Authentification dans les réseaux véhiculaires opérés

Christian Tchepnda

▶ **To cite this version:**

Christian Tchepnda. Authentification dans les réseaux véhiculaires opérés. domain_other. Télécom ParisTech, 2008. English. NNT : . pastel-00004554

HAL Id: pastel-00004554
https://pastel.hal.science/pastel-00004554

Submitted on 7 Jul 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

TELECOM ParisTech

École Doctorale d'Informatique, Télécommunications et Électronique de Paris

Thèse

Présentée pour Obtenir le Grade de Docteur
de l'Ecole Nationale Supérieure des Télécommunications

Spécialité: Informatique et Réseaux

Christian TCHEPNDA

Authentification dans les Réseaux Véhiculaires Opérés

Soutenue le 18 Décembre 2008 Devant le Jury Composé de:

Xavier Lagrange	Président
André-Luc Beylot	Rapporteur
Hossam Afifi	Rapporteur
Pascal Urien	Examinateur
Thierry Ernst	Examinateur
Gilles Bourdon	Examinateur
Mohamed Shawky	Invité
Houda Labiod	Directeur de Thèse
Hassnaa Moustafa	Co-encadrant de Thèse

Affiliations des Membres du Jury

Xavier Lagrange	Télécom Bretagne
André-Luc Beylot	ENSEEIHT Toulouse
Hossam Afifi	Telecom&Management Sud Paris
Pascal Urien	Télécom ParisTech
Thierry Ernst	INRIA Rocquencourt
Gilles Bourdon	France Télécom
Mohamed Shawky	Universite de Technologie de Compiègne
Houda Labiod	Télécom ParisTech
Hassnaa Moustafa	France Télécom R&D

Résumé

Nous nous proposons dans cette thèse de répondre à l'enjeu de l'authentification avec l'opérateur réseau dans le contexte particulier des réseaux véhiculaires; contexte marqué par une forte dynamique des nœuds, une connectivité intermittente et une diversité des modèles et des enjeux de sécurité suivant la typologie des services. Nous nous intéressons en particulier aux réseaux véhiculaires s'appuyant sur une technologie de type WLAN "Wireless Local Area Network" (*i.e.* portée de transmission maximale de l'ordre de 1000 m) dont les coûts de déploiement sont réputés moindres. Notre réponse à l'enjeu posé dans ce contexte s'articule autour de 4 contributions.

Dans la première et plus importante contribution, nous proposons et analysons des architectures et des protocoles pour l'authentification dans les réseaux véhiculaires. Ces architectures et protocoles implémentent divers mécanismes susceptibles d'assurer au-delà de l'authentification mutuelle et de la délivrance des lettres de créance, la sécurité des données d'authentification, l'intimité numérique des utilisateurs, l'interdiction d'accès aux protocoles et services de la couche 3 (*i.e.* couche réseau) avant l'achèvement du processus d'authentification, la disponibilité de l'authentification et le respect des contraintes temps réel. La traduction concrète de ces implémentations est faite au travers d'une part, d'une extension de l'authentification TLS appelée AUCRED, qui assure sur la base des certificats à clé publique ECC, l'authentification mutuelle entre le serveur d'authentification et les véhicules, mais aussi la délivrance des certificats volatiles anonymes à ces derniers, et d'autre part, du protocole EGEMO qui assure au niveau de la couche 2, l'acheminement géographique multi-sauts du protocole EAP, lui-même transporteur du protocole AUCRED.

A l'aune de l'analyse des protocoles précédents, nous introduisons à travers une deuxième contribution, une approche d'optimisation du transport de l'authentification visant à réduire le nombre de paquets générés dans le réseau lors du processus d'authentification, en particulier dans les scénarios de forte densité de véhicules.

Compte tenu du rôle particulier de l'authentification, considérée comme un service précédant et conditionnant l'accès aux ressources et aux autres services du réseau opéré, et en réponse à la mise en concurrence de ce service avec d'autres services des réseaux DSRC ("Dedicated Short Range Communications", ensemble de standards dédiés aux communications véhiculaires), nous proposons au travers d'une troisième contribution, une méthode de priorisation du service d'authentification utilisant la diversité des canaux radio DSRC.

Afin de maintenir des niveaux élevés de performance de l'authentification dans les scénarios de forte densité de véhicules, et ce, sans accroître la complexité matérielle des nœuds du réseau (*e.g.* une seule interface radio par nœud), nous proposons au travers d'une quatrième contribution, une approche de distribution ou de délégation de la fonction d'authentification.

Mots-clés: Authentification, Sécurité, Réseaux véhiculaires opérés, Réseaux Ad-hoc hybrides, WLAN, DSRC

Abstract

In this thesis, we address the challenge of users' authentication in vehicular networks managed by the network operator. The difficulty of our task lies in coping with the special characteristics of vehicular networks which are mainly high mobility, connectivity instability and diversity of security models and challenges following the services types. We employ a WLAN radio technology (*i.e.* the maximal transmission range is around 1000 m) which is known to be easier and less costly to deploy. The proposed work in this thesis comprises 4 main contributions.

In the first and most important contribution, we propose and analyze a set of architectures and protocols for authentication in vehicular networks. Our architectures and protocols implement a number of mechanisms achieving authentication and credential delivery to vehicles while garanteeing security of the authentication messages, privacy of drivers, access restriction to layer 3 (*i.e.* network layer) services and protocols before the successful completion of the authentication, availability of authentication and consideration of real time constraints. Our authentication framework mainly comprises 2 protocols: (i) the AUCRED protocol which is defined as an extension of the TLS authentication for the mutual authentication and volatile anonymous ECC based certificates delivery and (ii) the EGEMO protocol for the layer-2 geographic multi-hop transport of EAP protocol encapsulating the AUCRED protocol.

Based on the analysis of these protocols, we introduce as a second contribution, an optimization approach for the authentication transport process aiming to reduce the number of packets generated in the network during the authentication process, especially in high vehicles density scenarios.

Due to the special role of the authentication service which preceeds and conditions the access to the network resources and services and because of the forseeable competition between the authentication service and other services in DSRC ("Dedicated Short Range Communications", set of standards including IEEE 802.11p and dedicated to vehicular communications) networks, we introduce through a third contribution, a priotitization approach of the authentication service using DSRC channels diversity.

In order to maintain a high level of performance of the authentication service in high vehicles density scenarios without incurring any material complexity on network nodes (*e.g.* using only one network interface per node), we propose through the fourth contribution, a distribution or delegation scheme of the authentication function that is supposed to be centralized at the authentication server.

