

République Algérienne Démocratique et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Amar Telidji Laghouat



Faculté Des Sciences

Département D'informatique

Mémoire en vue de l'obtention du diplôme de Master en informatique
option : Réseaux ,Systèmes et Applications Réparties

Thème :

Analyse des architectures proposées pour sécuriser les communications dans les réseaux véhiculaires

Réalisé par :
Youcef CHETTIH

Encadré par :
Dr Nasreddine LAGRAA

Juillet 2011

à mes parents,
à mes frères et sœurs,
à tous ceux qui me sont chers,...
Je dédie affectueusement ce modeste travail

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à mon encadreur Mr. Nasreddine LAGRAA, pour son aide sans limites et ses précieux conseils qu'il m'a donné, et sans lesquels ce travail n'aurait pas vu le jour.

Je remercie également les membres de jury qui ont accepté d'examiner ce travail :

Mr. Mohamed Bachir YAGOUBI, maître de conférence à l'université de Laghouat, qui me fait le grand honneur d'accepter la présidence du jury.

Mr. Lahcene BENSAD et Melle.Zohra ABDELHAFIDI, maîtres assistants à l'université de LAGHOUAT pour l'honneur qu'ils me font en acceptant de participer à ce jury.

Je remercie également tous ceux qui de près ou de loin, m'ont accompagné et soutenu pour mener à bien ce travail.

Je remercie aussi mes camarades, mes amis et toutes les personnes qui m'ont aidé durant mes études universitaires.

Sans oublier tout mes professeurs qui nous ont enseigné sans hésiter à nous faire passer leurs informations.

Table des matières

Introduction générale	1
1 Les réseaux VANET	3
1.1 Introduction	3
1.2 Architectures de communications	3
1.2.1 Réseaux véhiculaire à infrastructure (V2I)	3
1.2.2 Réseaux véhiculaire ah-hoc (V2V)	4
1.2.3 Réseaux véhiculaire hybrides	4
1.3 Caractéristiques des réseaux VANET	5
1.4 Applications	6
1.4.1 Les applications ITS	6
1.4.2 Les applications non-ITS	7
1.5 Projets de recherche	7
1.6 Conclusion	9
2 La sécurité des réseaux VANET	10
2.1 Introduction	10
2.2 Attaques dans les réseaux véhiculaires	10
2.2.1 C'est quoi une attaque ?	10
2.2.2 Taxonomie des attaques	10
2.2.3 Les types d'attaques	12
2.3 Mécanismes et concepts de sécurité	16
2.4 Infrastructure à clés publiques PKI (Public Key Infrastructure)	17
2.5 Contraintes et objectifs des systèmes de sécurité	17
2.6 Conclusion	18
3 Architectures de sécurité	19
3.1 Introduction	19
3.2 Les architectures	19
3.2.1 Architecture de El zarki et <i>al</i>	19

3.2.2	Architecture de Raya et <i>al</i>	22
3.2.3	Architecture de Gerlach et <i>al</i>	27
3.2.4	Autres contributions	34
3.3	Discussion & comparaison	35
3.4	Conclusion	37
4	Analyse et scénarios d’attaques	38
4.1	Introduction	38
4.2	Les limites de la révocation des certificats	38
4.3	Scénarios d’attaques	40
4.3.1	Premier scénario : l’attaque sybil	40
4.3.2	Deuxième scénario : le déni de service distribué (DDOS)	41
4.3.3	Troisième scénario : l’attaque du rejeu (replay attack)	42
4.4	Conclusion	43
	Conclusion générale	44
	Bibliographie	45

Table des figures

1.1	Communication V2I	4
1.2	Communication V2V	4
1.3	Communication hybride	5
2.1	Identification non autorisée	12
2.2	Injection d'informations de trafic erronées	13
2.3	Fausse déclaration de localisation	13
2.4	Usurpation d'identité	14
2.5	Déni de service par brouillage de canal radio	15
2.6	Extraction du mot de passe d'une transaction commerciale	15
3.1	Scénario type de l'architecture	20
3.2	Unité embarquée dans les véhicules	21
3.3	Vue globale sur l'architecture de Raya et al	23
3.4	Déroulement du protocole RTPD (révocation de certificat)	26
3.5	Les couches fonctionnelles	28
3.6	L'organisation et les composants de l'architecture	30
3.7	Les composants locaux de l'application	32
3.8	La vue du modèle de référence	33
4.1	L'attaque sybil	41
4.2	DDOS véhicule à véhicule	42
4.3	DDOS véhicule à infrastructure	42
4.4	Attaque du rejeu	43

Résumé

Un nouveau type de réseau requière de nouveaux concepts de sécurité informatique, les réseaux véhiculaires avec leurs caractéristiques particulières présentent un défi majeur concernant la sécurisation des communications inter véhiculaires. Dans ce mémoire nous présentons les différentes menaces qui visent à compromettre la stabilité, la confidentialité, et surtout la disponibilité des réseaux véhiculaires. Nous présentons aussi les mécanismes à employer pour constituer une architecture de sécurité qui doit garantir le bon fonctionnement du réseau en assurant les différentes exigences de sécurité. Nous analysons quelques architectures après les avoir présentés en faisant une comparaison entre elles. Enfin nous présentons quelques scénarios d'attaques qui peuvent se manifester dans les réseaux véhiculaires, tout en désignant l'architecture appropriée pour contrer ou éviter ces attaques.

Mots-clés : VANET, Architecture de sécurité, signature numérique, révocation de certificat, attaque.

Abstract

A new type of network requires new concepts of security, vehicular networks with their specific characteristics presents a major challenge for securing inter vehicular communications. In this dissertation we present the different threats that aim to compromise stability, privacy, and especially the availability of vehicular networks. We also present the mechanisms used to build a security architecture that may guarantee the smooth operation of networks by providing different security requirements. We analyze some architectures after being presented with a comparison between them. Finally we present some attack scenarios that can occur in vehicular networks, while designating the appropriate architecture to counter or prevent these attacks.

Key words : VANET, Security architecture, digital signature, certificate revocation, attack

ملخص

الشبكات اللاسلكية للمركبات تشكل نوعا جديدا من الشبكات يتطلب مفاهيم جديدة للأمن. الخصائص المميزة لهذه الشبكات تشكل تحديا كبيرا يتطلب اليات جديدة لتأمين الاتصالات بين المركبات.

في هذه المذكرة فصلنا التهديدات المختلفة التي ترمي الى تقويض الاستقرار، والخصوصية، و الآليات المستخدمة لبناء هيكل أمني يمكن أن يضمن سلاسة الاتصالات و ذلك بتوفير المتطلبات الأمنية المختلفة. بعد ذلك قمنا بتحليل بعض الهياكل الأمنية مع القيام بدراسة مقارنة بينها. أخيرا، اقترحنا بعض السيناريوهات التي يمكن أن تحدث في اطار هجوم على شبكات المركبات، و تعيين البنية المناسبة لمواجهة أو منع هذه الهجمات.

الكلمات الرئيسية : هيكل الأمن، التوقيع الرقمي، إلغاء الشهادة، الهجوم.

Introduction générale

De nos jours, le volume de la circulation routière peut être un ennui quotidien, surtout dans les pays développés. En outre, les conditions du trafic routier affecte d'une façon directe la sécurité des individus, d'ailleurs 1,2 million de personnes à travers le monde meurent chaque année sur les routes. Pour cette raison, les industries de l'automobile et de télécommunications investissent beaucoup de ressources pour accroître la sécurité routière et l'efficacité du trafic.

L'un des domaines les plus prometteurs de la recherche est l'étude des communications entre les véhicules et les unités au bord de la route, plus précisément les réseaux VANET (Vehicular Ad-hoc NETWORKS). Ce type de réseaux est composé d'une collection de véhicules et d'infrastructures routières reliés les uns aux autres, et qui s'envoient des informations et des avertissements concernant la situation actuelle du trafic.

En dépit des nombreux scénarios d'applications, les réseaux VANET viennent avec leur propre ensemble de défis, en particulier dans les aspects de sécurité.

Dans ce modeste travail nous présentons une panoplie d'architectures de sécurité qui visent à rendre les communications entre les véhicules plus sûres en essayant d'assurer le maximum d'exigences de sécurité, tout en faisant une comparaison entre ces architectures. Nous présentons aussi quelques scénarios d'attaques qui peuvent se manifester dans les réseaux véhiculaires, en désignant l'architecture adaptée pour contrer ces attaques.

Ce mémoire se divise en quatre chapitres. Dans le chapitre 1, intitulé "Les réseaux VANET", nous présentons ce type de réseaux en soulignant les modes de communication possible, les caractéristiques qui le représentent ainsi que les deux classes d'applications sur ce réseaux, et enfin les projets de recherche travaillant dans ce type de réseaux. Le chapitre 2 constitue le do-

mainie qui nous intéresse à savoir la sécurité des communications véhiculaires, nous présentons les différentes attaques qui menacent l'efficacité des applications en particulier les applications ITS, ensuite nous mettons le point sur les exigences nécessaires pour avoir un réseau sécurisé. Dans le chapitre 3, nous présentons en détails, trois architectures de sécurité qui ont été proposées, ensuite nous décrivons brièvement une panoplie d'autres propositions, nous ferons par la suite une comparaison entre les trois architectures. Dans le chapitre 4 nous présentons trois scénarios d'attaques possible dans les réseaux véhiculaire, en indiquant l'architecture qui peut éviter ou contrer ces attaques.

Chapitre 1

Les réseaux VANET

1.1 Introduction

Les réseaux VANETs constituent une nouvelle forme de réseaux ad-hoc mobiles (MANET). Ils permettent d'établir des communications entre véhicules ou bien avec une infrastructure située aux bords de routes. Par rapport à un réseau ad-hoc classique, les réseaux VANET sont distingués par quelques caractéristiques qui les rendent un peu particuliers.

Dans ce chapitre nous présentons les caractéristiques, les applications et les principaux types de communication dans les réseaux véhiculaires. Nous commencerons par présenter les types de communication qui existent dans les réseaux véhiculaires, après nous verrons les caractéristiques générales et quelques exemples d'applications, ensuite nous abordons les projets de recherche qui travaillent dans ce domaine, et enfin nous concluons le chapitre.

1.2 Architectures de communications

La classification des types de communications dans les réseaux véhiculaires a donné naissance à trois architectures.

1.2.1 Réseaux véhiculaire à infrastructure (V2I)

Ce sont les réseaux dans lesquelles les véhicules communiquent obligatoirement par l'intermédiaire d'une infrastructure fixe relié au réseau filaire (cf. figure 1.1). Ce type de réseaux est très utile pour des applications telles que l'accès à Internet, les jeux en réseau, . . . etc.

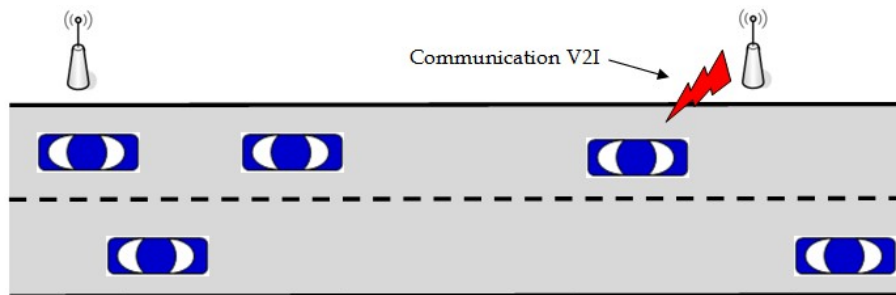


FIGURE 1.1 – Communication V2I

1.2.2 Réseaux véhiculaire ah-hoc (V2V)

Ce sont les réseaux dans lesquelles les véhicules communiquent directement entre eux ou indirectement par l'intermédiaire d'autres véhicules (cf. figure 1.2). Ce type de réseaux est indispensable pour les applications ou les services liés à la sécurité routière (par exemple, alerte accident, alerte ralentissement, alerte travaux, . . . etc).

