentrons pas donc seulement sur des simples systèmes de communications inter véhicules, mais prenons aussi en compte des applications qui utilisent des points d'infrastructure(RSU) Ceux-ci démultiplient les services grâce à des portails Internet communs. Des services à base d'infrastructure (accès à internet, échange de données par exemple de voiture-domestique, communications de voiture-à-garage pour le diagnostic distant,...etc.) profitent aux clients et peuvent motiver des conducteurs à investir dans l'équipement sans fil supplémentaire pour leurs véhicules.

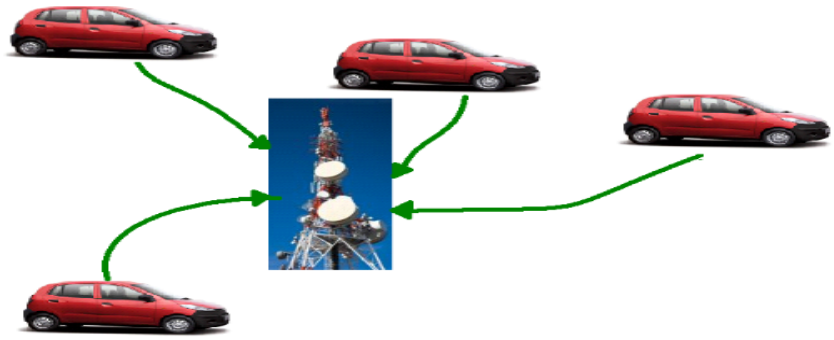

Figure 1.5 – Communication V2I.

c. **Hybride :** La combinaison de ces deux types d'architecture de communication permet d'obtenir une architecture hybride intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance.

Néanmoins, les communications inter-véhiculaires souffrent de problèmes de routage lors de transmission longue distance. Dans de telles situations, l'accès à une infrastructure peut améliorer les performances réseau. Nous comprenons donc la complémentarité des deux types de communication et l'intérêt d'une architecture hybride.

1.2.5 Projets de recherches et développement dans le domaine des VANETs

Plusieurs projets de recherche, de développement et de standardisation portant sur les communications véhiculaires sont actuellement en cours. Ci-dessous sont décrits quelques projets majeurs traitant des communications véhiculaires :

- **CAR 2 CAR Communication Consortium :** Le C2C-CC a comme objectif d'augmenter la sécurité routière grâce à la coopération des systèmes de transport intelligent déployé à l'aide des communications Inter-Véhiculaire soutenues par des communications Véhicule-à-Roadside. Le C2C-CC prend en charge la création d'une norme européenne pour les futurs véhicules communicants couvrants toutes les marques[25].
- **CARLINK Consortium :** CARLINK Consortium « Wireless Traffic Service Platform for Linking Cars Project », il s'agit d'une initiative Eureka Celtic qui a comme but de développer une plate-forme de service intelligent sans fil du trafic entre les voitures soutenues par des émetteurs-récepteurs sans fil du bord de la route. Les principales applications de cette plateforme sont des données météorologiques locales en temps réel, la gestion du trafic urbain de transport et de diffusion d'informations urbain [26].

- **EVITA « E-Safety Vehicle Intrusion Protected Applications » :** Les objectifs du projet EVITA sont de concevoir, de vérifier et de construire des blocs de prototypes pour les réseaux de véhicules où les données sensibles doivent être protégées contre la compromission. Ainsi, le projet EVITA fournira une base pour le déploiement sécurisé des communications véhicule à véhicule [27].
- **GeoNet « Geographic addressing and routing for vehicular communications » :** Le but de GeoNet est de mettre en œuvre et de tester un module logiciel autonome qui peut être incorporé dans les systèmes coopératifs afin de déployer des communications véhicule à véhicule, en améliorant encore les spécifications et les résultats de base du travail du CAR 2 CAR Communication Consortium afin de créer une implémentation logicielle interfaçage avec IPv6 [28].
- **NOW « Network On Wheels » :** Les principaux objectifs de ce projet sont de résoudre les questions techniques clés sur les protocoles de communication et de sécurité des données pour les communications Car-2-Car et de soumettre les résultats aux activités de normalisation de la CAR 2 CAR Communication Consortium [29].
- **SEVECOM « Secure Vehicle Communication » :** Sevecom est un projet financé par l'UE qui vise à fournir une définition complète et la mise en œuvre des exigences de sécurité pour les communications véhiculaires [30].

Conclusion

Dans ce chapitre nous avons présenté les réseaux VANETs qui sont apparus comme solution aux besoins des applications de sécurités routières ; mais actuellement ils permettent aussi de développer de nouveaux services aux usagers de la route comme (la localisation des stations d'essence, emplacements de parking libre et l'accès à Internet).

Afin de mieux comprendre les réseaux véhiculaires, nous avons présenté leurs caractéristiques principales et les différentes entités communicantes ainsi que les différents modes de communications existants.

Dans le chapitre suivant nous nous intérésserons à la sécurité dans les VANETs, ainsi que les attaques et mécanismes qui ont été mis en œuvre afin d'assurer la sécurité des véhicules et les messages échangés.

Chapitre 2

La sécurité dans les réseaux VANET

Introduction

Vu l'importance des informations échangées entre les véhicules eux-mêmes et avec les infrastructures, la sécurité des réseaux véhiculaires est donc un sujet très important à traiter.

Dans ce chapitre, nous présentons en premier lieu les caractéristiques et services de sécurité spécifiques aux VANETs, nous détaillons ensuite les modèles d'attaquants existants et leurs classifications, ainsi que les mécanismes et éléments de base de la sécurité. Nous étudions aussi la gestion de clé et les exigences des systèmes de gestion de clé dans les réseaux VANET.

2.1 Sécurité des VANETs

2.1.1 Caractéristiques de la sécurité

1. **Un support de transmission partagé :** L'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés entre les nœuds ou bien d'injecter de faux messages dans le réseau ;
2. **Communications multi-sauts :** Les protocoles de communications multi-sauts sont obligatoires afin d'avoir des communications sans-fil à longue portée dans les réseaux véhiculaires ; cela signifie que tous les nœuds doivent coopérer pour assurer le fonctionnement du réseau ;
3. **Diffusion d'information de la position géographique :** Avec certains protocoles dans les réseaux véhiculaires, les nœuds sont supposés envoyer périodiquement des messages indiquant leurs positions courantes ou éventuellement d'autres données nécessaires pour des services spécifiques. Par conséquent, les attaquants peuvent créer un profil sur les trajectoires des nœuds et donc les utilisateurs du réseau ;

4. **Opérations autonomes :** Les nœuds eux-mêmes déterminent leurs états et décident quelles sont les informations à envoyer de manière autonome. Par conséquent, il est facile pour les entités malveillantes qui ont le contrôle sur un ou plusieurs nœuds d'envoyer des informations falsifiées. Les systèmes de sécurité, à leur tour, doivent employer des mécanismes qui détectent et empêchent l'utilisation de ces informations.

2.1.2 Services de sécurité

Avant d'adresser des questions relatives à la sécurisation des communications dans les réseaux véhiculaire, il est d'abord nécessaire de discuter de requis ou bien de services de sécurité que doit respecter un système pour son bon fonctionnement. Lorsqu'un requis n'est pas respecté, ceci perce une faille de sécurité. La plupart de ces services tels que la confidentialité, l'authentification, l'intégrité, la non-répudiation, la disponibilité, le respect de la vie privée et le contrôle d'accès dérivent de principaux buts de sécurité de tous systèmes.
Avant de détailler ces services, nous définissons tout d'abord le terme « service » :

Service de sécurité : Service améliorant la sécurité des systèmes informatiques et des transferts d'information d'une organisation. Ces services sont conçus pour contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité [3].

1. Authentification

Pour les VANETs, il très important de connaitre plusieurs informations sur le nœud émetteur tel que son identifiant, son adresse, ses propriétés, sa position géographique. Il est donc important d'authentifier l'émetteur du message et le message qui circule sur le réseau. En effet, toutes les applications déployées dans les VANETs ont besoin d'avoir confiance en l'information qui est assurée par l'authentification [4].
Nous avons plusieurs types d'authentification parmi ces derniers :

- **L'authentification de l'Identifiant :** C'est le fait pour un nœud d'être capable d'identifier les transmetteurs d'un message donné de façon unique. C'est par cette authentification que passe l'accès au réseau du véhicule émetteur [4].
- **L'authentification de la propriété :** Elle aide à déterminer le type d'équipement qui est en communication. Il peut s'agir d'un autre véhicule, d'un « RSU » ou encore d'un autre équipement [11].

2. Intégrité

L'intégrité se divise en deux concepts :

- **Intégrité des messages :** Fonction permettant d'assurer que l'information n'a pas subi d'altération ;
- **Intégrité physique :** Fonction permettant d'assurer que le matériel (destiné aux opérations cryptographiques, à l'envoi de messages, à la collecte d'informations,...etc.) n'a pas subi d'altération.

Cet objectif de sécurité permet de s'assurer que les données échangées ne sont pas soumises à une altération volontaire ou accidentelle. Donc, il permet aux récepteurs de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants [2]. Certains protocoles de sécurité utilisent la signature électronique pour se rassurer que le message n'a pas été altéré durant la transaction. Ainsi, à l'arrivé du message, la signature est vérifiée pour juger de l'intégrité du message.

3. Confidentialité

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

- **Service global :** Protège toutes les données transmises entre les utilisateurs du réseau pendant une période donnée ;
- **Service restreint :** Assure la protection des messages par l'ajout de champs spécifiques à l'intérieur du message.

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

4. Non-répudiation

Ce requis permet d'empêcher une entité de nier d'avoir participer à une communication. Il permet de protéger le système contre le déni d'un nœud qui indique n'avoir pas participé à une communication alors qu'il l'a fait. La non-répudiation permet donc au récepteur de prouver qu'il a reçu le message d'un tiers de communication. Ainsi, pour chaque message reçu, l'émetteur peut être clairement identifié [5]. Cet objectif est indispensable dans les transactions électroniques et dans toutes les communications sensibles.

5. Disponibilité

Le réseau et les applications doivent rester disponibles même en présence de panne dans le réseau. Ce requis permet non seulement de sécuriser le système mais rend aussi celui-ci tolérant aux fautes. Ainsi les ressources doivent rester disponibles jusqu'à ce que la faute soit réparée [6].

6. Contrôle d'accès

Ce requis a pour rôle de déterminer les droits et les privilèges dans les réseaux. Certaines communications comme celle de la police ou d'autres autorités ne doivent pas être écoutés par les autres usagers. L'accès à certains services fournit par les infrastructures est réservé à une catégorie d'usagers. Il est donc primordial de mettre en place un système qui permet de définir toutes ces politiques d'accès pour garantir le contrôle d'accès dans le réseau [7].

7. Vie privée

La vie privée est un service primordial pour les VANETs. De nombreuses opérations présentent des risques d'atteinte à la vie privée, comme le péage ou la reconnaissance automatique des plaques d'immatriculation. De plus, les véhicules diffusent leurs positions de manière régulière ou en cas d'accident. Avec cette redondance d'information, un attaquant peut suivre les déplacements et les communications d'un véhicule. La protection de la vie privée est donc obligatoire pour permettre l'acceptation des VANETs par les utilisateurs.

2.1.3 Attaques dans les réseaux véhiculaires

1. Classification des attaques

En 2013, I.A.Sumra a proposé 5 classes différentes d'attaques, dont chacune devrait offrir de meilleures perspectives pour sécuriser les VANETs.

Attaque de surveillance
Attaque social
Attaque temporelle
Attaque d'application
Attaque de réseau

Table 2.1 – Classification des attaques

- Les attaques de réseau *(Network Attacks)* affectent l'ensemble du réseau, l'attaquant peut affecter directement les autres véhicules et les infrastructures ;
- Dans la classe d'attaque d'application, les attaquants s'intéressent au changement du contenu utile dans les applications tout en abusant pour leurs propres avantages ;
- L'objectif principal des attaquants des attaques temporelles *(Timing attacks)* est d'ajouter un créneau horaire dans le message original, pour créer des retards et bloquer ce message ;
- Tout message déclenché de mauvaises émotions d'autres conducteurs, est classé parmi les attaques sociales ;
- Les attaques qui comportent des activités de suivi sont classées dans les attaques de serveillance.

2. Modèles d'attaquants

Les réseaux véhiculaires sont exposés à un grand nombre de vulnérabilités, comme chaque réseau classique, il existe plusieurs attaques de sécurité. Afin de mieux cerner les attaques possibles sur un VANET et afin d'établir un environnement sécurisé qui satisfait les besoins de sécurité de chacune des application de VANETs, Il est nécessaire de définir les modèles d'attaquants possible. Ainsi, nous pouvons classifier un attaquant selon les dimensions suivantes :

<table>
<tr><th>Modèle d'attaquant</th><th>Rôle</th><th>Comparaison</th></tr>
<tr><td>Interne</td><td>- Membre authentifié du réseau qui peut communiquer avec les autres membres du réseau ;
- il possède déjà quelques avantages comme les clés publiques utilisées par les autres véhicules</td><td rowspan="2">Un attaquant interne peut causer plus de dommages au réseau que l'attaquant externe.</td></tr>
<tr><td>Externe</td><td>Il a un accès limité au système.</td></tr>
<tr><td>Passif</td><td>- Écoute discrète du canal de transmission ;
- Il peut être un voisinage curieux, ou bien une entreprise qui cherche à créer des profils de conducteurs ;</td><td rowspan="2">Un attaquant passif écoute les informations qui sont échangées entre les nœuds, tandis que l'attaquant actif agit sur les informations qui sont échangées.</td></tr>
<tr><td>Actif</td><td>- S'octroyer des privilèges afin d'améliorer son environnement de conduite ;
- Il peut usurper l'identité d'un véhicule de secours pour faciliter son déplacement.
- Il peut générer, modifier, rejeter ou rejouer des messages afin de disséminer de fausses informations.</td></tr>
</table>

Malveillant	- Il cherche à prouver une capacité ou une réussite personnelle ; - Il cherche à détecter des zones de vulnérabilité et à les exploiter pour perturber le système et causer le dysfonctionnement du réseau.	L'attaquant malveillant n'a pas d'intérêt personnel à travers ces attaques, tandis que l'attaquant rationnel cherche un profit personnel et que les attaques rationnelles sont plus prévisibles que les attaques malicieuses.
Rationnel	Il vise l'accomplissement d'une tâche spécifique sur le réseau en défaveur (ou en faveur) d'une personne identifiée.	
Mal intentionné	Un attaquant est dit mal intentionné s'il vise délibérément à remettre en cause le bon fonctionnement du réseau.	Un attaquant mal intentionné a des objectifs précis contrairement à l'attaquant involontaire .
Involontaire	Il peut par exemple lancer (sans le vouloir) une attaque à partir d'un capteur défectueux.	
Indépendant	Les attaquants peuvent agir indépendamment les uns des autres.	Les attaquants indépendants se coopèrent afin de rendre l'attaque plus efficace.
Collaboratif	Les attaquants s'échangent des messages.	
Local	Un attaquant est dit local quand la portée limitée des OBU et des RSU, rend l'attaque limitée.	L'attaque étendu est plus dangereuse que l'attaque local.
Étendu	Il contrôle plusieurs entités qui sont éparpillées sur le réseau.	