Key words: Authentication, Security, Managed vehicular networks, Hybrid ad-hoc networks, WLAN, DSRC

Table des Matières

Figures

Chapitre 2.2.

Chapitre 2.3.

Chapitre 2.4.

Chapitre 2.5.

Tableaux

Abréviations et Acronymes

AAA	Authentication Authorization Accounting
AI	Application ID
AP	Access Point
AR	Access Router
AS	Authentication Server || AAA Server
ARS	Ad hoc Relaying Stations
AUCRED	AUthentication and CREdential Delivery protocol
BAS	Business As uSual
BS	Base Station
CA	Certification Authority
CBC-MAC	Cipher Block Chaining – Message Authentication Code
CCMP	Counter mode with CBC-MAC Protocol
DDoS	Distributed DoS
DHCP	Dynamic Host Configuration Protocol
DoS	Denial Of Service
DSRC	Dedicated Short Range Communications
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAPoL	EAP Over LAN
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EGEMO	EAP Geographic and positioning Encapsulation for Multi-hOp transport
EP	Enforcement Point
GMK	Group Master Key
GSM	Global System for Mobile communication
GTK	Group Temporal Key
HNA	Hybrid Network Architecture
HWN	Hybrid Wireless Network
iCAR	Integrated Cellular and Ad hoc Relaying
ID	IDentifier
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
IRTF	Internet Research Task Force
ITS	Intelligent Transportation System
IVC	Inter-Vehicle Communication
KCK	Key Confirmation Key
KEK	Key Encryption Key
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Medium Access Control || Message Authentication Code
MADF	Mobile Assisted Data Forwarding
MANET	Mobile Ad hoc NETwork
MCN	Multi-hop Cellular Network

MIC	Message Integrity Code
MITM	Man-In-The-Middle
MN	Mobile Node
MS	Master Secret
MT	Mobile Terminal
NO	Network Operator
OBU	On Board Unit
PAA	PANA Authentication Agent
PaC	PANA Client
PANA	Protocol for Carrying Authentication for Network Access
PDA	Personal Digital Assistant
PEAP	Protected EAP
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PMS	Pre-Master Secret
PSK	Pre-Shared Key
PST	Provider Service Table
PTA	Public Transportation Authority
PTK	Pairwise Transient Key
P2P	Peer-to-Peer
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest Shamir Adleman
RSN	Robust Secure/Security Network
RSU	Road-Side Unit
RVC	Road-to-Vehicle Communication
SHA-1	Secure Hash Algorithm number 1
SOPRANO	Self-Organizing Packet Radio Ad hoc with Overlay
SRP	Secure Remote Password
TAP	Transit Access Point
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
UCAN	Unified Cellular and AdHoc Network Architecture
VANET	Vehicular Ad-hoc Networks
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WAVE	Wireless Access in Vehicular Environments
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
Wi-Fi	Wireless Fidelity
WSMP	WAVE Short Message Protocol
WTLS	Wireless Transport Layer Security
WWAN	Wireless Wide Area Network

Introduction

1. Contexte de la thèse

La quête de l'ubiquité générale des communications et les grandes avancées réalisées ces dernières années dans le domaine des technologies sans fil ont conduit à un essor fulgurant des communications sans fil dont de nouvelles applications se font sans cesse jour. Après les réseaux sans fil à infrastructure pour la téléphonie et les données (*e.g.* Wi-Fi, GSM, GPRS, UMTS, etc.), les multiples applications des réseaux ad-hoc ou auto-organisés (*e.g.* déploiement de réseaux en l'absence d'infrastructure fixe dans les champs de bataille, sur les lieux de catastrophes naturelles, dans des environnements hostiles ou difficile d'accès, etc.), aujourd'hui émerge une nouvelle application des réseaux sans fil dans laquelle des plateformes communicantes sont embarquées dans les véhicules aux fins de fournir une connectivité et des services divers aux conducteurs et aux passagers. Ces plateformes constituent alors ce que l'on appelle des réseaux véhiculaires.

La conception et la mise en œuvre des protocoles et des applications dans les réseaux véhiculaires, imposent que soient relevés de nombreux défis traditionnellement connus des communications sans fil mais qui prennent un tour nouveau et s'exacerbent dans le contexte de ces réseaux. C'est par exemple le cas de la mobilité dont la prégnance est accrue dans les réseaux véhiculaires avec des impacts forts et négatifs sur la connectivité radio. Les réseaux véhiculaires se différencient encore plus nettement des réseaux sans fil traditionnels par des caractéristiques spécifiques qui impactent leur conception. On peut citer à ce titre leur important potentiel énergétique qui tire sa justification de la capacité des véhicules à emporter des systèmes de batteries conséquents ou encore leurs caractéristiques applicatives où dominent les applications temps réel visant à rendre les routes plus sûres et les applications généralement moins contraintes apportant confort et convivialité sur les routes.

Depuis les premiers travaux sur les réseaux véhiculaires dans les années 80, les applications liées à la sécurité routière ont majoritairement fondé et justifié l'intérêt que l'on pouvait avoir pour ces réseaux. Cependant, avec la prise de conscience ces dernières années de la nécessité d'un modèle commercial crédible pour assurer l'attractivité et le déploiement de ces réseaux par des opérateurs privés, d'autres applications ont commencé, elles aussi, à susciter de l'intérêt et à s'installer dans l'immense paysage applicatif des réseaux véhiculaires.

Forts de ce contexte applicatif prolifique, les réseaux véhiculaires apparaissent peu à peu aux yeux des opérateurs, comme un débouché potentiel très prometteur en termes de fournitures de nouveaux services. Cependant, passer de la promesse à la réalité et surtout permettre à tous les acteurs (*e.g.* utilisateurs, opérateurs,

etc.) de tirer pleinement parti du concept de réseau véhiculaire, impose que soit traitée la problématique cruciale de l'authentification dont on sait qu'elle fonde l'autorisation, le contrôle et la discrimination d'accès aux services et plus généralement, la sécurité des communications. La difficulté qui se pose dans cette problématique consiste à y réussir l'intégration des caractéristiques et contraintes spécifiques (*e.g.* caractéristiques topologiques, cinétiques, applicatives, etc.) aux réseaux véhiculaires. Il est admis que l'absence de réponse à cette problématique essentielle est de nature à freiner ou à préempter le déploiement de ces réseaux dans la mesure où les services opérés - qui en sont fortement dépendants - et les implications commerciales sous-jacentes ont régulièrement sous-tendus les dynamiques de déploiement les plus massives.