On peut également trouver dans ce type de réseau les applications ou les services dits de divertissement telle que la messagerie instantanée inter-véhicules ou encore des jeux en réseau entre véhicules.

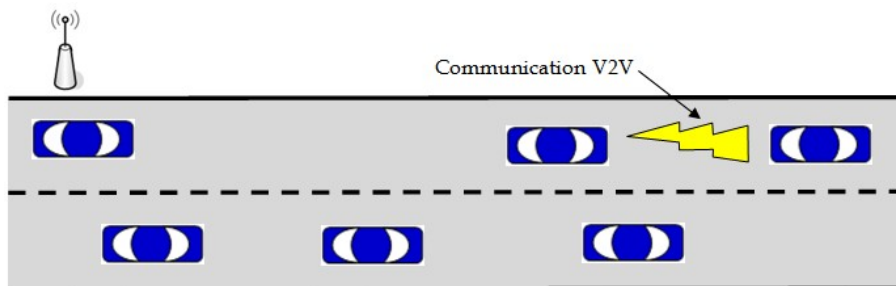


FIGURE 1.2 – Communication V2V

1.2.3 Réseaux véhiculaire hybrides

La combinaison des deux types de communications précédents permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance (cf. figure 1.3). Dans un but économique et en évitant de multiplier les bornes à chaque coin de rue, l'appel à l'utilisation de ce type de réseau est justifié.

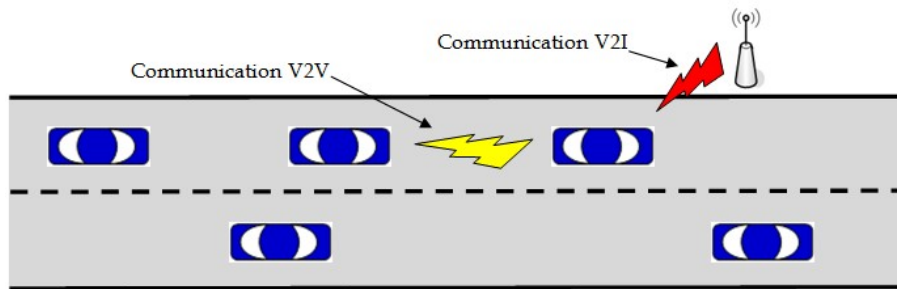


FIGURE 1.3 – Communication hybride

1.3 Caractéristiques des réseaux VANET

Les réseaux véhiculaires se distinguent des autres réseaux sans fil par un certain nombre de caractéristiques spécifiques dont on peut citer :

Le potentiel énergétique

”À la différence des réseaux sans fil traditionnels où la contrainte d’énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de grandes capacités énergétiques qu’elles tirent du système d’alimentation propre des véhicules” [11].

La topologie et la connectivité

”les réseaux VANET sont caractérisés par une connectivité sporadique, car un véhicule peut rejoindre ou quitter un groupe de véhicules en un temps très court, ce qui nous mène ainsi à avoir une topologie très dynamique constituée de plusieurs segments séparés” [13].

Le modèle de mobilité

”plusieurs facteurs peuvent affecter la mobilité dans ces réseaux comme les infrastructures routières, par exemple, route, autoroute, panneaux de signalisation. En outre, la mobilité dans les VANET est liée directement au comportement des conducteurs et leurs réactions face à des obstacles ou des situations différentes et complexes rencontrées, par exemple, embouteillage, accidents,...etc” [14].

Le modèle de communication

”Les réseaux véhiculaires ont été imaginés principalement pour les applications liées à la sécurité routière (e.g. diffusion de messages d’alerte). Dans ce type d’application, les communications se font presque exclusivement par relayages successifs d’une source vers une multitude de destinataires. Le modèle de transmission en Broadcast ou en Multicast est donc appelé à dominer largement dans les réseaux véhiculaires, ce qui n’est par exemple pas sans conséquence sur la charge du réseau et le modèle de sécurité à mettre en œuvre” [11].

La taille du réseau

”Étant donné les avancées importantes réalisées dans le domaine des communications sans fil et les bas coûts des équipements associés, les véhicules qui intègrent déjà massivement des systèmes GPS et des équipements Bluetooth, seront très probablement équipés et ce, tout aussi massivement, de plateformes de communication leur permettant de constituer de véritables réseaux. Ce faisant, et compte tenu de l’importance sans cesse grandissante de la densité et du parc des véhicules, on peut s’attendre à ce que la taille des réseaux véhiculaires dont les déploiements restent encore très confidentiels, soit d’une tout autre ampleur. L’importance potentielle de la taille des réseaux véhiculaires constitue donc une caractéristique majeure à prendre en compte dans la conception de ces réseaux” [11].

1.4 Applications

Il est attendu que les réseaux véhiculaires soient l’instrument de la fourniture d’une très grande variété d’applications parmi lesquelles on peut citer les alertes accident, ralentissement, déviation, travaux, intempéries, la conduite coopérative, la surveillance de l’état des véhicules, la localisation des véhicules, la gestion de flotte de véhicules, la messagerie instantanée, les jeux en réseau, l’accès Internet, les paiements automatiques, etc. Nous répertorions ces applications en deux grandes classes à savoir [11] :

1.4.1 Les applications ITS

Les applications ITS (Intelligent Transportation System) sont des applications liées à la sécurité routières (i.e. des applications influant directement la sécurité des personnes et des biens) et visant à bâtir un système

de transport intelligent. En d'autres termes, l'objectif ultime de ces applications est de réduire les accidents routiers. Parmi les exemples d'applications cités précédemment, les applications dites ITS pourront être : la conduite coopérative, l'aide aux dépassements de véhicules, les alertes des situations anormales, . . . etc [11].

1.4.2 Les applications non-ITS

Ce sont des applications commerciales, de confort, de divertissement ou plus généralement toutes les autres applications ne faisant pas partie de la catégorie des applications ITS. Parmi les exemples d'applications donnés plus haut, les applications dites non-ITS sont : la surveillance de l'état des véhicules, la localisation des véhicules, la gestion de flotte de véhicules, la messagerie instantanée, les jeux en réseau, l'accès à Internet, les paiements automatiques, . . . etc [11].

1.5 Projets de recherche

Beaucoup d'activités de recherche, de développement et de standardisation portant sur les communications inter véhicules sont actuellement en cours. En Europe et dans le monde entier. Ci-dessous sont décrits quelques projets majeurs traitant des communications véhiculaires [13] :

PReVENT

Le projet intégré européen PReVENT [15] vise à élaborer des applications relatives à la sécurité routière en utilisant des dispositifs avancés de détection et de communication intégrés dans les systèmes embarqués d'aide à la conduite. Ces systèmes analysent la nature et l'importance de tout danger potentiel, tout en tenant compte de l'état du conducteur.

SafeSpot

Le projet européen SafeSpot [16] a pour objectif principal l'amélioration de la sécurité routière. Des études ont montré que le conducteur est, à 90% , responsable des accidents, principalement pour des causes d'inattention ou des erreurs de jugement. Ainsi, le projet SafeSpot propose de développer un ensemble de mécanismes d'assistance fournissant au conducteur une indication de sa marge de sécurité. Ceci doit être effectué avant d'approcher une situation difficile.

Watch-Over

Le but de Watch-over [17] est de concevoir et de développer un système coopératif pour la prévention des accidents dans les zones accidentogènes. Le concept innovant est représenté par une plateforme embarquée et un module utilisateur. Le système repose sur la communication à faible portée et l'acquisition de données par des capteurs de vision.

CVIS

Le projet CVIS (Coopérative. Vehicle-Infrastructure Systems) [18] vise à concevoir, mettre en oeuvre et tester les nouvelles technologies nécessaires pour permettre aux véhicules de communiquer entre eux ainsi qu'avec les infrastructures routières situées à proximité. Il a pour ambition d'amorcer une révolution dans la mobilité des voyageurs et des marchandises en concevant de toutes nouvelles modalités d'interaction entre les conducteurs, leurs véhicules et les infrastructures routières. Ainsi, le projet CVIS vise à améliorer la sécurité et l'efficacité du transport routier.

GST

Le projet GST (Global System for Telematics) [19] a pour objectif général de créer un environnement dans lequel des services de télématique automobile innovants peuvent être développées et fournis de manière rentable. Il devrait permettre d'élargir l'éventail des services de télématique économiques qui sont à disposition des constructeurs et des consommateurs.

DRiVE

Le projet DRiVE (Dynamic Radio for IP Services in Vehicular Environments) [20] vise à travailler sur la convergence entre différentes technologies cellulaires et de réseaux hauts débit (GSM, UMTS, DAB et DVB-T) afin de mettre en place le substrat nécessaire au développement de services IP innovants à destination des véhicules.

NoW

Le projet NoW (Network-on-Wheels) [21], le successeur du projet Fleet-net [22], travaille sur la mise en oeuvre de protocoles de communications et d'algorithmes de sécurité des données dans les réseaux de véhicules. En essayant d'implanter un système de communication de référence sur la technologie sans fil IEEE 802.11 et un routage fondé sur la position dans un contexte de communication véhicule à véhicule ou véhicule à infrastructure, et de contribuer à la standardisation des solutions en Europe.

SeVeCom

Le projet SeVeCom (Secure Vehicular Communication) [23] s'intéresse à la sécurité des futurs réseaux de véhicules, incluant la sécurité et l'anonymat de la communication véhicule à véhicule et véhicule à infrastructure.

1.6 Conclusion

Dans ce chapitre, nous avons vu que les réseaux VANET diffèrent des autres réseaux sans fil traditionnel, par leurs caractéristiques qui présentent un défi majeur pour les chercheurs, ainsi que les services et les application offertes afin d'apporter de meilleures conditions de conduite. Dans le chapitre qui suit, nous nous intéresserons à la sécurité dans les réseaux VANET, qui représente l'un des défi les plus important à prendre en considération.

Chapitre 2

La sécurité des réseaux VANET

2.1 Introduction

Pour garantir les services liés à la sécurité routière de façon fiable et efficace, les réseaux véhiculaires ont besoin d'une architecture de sécurité appropriée qui les protégera contre les différents types d'attaque.

Dans ce chapitre nous présentons les types d'attaques dans ces réseaux ainsi qu'une taxonomie correspondante. Nous verrons après les mécanismes de base de la sécurité, nous abordons par la suite les principales exigences et défis de sécurité dans ces réseaux. Nous terminons ce chapitre par une conclusion.

2.2 Attaques dans les réseaux véhiculaires

Avant de développer les mécanismes de sécurité, il est important de définir ce que c'est une attaque, et de faire une classification générique des attaques recensées ou à venir dans les réseaux véhiculaires.

2.2.1 C'est quoi une attaque ?

C'est une action qui vise à compromettre la sécurité, la stabilité, ou la disponibilité d'un réseau en exploitant ses vulnérabilités.

2.2.2 Taxonomie des attaques

La sécurisation des réseaux véhiculaires passe par la détermination d'une typologie des attaques dans ces réseaux. Compte tenu de la diversité des applications que l'on peut y opérer et de celle des environnements d'opération, il est aisé d'imaginer que ces réseaux feront l'objet de nombreuses attaques.

Nous définissons quatre grandes déclinaisons pour toute attaque dans ces réseaux [2] :

Interne ou Externe

Une attaque est dite interne si elle est déclenchée par une entité identifiée comme légitime par les autres nœuds du réseau. De manière courante, une entité sera déclarée légitime si elle est authentifiée dans le réseau. Les attaques internes font partie des attaques les plus dangereuses puisque l'attaquant est injustement considéré comme étant de confiance et a généralement accès aux services du réseau. Une attaque externe est, quant à elle, menée par une entité a priori considérée et reconnue comme étrangère. L'attaquant dans ce cas n'est généralement pas authentifié dans le réseau et n'a pas accès aux services de ce réseau. Il est donc de ce fait limité dans la diversité des attaques qu'il peut entreprendre.