Table 2.2 – Modèle d'attaquants.

3. Attaques spécifiques aux VANETs

Pour obtenir une meilleure protection contre les attaquants, nous devons connaitre les attaques évidentes qui constituent un risque non négligeable en cas de réalisation. Ces attaques comprennent :

a. Attaques de bases

1. **Attaque sur la cohérence de l'information :** L'intention de l'attaquant est d'altérer la perception qu'ont ses victimes des conditions de circulation (position, vitesse, direction). L'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. La figure 2.1 illustre ce cas : un attaquant **(M)** diffuse des informations de trafic erronées amenant les véhicules **A** et **B** à changer de voie. Dans cette attaque, l'attaque est Interne ou Externe, Intentionnelle, Active et Indépendante.

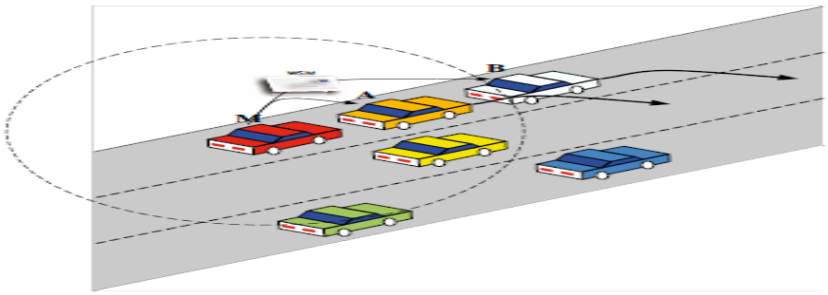

Figure 2.1 – Attaque sur l'incohérence de l'information.

2. **Attaque sur la vie privée :** L'attaquant essaie d'obtenir l'identité ou bien les informations personnelles d'un utilisateur du réseau. Il utilise toute chaine de caractères identificatrice qui peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat,...etc. Dans ce cas, l'attaquant peut être Interne ou Externe, Mal intentionné, Passif et Indépendant.
3. **Usurpation d'identité ou de rôle :** L'entité malveillante utilise l'identité d'un autre véhicule pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La figure suivante illustre un cas d'usurpation d'identité ou l'attaquant **M** usurpe l'identité du véhicule **A** pour récupérer des données auprès du véhicule **B**. Dans ce cas, l'attaque illustrée peut être Interne ou Externe, Intentionnelle, Active et Indépendante.

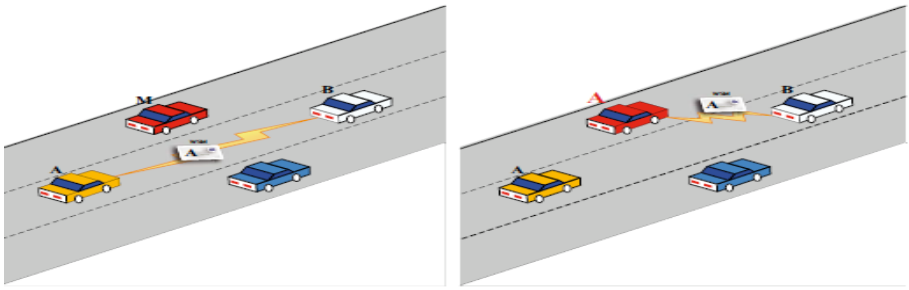

Figure 2.2 – Usurpation d'identité ou de rôle.

4. **Déni de service(DoS) :** Dans ce type d'attaque, l'attaquant empêche l'accès normal aux services du réseau. L'intérêt de cette attaque est de rendre le réseau dysfonctionnel. Ainsi le VANET ne sera plus disponible. La technique la plus naïve pour causer un déni de service consiste à causer le brouillage du canal (Le *Jamming* en anglais) ; la privation de sommeil une autre attaque qui consiste à demander un service que le nœud visé offre de manière répétitive afin de lui gaspiller ses ressources systèmes. Dans la figure suivante l'attaquant **M** empêche l'échange de messages entre le véhicule accidenté **B** et le véhicule **A**, une attaque qui peut être Interne ou Externe, Intentionnelle, Active et Indépendante.

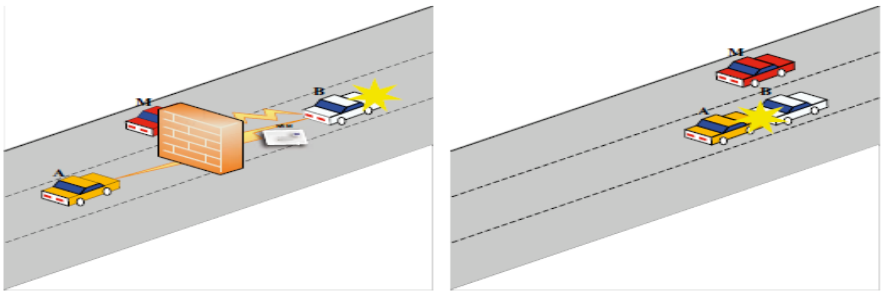

Figure 2.3 – Déni de service.

5. **L'écoute clandestine du réseau :** C'est l'attaque la plus courante contre la confidentialité, l'attaquant se positionne à une position dans un véhicule (en arrêt ou en mouvement) ou de se présenter comme un faux RSU. L'entité malveillante se met à l'écoute sur le support de transmission afin d'extraire des informations personnelles concernant d'autres nœuds pour les analyser et effectuer ensuite d'autres types d'attaques. Le requis mis en cause dans ce type d'attaque est celui de la confidentialité. Dans la figure 2-4, l'attaquant espionne une transaction commerciale « Un paiement électronique », en vue d'en extraire un mot de passe.

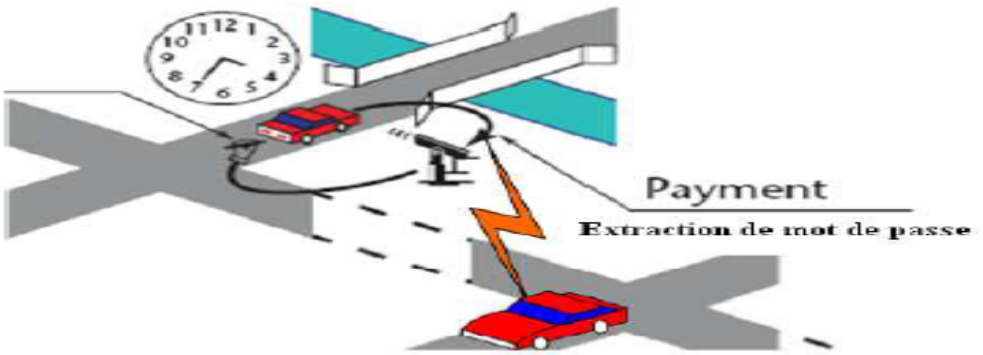

Figure 2.4 – Extraction du mot de passe d'une transaction commerciale.

b. Attaques complexe

Nous présentons dans ce qui suit quelques types d'attaques complexes :

1. **Véhicule caché :** Ce qu'on peut appeler aussi une fausse déclaration de localisation, C'est un exemple de falsification des informations de positionnement, et une variante du « Sybil attack ». Dans le protocole de distribution des messages d'alerte, si un véhicule diffusant l'alerte détecte un voisin mieux positionné que lui pour diffuser, alors il arrête d'émettre. Ce protocole permet de réduire la congestion du canal radio. La figure 2-5 illustre cette attaque. L'attaquant **M** fait donc croire qu'il est en meilleure position **M'** afin d'être le seul à émettre l'alerte. Mais il ne va pas diffuser l'information d'alerte, rendant le véhicule en danger **B** caché des autres véhicules **(A)**.

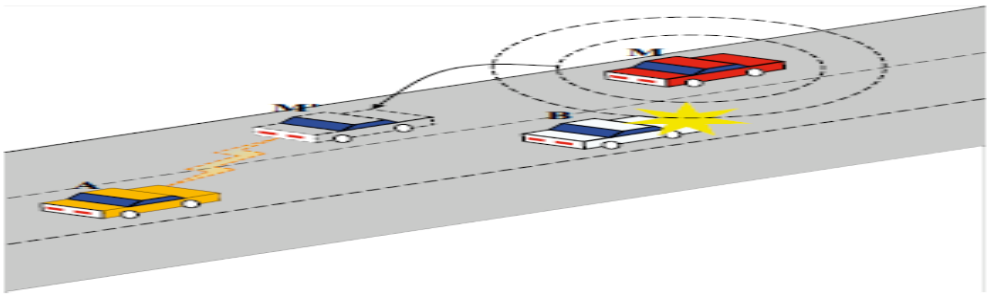

Figure 2.5 – Véhicule cachée.

2. **Tunnel :** Dans un tunnel ou bien dans certaines zones perturbatrices, le signal GPS risque d'être perdu, pour cela un attaquant peut exploiter cette perte de positionnement temporaire en envoyant de fausses données dès la sortie du « tunnel » avant que le véhicule victime ne reçoive une mise à jour de position authentique.

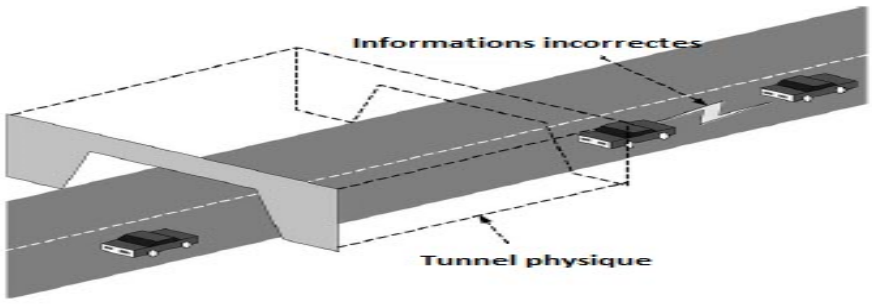

Figure 2.6 – Attaque « tunnel ».

3. **Attaque « Black Hole » :** L'attaquant attire d'abord les nœuds pour pouvoir transmettre le paquet lui même. Lorsque le paquet est transmis, le nœud le baisse silencieusement cela peut se faire en envoyant continuellement la réponse de l'itinéraire malveillant avec un itinéraire frais et bas nombre de sauts.

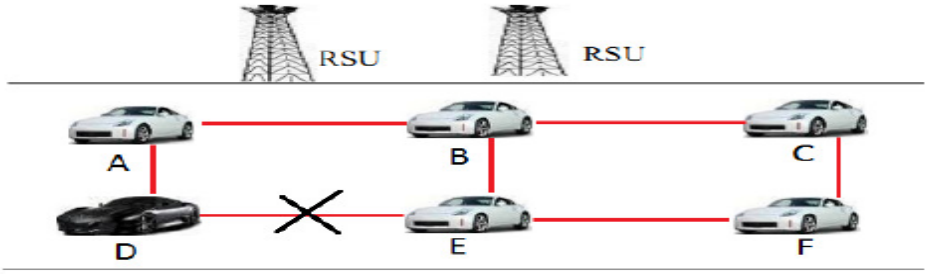

Figure 2.7 – Attaque « Black Hole ».

– **Attaque « Gray Hole » :** Dans ce type d'attaque, le nœud malveillant se comporte comme l'attaque du nœud noir, mais il supprime sélectivement le paquet.

4. **Attaque « Wormhole » :** Un attaquant contrôlant plusieurs entités éloignées, peut établir un tunnel entre ces entités, injecter des données d'un endroit à l'autre et diffuser ainsi des informations erronées à divers endroits.

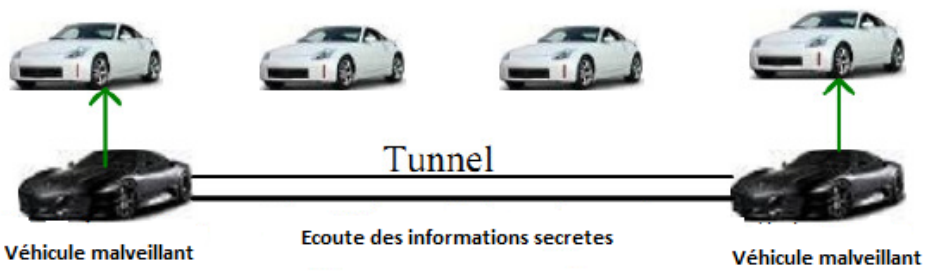

Figure 2.8 – Attaque « Wormhole ».

5. **Attaque temporelle :** Dans ce type d'attaque, le véhicule malveillant qui reçoit un message, ne le renvoi pas normalement, mais il ajoute quelques heures dans le message original. Ainsi, les véhicules voisins du véhicule malveillant reçoivent ce message après le moment où ils devraient le recevoir ou bien après une demande.

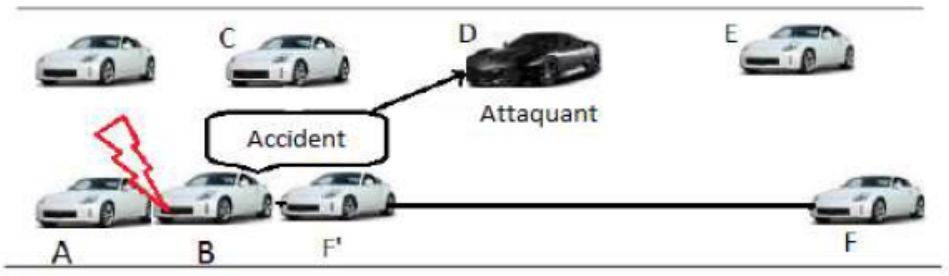

Figure 2.9 – Attaque temporelle.

La figure illustre un accident entre deux véhicules **A** et **B**. **D** a ajouté quelques temps dans le message original pour tarder la transmission du message aux autres véhicules alors qu'il a été annoncé à propos de cet accident. En raison du retard, **F** n'a reçu que le message d'accident lorsqu'il a atteint la position de l'accident **F'**.

6. **Attaque « Man In Middle » (MIMA) :** Dans ce type d'attaque, un véhicule malveillant écoute les communications entre deux véhicules, prétend être chacun d'entre eux afin de pouvoir répondre à l'autre et injecter de fausses informations entre véhicules. Dans la figure suivante, le véhicule malveillant **C** écoute la communication entre **B** et **D**, envoi ensuite de mauvaises informations reçues de **A** vers **E**.