2. Organisation du document

Avant de tenter de répondre à la problématique de l'authentification dans les réseaux véhiculaires, nous commençons dans la première partie de cette thèse par situer le contexte architectural de communication et le contexte de la sécurité dans les réseaux sans fil et dans les réseaux véhiculaires. Dans le Chapitre 1.1 en particulier, nous introduisons les architectures de communication des réseaux véhiculaires ainsi que divers exemples d'applications. Le Chapitre 1.2 quant à lui, étudie dans un premier temps la sécurité des réseaux sans fil et plus particulièrement celle des réseaux sans fil opérés IEEE 802.11. Des exemples d'attaques et les insuffisances des mécanismes qui y sont mis en œuvre sont relevés. Dans un second temps, une présentation de la sécurité dans les réseaux véhiculaires est entreprise. Les exigences et les défis de sécurité dans ces réseaux sont étudiés, des solutions potentielles et diverses contributions sont discutées.

Dans la seconde partie de la thèse nous présentons 4 principales contributions visant à répondre à la problématique de l'authentification et de sa mise en œuvre dans les réseaux véhiculaires opérés s'appuyant sur une technologie de type WLAN (Wireless Local Area Network). La première contribution qui s'étend sur les Chapitres 2.1 et 2.2 introduit les architectures et protocoles pour l'authentification dans les réseaux véhiculaires opérés ainsi que l'analyse des performances correspondante. La solution qui y est proposée pour l'authentification est conçue pour seoir non seulement aux caractéristiques de service, de mobilité, de connectivité et de topologie des réseaux véhiculaires mais aussi aux caractéristiques d'opération d'un réseau opérateur et aux exigences de sécurité de l'ensemble des services du réseau. La deuxième contribution qui fait l'objet du Chapitre 2.3 présente une approche d'optimisation du transport de l'authentification de notre solution initiale. La pertinence de cette approche dont l'objet essentiel est de réduire la bande passante consommée par l'authentification sans en altérer la disponibilité, y est évaluée et démontrée au travers d'une analyse des performances. La troisième contribution dont le Chapitre 2.4 révèle la teneur, présente une approche de priorisation de l'authentification mettant à contribution la diversité des canaux radio dans les réseaux DSRC (Dedicated Short Range Communications). L'intérêt de cette priorisation qui, sans remettre en cause le modèle

de priorité du système DSRC, tend à transmettre les paquets d'authentification dans des conditions préférentielles par rapport aux paquets d'autres services, y est démontré au travers d'une étude des performances. La quatrième et dernière contribution consolidée dans le Chapitre 2.5, introduit une approche de distribution de la fonction d'authentification visant à réaliser l'authentification des véhicules au plus près de ces derniers et ainsi améliorer les performances de l'authentification. La pertinence de cette approche de distribution entièrement contrôlée par le serveur d'authentification de l'opérateur et fondée sur la définition d'une densité seuil de véhicules de déclenchement de la distribution, y est démontrée par une analyse des performances.

Partie I

Chapitre 1.1. Réseaux Véhiculaires: Caractéristiques et Architectures

1. Introduction

Les réseaux ont connu dans les 3 dernières décennies un essor fulgurant marqué en particulier par la généralisation des communications sans fil. Le succès de ces communications, porté dans un premier temps par la transmission séparée de la voix et des données, puis dans un second temps par toute la panoplie des applications multimédias, a été tel qu'en l'espace d'à peine une décennie, le nombre de terminaux sans fil dans le monde a plus que supplanté le nombre de terminaux fixes.

Du point de vue des origines technologiques, les réseaux sans fil peuvent être répertoriés suivant 2 grandes familles, à savoir, les réseaux issus du monde des télécommunications (GSM, GPRS, UMTS, etc.) et ceux issus du monde de l'informatique (Bluetooth, Wi-Fi, WIMAX, etc.). Face à l'imbrication et à la convergence de ces 2 mondes, il est aujourd'hui plus pertinent d'établir une classification de ces réseaux suivant des critères structurants beaucoup plus transversaux. Ainsi, si on considère la structure opérationnelle des réseaux sans fil comme seul facteur différenciant, alors on retrouve une classification dominée par 3 grandes familles d'architectures que sont: les architectures de réseaux à infrastructure dans lesquelles les terminaux communiquent obligatoirement par l'intermédiaire d'un nœud fixe relié au réseau filaire, les architectures de réseaux ad-hoc dans lesquelles les terminaux communiquent directement entre eux ou indirectement par l'intermédiaire d'autres terminaux, et les architectures hybrides ou ad-hoc hybrides qui sont la résultante de la combinaison des 2 premières familles d'architectures.

Dans le processus de généralisation des communications sans fil, les communications véhiculaires dont résultent les réseaux éponymes, émergent et s'imposent peu à peu au rang des nouvelles applications de réseaux sans fil les plus prometteuses. Ces réseaux, sans déroger aux caractéristiques générales et aux différentes classifications des réseaux sans fil, ouvrent ces derniers sur un écosystème entier de nouveaux services. Dans cette perspective, il est attendu que les réseaux véhiculaires soient déployés dans des configurations ou combinaisons de configurations mêlant réseaux à infrastructure, réseaux ad-hoc et réseaux hybrides.

Dans ce chapitre nous présenterons, avec des exemples et références associés, les caractéristiques, les applications et les principales architectures de communication des réseaux véhiculaires.

Pour ce qui est de la structure du reste de ce chapitre, nous commencerons dans la section 2 par présenter les caractéristiques générales et quelques exemples d'applications des réseaux véhiculaires. Dans la section 3, nous

aborderons les architectures de ces réseaux et les applications associées. Nous y soulignerons en particulier le concept architectural ad-hoc hybride. La section 4 quant à elle conclura le chapitre.

2. Caractéristiques et applications

Les réseaux véhiculaires se distinguent des réseaux sans fil traditionnels 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 des véhicules. Même en cas d'arrêt du moteur et donc d'arrêt du système d'alimentation, il est toujours possible pour une plateforme embarquée de recourir à l'important dispositif de batteries dont seul un véhicule du fait de sa taille, peut disposer. Les plateformes embarquées dans les véhicules étant pleinement alimentées, elles peuvent, tout aussi pleinement, tirer parti de capacités de calcul plus massives et de multiples interfaces de communication.