Intentionnelle ou Non intentionnelle

Une attaque est dite intentionnelle si elle est déclenchée par une entité malveillante visant délibérément à remettre en cause le bon fonctionnement du réseau. Ce type d'attaque est à distinguer d'une attaque non intentionnelle ou involontaire qui peut par exemple être le fait d'une erreur de transmission radio ou d'une erreur protocolaire dans le réseau.

Active ou Passive

Une attaque est dite active lorsque l'attaquant injecte, modifie ou supprime du trafic dans le réseau. par contre, dans une attaque passive, l'attaquant ne fait qu'écouter et collecter le trafic pour une éventuelle utilisation malveillante ultérieure.

Indépendante ou Coordinée

Une attaque est dite indépendante lorsqu'elle est menée de manière isolée par un seul attaquant. Elle est en revanche dite coordonnée lorsque plusieurs attaquants partageant le même dessin se concertent pour la mener.

2.2.3 Les types d'attaques

En raison de l'impossibilité d'envisager toutes les attaques possibles dans les réseaux véhiculaires, nous nous limitons ici à la présentation et à la déclinaison dans la taxonomie introduite plus haut, de quelques exemples parmi les plus significatifs [11] :

Attaque sur l'intimité numérique

Dans cette attaque, l'entité malveillante essaie d'obtenir des informations personnelles d'un utilisateur du réseau. Il peut également s'agir pour l'attaquant de tracer l'activité et les déplacements de cet utilisateur. Pour identifier et tracer une victime, l'attaquant peut utiliser toute sorte d'identifiants dont la récurrence est constatée dans les échanges de la victime. comme par exemple une adresse IP, une adresse MAC, des informations d'identification d'un certificat,...etc. La Figure 2.1 illustre une attaque sur l'intimité numérique et en particulier une identification non-autorisée. D'après la taxonomie des attaques qui a été définie, cette attaque peut être interne ou externe, intentionnelle, passive et indépendante.

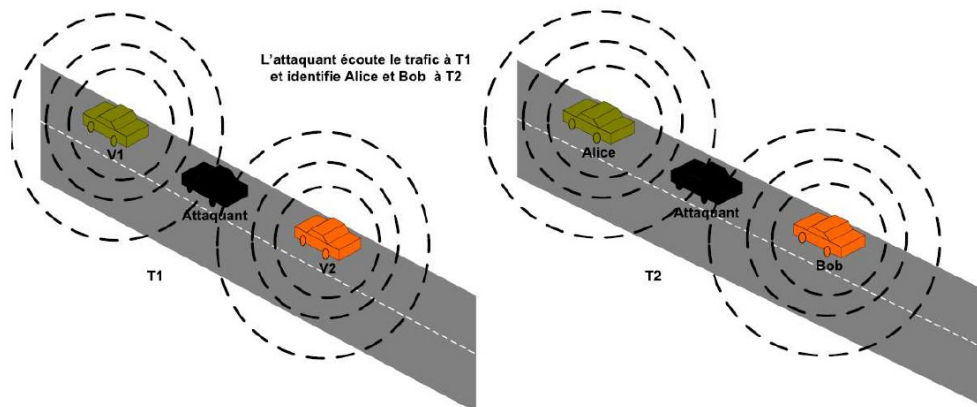


FIGURE 2.1 – Identification non autorisée

Attaque sur la cohérence de l'information

Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. L'intention de l'attaquant peut être d'altérer la perception qu'ont ses victimes, de sa position, de sa vitesse, de sa direction, et plus généralement des conditions de circulation. Ce faisant, l'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. Les Figures 2.2 et 2.3 illustrent deux exemple d'attaque possible. Sur la Figure

2.2 un attaquant diffuse des informations de trafic erronées et sur la Figure 2.3 des attaquants envoient de fausses données de localisation amenant les victimes à admettre l'existence d'un bouchon qui en réalité n'existe pas. L'attaque de la Figure 2.2 peut être interne ou externe, intentionnelle, active et indépendante alors que celle de la Figure 2.3 est interne ou externe, intentionnelle, active et coordonnée.

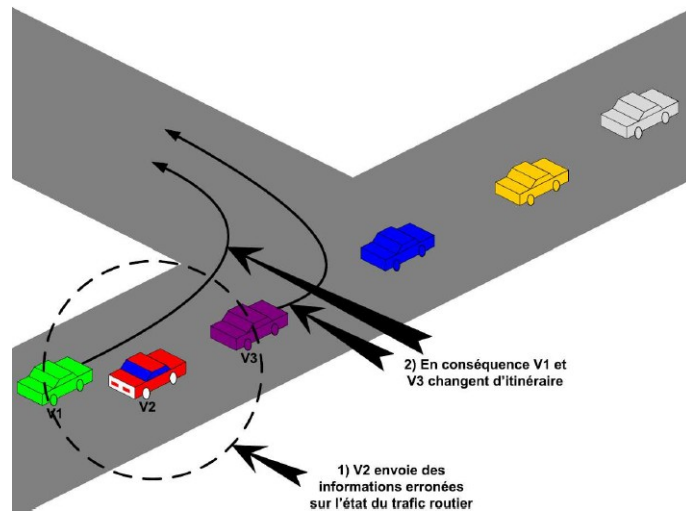


FIGURE 2.2 – Injection d'informations de trafic erronées

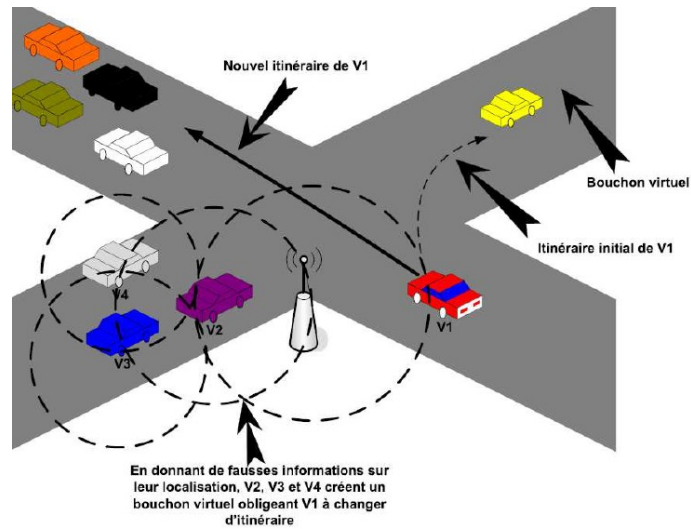


FIGURE 2.3 – Fausse déclaration de localisation

Usurpation d'identité ou de rôle

Dans cette attaque, l'entité malveillante utilise une fausse identité ou de faux messages pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Figure 2.4 illustre un cas d'usurpation d'identité. L'attaque illustrée peut être interne ou externe, intentionnelle, active et indépendante.

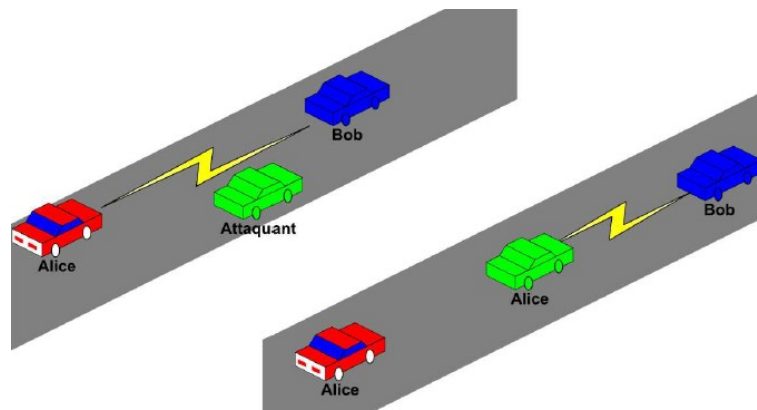


FIGURE 2.4 – Usurpation d'identité

Déni de service

Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau. Ce type d'attaque peut être monté en brouillant le canal radio, en surchargeant et en épuisant les ressources du réseau par des requêtes abondantes, en exploitant la vulnérabilité des protocoles, en ayant une attitude non coopérative (e.g. refus de relayer des paquets), etc. La Figure 2.5 illustre une attaque par déni de service aboutissant à une collision, où l'attaquant empêche l'échange de messages critiques entre des véhicules s'apprêtant à prendre une intersection. Cette attaque peut être interne ou externe, intentionnelle, active et indépendante.

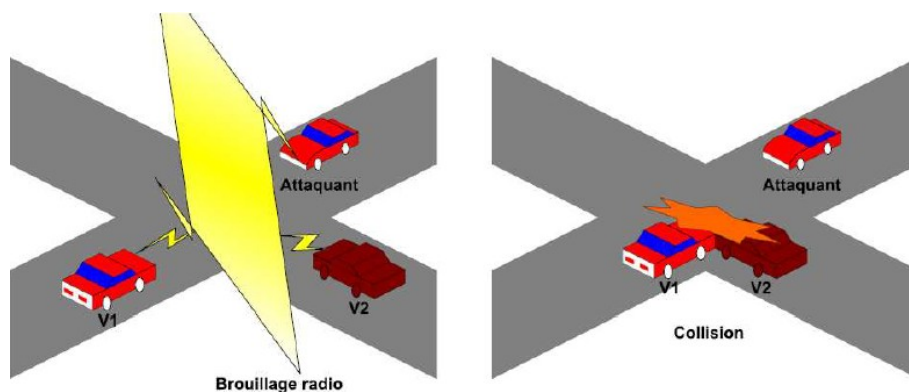


FIGURE 2.5 – Dénier de service par brouillage de canal radio

Écoute du réseau

Dans cette attaque, l'entité malveillante collecte les données transmises dans le réseau afin d'en extraire une information dont elle pourrait tirer profit. La Figure 2.6 illustre une telle attaque dans laquelle l'attaquant espionne une transaction commerciale (le paiement électronique), en vue d'en extraire un mot de passe. Cette attaque peut être interne ou externe, intentionnelle, passive et indépendante.

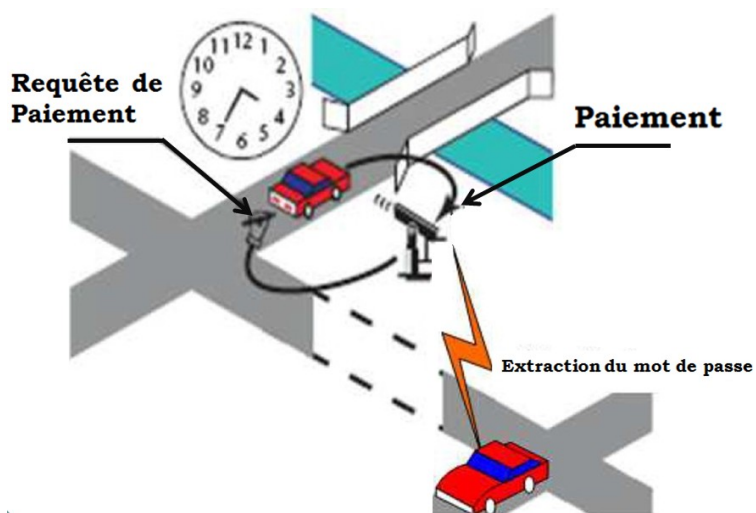


FIGURE 2.6 – Extraction du mot de passe d'une transaction commerciale

2.3 Mécanismes et concepts de sécurité

La cryptographie

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en employant souvent 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 l'en rendre incompréhensible) et de déchiffrement (afin de reconstruire le message original).

La cryptographie symétrique (ou cryptographie à clé secrète)

Elle consiste à utiliser une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer les données.

La cryptographie asymétrique (ou cryptographie à clé publique)

Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.