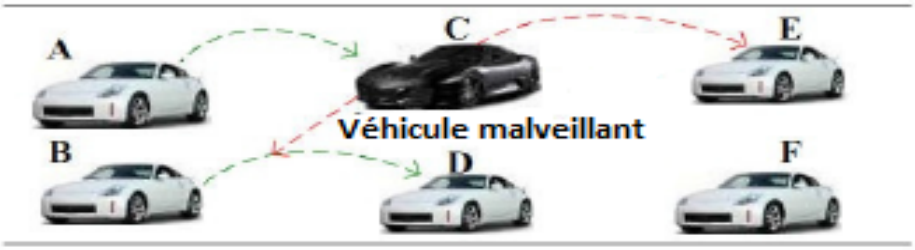

Figure 2.10 – Attaque « Man In Middle ».

c. Caractéristiques des attaques

Type d'attaque	**Modèle d'attaquant**	**Propriétés de sécurité**	**Classe d'attaques**
Attaque sur la cohérence de l'information	I.R.A.*	– Authentification – Intégrité	AA
Véhicule cachée	I.M.A.L	Authentification	AA
Tunnel	I.R.A.L	Authentification	AR, AA
Black hole	I.M.A.L	Disponibilité	AR
Wormhole	I.M.A.Ed	Disponibilité	AR
MIMA	*.*.A.L	– Disponibilité – Authentification	AR

Table 2.3 – Caractéristiques des attaquants.

Nous caractérisons un attaquant par l'adhésion, motivation, Méthode, portée ou :
- Adhésion pour *Interne* (I) ou *Externe* (E) ;
- Motivation pour *Malveillant* (M) ou *Rationnel* (R) ;
- Méthode pour *Active* (A) ou *Passive* (P) ;
- Portée pour *Local* (L) ou *Étendu* (Ed) ;
- Une étoile (*) indique que le champ correspondant peut prendre n'importe quelle valeur.

2.1.4 Mécanismes de sécurité

Avant de citer les différents mécanismes de sécurité, nous allons tout d'abord définir qu'est-ce qu'un mécanisme.

Mécanismes de sécurité : Mécanisme conçu pour détecter, prévenir ou contrer une attaque de sécurité.

1. **Cryptographie :** La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages et assurer les différents objectifs de sécurité, tout en employant des secrets ou des clés. Elle consiste à appliquer des transformations sur le contenu d'un message à l'aide des algorithmes de chiffrement (afin de le rendre incompréhensible) et de déchiffrement (afin de reconstruire le message original).
   - **Cryptographie symétrique** (À clé secrète) : Consiste à utiliser une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer les données.
   - **Cryptographie asymétrique** (À clé publique) : Repose sur l'utilisation d'une clé publique diffusée qui permet de coder le message et d'une autre clé privée gardée secrète pour le décoder.
2. **Hachage :** Consiste à déterminer une information de taille fixe et réduite (appelée le condensé) à partir d'une donnée de taille quelconque.
   - **Fonctions de hachage à sens unique :** Une fonction irréversible qui fournit le condensé à partir d'une chaine fournie en entrée. La particularité de cette fonction est qu'il est facile de calculer le haché d'une chaîne donnée, mais il est difficile de retrouver la chaîne initiale à partir du haché.
3. **Signature numérique :** Un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à la clé privée du signataire.
4. **MAC** (Message Authentication Code) : Un code accompagnant des données qui assure les mêmes fonctionnalités de la signature numérique, mais son implémentation se base sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage.

5. **Certificat numérique :** Une structure de données permet de prouver l'identité du propriétaire d'une clé publique. Un certificat numérique est signé et délivré par un tiers de confiance appelé l'autorité de certification (AC).

2.1.5 Éléments de bases de la sécurité des VANETs

1. TPD (Tamper-Proof Device) :

Un dispositif considéré comme inviolable utilisé pour :
- Stocker les informations sensibles (Les clés privées, les informations confidentielles) ;
- Signer les messages sortants.

Le TPD est conçu de manière à détruire automatiquement toutes les informations stockées lors de la manipulation matérielle. A cet effet, il contient un ensemble de capteurs qui lui permettent de détecter ces manipulations et effacer toutes les informations stockées afin de les empêcher d'être compromises [8].

2. Certificats dans les VANETs :

Grâce à la cryptographie asymétriques ; plusieurs solutions ont été proposés pour les VANETs, qui parait plus adéquate aux caractéristiques et exigences de ces réseaux. Pour cela, il est donc possible d'utiliser des certificats numériques pour identifier les véhicules de façon unique.
Dans les VANETs il existe deux types de certificats :

- **Certificat à court terme :** C'est un type de certificat dont la durée de vie est très courte (d'environ une minute). Il utilise un pseudonyme identifiant le véhicule d'une façon unique sans avoir des informations sur le propriétaire de ce véhicule. Ce type de certificat est utilisé généralement dans les protocoles de routage.
- **Certificats à long terme :** Un certificat est attribué à chaque véhicule, qui permet d'indiquer le véhicule et son propriétaire d'une manière permanente. Ce type de certificat est peut être utilisé pour établir une communication sécurisée avec l'autorité de certification et renouveler les certificats à court terme. Il contient d'autres informations en plus comme celles concernant les caractéristiques des équipements du véhicule.

2.2 Géstion de clés dans les VANETs

2.2.1 Définition

La gestion de clés représente un des aspects les plus difficiles de la configuration d'un système cryptographique de sécurité. Pour qu'un tel système fonctionne et soit sécurisé, chacun des utilisateurs doit disposer d'un ensemble de clés secrètes (dans un système à clés secrètes) ou de paire de clés publiques/privés (dans un système à clés publiques). Cela implique de générer les clés et de les distribuer de manière sécurisée aux utilisateurs ou d'offrir à l'utilisateur le moyen de les générer. Il doit aussi pouvoir enregistrer et gérer ses clés publiques et privés de manière sure [9].

La figure suivante montre toutes ces étapes :

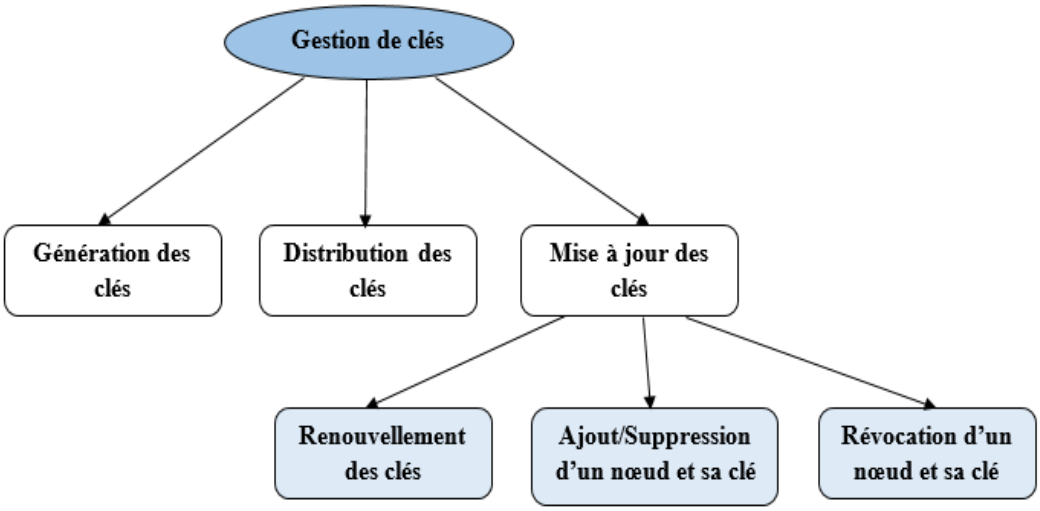

Figure 2.11 – Étapes de gestion de clés.

2.2.2 Exigences des systèmes de gestion de clés

- **Confirmation de clés :** L'authentification des clés avec confirmation des clés produit une authentification par clé explicites. Au cas d'une confirmation fournie par un protocole d'établissement de clés, les entités communicantes prouvent la possession du matériel de chiffrement authentifié.
- **Rafraîchissement de clés :** Ceci améliore la sécurité tout en assurant de nouvelles clés indépendantes entre les sessions de communication.
- **Renouvellement des clés :** La rénovation (Re-keying, en anglais) consiste à re-générer de nouvelles clés et les diffuser ensuite aux différents utilisateurs.

- **Forward secrecy :** Un système de gestion de clés avec la propriété Forward Secrecy empêche un adversaire de découvrir les clés ultérieures à partir d'un sous ensemble contigu d'anciennes clés corrompues [10].
- **Backward secrecy :** Un système de gestion de clés avec la propriété Backward Secrecy empêche un adversaire de découvrir les clés précédentes depuis un sous ensemble contigu d'anciennes clés corrompues [10].
- **Extensibilité :** L'efficacité et la disponibilité sont assurées tant que le nombre de nœuds change rapidement et de manière significative, pour cela le système de gestion de clés devrait être à la taille du réseau de manière transparente.

Conclusion

Les véhicules agissent en fonction des informations envoyées par les véhicules à proximité, d'où la sécurité des véhicules et des messages échangés est primordiale dans les VANETs. Afin de mieux comprendre comment sécuriser un VANET, nous avons d'abord présenté les services et caractéristiques de la sécurité que doit respecter un réseau VANET. Le fait que ces réseaux n'ont pas encore réellement été implémentés. Du coup, il est difficile de définir toutes les attaques pouvant y être perpétrés, pour cela nous avons cités les modèles d'attaquants et quelques attaques dont pourrait être encouru les réseaux véhiculaires. A la suite de cela, nous sommes intéressés à la gestion de clé qui est l'un des aspects les plus importants dans la sécurité des VANETs.

Dans le chapitre suivant, nous ferons un état de l'art sur les différents travaux qui ont été effectués sur la gestion de clés.

Chapitre 3

État de l'art

Introduction

Dans le chapitre précèdent nous avons parlé des attaques possible dans un réseau véhiculaire ainsi que le mécanisme nécessaire pour lutter contre ces attaques dont le mécanisme le plus important est la cryptographie. La confidentialité, intégrité et l'authentification sont des services critique permettant d'empêcher un adversaire de compromettre la sécurité d'un VANET, pour cela un bon système de gestion de clés est nécessaire pour assurer cette protection.

Dans ce chapitre nous allons résumer quelques approches basées sur deux techniques de gestion de clés pour pouvoir en tiré à la fin les avantages et inconvénients de chacune des deux techniques.

3.1 Techniques assurant la sécurité dans les VANETs

Deux techniques sont généralement employés pour assurer la sécurité dans les VANETs [11]. La première est basée sur les certificats anonymes et la deuxième est basée sur la signature de groupe.

3.1.1 Technique basée sur les certificats anonymes

L'idée fondamentale de cette technique est proposée par Raya et Hubaux [12], les auteurs utilisent cette technique pour cacher la vrai identité des utilisateurs (ex : pseudonyme).

Le certificat ne contient aucun rapport publiquement connu avec les identités réelles des utilisateurs, mais l'intimité peut encore être violée car les messages contiennent une clé échangée ce qui donne la possibilité de tracer l'identité réelle du véhicule.

Pour parer à cette attaque, la façon dont les certificats sont employés devrait être modi-

fiée de sorte qu'un attaquant ne puisse pas dépister le propriétaire de la clé. Une technique proposée par ces auteurs pour empêcher cette attaque de se reproduire, consiste à stocker un certain nombre de certificats (ainsi leur paire de clé publique/privée correspondantes) dans un véhicule, de sorte que ce dernier puisse les employer et éviter l'attaque. Cependant, vu la fréquence de changement de la clé, en fonction de la vitesse courante des véhicules, ces derniers devront stocker un grand nombre de paires de clés. Par conséquent, la sécurité, la distribution, la gestion et le stockage de clés deviennent très complexe.

3.1.2 Technique basée sur la signature de groupe

La signature de groupe [13] est une alternative pour réaliser la sécurité et préserver l'intimité dans les VANETs. Dans cette technique, il existe un *group manager* dont le rôle est de gérer le groupe (ex. émettre les paramètres de réseaux et tracer la vraie identité du véhicule).

Des membres peuvent joindre ou quitter le groupe dynamiquement, après l'enregistrement et l'adhésion au groupe, un membre peut anonymement signer un message au nom du groupe. Pour vérifier cette signature, le récepteur utilise la clé publique de groupe, mais il ne peut jamais savoir qui est l'émetteur du message. Cependant, il existe des cas exceptionnels ou le *group manager* peut révéler l'identité d'un expéditeur de n'importe quelle signature de groupe.

L'approche de la signature de groupe est apparue pour surmonter l'inconvénient de la technique de certificats anonymes.

3.2 Techniques de gestions de clés

La gestion de clés fournit des mécanismes efficaces, sécurisés et fiables de gestion de clés utilisées dans les opérations cryptographiques. Par conséquent, la gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Différentes techniques de gestion de clés sont proposées pour surmonter les problèmes ci-dessus.

3.2.1 Technique de gestion de clés partagée

Dans cette technique, la RSU n'est pas responsable du fait que la clé est partagée entre elles, une fois qu'un véhicule s'approche d'un autre véhicule [14]. Il se connecte automatiquement au véhicule sans l'aide du RSU. Cependant, le message est envoyé d'un véhicule à un autre véhicule. Le serveur centralisé n'est pas nécessaire, car les clés sont partagées entre les nœuds. L'authentification de groupe n'est pas nécessaire pour transférer les données.

3.2.2 Technique de gestion de clés distribuée

Cette technique distribuée a pris en charge la signature du groupe pour fournir la confidentialité dans le réseau, ce système contient 3 entités importantes :

1. **Autorité de certification :** Joue le rôle d'un serveur qui gère le VANET, génère et révoque les clés ;
2. **Road Side Unit (RSU) :** Joue le rôle de distributeur de clés privées de groupe et intermédiaire entre l'autorité de certification et les nœuds ;
3. **Nœuds :** Sont les véhicules qui communiquent entre eux dans le réseau.

3.3 Quelques approches proposées

3.3.1 A Distributed Key Management Framework with Cooperative Message Authentication in VANETs [15]

Yong et al. Ont proposé un système de gestion de clés distribuée pour les VANETs basé sur la signature de groupe. Une approche prometteuse pour la protection de la vie privée dans les réseaux véhiculaires (VANET). Ce modèle de réseaux se compose de 3 entités :

- **Autorités (CA) :** Les autorités sont responsable de la gestion des VANETs, génération et révocation de clés. Ces autorités sont puissantes et elles ont un niveau de sécurité très élevé, nous supposons qu'elles ne peuvent pas être compromise.
- **RSUs :** Les RSUs sont responsables de la distribution de clés privées de groupe de façon localisée. Les feux de signalisation ou les panneaux routier peuvent être utilisé comme des RSUs, ces derniers communiquent avec les autorités via un réseau câblé, les auteurs ont supposés que chaque RSU est équipée d'un TPM qui peut resister aux attaques logicielles.
- **Nœuds :** Les nœuds sont des véhicules ordinaires, chacun véhicule est équipé d'un récepteur GPS et d'une unité à bord OBU qui est responsable de toutes les tâches de communication et de calcul. Les nœuds ont le niveau de sécurité le plus bas.