- *L'environnement de communication et le modèle de mobilité*: Alors que les environnements de communications dans les réseaux sans fil traditionnels se résument généralement à des espaces complètement ouverts et sans obstacles ou à des espaces clos en intérieur, les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale. Du fait de la mobilité des véhicules, il est en effet possible de passer d'un environnement urbain caractérisé par de nombreux obstacles à la propagation des signaux, à un environnement périurbain ou autoroutier présentant des caractéristiques différentes. Il est également nécessaire de prévoir dans les réseaux véhiculaires une volatilité des conditions climatiques et des contraintes topologiques. En plus de cette diversité environnementale, les réseaux véhiculaires se distinguent également des réseaux sans fil ordinaires par un modèle de mobilité dont une des traductions les plus évidentes est l'importante vitesse des nœuds qui réduit considérablement les durées de temps pendant lesquelles les nœuds peuvent communiquer. Ces conditions sont de nature à poser pour les réseaux véhiculaires d'importants problèmes de connectivité couplés à une aggravation de l'instabilité de la propagation radio (*e.g.* multi-path fading, shadowing, path loss, etc.) [OISHI06].

- *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 multiplicité 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.

- *La taille du réseau*: Etant 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.

Au-delà des caractéristiques générales introduites ci-dessus, les réseaux véhiculaires se distinguent également par la variété des applications ou des services appelés à y être opérés. Ces services vont de ceux liés à la sécurité routière (*e.g.* diffusion des messages d'alerte: alerte collision, alerte travaux, alerte accident, etc.) et permettant de bâtir un système de transport intelligent (*en anglais*, Intelligent Transportation System "ITS"), à ceux visant le confort, la performance ou le divertissement (*e.g.* péage électronique, gestion de flotte, accès Internet, jeux en ligne, etc.). Ces différents services étant généralement liés aux architectures des réseaux véhiculaires, ils seront déclinés plus spécifiquement dans la section 3 qui traite de ces architectures.

3. Architectures de communication

3.1. Les réseaux véhiculaires à infrastructure

Les réseaux véhiculaires dont les déploiements sont les plus actifs se traduisent dans des architectures de réseaux à infrastructure. Il s'agit dans la plupart des cas d'une réutilisation des technologies des réseaux mobiles de télécommunications dans l'implémentation de certaines applications ou certains services spécifiques aux réseaux véhiculaires. Ainsi par exemple, les architectures présentées par [VINAY07] et [MAHFO08] et dont la Figure 1 donne une illustration, permettent de développer, via le réseau GPRS (General Packet Radio Service), des applications de surveillance de l'état des véhicules, de diagnostique à distance des pannes, d'émission automatique des appels d'urgence, de localisation des véhicules, de gestion de flotte de véhicules d'entreprise, etc.

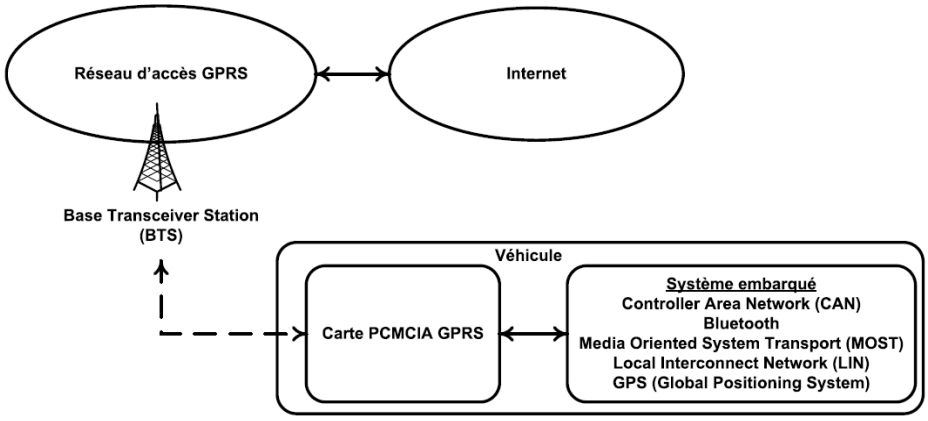


Figure 1: Réseau véhiculaire avec GPRS

Pour des applications telles que l'accès au courrier électronique, l'écoute de la musique en ligne, les jeux en réseau et plus généralement l'accès Internet, des opérateurs en partenariat avec des constructeurs automobiles ont mis en place des solutions permettant leur exploitation via le réseau mobile 3G (*e.g.* UMTS) ou 3G+ (*e.g.* HSPA). L'opérateur Orange par exemple, a conçu une passerelle miniaturisée appelée FlyBox fournissant une connectivité 3G/3G+ et permettant de créer un réseau Wi-Fi à l'intérieur des véhicules (voir Figure 2). Plus concrètement, la Flybox est un modem routeur avec module téléphonique intégré qui se connecte au réseau mobile grâce à une carte SIM (Subscriber Identity Module) incluse. Elle permet de sélectionner le meilleur réseau disponible (*e.g.* EDGE, 3G, 3G+) pour atteindre des débits jusqu'à 7 Mbits/s. La Flybox permet ainsi aux passagers d'accéder, en Wi-Fi, à l'internet haut débit en situation de mobilité et de connecter jusqu'à 4 terminaux simultanément en Wi-Fi ou par ports Ethernet. De fait, n'importe quel terminal Wi-Fi (SmartPhone, PC portable, PDA, etc.) ou Ethernet dans le véhicule peut profiter de l'accès à Internet.

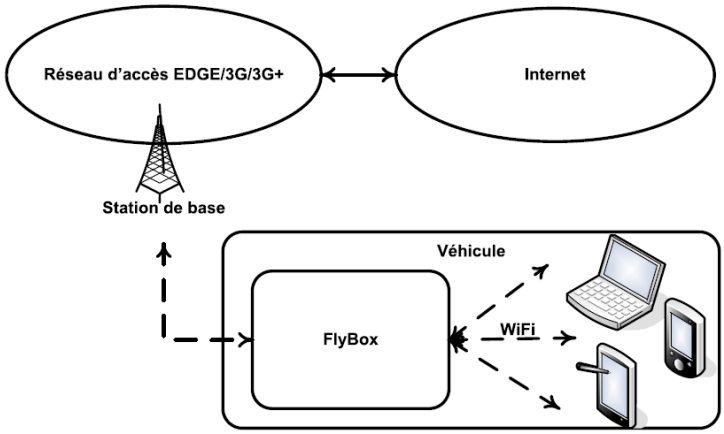


Figure 2: Réseau véhiculaire avec FlyBox

De nombreux autres projets développant des réseaux véhiculaires à infrastructure ont vu le jour en Europe ces dernières années. Le projet DRiVE (Dynamic Radio for IP Services in Vehicular Environments) [DRIVE] par exemple s'est attaché à promouvoir la convergence entre différentes technologies (GSM, UMTS, DAB et DVB-T) afin de jeter les bases du développement de services IP innovants à destination des véhicules. Le projet GST (Global Systems for Telematics) [GST] dont l'opérateur Orange fut un des acteurs, s'est intéressé dans le cadre du développement des applications liées à la sécurité routière sur le réseau GSM, à des problématiques de sécurisation de l'infrastructure réseau et service, de sûreté de fonctionnement et de facturation.