Le hachage

il consiste à déterminer une information de taille fixe et réduite (appelée l'empreinte ou le condensé) à partir d'une donnée de taille indifférente. une fonction de hachage est dite à sens unique ou fonction irréversible qui fournit l'empreinte à partir d'une chaîne fournie en entrée. L'irréversibilité signifie qu'il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile de retrouver ou déduire la chaîne initiale à partir de l'empreinte.

La signature numérique

C'est 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 l'utilisation de la clé privée du signataire.

Le certificat numérique

C'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'autorité de certification (AC).

2.4 Infrastructure à clés publiques PKI (Public Key Infrastructure)

Une infrastructure à clés publiques est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériels), de procédures humaines (vérifications, validation) et de logiciels (système et application) qui permettent de délivrer, révoquer, renouveler, et de façon générale gérer les certificats numériques [5].

2.5 Contraintes et objectifs des systèmes de sécurité

Selon les applications, une architecture de sécurité doit assurer certaine ou toutes les propriétés suivantes :

L'authenticité

L'architecture doit s'assurer que les données sont envoyées par une source de confiance (celle qui a réellement envoyé les données) .

L'intégrité

L'architecture doit s'assurer que les données n'ont pas été falsifiées ou n'ont pas été changées après qu'elles aient été produites.

La responsabilité

En cas d'un conflit, l'architecture doit avoir la capacité d'attribuer des actions à l'entité qui les a causés.

La non-répudiation

L'architecture doit avoir les mécanismes pour faire face à un nœud qui veut nier l'envoi d'un message qu'il a envoyé.

La possibilité de révocation

L'architecture doit avoir les possibilités de rejeter des messages à partir des unités compromises connues.

La contrainte temps réel

la solution de sécurité doit assurer qu'une communication se déroule sans retard afin d'avoir les données les plus récentes.

La disponibilité

L'architecture doit avoir des mécanismes qui permettent d'éviter un déni de service et assurer une connectivité omniprésente. Il est essentiel d'assurer la robustesse du réseau par les protocoles de sécurité qui fonctionnent en dépit des conducteurs.

La confidentialité

Elle n'est pas habituellement exigée pour des applications de sûreté. Cependant, la confidentialité est souvent exigée pour des applications privées, telles que le paiement de stationnement ou de péage.

2.6 Conclusion

Nous nous sommes intéressés dans ce chapitre à la sécurité des réseaux véhiculaires, nous avons montré à travers le prisme de leurs caractéristiques spécifiques et de quelques exemples d'attaques, que les exigences et les défis de sécurité ne s'y posaient pas nécessairement de la même manière selon que l'on traite les services ITS ou les services non-ITS.

Dans le chapitre qui suit, nous ferons une présentation de quelques architectures de sécurité proposées auparavant.

Chapitre 3

Architectures de sécurité

3.1 Introduction

La sécurité des réseaux véhiculaires est un champ d'investigation relativement récent n'ayant pas encore fait l'objet de développement ou de standardisation de solutions complètes [11]. Toute fois, il y a eu quelque contributions dans ce domaine que nous verrons dans ce chapitre.

Une architecture de sécurité intègre divers mécanismes et protocoles susceptibles d'assurer les différentes exigences de sécurité vues précédemment.

Dans ce chapitre nous présentons quelques architectures de sécurité proposées, tout en mettant en valeur les avantages et les inconvénients de chaque architectures, Nous effectuons pas la suite une comparaison entre ces architectures, et nous terminons ce chapitre par une conclusion.

3.2 Les architectures

3.2.1 Architecture de El zarki et *al*

Cette architecture est relativement ancienne, c'était la première contribution qui a été proposée par El zerki et *al* dans [8].

Pour développer l'architecture, les auteurs ont supposé que les véhicules se déplacent sur une route, et peuvent communiquer entre eux (localement) par l'intermédiaire d'un réseau sans fil ad-hoc, et globalement, par l'intermédiaire d'un réseau sans fil à infrastructure fixe (cf. la figure 3.1). Chaque véhicule est supposé équipée d'un ordinateur portable ou d'un PDA équipé d'une

carte réseau sans fil pour la communication locale, et d'un appareil sans fil (par exemple, un téléphone portable) pour la connectivité au réseau à infrastructure.

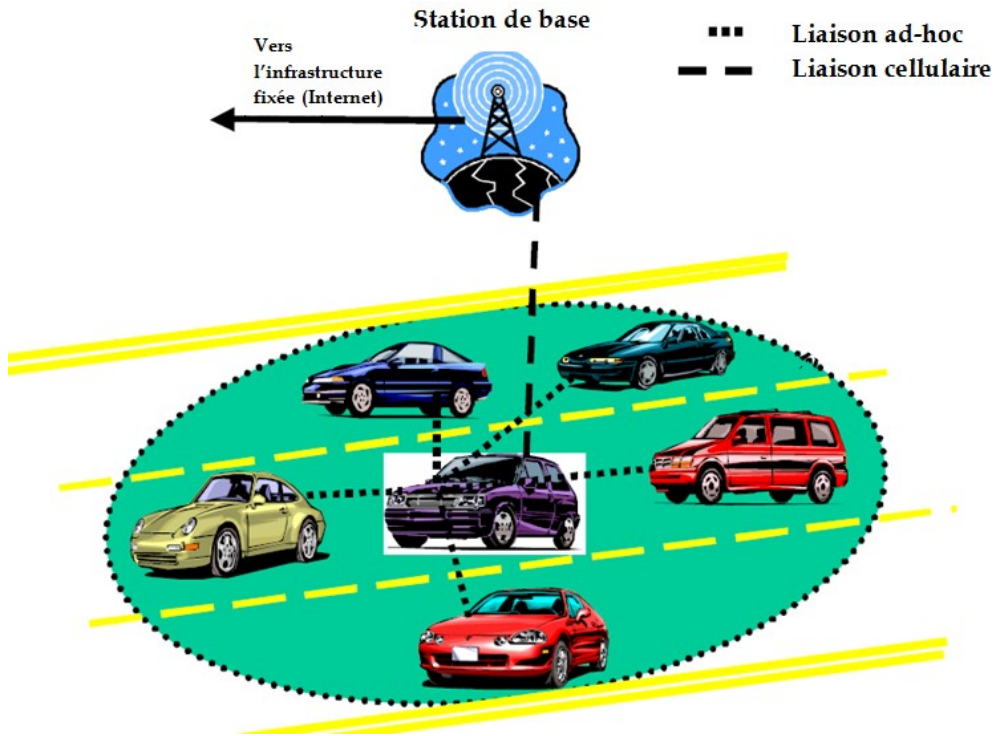


FIGURE 3.1 – Scénario type de l'architecture

Pour le bon fonctionnement de cette architecture, il est supposé que :

- Chaque véhicule forme autour de lui une zone locale de communication. Les véhicules qui sont loin, bien qu'ils puissent constituer une partie d'une zone voisine, ne font pas partie de la zone de transmission de ce véhicule.
- Tous les véhicules diffusent l'information d'une façon omnidirectionnelle et reçoivent des données de toutes les directions. Il n'y a aucune liaison point à point.
- Le but du réseau ad-hoc est de communiquer des informations, c'est à dire les signes essentiels du véhicule, aux véhicules à proximité et de recevoir les mêmes données d'eux.

- L'information est traitée localement pour fournir au conducteur une carte indiquant le statut de chaque véhicule à proximité, par exemple, accélération, état du clignotant, freinage,...etc.
- Chaque véhicule communique également, à une fréquence beaucoup plus basse, avec le réseau à infrastructure afin de communiquer ses signes essentiels. Ces données sont utilisées par l'infrastructure pour gérer et maintenir à jour l'état du trafic. Elles constituent également une base de données dynamique que les utilisateurs (conducteurs) peuvent questionner afin d'extraire des informations sur le trafic.
- Chaque véhicule sera également équipé d'un récepteur GPS et plusieurs capteurs qui collectent des informations concernant les signes essentiels du véhicule.
- Chaque véhicule aura sur chacun de ses quatre côtés, un simple dispositif de détection qui surveillera la présence (ou l'absence) d'un autre véhicule à proximité. La figure 3.2 montre une unité (c'est à dire, ordinateur portable ou PDA) qui sera embarquée dans chaque véhicule.

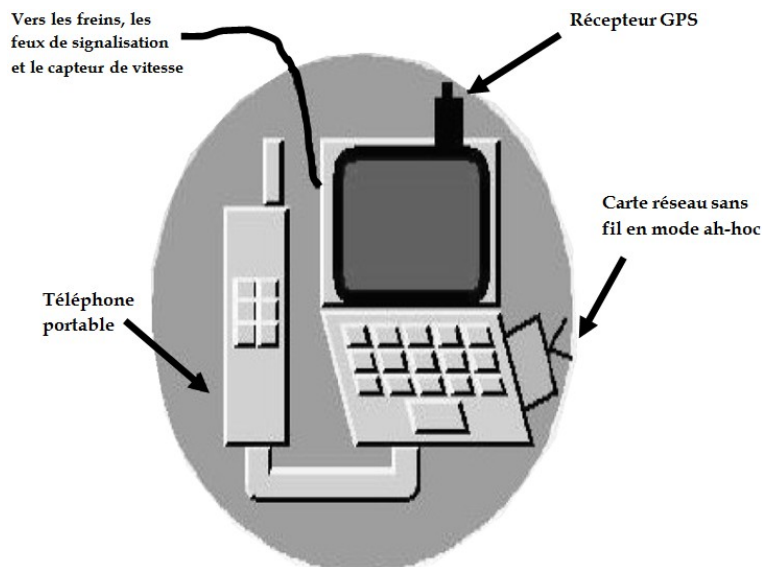


FIGURE 3.2 – Unité embarquée dans les véhicules

L'architecture de sécurité est constitué d'une infrastructure de certification ,qui doit prendre en compte la particularité des caractéristiques des réseaux véhiculaire. Ainsi, les bases de données de l'infrastructure stockent une série d'informations spatiales et spatio-temporelles sur les véhicules en déplacement. Ces informations inclut celles à propos des véhicules et leurs emplacement, l'état du trafic, les plaques de signalisation des routes, les feux

de signalisation, et le réseau routier.

Cette architecture se base sur les fonctions suivantes :

La signature numérique

Toutes les transmissions doivent être signées par l'émetteur pour deux raisons :

1. Chaque véhicule (ou infrastructure) recevra beaucoup plus de messages qu'il n'en enverra,
2. Le coût de la vérification de la signature est plus important que celui de sa génération.

Estampillage du temps & séquencement

Toutes les communications doivent inclure des numéros de séquence, ainsi qu'une estampille, la synchronisation de l'horloge n'est pas un problème, puisque tous les véhicules et toutes les infrastructures sont équipés d'un récepteur GPS.

3.2.2 Architecture de Raya et *al*

Cette architecture est proposée par M.Raya et *al* dans [4], et elle suppose l'existence d'une infrastructure à clé publique (PKI), et d'un équipement spécial embarqué dans les véhicules.

Cette architecture assure les fonctionnalités suivantes :

- L'authentification
- La révocation de certificat
- La confidentialité

La figure 3.3 illustre une vue générale de l'architecture, dont les composants sont décrits ci-dessous.