Chaque véhicule et RSU a une paire de clés privée/publique globale à long terme signée par la CA, cette paire est définie en tant que clé d'identité *I-Key*. Ainsi qu'une paire de clés privée/publique locale à court terme définit en tant que clé de groupe *G-key*. On peut également identifier un utilisateur après avoir obtenu sa clé privée. Chaque véhicule possède deux identifiants uniques :

- I-key et G-key, Elles sont considérées comme des identifiants pour les véhicules et les RSU ;
- Un identificateur unique, attribué par l'autorité, comme numéro de plaque d'immatriculation.

Ce système se compose de 3 étapes :

Étape 1 : Enregistrement

1. Premièrement, les RSU diffusent les clés I-publique, la partie restante des clés G-publique d'elles mêmes et de leur voisin RSU avec les certificats et les identités des RSU révoquées dans leurs quartiers régulièrement aux véhicules enregistrés ;
2. Lorsqu'un véhicule détecte le message *« Hello »*, il commence l'enregistrement en envoyant sa clé publique I et le certificat pour la RSU si la RSU n'est pas révoquée. Dans ce modèle de système, La clé publique I de chaque véhicule est unique, donc c'est aussi un identifiant du véhicule. Il est crypté pour protéger la vie privée du véhicule.
3. La RSU envoie la valeur du hachage de la clé G-privée (la clé privée du groupe) qui prévoit être affectée au véhicule et la signature de la valeur du hachage, la clé publique I du véhicule et sa clé publique pour le véhicule. La clé publique I-RSU est également unique. Le véhicule peut identifier la légitimité de la RSU après avoir vérifié ce message car le RSU utilise sa clé privée I dans le message.
4. Le véhicule chiffre son N_{pri} et l'horodatage (TimeStamp) en utilisant la clé publique des autorités. Il envoie ensuite les données cryptées avec l'horodatage et la signature de l'information correspondante à la RSU, comme le montre la figure 3.1 message 4.
5. La RSU envoie la clé G-privée et une partie de la clé G-publique de la prochaine RSU au véhicule. Le véhicule finit sa procédure d'enregistrement après avoir obtenu une clé G-privée valide.

Si les autorités ont besoin d'informations d'un véhicule, la RSU doit leurs envoyer ces informations. Les clés de groupe que produisent les RSU sont partagées entre les véhicules du groupe. Peu de clés sont générées et elles sont attribuées aux véhicules comme des paires de clés uniques. Cela réduit les frais généraux dans la génération de clé. Une partie de la clé publique du groupe actuel sera obtenue à partir du voisin ou précédent RSU que le véhicule a visité. Cela évite la compromission de la RSU dans une certaine mesure.

Notations	*Descriptions*
R_{pub}/R_{priv}	Paire de clés publique/privée du RSU (I-Key).
N_{pub}/N_{priv}	Paire de clés publique/privée du véhicule.
SigA (M)	Signature du message M avec la clé privée de A.
(M)k	Le chiffrement du message M avec la clé publique de K.
G_{pub_k}/G_{priv_k}	Paire de clés de groupe publique/privée pour l'utilisateur K.
T	L'Horodatage.
h(.)	Fonction de hachage à sens unique.

Table 3.1 – Signification physique des symboles.

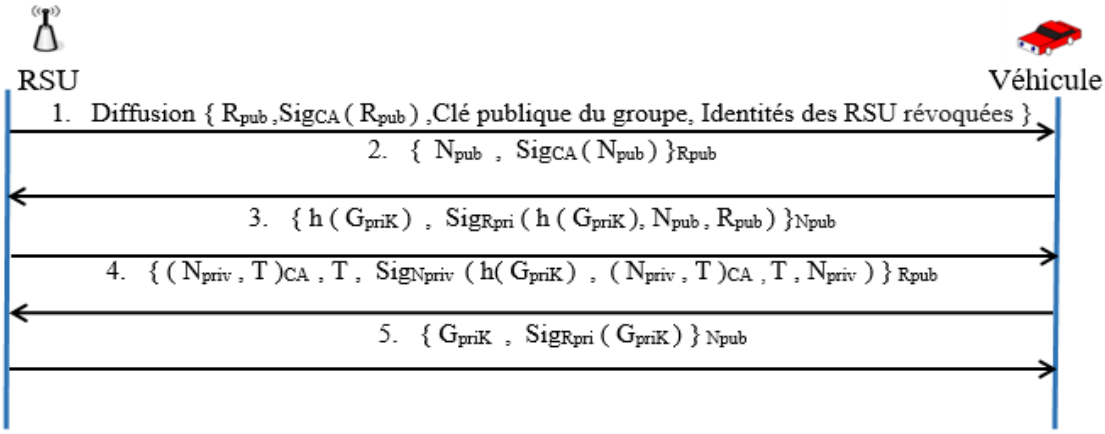

Figure 3.1 – Flux de messages d'enregistrement.

Étape 2 : Message de diffusion

Les véhicules peuvent diffuser des messages sous le nom du groupe après avoir reçu des clés privées de groupe (G_{priv}) de la RSU.

Étape 3 : Accusation

Lorsqu'un véhicule constate que d'autres véhicules envoient de faux messages , il fait un rapport aux autorités. Après avoir reçu une accusation, ces dernières vérifient la signature du message d'accusation en utilisant la clé publique du groupe (G_{pub}). Ensuite, elles effectuent des opérations de récupération de clés. Par la suite, les autorités communiquent avec les RSU pour avoir les informations de l'accusé et l'accusateur. Après cela, elles calculent le h(N_{pri}, T) de l'accusé et de l'accusateur en utilisant la clé I-privée des véhicules et les horodatages qui sont obtenus à partir du message d'accusation et du message. Si la valeur calculée par les autorités est la même que la valeur qu'ils ont obtenu du rapport, l'utilisateur sera considéré

comme légitime.

3.3.2 Key Management Technique for group communication in Vehicular Ad Hoc Networks [16]

Alka et al. Ont proposé une technique de gestion de clés distribuée pour fournir une communication de groupe sécurisée dans le VANET.

Le réseau VANET comprend trois entités principales, dont la Road Side Unit (RSU), est une structure statique composante qui sert de passerelle vers un VANET et permet également la connexion à Internet. Les véhicules (utilisateurs), sont les nœuds du réseau qui communiquent les uns avec les autres. L'Autorité de Confiance (Trusted Authority, (TA)), fournit une identité pour les véhicules et surveille le réseau.

L'objectif de cette approche est de fournir uniquement des communications pour des nœuds sélectifs qui sont prêts à communiquer entre eux. La protection de la vie privée est également considérée comme un aspect majeur de la communication. Pour cet algorithme. Dans leur approche ils ont supposé que les nœuds d'un groupe ont des connaissances les uns sur les autres. Chaque nœud possède les informations sur tous les autres nœuds du réseau. Cette information inclut la clé publique des nœuds.

Cet algorithme se compose de 3 scénarios :

Scénario 1 : Initialisation du réseau

Pendant l'initialisation du réseau, chaque nœud partage avec la RSU son identifiant, le haché de son identité avec un nombre aléatoire inclue, tout en renvoyant les clés de session afin d'empêcher la découverte de son identité dans les prochaines phases. Comme il partage aussi une autre information avec la RSU qui est la façon dont il va traiter un nouveau nœud, lui permette de communiquer ou le restreindre. Tout ce message est chiffré avec la clé publique de la RSU.

Sur la base de la liste de préférences de tous les nœuds du réseau, la RSU prépare une liste finale des nœuds qui souhaitent communiquer entre eux. Un nœud peut appartenir à plusieurs groupes. Selon cette liste finale, RSU identifie le groupe, attribue l'ID de groupe et crée des clés de session. Chaque nœud a autant de clés de session que de groupes auxquels il appartient. La RSU envoie ces clés de session aux nœuds sous forme de clés de session, ID du groupe, le tout haché. Ce message est chiffré deux fois pour fournir l'authentification et l'intégrité. Maintenant, chaque nœud aura une clé de session d'envoi et autant de clés de réception que le nombre de nœuds qui sont dans sa liste de réception.

Lorsqu'un nœud veut communiquer dans un groupe, il envoie un message chiffré avec la clé de session d'envoi (SSK) et un identifiant de message d'information supplémentaire, un

identifiant de groupe et un haché des deux. Ce message est signé avec la clé privée du nœud . Lorsque le récepteur reçoit le message, il vérifie d'abord la signature, si elle correspond, il l'accepte, sinon, il le rejette. Puis il vérifie l'identification de groupe, afin de s'assurer si ce message appartient à ce nœud ou pas. Par la suite il vérifie l'identification du message, pour s'assurer qu'il n'a pas reçu le même message avant.
Voici les abréviations utilisées dans l'algorithme :

Notations	*Descriptions*
ID_n	Identité du nœud
$H(a\|\|b)$	Hachage de a avec b
Pb_R	Clé publique de RSU
Pv_R	Clé privée de RSU
Pb_N	Clé publique d'un nœud
Pv_N	Clé privée d'un nœud
SSK	La clé de session d'envoi

Table 3.2 – Signification des symboles.

L'algorithme se déroule en 3 étapes :
Étape 1 : Pendant l'initialisation du réseau, chaque nœud envoie la liste de préférences avec l'information qu'il veut communiquer avec le nouveau nœud, son identifiant, le haché de son identité avec le nombre aléatoire « a », comme il partage aussi une autre information avec la RSU qui est la façon dont il va traiter un nouveau nœud, lui permette de communiquer ou le restreindre. Ce message est chiffré avec la clé publique du RSU (Pb_R).

[Liste de préférence, critères pour nouveau nœud, ID_n, $H(ID_n||a)$] Pb_R.

Étape 2 : RSU applique l'algorithme :
- Regrouper les nœuds selon leur liste de préférences ;
- Attribuer des ID de groupe, dont le nombre d'ID ne doit pas dépasser le nombre total de nœuds dans le réseau ;
- Générer des clés de session.

Étape 3 : RSU envoie des clés de session pertinentes, avec le haché précédemment reçu du nœud et l'ID du groupe, chiffré avec sa clé privée le tout chiffré avec la clé publique du nœud.

[(Clé de session + $H(ID_n||a)$ + ID de groupe)Pv_R]Pb_N.

Étape 4 : Pour communiquer avec les autres nœuds dans un groupe, un nœud échange les messages suivants :
- Le message est chiffré avec la clé de session d'envoi (SSK) ;

– L'ID du groupe, l'ID du message et le haché des deux sont joint avec le message [[Message] SSK, ID de groupe, ID de message et $H(IDgroupe \| IDMessage)$] ;
– L'expéditeur signe le message avec sa clé privée [[Message] SSK, ID de groupe, ID de message et $H(IDgroupe \| IDMessage)$] Pv_N.

Étape 5 : Lorsque le récepteur reçoit un message :
- Vérifier la signature, Si vérifié, passez à la prochaine étape, sinon, supprimer le message ;
- Vérifier le haché, Si vérifié, passez à la prochaine étape, sinon, supprimer le message ;
- Vérifier l'ID de groupe, Si l'identifiant de groupe appartient au nœud, passez à étape suivante, sinon, avancez le paquet tel qu'il est ;
- Vérifier l'ID du message, S'il existe déjà, supprimer le message, sinon, décrypter le message en utilisant la clé de session de réception.

Nœud	Liste d'envoi	Liste de réception
P	Q, S, T	Q, R, T
Q	P, R, S, T	P, R, S, T
R	P, Q, T	T
S	P, Q, R, T	P, Q, R, T
T	S	S

Table 3.3 – Liste de préférence des nœuds.

Nœud	Liste d'envoi	Liste de réception	Clé de session
P	Q, S	Q, R	1+2
Q	P, S	P, R, S	1+3
R	P, Q	T	1
S	Q, T	P, Q, T	1+3
T	S	S	1+1

Table 3.4 – Application de l'algorithme sur la liste de préférence.

Scénario 2 : Ajout d'un nouveau nœud

Lorsqu'un nouveau nœud rejoint le réseau, il envoie également sa liste de préférences à la RSU. La RSU vérifie si le nœud dans la liste d'envoi du nouveau nœud A est disposé à recevoir du nouveau nœud ou non. De même, il vérifie pour le nœud dans la liste de réception de A.

Nœud	Liste d'envoi	Liste de réception
P	P, Q, S	Q, R

Table 3.5 – Liste de préférences du nouveau nœud A.

Le tableau montre les préférences du nouveau nœud A. Après l'avoir reçu, la RSU applique l'algorithme à nouveau. Le nouveau nœud A veut envoyer un message au nœud Q et Q est également prêt à recevoir du nouveau nœud . la RSU ajoute le nœud A à la liste de réception du noeud Q et ajoute Q à la liste d'envoi du nœud A.
Le tableau suivant montre liste de préférences après l'ajout du nouveau nœud A.

Nœud	Liste d'envoi	Liste de réception	Clé de session
P	Q, S	Q, R	1+2
Q	P, S	P, R, S, A	1+4
R	P, Q, A		1
S	Q, T	P, Q, T	1+3
T	S	S	1+1
A	Q	R	1+1

Table 3.6 – Liste de préférences après l'ajout du nouveau nœud A.

Scénario 3 : Retrait d'un nouveau nœud
Lorsqu'un nœud quitte le réseau, l'algorithme supprime le nœud de la liste d'envoi et de réception de tous les autres nœud S et actualise toutes les clés qui sont partagées avec le nœud de départ. Dans le tableau suivant le nœud S quitte le réseau. La RSU supprime l'entrée du nœud S de la liste des préférences et actualise les clés de session partagées.

Nœud	Liste d'envoi	Liste de réception	Clé de session
P	Q	Q, R	1+2
Q	P	P, R, A	1+3
R	P, Q, A		1
A	Q	R	1+1

Table 3.7 – Liste de préférences après le retrait d'un nœud .

3.3.3 A Survey on Group Key Technique and Cooperative Authentication in VANET [17]

Jayanth et al. Ont proposé un processus d'authentification de message coopératif qui permet de réduire la surcharge de vérification pour la TA (Trusted Autority) et cela en partageant la responsabilité d'authentification avec un utilisateur principal. Cette technique proposée aborde les problèmes de frais généraux et de stockage sur la TA.

En outre, un système de gestion de clés de groupe a été proposé par lequel un nombre d'utilisateurs est regroupé et une paire de clés est attribuée à l'ensemble de groupe. Ceci est également utilisé pour la mise à jour de la clé périodiquement au lieu des opérations d'ajout et de suppression. En utilisant ces schémas, les utilisateurs de VANET devraient pouvoir envoyer et recevoir des messages à destination et en provenance de l'autorité et des utilisateurs à travers les RSUs en toute sécurité.