3.2. Les réseaux véhiculaires ad-hoc

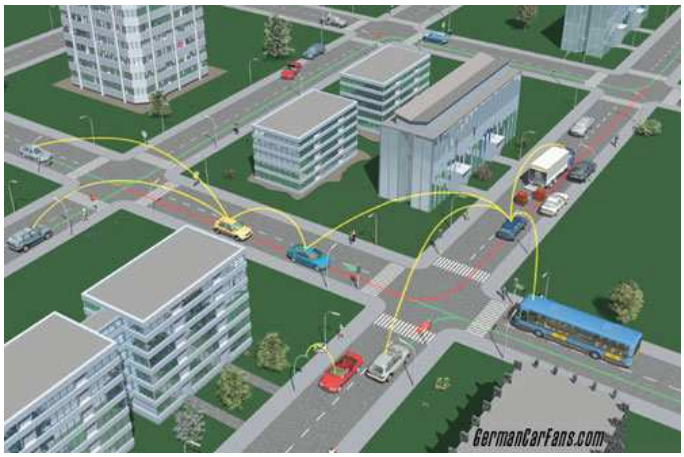


Figure 3: Exemple de VANET [KOSCH05]

Les réseaux véhiculaire ad-hoc, plus connus sous la dénomination VANET (Vehicular Ad-hoc Networks), reprennent les mêmes principes architecturaux que les MANETs (voir Figure 3). Par delà les applications ou les services liés à la sécurité routière (*e.g.* alerte accident, alerte ralentissement, alerte déviation, alerte travaux, alerte intempéries, aide aux dépassements de véhicules, prévention des sorties de voies en ligne ou en virage, conduite coopérative, etc.) dont l'essor dans les VANETs est porté par l'accroissement du parc des véhicules et la nécessité dans le monde contemporain de maximiser la sécurité des biens et des personnes, on peut également identifier les applications ou les services dits de divertissement à l'instar de la messagerie instantanée inter-véhicules ou encore des jeux en réseau entre véhicules.

Pour mettre en œuvre ces applications, divers projets ont fleuri à travers le monde. Ainsi par exemple, le projet européen CARTALK2000 [CARTALK], coordonné par le constructeur automobile Daimler Chrysler entre 2001 et 2004, a développé des systèmes coopératifs d'aide à la conduite et déployé un VANET auto-organisé utilisant un protocole de routage géographique multi-sauts. Le projet a également étudié des stratégies d'introduction au marché comprenant des analyses de coûts et des aspects légaux. Le projet français MobiVip

[MOBIVIP] s'est quant à lui départi des aspects réseaux pour ne s'intéresser qu'aux briques logicielles pour les services applicatifs dans des VANETs organisés autour des "Véhicules Individuels Publics".

D'un point de vue historique, les premiers travaux dédiés aux applications des VANETs ont commencé dans les années 80 au Japon avec l'AETATD (Association of Electronic Technology for Automobile Traffic and Driving) suite à l'accroissement des problèmes liés aux déplacements des personnes et des biens. Ces travaux ont initié l'exploration de diverses applications (*e.g.* conduite automatique et coopérative) associées à la circulation routière. Plusieurs institutions à travers le monde (ITS "Intelligent Transportation Society" et NAHSC "National Automated Highway System Consortium" aux Etats-Unis, PROMETHEUS "PROgraM for European Traffic with Highest Efficiency and Unprecedented Safety" en Europe, etc.), ont ensuite mené des projets qui ont abouti à l'expérimentation de prototypes et de solutions variés. Avec les dernières avancées dans le domaine des technologies de communication, de calcul et de localisation, de nouveaux projets autour des applications des VANETs continuent de voir le jour.

3.3. Les réseaux véhiculaires ad-hoc hybrides

Avant de nous intéresser de manière spécifique aux réseaux véhiculaires ad-hoc hybrides, il convient dans un premier temps de cerner le concept architectural ad-hoc hybride ainsi que ses applications. Nous commencerons donc dans cette section par introduire les architectures de réseaux ad-hoc hybrides pour ensuite revenir au cas particulier des réseaux véhiculaires.

3.3.1. Le concept architectural ad-hoc hybride

Les réseaux hybrides ou réseaux ad-hoc hybrides, sont des réseaux sans fil ayant une organisation duale recoupant à la fois celle des réseaux à infrastructure et celle des réseaux ad-hoc. Plus concrètement, en plus des communications sur un saut entre terminaux et infrastructure fixe et des communications multi-sauts entre terminaux, dans les réseaux hybrides, les terminaux sont également susceptibles de communiquer avec l'infrastructure fixe sur plusieurs sauts par l'intermédiaire d'autres terminaux ou de nœuds relais dédiés. Dans ce type de réseau, les technologies utilisées pour les communications sur un saut entre les terminaux et l'infrastructure fixe et celles utilisées pour les communications multi-sauts peuvent être de divers ordres. C'est ainsi qu'apparaissent les concepts d'architectures "intra-technologie" (*en anglais*, intra-technology) et d'architectures "inter-technologies" (*en anglais*, inter-technology) [DUDA06]. Dans le premier type d'architectures (*i.e.* architectures "intra-technologie"), la même technologie est utilisée à la fois pour les communications sur un saut avec l'infrastructure fixe et pour les communications multi-sauts. C'est par exemple le cas des réseaux hybrides constitués sur la base de la norme IEEE 802.11 pour les communications avec les

points d'accès et pour les communications en mode ad-hoc. Dans le second type d'architectures (*i.e.* architectures "inter-technologies"), des technologies distinctes sont utilisées pour les communications sur un saut avec l'infrastructure fixe et pour les communications multi-sauts. C'est notamment le cas lorsqu'un réseau hybride est mis en œuvre à partir d'une technologie radio 3G pour les communications sur un saut avec la station de base et d'une autre technologie telle que l'IEEE 802.11 pour les communications en mode ad-hoc.