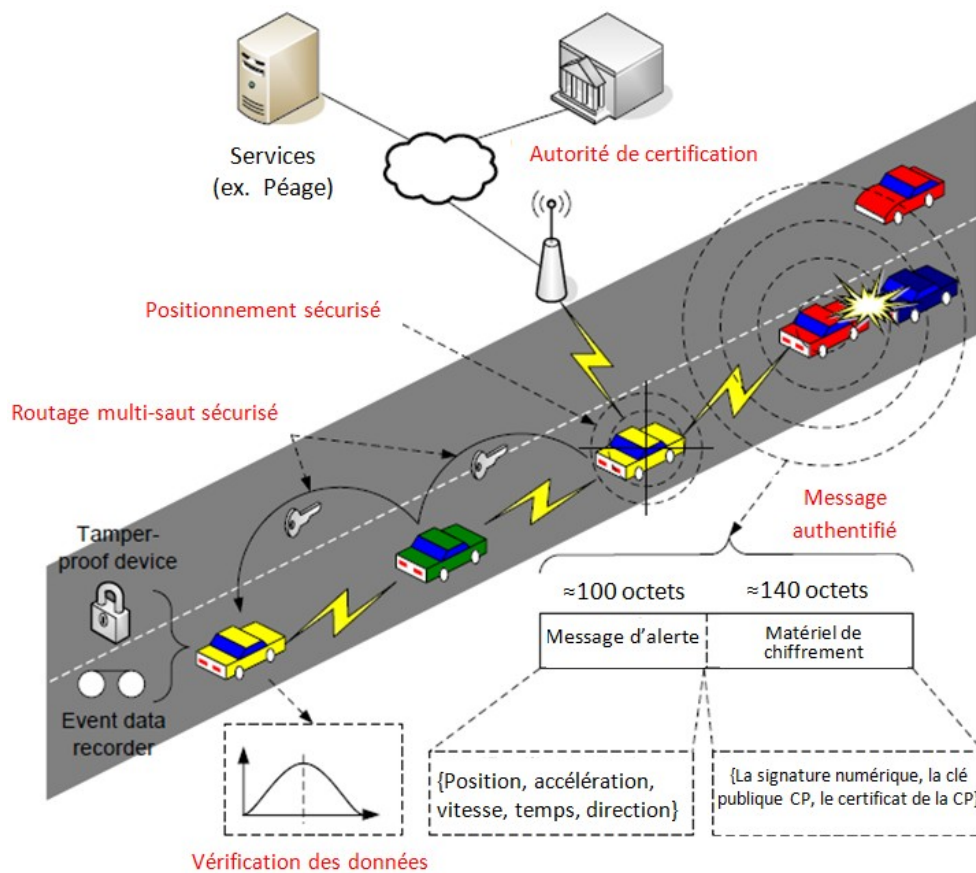


FIGURE 3.3 – Vue globale sur l'architecture de Raya et al

1. **Équipement des véhicules** Les véhicules sont supposés équipés de deux dispositifs :
 - a **Event Data Recorder (EDR)** : Ce dispositif est responsable de l'enregistrement des données importantes du véhicule, comme la position, la vitesse, l'heure,...etc, au moment d'une urgence. Ces données vont aider à la reconstitution du scénario de l'accident. Ce dispositif est similaire à la boîte noire d'un avion.
 - b **Temper-Proof Device (TPD)** : Ce dispositif s'occupe de deux tâches, stockage des clés de chiffrement, et l'exécution des opérations cryptographiques, en particulier la signature et la vérification des messages de sécurité.
2. **Infrastructure à clé publique véhiculaire (VPKI)**
 Le nombre important de véhicules enregistrés dans les différents pays et le fait de parcourir de longues distances, en dehors de leurs régions

d'enregistrement, exigent un système de gestion de clés, robuste et scalable. L'implication des autorités dans l'enregistrement des véhicules entraîne la nécessité d'un certain niveau de centralisation. La communication via les stations de base (comme dans les réseaux cellulaires) ne suffit pas pour les Communications véhiculaire (CV), principalement parce que les véhicules ont besoin de s'authentifier non seulement aux stations de base, mais aussi les uns avec les autres (sans utiliser un serveur), ce qui crée un problème de scalabilité.

Ceci implique la nécessité d'une infrastructure à clé publique (PKI) où les autorités de certification (AC) créent des paires de clés publique/privée certifiées pour les véhicules (avec plusieurs paires par véhicule pour des raisons de confidentialité), de même pour l'AC de la région courante, parce qu'il y en a plusieurs, chacune correspond à une région (pays, état, ...). Autres candidats qui peuvent jouer le rôle d'une AC sont les fabricants de véhicules. Dans les deux cas, les différentes AC doivent se certifier mutuellement afin que les véhicules de régions ou de marques différentes puissent s'authentifier entre eux. Pour cela, il faut que les véhicules stockent les clés publiques de toutes les AC dont les certificats pourront avoir besoin d'être vérifiés. D'autre part, dans le cas où les AC sont les autorités régionales, les véhicules peuvent demander une nouvelle paire de clés publique/privée, d'une autre région qu'ils entrent.

3. L'authentification

La fonction fondamentale dans la sécurité des communications véhiculaires consiste à authentifier la source des données. Afin de s'authentifier mutuellement, les véhicules signent chaque message avec leur clé privée, et lui attache le certificat correspondant. Ainsi, quand un autre véhicule reçoit le message, il vérifie la clé utilisée pour signer ce message, et une fois c'est fait, il vérifie le message.

4. La révocation de certificat

Les avantages de l'utilisation d'une PKI pour les CV sont accompagnés par quelques problèmes, notamment, de révocation de certificats. Par exemple, les certificats d'un attaquant détecté ou d'un dispositif défectueux doivent être révoqués, c'est à dire qu'ils ne devraient plus être en mesure d'utiliser leurs clés, ou, si c'est toujours le cas, les autres véhicules devraient être informés de leurs invalidités.

La façon la plus simple de révocation est la distribution des Listes de

Révocation de Certificats (LRC) qui contiennent les certificats qui ont étaient révoqués récemment.

Cette approche a plusieurs inconvénients, tout d'abord, la LRC peut être très longue en raison du nombre important de véhicules et de leurs grandes mobilités, deuxièmement, la durée de vie courte des certificats crée toujours une fenêtre de vulnérabilité, enfin l'indisponibilité des infrastructures dans certains cas, particulièrement durant les premières années de déploiement.

Afin d'éviter ces inconvénients une solution a été proposée par les auteurs qui consiste à utiliser trois protocoles de révocation, le RTPD (Revocation protocol of the Temper-Proof Device), RCCRL (Revocation protocol using Compressed Certificate Revocation Lists) et le DRP (Distributed Revocation Protocol).

Le protocole RTPD

Une fois que l'AC décide de révoquer un certificat d'un véhicule M (cf. figure 3.4), elle lui envoie un message de révocation chiffré avec sa clé publique (celle de M). Ce message est reçu et déchiffré par le TPD du véhicule. Le TPD efface toutes les clés et arrête de signer des messages de sécurité, puis il envoie un Ack a l'AC. Toutes les communications entre l'AC et M se font par l'intermédiaire d'une infrastructure, en fait, l'AC doit savoir la position de M afin de choisir la station de base par laquelle elle envoie le message de révocation, sinon elle récupère la plus récente position du véhicule d'une base de données de localisation, et définit une zone de pagination avec les stations de base qui couvrent cette zone. Puis, elle envoie le message de révocation en multicast à toutes ces stations de base. Dans le cas où il n'existe pas de position récente, ou bien, l'Ack n'est pas reçu après un certain temps(timeout), l'AC diffuse le message de révocation en broadcast.

Le protocole RCCRL

Ce protocole est utilisé quand l'AC veut retirer seulement un sous-ensemble des clefs d'un véhicule ou quand le TPD du véhicule cible est inaccessible. Etant donné de la grande taille de la LRC dans les réseaux véhiculaires, l'idée principale de ce protocole est d'utiliser des filtres de fleur (une structure de données probabiliste employée pour examiner si

un élément est un membre d'un ensemble). Ainsi, la taille d'un LRCC (LRC Compressée) sera seulement de quelques kilo octets. RCCRL se base également sur la disponibilité de l'infrastructure qui annonce les LRCC une fois toutes les 10 minutes. Comparé au RTPD, le protocole RCCRL a la particularité d'avertir les voisins d'un véhicule révoqué pendant qu'ils reçoivent la LRCC.

Le protocole DRP

Ce protocole est utilisé dans le mode ad-hoc pur où les véhicules accumulent des accusations contre les comportements d'un véhicule. L'évaluation du comportement se fait par un système de réputation, et, au cas où un mauvais comportement serait détecté, les véhicules le signalent à l'AC dès qu'une connexion sera disponible. À la différence de RTPD et de RCCRL, la révocation dans le protocole DRP est déclenchée par les voisins d'un véhicule après la détection d'un mauvais comportement.

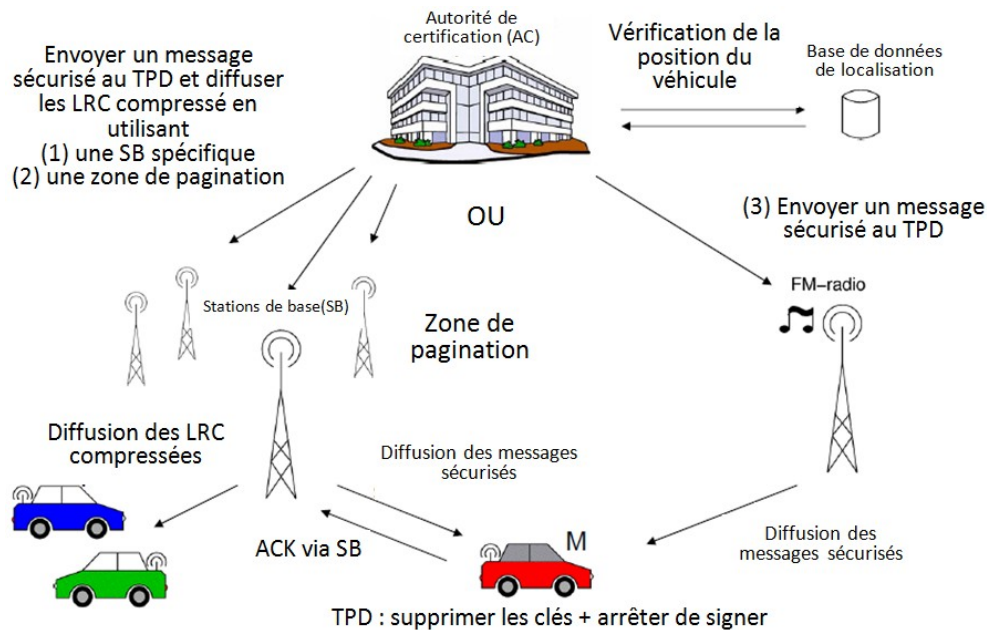


FIGURE 3.4 – Déroulement du protocole RTPD (révocation de certificat)

5. La confidentialité

Pour assurer l'exigence de la confidentialité, la solution proposée est d'utiliser un jeu de clés anonymes qui changent fréquemment (toutes les deux minutes) en fonction de la vitesse de conduite. Chaque clé expire après son utilisation, une seule clé peut être utilisée à la fois. Ces clés sont pré-chargées dans le TPD du véhicule pour une longue durée, par exemple, pour toute une année, le TPD se charge de toutes les opérations liées à la gestion et l'utilisation des clés. Chaque clé est certifiée par l'AC émettrice et a une durée de vie relativement courte (par exemple, une semaine particulière de l'année). En plus, elle peut pister l'identité réelle du véhicule.

3.2.3 Architecture de Gerlach et *al*

Dans le cadre du projet NoW [21], une architecture de sécurité a été proposée par M. Gerlach et *al* [6].

Cette architecture est décrite en utilisant divers points de vue (méthode utilisé en génie logiciel [7]).

les quatre vue spécifiées pour cette architecture sont :

- la vue des couches fonctionnelles,
- la vue organisationnelle / les composants,
- la vue du modèle de référence, et
- la vue centrée sur l'information.

1. La vue des couches fonctionnelles

Les couches fonctionnelles représentées dans la figure 3.5 décrivent une décomposition du système de sécurité dans des groupes en fonction des cas d'utilisation d'une fonctionnalité spécifique. Tandis que la plus basse couche est concernée par le véhicule et l'enregistrement et l'identification d'application, les couches plus hautes sont concernées par l'exploitation adéquate du système, les mesures de sécurité appropriées et la confidentialité des utilisateurs.