- **Une autorité de confiance (TA) :** Agit comme un contrôle de vérification qui est conçue pour fournir des services d'authentification, gérer et stocker les clés de plusieurs utilisateurs de VANET. Elle est aussi responsable de l'enregistrement des utilisateurs et le stockage de leurs informations afin de pouvoir les authentifier plus tard.

1. Enregistrement des utilisateurs

Un utilisateur subit un processus d'inscription pour utiliser la technologie VANET.

Étape 1 : L'utilisateur se rend à l'endroit de la TA directement pour s'inscrire lui même et au véhicule ;

Étape 2 : L'utilisateur fournit son nom, ses coordonnées, ses informations ainsi que son empreinte digitale ;

Étape 3 : La TA enregistre immédiatement l'information avec l'empreinte digitale ;

Étape 4 : Après avoir enregistré avec succès, la TA fournit à l'utilisateur sa clé publique et privée :

- La clé privée est utilisée pour générer un code de hachage par l'algorithme de code de hachage PJW ;
- La TA compare ce code haché avec le code enregistré et authentifie l'utilisateur s'il correspond ou pas.

2. Processus d'authentification

La procédure générale d'authentification de l'utilisateur est la suivante :

Étape 1 : L'utilisateur, qui a besoin d'entrer dans le VANET, scanne son empreinte digitale à l'aide du périphérique de scanne d'empreinte digitale ;

Étape 2 : Un code haché correspondant à l'empreinte digitale est généré ;

Étape 3 : Ce code haché est chiffré avec la clé de l'utilisateur et envoyé au TA à travers les RSUs ;

Étape 4 : La TA reçoit le code haché, le décrypte et le compare après avec un code déjà enregistré ;

Étape 5 : S'il s'agit d'une correspondance, il authentifie l'utilisateur et l'ajoute au VANET, Sinon, le véhicule est un autre véhicule qui ne possède pas la technologie

VANET.

Dans ce processus d'authentification de message coopératif, si plusieurs demandes d'authentification s'approchent simultanément de l'autorité ; elles seront remises à un utilisateur déjà authentifié qui possède l'accès à la base de données de la TA. En effectuant cette procédure, l'utilisateur qui fournit le service d'authentification devient l'utilisateur principal (PU) et l'utilisateur authentifié deviendra l'utilisateur secondaire (SU). Ce processus a permis de réduire la surcharge de vérification sur le TA et cela en partageant la responsabilité avec un utilisateur principal.

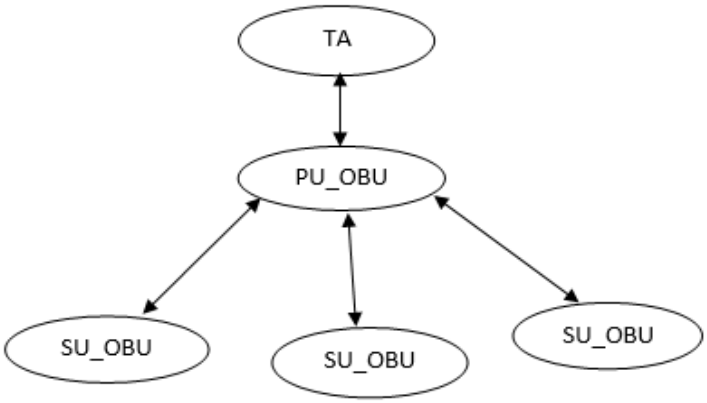

Figure 3.2 – Authentification de messages coopératifs.

3. Techniques de gestion de clés de groupe proposées

a. Grouper et gérer les utilisateurs du groupe

Les utilisateurs secondaires (SU) qui ont été authentifié par un utilisateur principal (PU) peuvent être regroupés en un seul groupe, de ce fait une seule paire de clés est attribué afin de pouvoir réduire les frais généraux de stockage.

Toute information échangée entre la TA et les utilisateurs secondaires doit être acheminée seulement à travers les correspondants de l'utilisateur principal. Ainsi, l'utilisateur principal a l'accès à tous ses utilisateurs secondaires. Tous les utilisateurs secondaires regroupés avec l'utilisateur principal sont accessibles en utilisant seulement les informations d'identification de cet utilisateur principal. Cela réduira le problème du stockage d'informations inutiles et cet espace de stockage peut être utilisé à des fins utiles.

b. Mise à jour des clés

La clé attribuée comme clé publique est connue par tous les utilisateurs de VANET. Donc, pour maintenir un échange de messages sécurisé, la clé publique du système doit être mise à jour. La plupart des systèmes existants effectuent uniquement des opérations de ré-écriture après chaque opération d'ajout ou de retrait. Mais cela sera inefficace car la différence de temps entre ces deux opérations seront beaucoup moins proches du temps négligeable. Ainsi, au lieu d'effectuer une mise à jour après une opération de d'ajout ou de retrait, les clés peuvent être mises à jour périodiquement après un quantum de temps. Ce qui assure une réutilisation efficace et l'utilisateur obtient la mise à jour correcte de la clé.

Ceci minimise les frais généraux de calcul sur la TA et les utilisateurs lors de la mise à jour d'une clé. La TA doit effectuer seulement une simple addition ou soustraction pour générer une nouvelle clé et les utilisateurs doivent effectuer une seule division modulo pour obtenir la nouvelle clé.

4. Analyse de performance

Aspects	*Système littéraire*	*Système proposé*
Sécurité	Authentication seulement.	Authentication et confidentialité.
Authentication	Effectuer par la TA.	Effectuer par la TA et PU.
Gestion de clés	Les informations de tous les utilisateurs sont nécessairement stockées individuellement	Seule l'information des utilisateurs nécessaires sera stockée en termes de clés de groupe.
Mise à jour	Faite après chaque opération d'ajout/retrait.	Faite périodiquement.

Table 3.8 – Analyse de performance.

3.3.4 A Memory Efficient Key Management and Distribution Scheme for Vehicular Adhoc Network [18]

Ankur et al. Ont proposé des algorithmes pour l'ajout et le retrait d'un nœud dans un système de gestion de clés distribué.

Tout d'abord, ils ont configuré un réseau de 50 véhicules. 2 Clusters sont formés avec chacun 25 véhicules. Une autorité de certification est formée et placée au centre de la feuille de route. Les clés générées par l'algorithme de gestion de clés multi groupes sont distribuées à tous les véhicules par la CA. Tous les véhicules communiquent en chiffrant des messages avant de les envoyer, ces derniers sont déchiffrés avec la clé publique de l'expéditeur.

Trois algorithmes ont été proposés :

a. Algorithme principal

1. Configurez le réseau pour 50 nœuds ;
2. Formez 2 groupes de 25 nœuds chacun ;
3. Formez une autorité de certification (CA) pour la génération et la gestion des clés ;
4. Générer des clés pour la CA en utilisant RSA qui sera utilisé pour la signature numérique ;
5. Distribuez des paires de clés à tous les nœuds mobiles dans les réseaux ;
6. Chiffrer en utilisant la clé privée de l'expéditeur.

b. Algorithme Retrait d'un nœud

1. Révocation de la clé du nœud qui a quitté le réseau par la CA ;
2. Informez tous les nœuds du réseau afin qu'ils puissent supprimer cette clé publique de leur liste.

c. Algorithme Ajout d'un nœud

1. Générer une paire de clés pour le nouveau noeud parla CA ;
2. Distribuer la clé publique pour le nouveau noeud dans le cluster qu'il a rejoint.

3.3.5 Key Management Techniques for VANETs [19]

Dhanalakshmi et al. Ont proposé un système de gestion de clés partagées, basé sur l'authentification coopérative des messages, où les clés participantes sont prioritaires dans cette méthode, chose qui ne se fait pas dans le système de gestion des clés distribuées où l'envoi et la réception de messages finissent par retarder la transmission des problèmes liés à la sécurité des messages lors du piratage des données par paquets et l'authentification des messages est biaisée à distance.

Dans cette méthode, la RSU peut ne pas être responsables car la clé est partagée entre les véhicules, mais les messages qui sont envoyés et reçus d'un véhicule à un autre nécessite l'aide du RSU pour établir une communication sécurisée.

Ce cadre de gestion de clés partagées utilise principalement le cryptage de données et l'authentification du client pour lequel le serveur centralisé peut ne pas être requis. Étant donné que les clés sont distribuées, chaque clé peut être communiquée entre elles par une authentification coopérative de messages et ne nécessite pas l'authentification par groupe, pour cela il n'est pas nécessaire de disposer d'un protocole supplémentaire pour l'authentification.

Pour établir une communication sécurisée, ce système utilise l'algorithme de hachage et RSA. Le hachage est utilisée car la structure n'a pas besoin d'une plage spécifique, vu que la longueur de la clé est fixe et plus grande, ce qui est défini dans la RSU. Les nœuds sont des véhicules ordinaires sur la route qui peuvent communiquer les uns avec les autres. Dans un scénario d'autoroute, les RSU sont éloignés les uns des autres.

Algorithme RSA

* *Chiffrement*
  - Alice transmet sa clé publique *(n, e)* à Bob et garde le secret de la clé privée ;
  - Bob souhaite envoyer le message M à Alice. Il transforme d'abord M en un entier $0 < m < n$ en utilisant un protocole réversible convenu connu sous le nom de régime de rembourrage ;
  - Bob calcule le texte chiffré C correspondant à : $C{=}m^e mod\ n$;
  - Bob envoi C pour Alice.
* *Déchiffrement*
  - Alice déchiffre C pour récupérer le message men utilisant sa clé privée d ;
  - Alice calcule le texte en clair m correspondant à : $m{=}C^d mod\ n$;
  - Alice récupère le message original M en inversant le protocole de régime de rembourrage.

3.4 Comparaison entre les deux techniques

	Technique de gestion de clés distribuée	**Technique de gestion de clés partagée**
Avantages	- Une gestion meilleure du VANET ; - La protection de la vie privée est améliorée car les clés privées des véhicules changent ; - La révocation est plus efficace, la liste de révocation est stockée dans les RSU ; - Les clés sont distribuées dynamiquement.	- Technique simple ; - Les frais généraux de communication ne sont pas grands.
Inconvénients	- Les RSU sont des périphériques semi-fiables qui peuvent être compromise lors de la distribution de clés ; - Les RSU peuvent être complice avec les nœuds malveillants cela en leur transmettant les informations des autres nœuds, le nœud malveillant utilise ces informations et se prend pour l'un des nœuds fiable du réseau ; - Lors d'une accusation la RSU peut fournir de fausses informations du nœud malveillant à la TA dans le but de protéger le nœud malveillant.	- La liste de révocation doit être modifiée rapidement en raison du grand nombre de véhicules ; - Nécessite une communication préalable de la clé via une chaîne sécurisée, qui est souvent indisponible ; - Les véhicules utilisent toujours la même clé privée ; - Il est difficile de détecter les nœuds malveillants.

Table 3.9 – Comparaison entre les deux techniques de gestion de clés.

Conclusion

Dans ce chapitre, nous avons présenté les techniques de gestion de clés et la différence entre eux, puis nous avons résumé quelques approches proposées par certain auteurs qui traitent le problème de gestion de clés dans un VANET. Une technique de signature de groupe est utilisée pour assurer la confidentialité et la vie privée. Cette dernière présente un problème de compromission des RSU et des nœuds.

Dans le chapitre qui suit nous allons proposer une solution qui va résoudre ce problème de sécurité dans les VANETs.

Chapitre 4

Proposition

Introduction

L'état de l'art effectuée dans le chapitre précèdent a décelé que la technique de gestion de clés la plus appropriée pour assurer des communications plus sécurisées dans un réseau véhiculaire est la gestion de clés distribuée.

Dans ce chapitre, nous allons présenter notre solution pour la gestion de clés dans un VANET. Nous commencerons d'abord par un schéma qui résume notre proposition, nous détaillerons ensuite chaque étape pour l'élaboration de cette solution.

4.1 Solution proposée

D'après les approches que nous avons étudiés dans le chapitre précèdent, nous avons pu déduire les avantages et inconvénients de chaque technique de gestion de clés. Dans ce qui suit, nous allons présenter un schéma de gestion de clés hybride, basé sur la cryptographie symétrique et asymétrique ainsi que la définition d'un leader de groupe dont le rôle est de gérer un groupe de véhicules. Ce leader de groupe est désigné par l'autorité de certification (CA) et pré-chargé de quelques fonctionnalités de la CA dans le but de réduire la surcharge sur cette dernière et de garantir une meilleure sécurité de communication dans le VANET. Une plate-forme de confiance appelée TPM *(Trusted Platform Module)* résistante aux attaques, est utilisée dans notre solution.

L'utilisation de la cryptographie asymétrique nous permet de chiffrer les messages échangés entre la CA et les RSUs, ainsi qu'entre les RSUs et les leaders de groupe. La cryptographie symétrique nous permet de chiffrer les les messages échangés entre les leaders de groupe et leurs membres ainsi qu'avec d'autres leaders de groupe.

Notre approche est basée sur quatre composantes essentielles :

1. **Autorité de Certification (CA) :** Elle est responsable de la gestion du réseau, génération et révocation de clés. Nous supposons que cette autorité désigne un nœud principal comme leader de groupe (LG), dans le but de réduire la surcharge de vérification pour la CA, donc gérer le groupe.
2. **Road-Side-Unit (RSU) :** Joue le rôle d'une station de base. Elle est responsable de la distribution de clés, et joue aussi le rôle d'un relai entre la CA et les LGs.
3. **Leader de groupe (LG) :** Est un nœud principal désigné par la CA, dont le rôle principal est de gérer un groupe de nœuds qui veulent communiquer entre eux.
4. **Nœud (N) :** Sont des véhicules ordinaires qui communiquent entre eux dans un réseau. Un nombre de véhicules précis forme un groupe qui est géré par un leader.

4.1.1 Description du module TPM

Le module TPM, de nom courant « Trusted Platform Module » est une puce matérielle proposée par le groupe *Trusted Computing Group Association* [29]. Ce module possède un générateur de nombres aléatoires, un moteur SHA-1, des capacités cryptographiques symétrique et asymétrique utilisant la RSA et la courbe elliptique, aussi il est résistant aux attaques. La composition d'un module TPM est donnée dans la figure suivante.