Les motivations qui président à la conception et au déploiement des architectures de réseaux ad-hoc hybrides sont multiples et de divers ordres. On peut citer:

- *L'amélioration de la qualité de service*: Le couplage du mode ad-hoc et du mode infrastructure peut concourir à améliorer de manière sensible les performances des communications en termes notamment de délai et de débit. C'est par exemple le cas des terminaux (situés en limite de zone de couverture de l'infrastructure fixe) qui, en basculant en mode ad-hoc pour atteindre l'infrastructure fixe, peuvent augmenter leur débit et réduire significativement les délais de transmission.

- *L'équilibrage des charges entre les cellules d'un réseau à infrastructur*e: Un terminal situé dans la zone de couverture d'une infrastructure fixe surchargée peut avantageusement passer en mode ad-hoc pour atteindre une infrastructure fixe voisine qui elle serait moins chargée. Il en résulte ainsi une réduction des échecs de communication et une optimisation de l'utilisation des ressources.

- *L'extension de la zone de couverture, la réduction des coûts de déploiement et l'accès ubiquitaire aux services*: Des terminaux situés en dehors de la zone de couverture de l'infrastructure fixe peuvent malgré tout bénéficier des services (*e.g.* Internet) de cette infrastructure via des communications multi-sauts. Une telle possibilité est de nature à optimiser le déploiement de l'infrastructure fixe et donc réduire les coûts associés. De plus, bénéficier des services d'un opérateur même en dehors de toute zone de couverture, est un pas supplémentaire vers l'objectif ultime de l'accès ubiquitaire aux services.

- *La simplification des protocoles des réseaux ad-hoc*: La nature des réseaux ad-hoc impose la conception et la mise en œuvre de protocoles totalement distribués. La complexité de ces protocoles et leur coût de mise en œuvre peuvent se montrer rédhibitoires dans des contextes de réseaux ad-hoc énergiquement contraints. En offrant la possibilité de s'appuyer sur une infrastructure fixe, les réseaux hybrides peuvent concourir à simplifier les protocoles des réseaux ad-hoc et donc faciliter leur mise en œuvre. Cette simplification est opérée en concentrant certains traitements sur l'infrastructure fixe qui peut ainsi assister les terminaux du réseau ad-hoc dans l'exécution des protocoles.

- *Le contexte technologique et de marché favorable*: De plus en plus de terminaux sans fil sont équipés de plusieurs interfaces de communication leur permettant de fonctionner en mode infrastructure et en mode ad-hoc. C'est par exemple le cas des portables, des PDAs et autres SmartPhones qui intègrent de plus en plus une interface GSM ou 3G et une interface Wi-Fi.

L'intérêt porté aux architectures de réseaux ad-hoc hybrides a encouragé nombre de travaux aussi bien dans le monde académique que dans celui de l'industrie. Les principaux thèmes de ces travaux s'articulent autour de la spécification des architectures, du routage et de la gestion des ressources radio. Dans [ANAN01] par exemple, une architecture hybride appelée MCN (Multi-hop Cellular Network) permettant aux terminaux (*i.e.* MNs "Mobile Nodes") à l'intérieur d'une cellule de communiquer sur plusieurs sauts avec la station de base de cette même cellule, est proposée. Comme illustré sur la Figure 4 l'architecture définit un canal de contrôle et un canal pour la transmission des données. La portée de transmission de la station de base et des terminaux sur le canal des données est réduite par rapport à leur portée de transmission sur le canal de contrôle qui, elle, couvre l'ensemble de la cellule. Cette caractéristique permet de tirer parti de la réutilisation spatiale lors de la transmission des données et ainsi potentiellement d'augmenter les débits. En plus de cette spécification architecturale, un protocole de routage dans lequel le calcul des routes est réalisé par la station de base, est proposé. Finalement, la principale faiblesse identifiée dans l'architecture proposée, est le partage du canal de contrôle dont la seule saturation suffirait à mettre les communications en échec.

Dans la foulée de l'architecture MCN, une architecture assez proche appelée UCAN (Unified Cellular and AdHoc Network Architecture) est proposée dans [LUO03]. À la différence de l'architecture MCN, dans l'architecture UCAN, la communication en mode ad-hoc pour atteindre la station de base n'est utilisée que si la qualité du canal radio avec l'infrastructure est insuffisante. Dans ce cas en effet, les paquets sont acheminés par l'intermédiaire des terminaux pour lesquels le canal radio avec l'infrastructure est de bien meilleure qualité. Des débits plus importants et des réductions de délais peuvent ainsi être obtenus. Notons toutefois qu'ici les communications en mode infrastructure utilisent une technologie 3G alors que les communications en mode ad-hoc utilisent l'IEEE 802.11. Cette complexité matérielle (puisqu'il faut jusqu'à 2 interfaces par terminal) est de nature à épuiser assez rapidement les faibles batteries des terminaux.

Une autre architecture baptisée ICAR (Integrated Cellular and Ad-hoc Relaying) et permettant aux réseaux cellulaires d'approcher des débits proches de la capacité théorique, est proposée dans [WU01]. Cette architecture permet de réaliser un équilibrage des charges dynamique entre les différentes cellules du réseau. Comme présenté sur la Figure 5, des nœuds dédiés appelés ARS (Ad hoc Relaying Stations), sont déployés à des endroits stratégiques pour relayer, lorsqu'il y a lieu, les excédents de trafic des cellules surchargées vers des cellules mitoyennes moins chargées. Les ARS communiquent dans ce contexte en mode infrastructure avec les stations de base et en mode ad-hoc avec les terminaux et d'autres ARS. Au-delà des débits plus importants

obtenus et d'une meilleure gestion de la capacité radio, cette architecture impose malgré tout, une complexité matérielle non négligeable au niveau des terminaux mobiles.