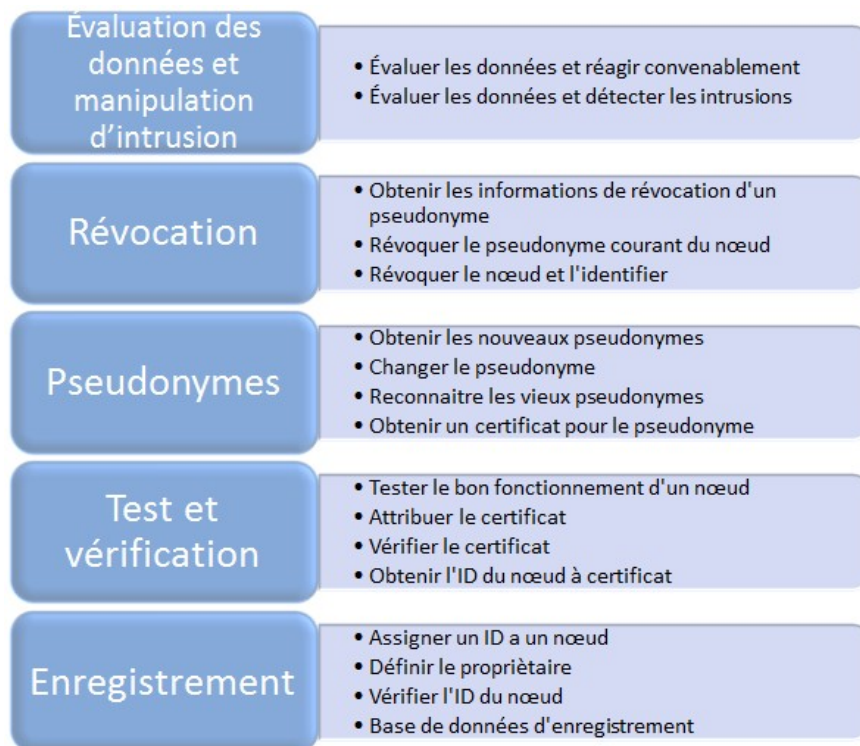


FIGURE 3.5 – Les couches fonctionnelles

Cette décomposition décrit une vue complète d'une solution de sécurité sous des conditions plutôt générales. Par conséquent, une solution concrète de sécurité pourrait ne pas avoir besoin de tous les composants ou même de toutes les couches.

La couche Enregistrement : elle est concernée par l'enregistrement des nœuds, c'est à dire, les OBUs et les RSUs (On Board Unit, Road Side Unit). Cette couche contient la base de données d'enregistrement qui peut contenir n'importe quelle information concernant le véhicule, comme son numéro d'identification, sa couleur, sa marque, ...etc.

La couche Test et vérification : elle est responsable d'évaluer le bon fonctionnement d'un nœud. Ce processus s'assure que seuls les nœuds avec les propriétés vérifiées peuvent participer à la communication. Les certificats délivrés par l'autorité garantissent le bon fonctionnement du nœud. Le processus test et vérification est une mesure de protection contre l'insertion non autorisée des données dans le réseau.

C'est un moyen de contrôler la réalisation des exigences par rapport à la performance, le comportement et la fiabilité d'un système.

La couche Pseudonymes : elle fournit un niveau de base d'anonymat en introduisant la possibilité d'utiliser des pseudonymes qui changent régulièrement et qui ne peuvent pas être pistés par les parties non autorisées. Les pseudonymes jouent le même rôle que le certificat assigné pour le nœud. Ils sont utilisés pour le système de communication et sont similaires à une adresse MAC/IP certifiée qui est liée à une clef de chiffrement. Les pseudonymes changeants fournissent une confidentialité aux utilisateurs tout en permettant de retirer cette confidentialité si c'est exigé par certaines applications.

La couche Révocation : elle concerne l'exclusion des nœuds du système. Elle contient une base de données des pseudonymes révoqués et distribue ces données à tous les nœuds du système (si nécessaire) selon l'ampleur de la décision de révocation, l'ampleur peut s'étendre du nœud en question, à l'ensemble du système. Une des réactions aux attaques détectées effectuées par un nœud est de l'exclure du système.

La couche évaluation des données et manipulation d'intrusions : elle est responsable d'évaluer et vérifier les données, ainsi que détecter et manipuler les intrusions. Parfois les intrusions et les nœuds défectueux ne peuvent pas être repérés. La décision d'ignorer des données ou de lancer le processus de révocation est prise par cette couche. Si la révocation des nœuds est une issue, une autorité et des mécanismes appropriés doivent exister pour décider si un nœud doit être exclu ou pas. Dans les grands réseaux, où la détection et la réaction automatiques sont nécessaires, cette couche est particulièrement importante,

2. La vue organisationnelle / les composants

Cette vue décrit les acteurs et les constituant qui compose l'architecture de sécurité. La figure 3.6 décrit les différents composants (systèmes, humains, organismes et autorités) :

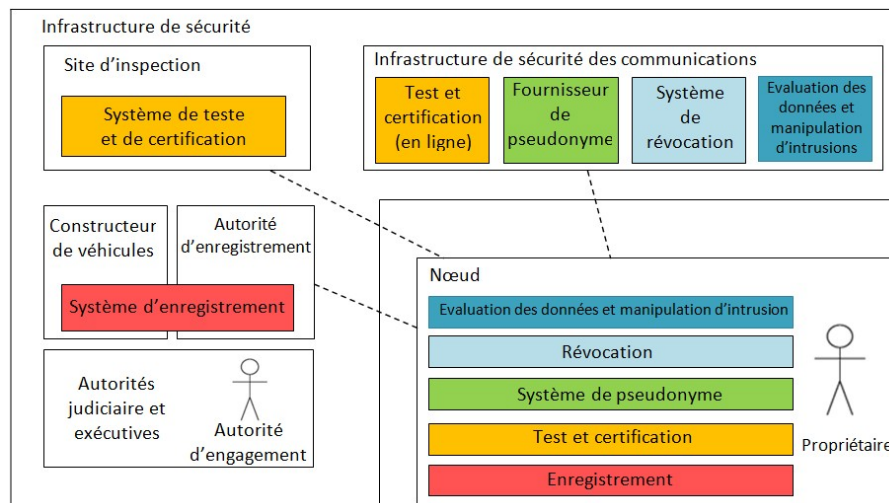


FIGURE 3.6 – L’organisation et les composants de l’architecture

On distingue que cette vue se compose de deux parties, l’infrastructure de sécurité, et le nœud.

1. L’infrastructure de sécurité :

Elle comprend les composants suivants :

- Le constructeur de véhicules et l’autorité d’enregistrement pour enregistrer les nœuds.
- Le site d’inspection pour tester et certifier les nœuds.
- L’autorité judiciaire et exécutive qui inclut l’autorité d’engagement qui s’occupe de l’identification et de la révocation des nœuds.
- L’infrastructure de sécurité des communications qui comprend les systèmes de communications, les processus et les bases de données nécessaires pour effectuer les essais en ligne, provision de pseudonymes pour les nœuds. La révocation des nœuds, et l’infrastructure qui s’occupe de l’évaluation de données et la manipulation d’intrusions.

Le constructeur de véhicules et l’autorité d’enregistrement ensemble couvrent deux tâches majeures, D’abord, l’attribution d’un identifiant unique au véhicule, puis, l’enregistrement du propriétaire du véhicule et de son véhicule auprès de l’autorité appropriée. Pour les RSUs, le propriétaire serait l’autorité ou la compagnie qui l’exploite.

Le site d’inspection peut être vu comme un espace réservé pour une organisation où l’OBU ou le RSU peut être testé, après avoir terminé le test avec succès, un certificat est délivré pour le nœud. Ce certifi-

cat à son tour peut être utilisé pour obtenir des pseudonymes valides nécessaire pour le fonctionnement du réseau en utilisant l'infrastructure de sécurité des communications.

L'entité d'engagement représente les tribunaux, les policiers, et le personnel technique qui, ensemble, décident si un nœud sera révoqué ou pas dans certaines circonstances. Son implication dépend du niveau de la révocation, de retirer temporairement un pseudonyme à l'identification du propriétaire du véhicule.

2. Le nœud :

Le nœud contient des modules équivalents de chaque fonctionnalité du système de sécurité. Dans certains cas, la fonctionnalité entière d'une couche peut être exécutée par le nœud, il peut être enregistrée, certifié, révoqué et peut obtenir de nouveaux pseudonymes. Un nœud est lié à son propriétaire qui est responsable de l'entretien régulier du véhicule et du système de communication.

Les lignes pointillées entre le nœud et l'infrastructure de sécurité indiquent que les composants communiquent entre eux. Pour l'enregistrement, le propriétaire du véhicule communiquerait avec l'autorité directement. Pour l'essai et le processus de certification, un raccordement filaire ou sans fil peut être assumé, par exemple pour tester un protocole de réseau.

L'interaction avec l'infrastructure de sécurité des communications dépend de quel module est impliqué. Il est important de noter que l'accès sporadique à l'infrastructure doit être assumé.

Certains modules, tels que le fournisseur de pseudonyme, le test en ligne et la certification peuvent avoir besoin d'une connectivité fiable et à la demande, qui pourrait être fournie par des technologies cellulaires. Comme discuté dans [9], la distribution de l'information de révocation peut également être réalisée par une simple diffusion terrestre.

3. Implémentation

Cette architecture utilise quatre concepts de sécurité :

- les signatures numériques et les certificats,
- le contrôle de plausibilité inter-couche et inter-application,
- évaluation de la confiance des données, et
- la pseudonymité et le mélange de contexte.

Pour implémenter ces différents concepts, deux approches de conception ont été établies. Pour les deux approches, le système de communication fournit l'anonymat et la sécurité pour envoyer, faire suivre, et recevoir des données, contrôlé par une application de sécurité de base (ASB). La différence principale entre les deux approches se situe dans la manière de l'évaluation de la confiance des données et dans l'implémentation du filtrage.

Dans la première approche, les différentes applications exécutent des fonctions de sécurité de façon autonome (cf. figure 3.7). La deuxième approche soulage les applications d'exécuter les fonctions de sécurité autant que possible, elle intègre ces fonctions dans l'ASB comme un service que les applications peuvent utiliser. La première approche réduit la dépendance entre les applications, et par conséquent, diminue la complexité de l'exécution. Mais d'autre part l'évaluation de la confiance entre les applications serait à peine réalisable puisqu'elle exige un échange structuré des valeurs de la confiance entre les différentes applications dans le nœud.

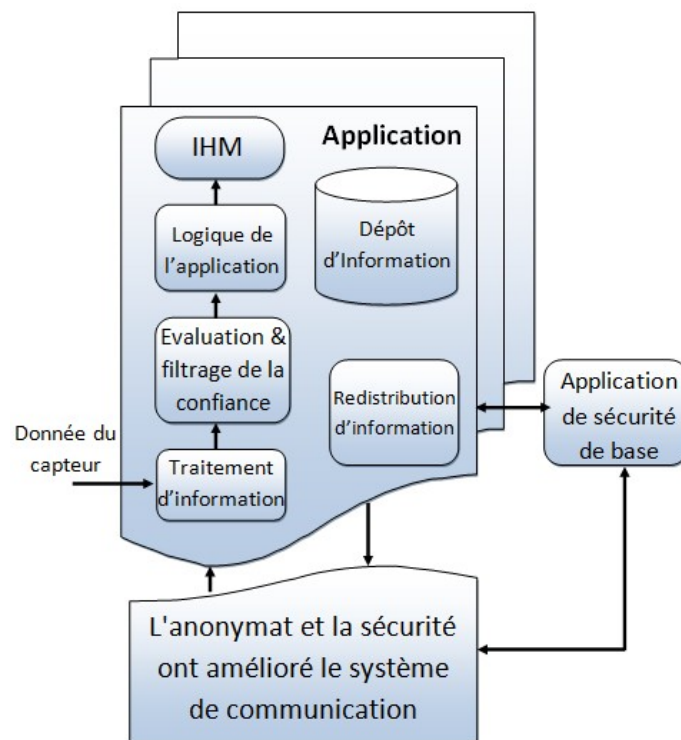


FIGURE 3.7 – Les composants locaux de l'application

L'évaluation de la confiance inter-application peut être accomplie par la deuxième approche, mais exige la connaissance des applications locales de l'ASB, elle exige aussi un échange d'information efficace entre le système de communication, l'application de sécurité de base, et les applications. Car l'évaluation de la confiance peut se baser sur des algorithmes qui sont indépendants de la logique spécifique de l'application, la deuxième approche semble être bénéfique.