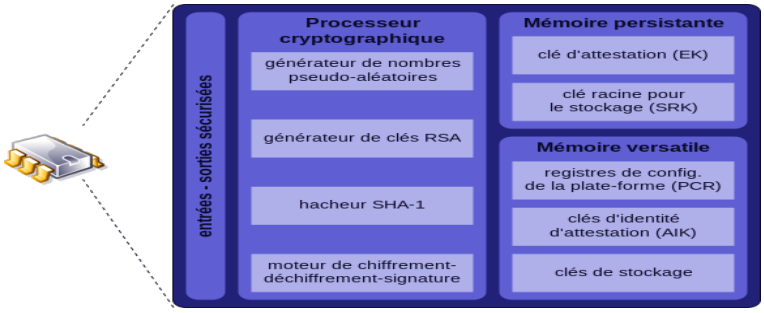

Figure 4.1 – Les composantes d'un module TPM[31].

Chaque module TPM possède et stocke de manière sécurisé une clé unique d'endossement (EK) générée par le fabricant, cette clé est utilisée uniquement pour les fonctions internes du module TPM, chaque module possède aussi une clé d'attestation identitaire (AIK) et le certificat correspondant. Cette clé est un alias de la clé d'endossement utilisé pour attester de son identité lors des échanges de messages ; tout comme la clé (EK), cette clé est générée par le fabricant.

4.1.2 Hypothèses

Notre proposition est fondée sur les hypothèses suivantes :

- L'Autorités de Certification (CA), a un niveau de sécurité très élevée, elle ne peut pas être compromise ;
- La CA peut atteindre toutes les RSUs ;
- Les leaders de groupe (LG) sont déjà choisis par la CA et enregistré ;
- Toutes les (RSU) sont équipés d'un module TPM (c'est-à-dire elles ne peuvent pas être compromise, elles sont résistantes aux attaques) ;
- Chaque leader de groupe dispose d'un module TPM ;
- Les nœuds sont homogènes, c'est-à-dire tous les nœuds sont similaire dans leurs capacité de traitement, d'énergie et de stockage. Les nœuds peuvent être compromis ;
- Les nœuds interagissent seulement avec leur LG, il n'y a pas d'interaction directe avec les nœuds membre ;
- Avant le déploiement, tous les nœuds du réseau son sur.

4.1.3 Schéma proposé

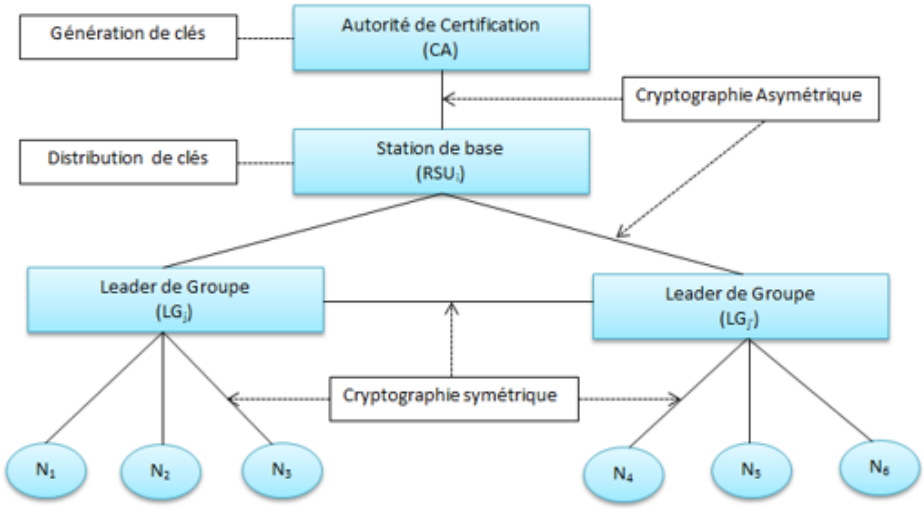

Figure 4.2 – Schéma proposé.

4.1.4 Notations

Le tableau ci-dessous présente les notations que nous allons utiliser dans notre approche et leurs descriptions :

Notation	***Description***
CA	Autorité de Certification.
RSU_m	Identifiant de la m^{ème} RSU.
LG_j	Identifiant du j^{ème} LG.
N_i	Identifiant du i^{ème} nœud.
k	Clé du réseau.
$K_{CA}/{K_{CA}}^{-1}$	Clé publique/privée de la CA .
$K_{R_m}/{K_{R_m}}^{-1}$	Clé publique/privée de la m^{ème} RSU.
$K_{L_j}/{K_{L_j}}^{-1}$	Clé publique/privée du j^{ème} LG.
$K_{L_j,L_{j'}}$	Clé symétrique partagée entre le LG_j et le $LG_{j'}$.
K_{N_i,L_j}	Clé symétrique partagée entre le i^{ème} nœud et le j^{ème} LG.
M	Message à envoyer.
T	Estampille.
$List_m$	Liste des nœuds appartenant à la m^{ème} RSU.
N_N	Nouveau nœud qui rejoint un groupe.
t	Intervalle de temps.
join	Demande d'ajout.
leave	Demande de retrait.
Cpt	Compte à rebours.

Table 4.1 – Les différentes notations utilisées dans la solution proposée.

4.1.5 Phases de l'approche proposée

La solution proposée se compose de six phases importantes qui permettent une bonne gestion de clés. Les différentes phases sont détaillées ci-dessous.

Phase 1 : Initialisation du réseau

Un réseau est formé d'une autorité de certification, des RSUs, des leaders de groupe et des nœuds. Pour une communication sécurisée, ces composantes utilisent un système de gestion de clés distribué.

Tous les nœuds du réseau que ce soit la CA, les véhicules ou les RSUs, sont pré-chargés d'une clé commune k appelée « Clé du réseau ». Cette clé sert à échanger, de façon sécurisée,

les premiers messages entre les différentes entités du réseau. La clé k sera ensuite supprimée de la mémoire de tous les nœuds une fois que toutes les clés du réseau ont été générés et distribuer aux entités correspondantes. Cette clé va donc permettre de garantir la sécurité de la distribution des clés générées par la CA.

Lorsqu'un nœud (véhicule) s'approche de la RSU, il lui envoie un message chiffré contenant son identifiant ainsi que l'estampille T.

$$(1) \quad N_i \rightarrow RSU_m : \{N_i,\ T,\ (N_i, T)_k\}.$$

À la réception de ce message, la RSU_m le déchiffre avec la clé K et met l'identifiant du nœud dans une liste $List_m$. Cette liste sera ensuite transmise à la CA.

$$(2) \quad RSU_m \rightarrow CA : \{RSU_m,\ List_m,\ T,\ (RSU_m, List_m, T)_K\}.$$

À la réception de ce message, la CA le déchiffre avec la clé K puis commence la génération des clés nécessaires aux différents nœuds dont l'identifiant appartient à la liste $List_m$.

Phase 2 : Génération des clés

L'autorité de certification est responsable de la génération de toutes les clés du réseau.

a. Génération de la paire de clés (K_{CA} / ${K_{CA}}^{-1}$)

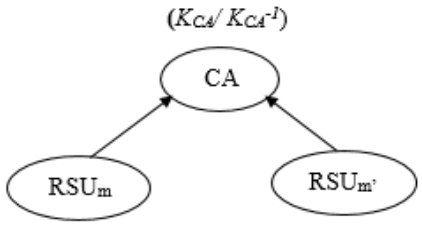

Figure 4.3 – Génération de la paire de clés (K_{CA} / ${K_{CA}}^{-1}$).

La CA génère sa propre paire de clé (K_{CA} / ${K_{CA}}^{-1}$) qui lui servira de communiquer de façon sécurisée avec les RSUs.

b. Génération de la paire de clés ($K_{R_m}/{K_{R_m}}^{-1}$)

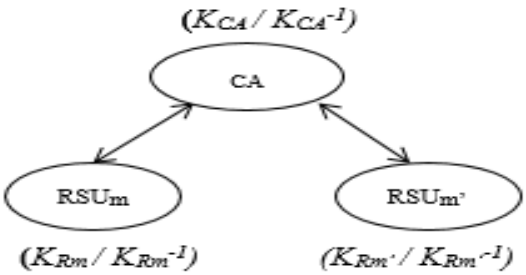

Figure 4.4 – Génération de la paire de clés ($K_{R_m}/{K_{R_m}}^{-1}$).

La paire de clés ($K_{R_m}/{K_{R_m}}^{-1}$) est la clé asymétrique de la m$^{\text{ème}}$ RSU. La CA génère une paire de clés pour chaque RSU dont le but de communiquer avec elles de manière sécurisée.

Pour chaque RSU_m faire
    Générer une paire de clés ($K_{R_m}/{K_{R_m}}^{-1}$)
Fait

c. Génération des clés ($K_{L_j}/{K_{L_j}}^{-1}$) et ($K_{L_j,L_{j'}}$)

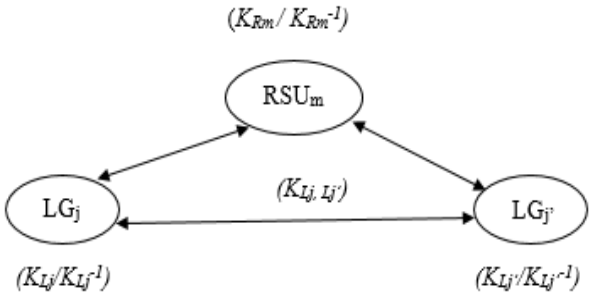

Figure 4.5 – Génération des clés ($K_{L_j}/{K_{L_j}}^{-1}$) et ($K_{L_j,L_{j'}}$).

Pour un échange d'informations sécurisé entre un leader de groupe et son RSU, un leader et un autre leader, des clés de chiffrement sont nécessaire.

La CA génère pour chaque leader une paire de clés asymétrique ($K_{L_j}/{K_{L_j}}^{-1}$) ainsi que des clés symétrique ($K_{L_j,L_{j'}}$) qu'ils vont partager avec les leaders voisins.

Pour chaque ($LG_j \in RSU_m$) *faire*
  Générer une paire de clés ($K_{L_j}/{K_{L_j}}^{-1}$)
  Pour chaque ($LG_{j'} \in RSU_m$) \($j' > j$) *faire*
    Générer une clé symétrique ($K_{L_j,L_{j'}}$)
  Fait
Fait

d. Génération de la clé (K_{N_i,L_j}).

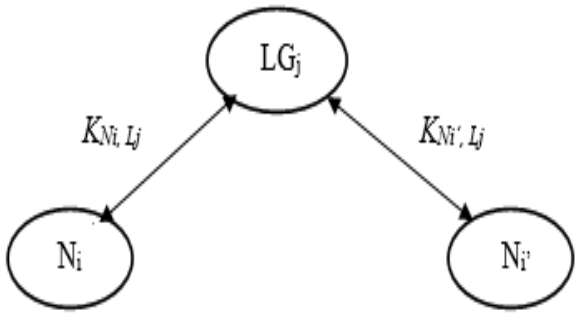

Figure 4.6 – Génération de la clé (K_{N_i,L_j}).

Afin de sécuriser les communications entre les nœuds et leurs leader, la CA génère pour chaque nœud N_i une clé symétrique qu'il partagera avec son leader.

Pour chaque (Nœud rattaché au groupe dont le leader est LG_j*) faire*
  Générer une clé symétrique (K_{N_i,L_j})
Fait

Phase 3 : Distribution des clés

Une fois que toutes les clés nécessaire ont été générées (phase 2), ces dernière doivent être distribuées de façon sécurisée aux entités correspondantes. La CA envoie à la RSU_m sa clé publique, ainsi que toutes les autres clés qu'elle a généré pour que la RSU les transmette à l'entité suivante. Ce message sera chiffré avec la clé K du réseau comme suit :

(1) $CA \rightarrow RSU_m : \{ CA, RSU_m, ((CA, K_{CA}), (RSU_m, (K_{R_m}/{K_{R_m}}^{-1})), (LG_j, (K_{L_j}/{K_{L_j}}^{-1})), (LG_j, LG_{j'}, K_{L_j,L_{j'}}), (N_i, LG_j, K_{N_i,L_j}))\}_{.K}$

Lorsque la RSU_m reçoit ce message, elle le déchiffre avec la clé K, sauvegarde sa paire de clé ($K_{R_m}/{K_{R_m}}^{-1}$), la clé publique de la CA (K_{CA}) ainsi que celles des leaders (K_{L_j}), le reste du

message le chiffre avec K et l'envoie aux leaders. La RSU envoie au leader le message suivant :

(2) $RSU_m \rightarrow LG_j : \{RSU_m, LG_j, ((RSU_m, K_{R_m}), (LG_j, (K_{L_j}/{K_{L_j}}^{-1})), (LG_j, LG_{j'}, K_{L_j,L_{j'}}), (N_i, LG_j, K_{N_i,L_j}), (CA, K_{CA}))\}_{.K}$

À la réception de ce message, le LG_j le déchiffre avec la clé du réseau K, sauvegarde toutes les clés que son RSU lui a envoyé, sachant que chaque leader dispose d'un module TMP qui assure un niveau de sécurité très élevé dans le stockage de clés. Le leader envoie à chaque nœud la clé symétrique qu'il va partager avec lui, chiffrée avec la clé K.

(3) $LG_j \rightarrow N_i : \{LG_j, N_i, ((LG_j, N_i, K_{N_i,L_j}), (CA, K_{CA}))\}_{.K}$

Le nœud N_i déchiffre avec la clé K sauvegarde la clé publique de la CA ainsi que la clé (K_{N_i,L_j}).

À la fin de cette phase c'est à dire après la distribution de toutes les clés, la clé du réseau K sera supprimée de la mémoire de toutes les entités.

Phase 4 : Communication

Après avoir terminé avec les phases de génération et distribution des clés, nous pouvons établir des communications sécurisées dans le réseau. À l'envoi d'un message une estampille T est envoyée pour vérifier la fraicheur du message.

1. Communication entre la CA et la RSU

- CA vers RSU_m

  Si la CA veut communiquer avec une de ses RSU_m, elle lui envoie un message contenant leur identifiants et l'information à envoyer, chiffré avec la clé publique de la RSU_m (K_{R_m}), la RSU_m déchiffre avec sa clé privée.

$$CA \rightarrow RSU_m : \{CA,\ RSU_m,\ T,\ (CA, RSU_m, T, M)_{K_{Rm}}\}.$$

- RSU_m vers CA

  Si une RSU_m veut communiquer avec la CA, elle lui envoie un message contenant leur identifiants et l'information à envoyer, chiffré avec la clé publique de la CA (K_{CA}).

$$RSU_m \rightarrow CA : \{RSU_m, CA, T,\ (RSU_m, CA, T, M)_{K_{CA}}\}.$$

Ce message sera déchiffré par la CA avec sa clé privée ($K_{CA}{}^{-1}$).

2. Communication entre la RSU et LG

- RSU_m vers LG_j

La RSU_m envoie un message qui sera chiffré avec la clé publique du LG_j avec qui elle veut communiquer, comme suit :

$$RSU_m \rightarrow LG_j : \{RSU_m,\ LG_j, T,\ (RSU_m, LG_j, T, M)_{K_{L_j}}\}.$$

Le LG_j ne pourra déchiffrer ce message qu'à l'aide de sa clé privée ($K_{L_j}{}^{-1}$).