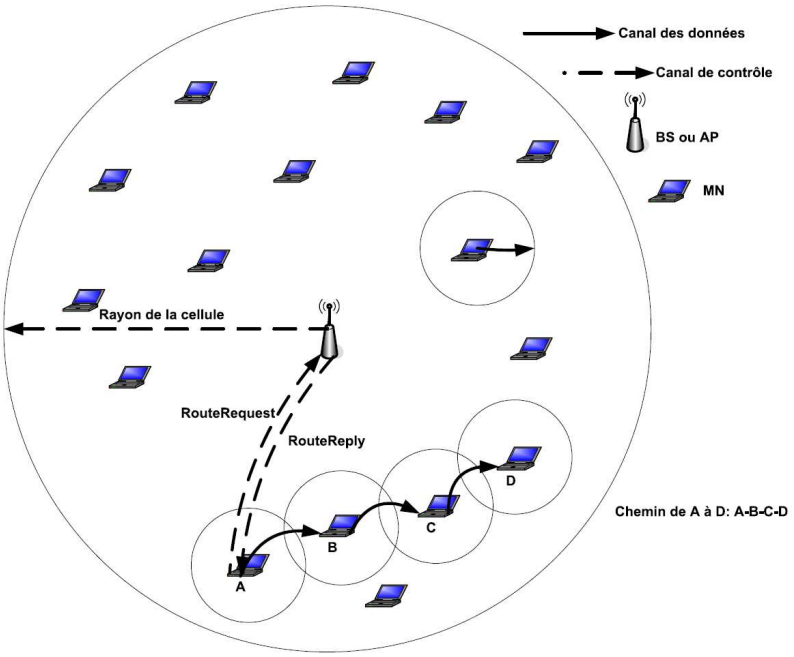


Figure 4: Réseau hybride MCN

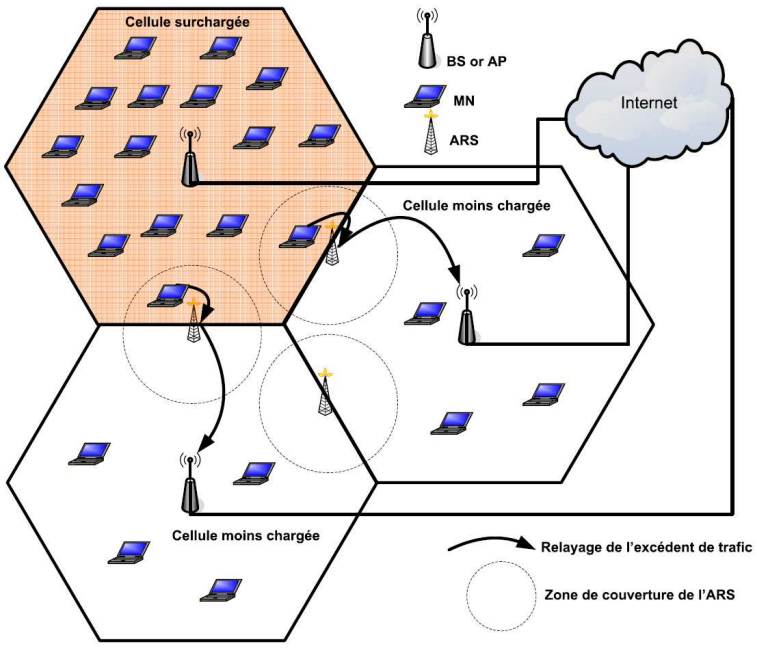


Figure 5: Réseau hybride ICAR

Une architecture encore plus générale que les architectures précédentes est proposée dans [ZADEH02]. Cette architecture qui est promue sous l'appellation SOPRANO (Self-Organizing Packet Radio Ad hoc with Overlay), généralise pour tous les terminaux du réseau, des communications multi-sauts avec la station de base via des nœuds relais dédiés (voir Figure 6). Dans cette architecture, seuls les nœuds relais dédiés doivent disposer de 2 interfaces (*i.e.* une interface pour le mode infrastructure et une interface pour le mode ad-hoc) chacun. Les terminaux ne doivent disposer chacun que d'une unique interface leur permettant de communiquer en mode ad-hoc avec les nœuds relais, charge ensuite à ces derniers de relayer les paquets des terminaux vers la station de base. En plus de l'extension de la zone de couverture des stations de base, cette architecture permet non seulement un équilibrage des charges entre les différentes cellules, mais aussi l'obtention de débits plus élevés du fait de la réutilisation spatiale[1]; tout ce ceci sans induire la moindre complexité matérielle pour les terminaux.

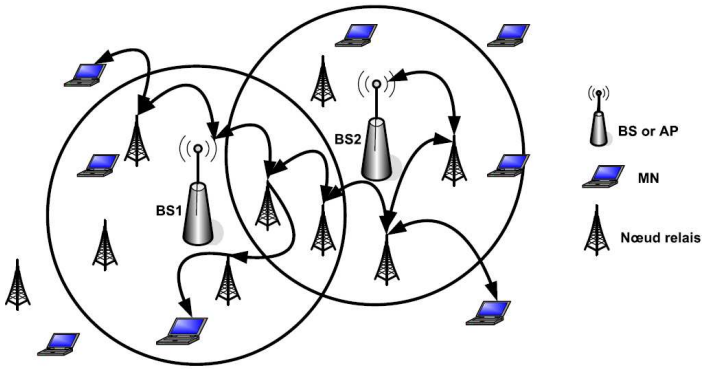


Figure 6: Réseau hybride SOPRANO

Les auteurs de [ZOIC05], proposent et étudient quant à eux, une architecture hybride appelée HNA (Hybrid Network Architecture). Comme illustré sur la Figure 7, cette architecture mêle la technologie IEEE 802.16 [IEEE-802.16] pour constituer un réseau maillé de collecte Internet et la technologie IEEE 802.11 pour constituer à la fois des Hot Spots[2] et des communications en mode ad-hoc. Les terminaux situés à l'intérieur comme à l'extérieur des zones de couverture des Hot Spots peuvent accéder à Internet grâce à la définition d'un protocole de routage hiérarchique appelé FMARP (Flexible Mobile Access Routing Protocol) basé sur la construction d'un arbre logique ayant comme racine, la passerelle du réseau (*en anglais*, Gateway). L'intérêt principal de ce type d'architecture est de permettre l'extension de la zone de couverture des services, en particulier jusqu'aux zones où l'infrastructure filaire est inexistante ou défaillante.

[1] La portée de transmission des nœuds du réseau étant réduite, il y a moins d'interférences et les débits peuvent être plus élevées.
[2] Zones desservies par des points d'accès, généralement de type Wi-Fi. Ces zones sont calquées sur la zone de couverture des points d'accès.