Dans l'approche d'exécution proposée, les deux approches coexistent, et c'est au concepteur de décider laquelle choisir.

La conception d'un modèle de référence qui ajoute des mécanismes de sécurité aux couches supérieures, telle que l'application de sécurité de base et le filtre de confiance (cf. figure 3.8).

le modèle de référence, est mis en valeur par les composants indiqués dans la figure 3.8, notamment une application de sécurité de base, le filtre de confiance, et le composant de sécurité de la couche réseau, sont expliqués ci-dessous.

Afin de réaliser les procédures assurant l'interaction inter-couche et inter-application, trois concepts d'exécution ont été utilisés, à savoir le connecteur d'information, le marquage de confiance, et le modules de filtrage de confiance.

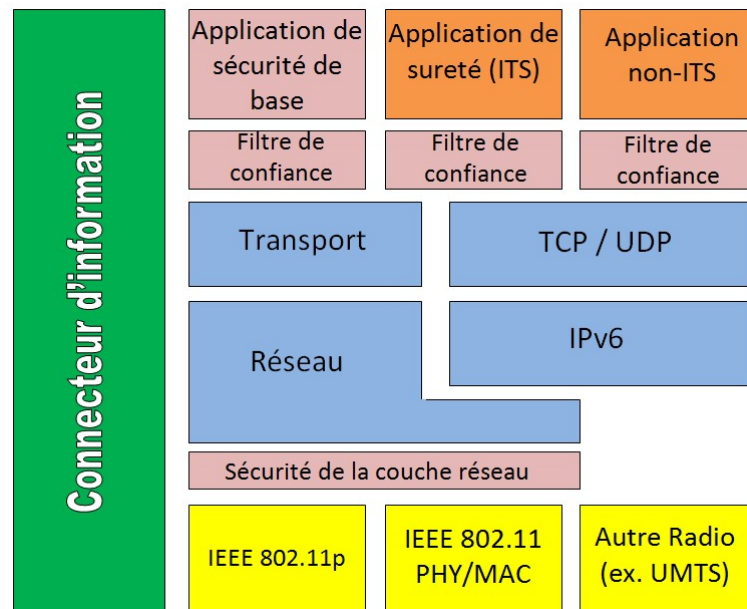


FIGURE 3.8 – La vue du modèle de référence

- A. L'application de sécurité de base** est responsable de la protection d'intimité, le changement de pseudonyme, l'obtention de nouveaux pseudonymes, et le marquage de confiance inter-couche.
- B. L'évaluation du filtrage de confiance** peut être faite pour une seule application, ou (si l'information est utile pour plusieurs applications) utilisée comme module dans l'application de sécurité de base. Le système de sécurité (c'est à dire, la sécurité de la couche réseau et les modules dans l'application de sécurité de base) attache des valeurs de confiance aux éléments de l'information qui sont échangés entre les différents composants dans le système. Le filtre de confiance évalue la confiance de l'information dérivée par le système et permet d'adapter dynamiquement le seuil de confiance. Cela permet de satisfaire les différentes exigences de sécurité pour des applications et représente l'interface entre le système de sécurité et l'application.
- C. L'adressage multi-couche pour la Pseudonymité**, Afin d'assurer d'anonymat dans les communications véhiculaires, un nœud choisit aléatoirement un pseudonyme qui change régulièrement. Déclenchée par l'ASB, les adresses du système de communication, y compris l'adresse IPv6, ainsi que le certificat correspondant sont modifiées. Le certificat est une partie intégrale d'un pseudonyme qui représente des autorisations du système de communication et (si nécessaire) les domaines l'application.

3.2.4 Autres contributions

Plusieurs améliorations ont été proposées dans la littérature visant des objectifs différents.

Dans [24] les auteurs ont introduit une métrique pour la confidentialité appelée entropie d'anonymisation. ils ont aussi utilisé la cryptographie à clé publique ainsi que des mécanismes de vérification de la localisation.

Dans [25] une architecture de sécurité a été proposée qui contient une PKI, un système de détection d'intrusion et une infrastructure de routage sécurisée.

Dans [26], une proposition d'une architecture de sécurité s'appuyant sur une PKI et le protocole EAP-Kerberos. Cette architecture dont l'objectif principal est de sécuriser les services non-ITS dans un réseau véhiculaire.

Dans [27], les auteurs ont proposé une infrastructure de routage géographique sécurisée s'appuyant sur une combinaison des schémas de signature saut-par-saut et de bout-en-bout pour assurer l'authentification, l'intégrité et la

non-répudiation. Des mécanismes de corrélation visant à réduire l'impact de l'injection de fausses données dans le protocole de routage sont également proposés.

3.3 Discussion & comparaison

La première architecture repose sur une architecture réseau qui est dispensée de toute fonction de routage et qui ne s'appuie que sur des communications en Broadcast à sens unique. La sécurité des communications est assurée par des signatures dont les clés sont fournies par une PKI. De plus, les contraintes temps réels des services ITS sont prises en compte dans les mécanismes de sécurité mis en œuvre.

Cette proposition souffre de nombreuses faiblesses dont son modèle de communication restrictif (le sens des communications), l'absence de prise en compte des problématiques d'intimité et la sécurité des services non-ITS. Toutes ces faiblesses ne permettent pas d'envisager la solution proposée dans une perspective de déploiement.

La deuxième architecture est une architecture de sécurité pour les services ITS. Une PKI, des clés publiques anonymes et des protocoles de révocation des certificats sont spécifiés. Cette contribution souffre toutefois de ne pas prendre en compte toute la diversité des exigences de sécurité des réseaux véhiculaires dont notamment celles relatives aux services non-ITS.

Dans la troisième architecture, les couches fonctionnelles et la structure organisationnelle, décrivent à quoi le système de sécurité global devrait ressembler. Dans la vue des couches fonctionnelle, il est montré comment empiler les divers mécanismes et les algorithmes de sécurité existants, il est aussi montré comment les fonctions peuvent être réparties sur différentes autorités et entités dans la vue organisationnelle. Cette dernière, c'est à dire, les composants, et la vue du modèle de référence, décrivent comment le système peut être mis en application réellement. Tous ces composants représentent un coût considérable d'implémentation et de mise en œuvre.

Ces travaux ont contribué à la sécurité des réseaux véhiculaires, en particulier des services ITS. Cependant, ils ne donnent pas de perspective globale intégrant à la fois la sécurité des services ITS et celle des services non-ITS.

Pour faire une comparaison entre les trois architectures présentées précédemment,

nous avons défini quelques critères de comparaison, à savoir :

- L'adaptation des architectures au changement de la topologie du réseau, c'est à dire, si l'architecture fait face à la forte mobilité des véhicules.
- L'adaptation au grand nombre de véhicules, c'est à dire, la gestion d'un grand nombre de véhicules.
- le taux de scalabilité, c'est à dire, si l'architecture peut s'étendre à un réseau à grande échelle.

le tableau suivant résume les architectures par rapport à ces critères :

	adaptation au changement de topologie	adaptation au grand nombre de véhicules	Scalabilité
Arch de El zerki et al	bonne	mauvaise	moyenne
Arch de Raya et al	bonne	bonne	bonne
Arch de Gerlach et al	bonne	bonne	bonne

TABLE 3.1 – Premier tableau de comparaison

Nous avons aussi essayé de comparer les architectures par rapport aux exigences de sécurité vues précédemment, à travers le tableau suivant :

	Authenticité	Intégrité	Non-répudiation	Révocation	Temps réel	Confidentialité
Arch de El zerki et al	+	+	-	-	+	-
Arch de Raya et al	+	+	+	+	+	+
Arch de Gerlach et al	+	+	+	+	+	+

TABLE 3.2 – Deuxième tableau de comparaison

3.4 Conclusion

Dans ce chapitre nous avons présenté quelques architectures qui ont été proposées pour sécuriser les communications véhiculaires, malheureusement ces contributions n'ont pas une vision architecturale globale intégrant à la fois la sécurité des services ITS et celle des services non-ITS.

Nous avons aussi fait une comparaison entre les trois architectures présentées, en se basant sur des critères issues de différents aspects architectural, et des différentes exigences de sécurité.

Dans le chapitre qui suit nous verrons trois scénarios d'attaque, les solutions proposées pour les contrer et l'architecture de sécurité appropriée.

Chapitre 4

Analyse et scénarios d'attaques

4.1 Introduction

Dans ce chapitre, nous analysons les trois algorithmes de révocation de certificats proposés dans l'architecture de RAYA et al, en présentant quelque inconvénients. Ensuite nous présentons trois scénarios d'attaques qui peuvent avoir lieu dans les réseaux véhiculaires, en désignant l'architecture la plus adaptée pour contrer ces attaques.

4.2 Les limites de la révocation des certificats

Les algorithmes suivants décrivent les trois protocoles de révocation de certificats proposés dans l'architecture de Raya :

Le protocole RTPD

AC : autorité de certification

M : Véhicule

MSG : Message de révocation

LRCC : Liste de Révocation de Certificats Compressé

DEBUT

L'AC décide de révoquer le certificat du véhicule M

Si l'AC connaît la position de M alors

AC chiffre MSG avec la clé publique de M;

AC envoie MSG à M;

M déchiffre MSG;

M arrête d'envoyer des messages;

M envoie ack à AC;

Sinon

Si la BD contient une position récente de M alors

AC crée une zone de pagination;

AC envoie MSG en multicast à toute les stations de base dans cette zone;

Sinon

AC envoie MSG en broadcast;

Finsi

Finsi

Si AC ne reçoit pas de ack alors

AC envoie MSG en broadcast;

Finsi

FIN

Le protocole RCCRL

DEBUT

L'AC décide de révoquer un ensemble de clés du véhicule M ;

AC génère la LRCC ;

AC signe la LRCC avec sa clé privée ;

AC envoie la LRCC en broadcast ;

FIN

Le protocole DRP

DEBUT

Les véhicules accumulent des accusations contre un véhicule M ;
Les véhicules signalent M à l'AC ;
Si le nombre d'accusation dépasse un seuil prédéfini alors
L'AC exécute le protocole de révocation ;

Finsi

FIN

Analyse

A première vue, il paraît que cette solution résout le problème de la révocation, mais elle exhibe quelques inconvénients :

Afin de signaler un mauvais comportement, la plupart des véhicules doivent être équipés de matériel spécial pour la détection de ce genre de comportement.

4.3 Scénarios d'attaques

4.3.1 Premier scénario : l'attaque sybil

Dans l'attaque sybil [28], l'attaquant envoie plusieurs messages à d'autres véhicules en utilisant à chaque fois une identité fabriquée différente, visant à créer un environnement virtuel qui répond le mieux à ses fins. La figure 4.1 illustre un exemple de l'attaque Sybil dans laquelle l'attaquant crée plusieurs véhicules sur la route avec la même identité. dont l'objectif est de dégager la route.

Cette attaque est interne, c'est à dire qu'au moment où l'attaquant envoie des messages, il apparaît comme étant un nœud légitime, elle est intentionnelle et active, c'est à dire que l'attaquant distribue délibérément des messages forgés, et elle est indépendante, parce que l'attaquant agit tout seul.