- LG_j vers RSU_m

Si un LG_j veut envoyer un message à son RSU_m, il chiffrera ce message avec la clé publique (K_{R_m}). À la réception de ce message, la RSU_m va le déchiffrer avec sa clé privée, vérifie l'identité de l'émetteur, ainsi que l'estampille T.

$$LG_j \rightarrow RSU_m : \{LG_j,\ RSU_m, T,\ (LG_j, RSU_m, T, M)_{K_{R_m}}\}.$$

3. Communication entre les leaders

- LG_j vers $LG_{j'}$

Si deux leader (LG_j, $LG_{j'}$) appartenant à une même RSU_m veulent échanger des informations, le message envoyé comportera leurs identifiants, l'information à transmettre chiffrée avec la clé symétrique partagée entre eux ($K_{L_j,L_{j'}}$) ainsi qu'une estampille T .

$$LG_j \rightarrow LG_{j'} : \{LG_j,\ LG_{j'}, T,\ (LG_j, LG_{j'}, T, M)_{K_{L_j,L_{j'}}}\}.$$

$$LG_{j'} \rightarrow LG_j : \{LG_{j'},\ LG_j, T,\ (LG_{j'}, LG_j, T, M)_{K_{L_j,L_{j'}}}\}.$$

4. Communication entre un LG et N_i

- LG_j vers N_i

Si un nœud N_i veut communiquer avec son leader, il lui transmettra un message contenant leurs identifiants (émetteur, récepteur), l'estampille T qui garantira la fraicheur du message et l'information M, le tous chiffré avec la clé symétrique partagée entre eux (K_{N_i,L_j}).

$$LG_j \rightarrow N_i : \{LG_j,\ N_i, T,\ (LG_j, N_i, T, M)_{K_{N_i,L_j}}\}.$$

$$N_i \rightarrow LG_j : \{N_i,\ LG_j, T,\ (N_i, LG_j, T, M)_{K_{N_i,L_j}}\}.$$

5. Communication entre deux nœuds

- $\underline{N_i \rightarrow N_{i'}}$

Dans cette communication nous distinguons deux cas possibles :

5.1. Communication intra-groupe

N_i et $N_{i'}$ appartiennent au même groupe :

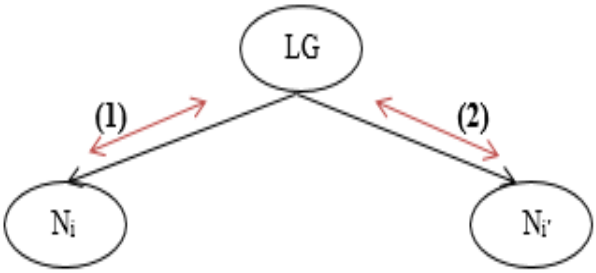

Figure 4.7 – Communication entre les nœuds du même groupe.

- Si le nœud N_i veut communiquer avec le nœud $N_{i'}$, il envoie un message à son LG_j qui contient son identifiant N_i, l'identifiant de son LG_j et l'identifiant du nœud destinataire $N_{i'}$ et l'information à transmettre. Ce message est chiffré avec la clé symétrique partagée entre eux (K_{N_i,L_j}).

$$(1)\ N_i \rightarrow LG_j : \{\ N_i, LG_j,\ N_{i'},\ T,\ (N_i, LG_j, N_{i'}, M, T)_{K_{N_i,L_j}}\}.$$

- Le leader de groupe déchiffre ce message avec la même clé privée (K_{N_i,L_j}), vérifie l'identifiant du destinataire $N_{i'}$ et la valeur de l'estampille pour s'assurer que ce message vient du nœud N_i, puis le chiffre à nouveau avec la clé privée partagée avec le nœud récepteur $N_{i'}$ ($K_{N_{i'},L_j}$).

$$(2)\ LG_j \rightarrow N_{i'} : \{LG_j,\ N_{i'},\ N_i, T,\ (LG_j, N_{i'}, N_i,\ T, M)_{K_{N_{i'},L_j}}\}.$$

- Le nœud $N_{i'}$ décrypte le message reçu de son LG_j avec la clé symétrique ($K_{N_{i'},L_j}$) partagée avec son leader LG, puis vérifie l'identifiant de l'émetteur ainsi que l'estampille T et récupère le message.

5.2. Communication inter-groupes

Dans le cas où N_i et $N_{i'}$ n'appartiennent pas au même groupe, cette communication passe par 3 étapes :

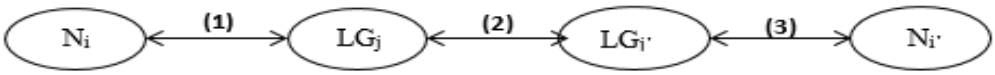

Figure 4.8 – Communication inter-groupes.

Étape 1 : $N_i \rightarrow LG_j$
Si un nœud N_i souhaite communiquer avec le nœud $N_{i'}$, il doit d'abord passer par son LG_j qui transmettra le message au leader $LG_{j'}$ du groupe voisin qui à son tour le délivre au nœud destinataire $N_{i'}$. Le nœud N_i envoie un message qui contient leurs identifiants, l'identifiant du nœud récepteur et l'information à transmettre, chiffré avec la clé symétrique partagée avec son leader (K_{N_i,L_j}).

$$(1)\ N_i \rightarrow LG_j : \{\ N_i,\ LG_j,\ N_{i'},\ T,\ (N_i, LG_j, N_{i'}, T, M)_{K_{N_i,L_j}}\}.$$

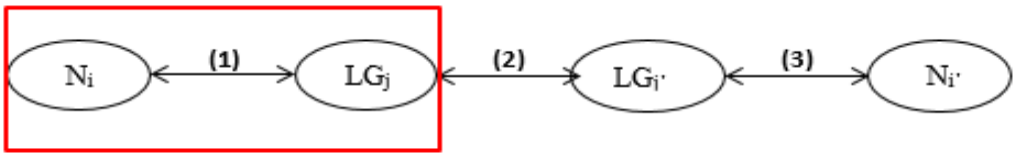

Figure 4.9 – Première étape de la communication inter-groupes.

Étape 2 : $LG_j \rightarrow LG_{j'}$
À la réception du message (1), le LG_j le déchiffre avec la même clé symétrique (K_{N_i,L_j}), extrait l'identifiant du destinataire $N_{i'}$, vérifie T et chiffre le message à nouveau avec la clé partagée avec le leader auquel le nœud destinataire est rattaché ($K_{L_j,L_{j'}}$).

$$(2)\ LG_j \rightarrow LG_{j'} : \{LG_j,\ LG_{j'},\ N_i,\ N_{i'},\ T,\ (LG_j, LG_{j'}, N_i, N_{i'}, T, M)_{K_{L_j,L_{j'}}}\}.$$

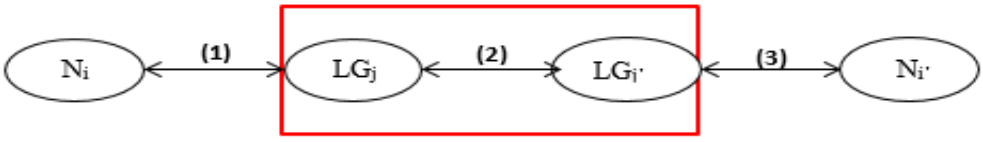

Figure 4.10 – Deuxième étape de la communication inter-groupes.

Étape 3 : $LG_{j'} \rightarrow N_{i'}$
Lorsque $LG_{j'}$ reçoit le message (2), il le déchiffre avec la clé symétrique ($K_{L_j,L_{j'}}$) pour savoir à quel nœud, le message est destiné puis le chiffre à nouveau avec la clé symétrique partagée avec ce nœud ($K_{N_{i'},L_{j'}}$) et l'envoie à $N_{i'}$.

$$(3)\ LG_{j'} \rightarrow N_{i'} : \{LG_{j'},\ N_i,\ N_{i'},\ T,\ (LG_{j'}, N_i, N_{i'}, M, T)_{K_{N_{i'},L_{j'}}}\}.$$

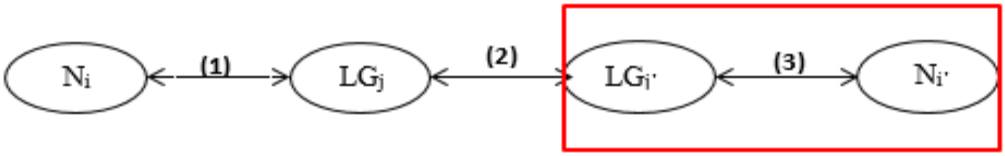

Figure 4.11 – Troisième étape de communication inter-groupes.

À la réception du message (3), le nœud $N_{i'}$ le déchiffre avec la clé symétrique partagée avec son leader ($K_{N_{i'},L_{j'}}$), il vérifie l'estampille et extrait l'identifiant de l'émetteur et le message M.

Phase 5 : Ajout d'un nœud

Quand un nœud se déplace, il peut se retrouver dans deux cas : rejoindre un groupe qu'il a déjà quitté, ou encore rejoindre un nouveau groupe. Le nouveau nœud N_N est pré-chargé d'une clé (K'). Lorsque un nouveau nœud veut rejoindre un groupe il diffuse un message contenant son identifiant et une demande d'ajout *(join)*. Le leader de groupe le plus proche qui détecte ce message répond par son identifiant et sa clé publique.

$(1)\ N_N \rightarrow * : \{N_N,\ join\}.$
$(2)\ LG_j \rightarrow N_N : \{LG_j\ ,\ N_N,\ K_{L_j}\}.$

Le nouveau nœud envoie à ce LG_j son identifiant ainsi que la clé K', chiffré avec la clé publique du LG_j .K_{L_j}

$$(3)\ N_N \rightarrow LG_j : \{N_N,\ LG_j,\ (N_N, LG_j, K')_{K_{L_j}}\}.$$

À la réception de ce message, le LG_j le déchiffre avec sa clé privée (${K_{L_j}}^{-1}$), sauvegarde la clé K', chiffre à nouveau cette partie avec la clé publique de la CA (${K_{R_m}}^{-1}$), puis avec la

clé publique de son RSU_m.

$$(4)\ LG_j \rightarrow RSU_m : \{(N_N, LG_j, RSU_m, CA, T, (N_N, LG_j, K', T)_{K_{CA}})_{K_{R_m}}\}.$$

La RSU_m déchiffre ce message avec sa clé privée (${K_{CA}}^{-1}$), reconnait que ce message est destiné pour la CA. La RSU_m l'envoie directement à cette dernière.

$$(5)\ RSU_m \rightarrow CA : \{N_N, LG_j,\ RSU_m,\ \text{CA},\ \text{T},\ (N_N, LG_j, K', T)_{K_{CA}}\}.$$

La CA déchiffre avec sa clé privée (${K_{CA}}^{-1}$), vérifie la clé K', génère une clé symétrique (K_{N_N,L_j}) pour les deux entités (N_N, LG_j) qu'elles vont partager entre elles pour garantir une communication plus sécurisée.

La CA envoie cette nouvelle clé à la RSU_m chiffrée avec la clé K' que seul le LG_j et le nouveau nœud N_N puisse déchiffrer, tout le message sera chiffré avec la clé publique de la RSU_m (K_{R_m}).

$$(6)\ \text{CA} \rightarrow RSU_m : \{(CA, RSU_m, LG_j, N_N, T, (LG_j, N_N, K_{N_N,L_j}, T)_{K'})_{K_{R_m}}\}.$$

La RSU_m déchiffre avec sa clé privée (${K_{R_m}}^{-1}$) puis le chiffre à nouveau avec la clé publique (K_{L_j}) du LG_j. Il le transmit par la suite au leader LG_j.

$$(7)\ RSU_m \rightarrow LG_j : \{(RSU_m, LG_j, N_N, T, (LG_j, N_N, K_{N_N,L_j}, T)_{K'})_{K_{L_j}}\}.$$

Le LG_j déchiffre avec sa clé privée (${K_{L_j}}^{-1}$), utilise la clé K' pour déchiffrer l'autre partie du message. S'il parvient à le déchiffrer donc la clé K' est authentique. Le LG_j sauvegarde la clé symétrique (K_{N_i,L_j}) puis chiffre à nouveau le message avec la clé K' pour transmettre la nouvelle clé au nouveau nœud.

$$(8)\ LG_j \rightarrow N_N : \{LG_j,\ N_N,\ \text{T},\ (LG_j, N_N, K_{N_N,L_j}, T)_{K'}\}.$$

Le N_N déchiffre avec la clé K', sauvegarde la nouvelle clé (K_{N_i,L_j}). Une fois que cette phase est terminée, la clé K' sera supprimée de la mémoire des nœuds (N_N, LG_j).

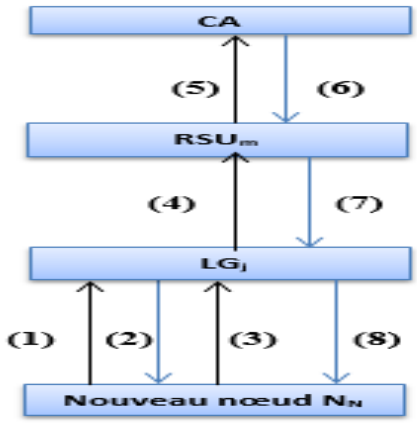

Figure 4.12 – Processus d'ajout d'un nœud.

Phase 6 : Suppression d'un nœud

Dans cette phase nous avons plusieurs cas possible :

- **Suppression d'un nœud (N_i) :** Un nœud peut quitter son groupe en raison de défaillance, changement d'emplacement physique ou encore l'échec de communication avec son LG. Nous distinguons deux cas :

  1. Quitter volontairement le groupe : Quand un nœud décide de quitter son groupe par exemple (En remarquant l'affaiblissement de la force du signal dû à l'éloignement progressif de son LG), il envoie un message *(Leave)* signalant son départ contenant son identifiant et la raison de son départ chiffré avec la clé partagée avec son leader (K_{N_i,L_j}). Quand le LG reçoit le message, il sauvegarde ces informations pendant une certaine période t, qui lui serviront à authentifier de nouveau ce nœud s'il revient une autre fois. Si ce nœud ne revient pas durant cette période t,le leader supprime ces informations de sa mémoire.

  $$N_i \rightarrow LG_j : \{N_i,\ LG_j,\ (N_i, LG_j, leave)_{K_{N_i,L_j}}\}.$$

  2. Quitter involontairement le groupe : Quand un nœud N_i est compromis, le LG supprime ce nœud de son groupe ainsi que la clé symétrique qu'il partageait avec lui, avertit la RSU et les autres nœuds de la non disponibilité de ce nœud. La compromission d'un nœud n'affecte que la clé partagée avec son leader.

- **Suppression d'un leader de groupe (LG) :** Dans ce cas la RSU supprime le LG_j ainsi que que la clé publique du leader (K_{L_j}) qu'il sauvegardait. Tous les

nœuds membre de ce leader supprimerons aussi les clés symétrique (K_{N_i,L_j}) qu'ils partageaient avec lui. La CA désignera un nouveau LG et de nouvelles clés.

- **Suppression d'une (RSU) :** Une RSU ne peut pas être compromise donc elle ne sera supprimée que si elle est endommagée. La RSU voisine la remplacera en attendant sa réparation ou la construction d'une nouvelle RSU, la CA ne génère aucune nouvelle clé puisque chaque entité ($RSU_{m'}$, LG_j) possède déjà sa propre paire de clés.

Phase 7 : Mise à jour des clés

La mise à jour des clés est nécessaire pour garantir la sécurité du réseau. Cette mise à jour consiste à rafraichir toutes les clés du réseau. Après la phase de distribution, la CA lance un compte à rebours *Cpt* , lorsque *Cpt=0* la CA procède aux rafraîchissement des clés pour toutes les entités du réseau.

4.2 Évaluation de performance

Dans cette section nous allons évaluer les performances de notre approche par apport à la complexité en termes de mémoire, c'est-à-dire la capacité de stockage de clés pour chaque entité et de communication, le nombre de message échangés lors de la distribution de clés.

a. Complexité en mémoire

Nous allons déterminer le nombre de clés sauvegardées dans la mémoire de chaque entité communicante (CA, RSU, LG et Nœud).

– **Nœuds :** Chaque nœud détient :
  - Une seule clé symétrique (K_{N_i,L_j}) partagée avec son leader.
  - La clé publique de la CA (K_{CA}).

– **LG :** Le leader de groupe dispose d'un module TPM doté d'une très grande capacité de stockage et surtout d'un niveau de sécurité très élevé, d'où cette entité peut stocker un grand nombre de clés dont les clés suivantes :
  - Une paire de clé asymétrique ($K_{L_j}/{K_{L_j}}^{-1}$) ;
  - La clé publique de son RSU K_{R_m} ;
  - Les clés symétrique partagées avec les leaders voisin ($K_{L_j,L_{j'}}$) ;
  - Les clés symétrique partagées avec leurs nœuds membre (K_{N_i,L_j}).

– **RSU :** Toutes les RSUs disposent aussi d'un module TPM. Une RSU sauvegarde les clés dont elle a besoin pour garder la sécurité des informations échangées :

  - Une paire de clé asymétrique ($K_{R_m}/{K_{R_m}}^{-1}$) ;

- Les clés publiques de tous ses leaders (K_{L_j}) ;
- La clé publique de la CA (K_{CA}).

– **CA :** L'autorité de certification est responsable de la génération de toutes les clés du réseau,y compris sa paire de clés asymétrique. Elle stocke toutes les clés du VANET.

Le tableau ci-dessous résume toutes les clés que stocke chaque entité :

Entités	**Clés sauvegardées**	**Nombre de clés**
N_i	1(K_{N_i,L_j}), 1(K_{CA})	2
LG_j	1($K_{L_j}/{K_{L_j}}^{-1}$),(L-1)($K_{L_j,L_{j'}}$),V(K_{N_i,L_j}), 1(K_{R_m}), 1(K_{CA})	4+ (L-1) + V
RSU_m	1($K_{R_m}/{K_{R_m}}^{-1}$),L(K_{L_j}), 1(K_{CA})	3+L
CA	1($K_{CA}/{K_{CA}}^{-1}$),R($K_{R_m}/{K_{R_m}}^{-1}$),R*L($K_{L_j}/{K_{L_j}}^{-1}$),(R*L(L-1))/2($K_{L_j,L_{j'}}$),R*L*V(K_{N_i,L_j})	2+2R+2RL+ (R*L(L-1))/2 +RLV

Table 4.2 – Nombre de clés sauvegardées pour chaque entité.

L : Le nombre de LG qui appartiennent à la même RSU.
V : Le nombre de nœuds qui appartiennent à la même LG.
R : Le nombre des RSU.

b. Complexité en communication

Dans la phase de distribution des clés, les entités du réseau échangent un certain nombre de messages que nous allons déterminer ici, sachant que la RSU est responsable de la distribution de toutes ces clés :

Phase	**N° de messages**	**Nombre de messages**
1	(1),(2)	2
3	(1),(2),(3)	3
Total		5

Table 4.3 – Nombre de messages échangés.

Pour l'établissement et la distribution de toutes les clés du réseau, 5 messages sont nécessaire.

Conclusion

La gestion de clés est un élément primordial pour fournir la plupart des services de sécurité des réseaux véhiculaires. Dans ce chapitre nous avons proposé un nouveau schéma de gestion de clés permettant de faciliter la génération et la distribution de clés dans un réseau VANET.

Notre solution est basée sur des mécanismes de cryptographie symétrique et asymétrique qui permet de chiffrer les messages échangés entre les différents utilisateurs d'un réseau véhiculaire.

Parmi les avantages de notre solution, les nœuds ne stockent pas beaucoups de clés, si un nœud est compromis il n'affecte que la clé partagée avec son leader.

Conclusion générale

Les réseaux véhiculaires ou VANET constituent un nouveau type de réseaux mobiles ad-hoc, ils permettent aux véhicules de se communiquer les uns avec les autres tout au long de la route. Cet échange d'informations empêche certaines situations que le conducteur peut faire face telles que les accidents, les situations de trafics aux heures de pointe, localisation des stations d'essence, emplacements de parking libre,...etc. Le développement de nouvelles technologies a favorisé l'évolution des réseaux véhiculaires, en d'autres termes le système devient plus fiable et efficace. L'implémentation des réseaux véhiculaires donne lieu à d'autres applications telles que la maintenance à distance et l'accès aux différents services ainsi que d'autres applications de confort telles que la musique, les vidéos et les jeux en réseaux.

Malgré toutes ces évolutions, les VANETs sont exposés à un grand nombre de vulnérabilités et susceptible de subir tout type d'attaques menaçant la vie des usagers, d'où la sécurité de ces réseaux est un pré requis pour leurs déploiement. Plusieurs techniques cryptographiques ont été définit dont la gestion de clés fait partie.

Dans le cadre de ce mémoire, nous nous sommes intéressés au problème de sécurité dans les VANETs et plus exactement à la gestion de clés. Nous avons présenté les caractéristiques essentielles et les notions fondamentales des réseaux véhiculaires. Nous avons étudié plus particulièrement les concepts et services de sécurité spécifiques au VANETs ainsi que les différentes attaques et mécanismes de sécurité.

La gestion de clé est une fonction très importante dans la conception d'un système cryptographique qui permet de garantir une communication sécurisée entre les différentes entités d'un réseau VANET.

Nous avons également dressé un état de l'art dans la littérature autour de ces réseaux en termes de projets de recherches et approches propochées. Nous avons présenté leurs principes de foctionnement, les avantages et inconvénients des différentes techniques. Cette étude nous a permis de proposer une solution de gestion de clés hybride basée sur la cryptographie symétrique et asymétrique dans le but de sécuriser ce type de réseau. Notre solution a pour but de résoudre le problème de compromission de nœuds tout en intégrant une plate forme de confiance appelée TPM. Ainsi que, de réduire la surcharge sur l'autorité de certification CA et cela en désignant des leaders.

En guise de perspectives, ce travail peut être enrichi par des simulations afin de mesurer les forces et les faiblesses de notre solution et de concrétiser des résultats pour d'éventuelles comparaisons et améliorations.

Références bibliographiques

Bibliographie

[1] C.BURGOD. *« Contribution à la sécurisation du routage dans les réseaux ad hoc »*, Université de Limoges,Thése de doctorat,2009.

[2] N.CHAIB. *« La sécurité des communications dans les réseaux VANET »*,Université El Hadj Lakhder Batna.

[3] J.PETIT. *« Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires »*,Université de Toulouse, Thèse de doctorat, 2011.

[4] R.ENGOULOU. *« Sécurisation des VANETS par la méthode de réputation des nœuds »*, UNIVERSITÉ DE MONTRÉAL, 2013.

[5] C.TCHEPNDA. *« Authentification dans les Réseaux Véhiculaires Opérés »*,Ecole doc torale d'Informatique, Télécommunication et Electronique de paris, Thèse de doctorat, 2008.

[6] M.ERITALI. *« Contribution à la sécurisation des réseaux ad hoc véhiculaires »*, Université Mohammed V_AGDAL Rabat, Thése de doctorat, 2013.

[7] F.ARMKNECHT, A.FESTAG, D.WESTHOFF et K.ZENG. *« Cross-layer privacy enhancement and non-repudiation in vehicular communication »*, Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference, pp. 1-12, 2007.

[8] Q.YI et N.MOAYER. *« Design of secure and application-oriented VANETs »*,in Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, 2008, pp. 2794-2799.

[9] N.MERANI et N.KHIMOUM. *« Simulation et évaluation de protocoles de gestion de clés dans les réseaux de capteurs »*,Mémoire d'ingénieur détat en informatique, Béjaia 2009.

[10] Y.KIM, A.PERRRIG et G.TSUDIK. *« Tree-based group key agreement.ACM Trans.Info-rm.Syst.Sec. »*7,1,60-96.2004.

[11] J.KONG, P.ZERFOS, H.LUO, S.LU et L.ZHANG. *« Providing robust and ubiquitous security support for mobile ad hoc networks. In Proceedings of the Ninth International Conference on Network Protocols (ICNPâĂŹ01) »*,2001.

[12] L.ZHANG. *« Research on Security and Privacy in Vehicular Ad Hoc Networks »*,

Ph.D. Dissertation, Université de Rovira Virgili, 2010.

[13] M.RAYA, A.AZIZ et J.-P.HUBAUX. *« Efficient secure aggregation in VANETs »*, The 3rd International Workshop on Vehicular Ad Hoc Networks, VANET 2006,pp. 67-75.

[14] M.RAYA et J.-P.HUBAUX. *« Securing vehicular ad hoc networks »*,Journal of Computer Security, vol. 15, p.39-68, 2007.

[15] Y.HAO, Y.CHENG, C.ZHOU et W.SONG. *« A Distributed Key Management Framework with Cooperative Message Authentification in VANETs »*,IEEE Journal on Selected Areas In Communications, Vol.29, no.3, March 2011.

[16] S.ALKA et S.TANWAR. *« Key Management Technique for group communication in Vehicular Ad Hoc Networks »*,International Journal of Multidisciplinary Research and Development 2014 ; 1 (6) : pp. 145-147.

[17] S.JAYANTH, I.S.SARAVANAN et R.K.KAPILAVANI. *« A Survey on Group Key Technique and Cooperative Authentification in VANET »*,International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, Fevrier 2017. pp 1447-1451.

[18] J.ANKUR, R.DUBEY et R.VINEET. *« A Memory Efficient Key Management and Distribution Scheme for Vehicular Adhoc Network »*.

[19] K.S.DHANALAKSHMI et G.SASIKALA. *« Key Management Techniques for VANETs Special »*,Issue of International Journal of Computer Applications (0975-8887) on International Conference on Electronics, Communication and Information Systems (ICECI12).

[20] Y.WANG et F.LI. *« Vehicular Ad Hoc Networks »*,London : Springer-Verlag 2009.

[21] S.ZEADALLY, R.HUNT, Y.-S.CHEN, A.IRWIN et A.HASSAN. *« Vehicular ad hoc networks (VANETS) : status, results, and challenges »*,Springer Science, 2010.

[22] T.LEINMULLER, R.K.SCHMIDT, E.SCHOCH, A.HELD et G.SCHAFER. *« Contribution à la sécurisation du routage dans les réseaux ad hoc »*,Université de Limoges, Thèse de doctorat, 2009.

[23] X.LIN, R.LU, C.ZHANG, H.ZHU, P.H.HO et X.SHEN. *« Security in vehicular ad hoc networks »*, IEEE Communications Magazine, vol. 46, no. 4, pp. 88-95, April 2008.

[24] J.-P.HUBAUX. *« The Security and Privacy of Smart Vehicles »*,Presentation at ZISC Information Security Colloquium, Nov 2004.

Webographie

[25] *« Car-to-car communication consortium C2C-CC »*,http ://www.car-to-car.org, 2017.

[26] *« Carlink consortium »*,http ://carlink.lcc.uma.es/, 2017.

[27] *« E-Safety Vehicle Intrusion Protected Applications »*,http ://evita-project.org/, 2017.

[28] *« Geographic addressing and routing for vehicular communications »*,http ://www.geonet-project.eu/ ,2017.

[29] *« Network On Wheels »*,http ://www.network-on-wheels.de/about.html, 2017.

[30] *« Secure Vehicle Communication »*,http ://www.sevecom.org/, 2017.

[31] *« Le site du trusted platform-module (tpm) »*,http ://www.trustedcomputinggroup.org/groups/tpm/, 2017.

Résumé

Aujourd'hui les technologies sans fil connaissent un très grand succès dans la société. La flexibilité et le développement rapide de ces technologies a fait d'elles un des domaines de recherche les plus attractifs. Les chercheurs ont réussi à définir les réseaux véhiculaires, en tant que nouvelle sous classe émergente des réseaux MANETs. Les VANETs représentent une des composantes les plus prometteuses des systèmes de transport Intelligent (ITS) qui visent à assurer la sécurité routière.

Nous avons présenté dans ce mémoire une solution pour la gestion de clés des réseaux VANETs, cette solution se déroule en sept phases : commeçnant par l'initialisation du réseau, puis la génération et distribution de clés, ensuite l'ajout et la suppression de nœuds et en fin la mise à jour des clés du réseau. Notre proposition est basée sur une combinaison entre la cryptographie symétrique et asymétrique. Nous avons ainsi proposé un schéma décrivant l'utilisation de ces deux types de cryptographie afin d'assurer une gestion robuste et sécurisée de clés adaptée au contexte de VANET.

Mot clés : Réseaux véhiculaires, VANET, Sécurité, Gestion de clés.

Abstract

Today, wireless technologies are very successful in society. The flexibility and rapid development of these technologies has made them one of the most attractive areas of research. The researchers have succeeded in defining vehicular networks, as a new emerging subclass of the Manet networks. VANETs are one of the most promising components of Intelligent Transport Systems (ITS) designed to ensure road safety.

In this paper, we have presented a solution for the management of VANET networks keys. This solution is carried out in five phases : starting with the initialization of the network and then the generation and distribution of keys, then the addition and deletion of Nodes and at the end the updating of the keys of the network. Our proposal is based on a combination of the two symmetric and asymmetric cryptography. We have thus proposed a scheme describing the use of these two types of cryptography in order to ensure robust and secure management of keys adapted to the VANET context.

Key words : Vehicle networks, VANET, Security, Key management.