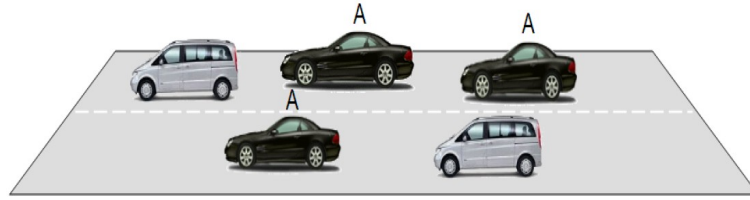


FIGURE 4.1 – L’attaque sybil

La solution la plus adaptée pour éviter cette attaque est d’utiliser les signatures numériques et les certificats délivrés par une autorités de certification. Dans ce schéma de sécurité, chaque véhicule ne doit utiliser qu’une seule signature et un seul certificat à la fois, alors, deux véhicules ayant des certificats différents signés avec des clés différentes ne peuvent pas avoir la même identité ou utiliser des identité falsifiées.

L’architecture de El zerki et al utilise seulement le mécanisme de signature numérique, mais ne fait pas appel aux autorités de certification. Il est claire que l’utilisation de la fonction de signature numérique ne suffit pas pour identifier un véhicule qui utilise des identités multiples puisqu’il signe les messages avec des clés valides, par contre l’architecture de Raya et al, et celle de Gerlash et al, peuvent toutes les deux éviter cette attaque puisque’elles supposent la présence d’une AC et assurent la fonction de signature numérique.

4.3.2 Deuxième scénario : le déni de service distribué (DDOS)

Les attaques DDOS ont un impact sévère sur n’importe quel réseau et spécialement sur les réseaux véhiculaires à cause de la difficulté de l’identification des sources d’attaquants. Les attaque peuvent se lancer à partir de divers endroits, et à des moments différents. Le type des messages et le moment d’émission peuvent varier d’un attaquant à un autre. L’objectif principal d’une telle attaque est de compromettre la disponibilité du réseau.

La figure 4.2 illustre le cas d’un DDOS dans un réseau véhiculaire purement ad-hoc. Les véhicules B, C, D gérés par des entités malveillantes lancent simultanément un DDOS contre le véhicule A pour par exemple, l’empêcher de faire de communications.

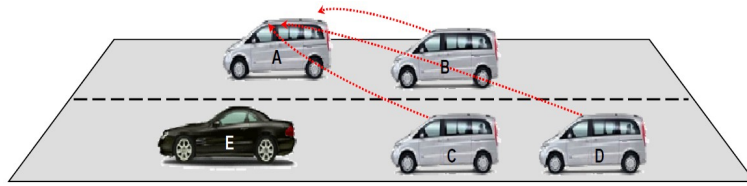


FIGURE 4.2 – DDOS véhicule à véhicule

La figure 4.3 représente l'attaque DDOS contre une infrastructure où plusieurs attaquants lancent des requêtes en coordination vers l'infrastructure de différents endroits. une fois la bande passante occupée et l'infrastructure inondée par des requêtes, aucun véhicule ne peut communiquer avec elle. L'attaque DDOS est interne, intentionnelle, active et coordonnée.

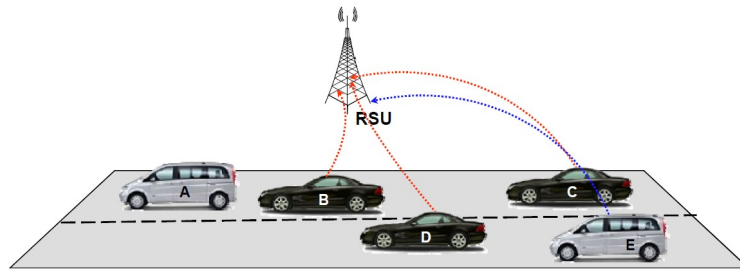


FIGURE 4.3 – DDOS véhicule à infrastructure

Il est difficile pour n'importe quel système de sécurité de contrer cette attaque, même en utilisant les mécanismes de révocations de certificats. mais l'intégration d'un système de détection d'intrusions peut contribuer à résoudre ce problème, en apprenant au fil du temps le comportement des attaquants. pour cela l'architecture de Gerlach et al est considérée comme étant la plus adaptée pour contrer cette attaque.

4.3.3 Troisième scénario : l'attaque du rejeu (replay attack)

Cette attaque utilise les données précédemment produites dans de nouvelles connexions. Un attaquant peut capturer des données en transit et les utiliser ultérieurement dans d'autres parties du réseau (cf. figure 4.4). L'attaque du rejeu est habituellement déclenchée par des utilisateurs malveillants ou non autorisés pour se faire passer par un utilisateur (ou une infrastructure) légitime.

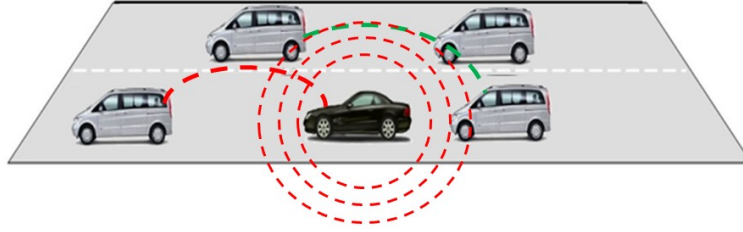


FIGURE 4.4 – Attaque du rejeu

L'attaque du rejeu peut être externe, intentionnelle, active et indépendante.

Afin d'empêcher cette attaque, une solution a été proposée dans [29] qui utilise la synchronisation globale du temps basée sur les informations GPS pour tous les nœuds.

Cette solution peut être réalisée par l'architecture de El zerki et al, puisqu'elle suppose que les véhicules sont équipés par un récepteur GPS, en plus elle assure la fonction de l'estampillage du temps.

4.4 Conclusion

Dans ce chapitre nous avons présenté les limites du mécanisme de révocation, surtout la révocation distribuée. Nous avons aussi présenté trois scénarios d'attaques qui peuvent être déclenchées dans les réseaux véhiculaires, tout en désignant l'architecture adaptée pour contrer ces attaques.

Conclusion générale

Les réseaux véhiculaires constituent un nouveau type de réseaux issu des réseaux sans file. Leur particularité provient des communications éphémères qui peuvent s'instaurer entre les véhicules, ou bien, entre les véhicules et une infrastructure, ainsi que la forte mobilité qui représente une caractéristique largement plus contrainte que dans les réseaux ad-hoc traditionnels.

Les réseaux véhiculaires sont vulnérables aux attaques qui représentent un réel danger qui menacent la vie des utilisateurs et leurs biens, ce qui nécessite le déploiement de mécanismes de sécurité pour ces réseaux dans certains cas. Les techniques cryptographiques peuvent assurer les objectifs de l'authentification, l'intégrité et la confidentialité dans une certaine mesure, mais la disponibilité est difficile à assurer car l'aspect décentralisé des réseaux VANET donne la possibilité d'avoir plusieurs attaques.

Il y a eu quelques contributions concernant la sécurisation des réseaux véhiculaires, particulièrement celles qui concernent les services liés à la sécurité routière (ITS).

Dans ce mémoire, nous avons présenté quelques architectures de sécurité qui ont été proposées, en faisant une comparaison entre elles. L'étude détaillée de ces architectures, nous a permis d'imaginer quelques scénarios d'attaques qui peuvent se manifester contre ces architectures, en désignant à chaque fois l'architecture adaptée pour contrer ces attaques.

Comme perspective à notre travail, nous proposons de faire l'analyse des autres architectures de sécurité, définir d'autres critères de comparaisons, et éventuellement proposer notre propre architecture de sécurité.

Bibliographie

- [1] J.Oishi, K.Asakura and T.Watanabe, "A Communication Model for Inter-vehicle Communication Simulation Systems Based on Properties of Urban Areas", IJCSNS (International Journal of Computer Science and Network Security), VOL.6 No.10, October 2006
- [2] M.Raya and J.Hubaux, "The Security of Vehicular Ad-hoc Networks", in Proceedings of ACM Workshop on Security of Ad-hoc and Sensor Networks (ACM SASN), 2005
- [3] X. Yang, J. Liu, F. Zhao and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning" in Proceedings of the International Conference on Mobile and Ubiquitous Systems (MobiQuitous), 2004
- [4] M.Raya, P.Papadimitratos and J.Hubaux, EPFL, "Securing Vehicular Communications" in Proceedings of the IEEE Wireless Communications , October 2006
- [5] [http ://fr.wikipedia.org/wiki/Infrastructure-à-clés-publiques](http://fr.wikipedia.org/wiki/Infrastructure-à-clés-publiques). consulté le : 07/06/2011.
- [6] M.Gerlach, A.Festag, T.Leinmüller, G.Goldacker and C.Harsch, "Security architecture for vehicular communication", in Proceedings of the 5th International Workshop on Intelligent Transportation (WIT), Hamburg, Germany, March 2007.
- [7] IEEE, "IEEE standard 1471-2000 : IEEE recommended practice for architectural description of software-intensive systems" 2000.
- [8] M.El Zarki, S.Mehrotra, G.Tsudik and N.Venkatasubramanian, "Security Issues in a Future Vehicular Network", in Proceedings of the European Wireless Conference, Florence, Italy, February 2002.
- [9] M.Raya, D.Jungels, P.Papadimitratos, I.Aad, and J.Hubaux, "Certificate Revocation in Vehicular Networks," Laboratory for Computer Communications and Applications (LCA), EPFL, Tech. Rep. LCAREPORT-2006.

- [10] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages" 2006.
- [11] C.Tchepnda, "Authentification dans les Réseaux Véhiculaires Opérés", thèse de doctorat, Ecole doctorale d'informatique, telecommunication et electronique de Paris, Décembre 2008.
- [12] J.Guo, "Security and Privacy in Vehicular Networks", National Workshop on High-Confidence Automotive Cyber-Physical Systems, 2007
- [13] M.JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections" Université d'evry val d'essonne, thèse de doctorat, 2008.
- [14] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation for VANETs," in Proceedings of the 40th Annual Simulation Symposium, Norfolk, VA , 2007, pp. 301-309.
- [15] Prevent, [http ://www.prevent-ip.org/](http://www.prevent-ip.org/)
- [16] SafeSpot (Cooperative vehicles and road infrastructure for road safety), [http ://www.safespot-eu.org/](http://www.safespot-eu.org/)
- [17] Watch-Over, [http ://www.watchover-eu.org/](http://www.watchover-eu.org/)
- [18] CVIS (Cooperative Vehicle-Infrastructure Systems), [http ://www.cvisproject.org/](http://www.cvisproject.org/)
- [19] GST (Global Systems for Telematics), [http ://www.gstforum.org/](http://www.gstforum.org/)
- [20] DRiVE (Dynamic Radio for IP Services in Vehicular Environments), [http ://www.istdrive.org/index2.html/](http://www.istdrive.org/index2.html/)
- [21] NoW (Network-on-Wheels), [http ://www.network-on-wheels.de](http://www.network-on-wheels.de)
- [22] FleetNet project- Internet on the road, [http ://www.et2.tuharburg.de/fleetnet](http://www.et2.tuharburg.de/fleetnet)
- [23] SeVeCom (Secure Vehicular Communication), [http ://www.sevecom.org/](http://www.sevecom.org/)
- [24] J.Hubeaux, Srdjan, Capkun and J.Luo, "The Security and Privacy of Smart Vehicles", IEEE Computer Society, 2004
- [25] J.Blum, A.Eskandarian, "The Threat of Intelligent Collisions", IEEE Computer Society, 2004
- [26] H.Moustafa, G.Bourdon and Y.Gourhant, "Providing authentication and access control in vehicular network environment", IFIP/SEC, May 2006
- [27] C.Harsch, A.Festag and P.Papadimitratos, "Secure Position-Based Routing for VANETs", IEEE VTC-Fall, 2008

- [28] J.Douceur, "The sybil Attack", in Proceedings of the First international workshop on peer to peer(P2P) system, march 2002, pp :251-260.
- [29] R.Panayappan, J.Trivedi, A.Studer, and A.Perrig, "VANET-based approach for parking space availability," in Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007), Montreal, Quebec, Canada, pp. 75-76, Sept. 2007.