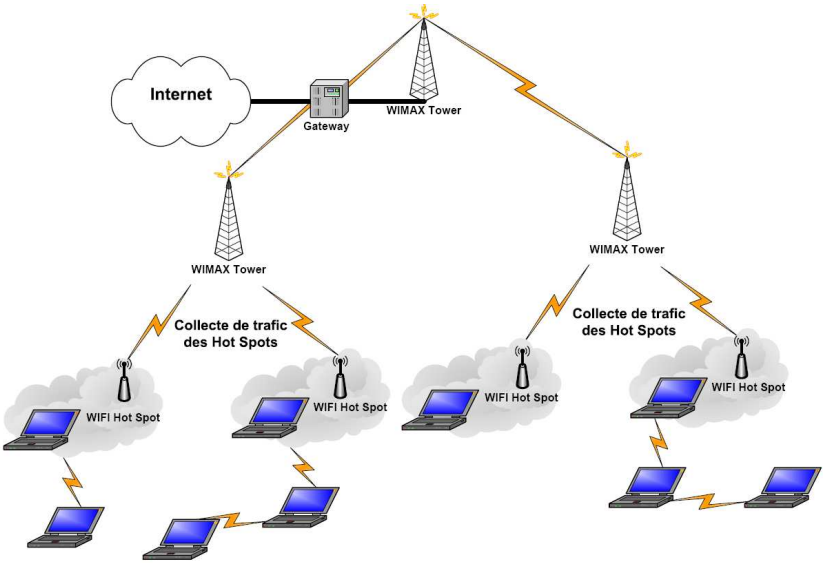


Figure 7: Réseau hybride HNA

Au-delà des différentes propositions architecturales précédentes, des efforts de standardisation dans le domaine des réseaux ad-hoc hybrides sont également réalisés. Ainsi le groupe de travail IEEE 802.11s [IEEE-802.11s] s'attache à la spécification des réseaux maillés (*en anglais*, mesh networks) dans les réseaux locaux 802.11 alors le groupe de travail IEEE 802.11u [IEEE-802.11u] s'intéresse dans ce contexte à l'interconnexion avec d'autres types de réseaux (*e.g.* 3G, WIMAX, etc.) dits externes. Des tentatives de standardisation associées aux réseaux ad-hoc hybrides au niveau de la couche IP et des couches supérieures sont également menées au sein de l'IETF (Internet Engineering Task Force) et de l'IRTF (Internet Research Task Force) au travers par exemple des groupes de travail AutoConf [AUTOCONF] et MOBOPTS [MOBOPTS].

3.3.2. Le concept ad-hoc hybride appliqué aux réseaux véhiculaires

Les réseaux véhiculaires ont été définis dans des architectures ad-hoc hybrides pour opérer à la fois des applications liées à la sécurité routière nécessitant une configuration ad-hoc du réseau et des applications s'inscrivant davantage dans un contexte de fourniture de service depuis l'infrastructure fixe. C'est par exemple le cas de l'architecture cible définie dans le cadre du consortium européen C2C-CC (Car2Car Communication Consortium) [C2C-CC] dont les principales ambitions sont: (i) la création d'un standard européen ouvert pour les communications V2V (Vehicle-to-Vehicle) ou IVC (Inter-Vehicle Communication) et les communications V2I (Vehicle-to-Infrastructure) ou V2R (Vehicle-to-Road), (ii) le développement de prototypes et de démonstrateurs pour les applications des réseaux véhiculaires, (iii) l'attribution d'une bande de fréquence exclusive et libre pour les applications des réseaux véhiculaires, et (iv) le développement de stratégies de

déploiement et de modèles économiques pour la pénétration du marché. Cette architecture envisage l'utilisation d'une variété de technologies dont principalement l'IEEE 802.11p (WAVE "Wireless Access in Vehicular Environments") [IEEE-802.11p] qui spécifie des communications en mode infrastructure et en mode ad-hoc (voir Figure 8). Dans ce contexte, chaque véhicule embarque une plateforme de communication appelée OBU (On Board Unit). Cette plateforme est utilisée par une ou plusieurs applications appelées AUs (Applications Units). Quant aux points d'accès disposés le long des routes et constituant l'infrastructure fixe, ils sont nommés RSUs (Road-Side Units).

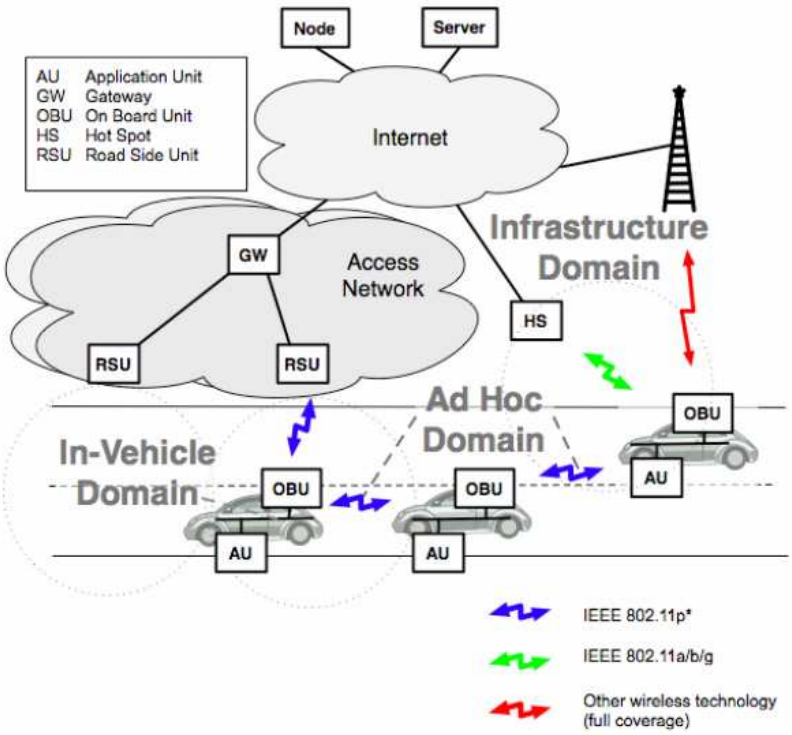


Figure 8: Architecture ad-hoc hybride C2C-CC [C2C-CC07]

L'architecture ad-hoc hybride envisagée au sein du C2C-CC est également reprise dans le projet allemand NOW (Network-On-Wheels) [NOW] dont les travaux se font en étroite collaboration avec le consortium. Les protocoles et systèmes (*e.g.* protocole de routage géographique, protocole de sécurité, antenne radio, etc.) développés au sein de ce projet intéressent aussi bien les applications liées à la sécurité routière que les applications de divertissement; et ce, que ce soit dans les modes de communication ad-hoc (*i.e.* V2V) ou infrastructure (*i.e.* V2I). Notons que le projet FleetNet [FLEETNET] avant le projet NOW avait déjà développé et intégré une architecture hybride dans laquelle les communications avec l'infrastructure et l'Internet se faisaient en GPRS et les communications ad-hoc en 802.11 (voir Figure 9). Les protocoles de routage géographiques conçus et implémentés dans ce projet ont été validés dans le cadre d'un démonstrateur de 6 véhicules équipés de systèmes de positionnement GPS pour alimenter ces protocoles. Les applications visées

étaient essentiellement l'échange de messages entre véhicules pour la conduite coopérative, la gestion de flottes et l'accès Internet.

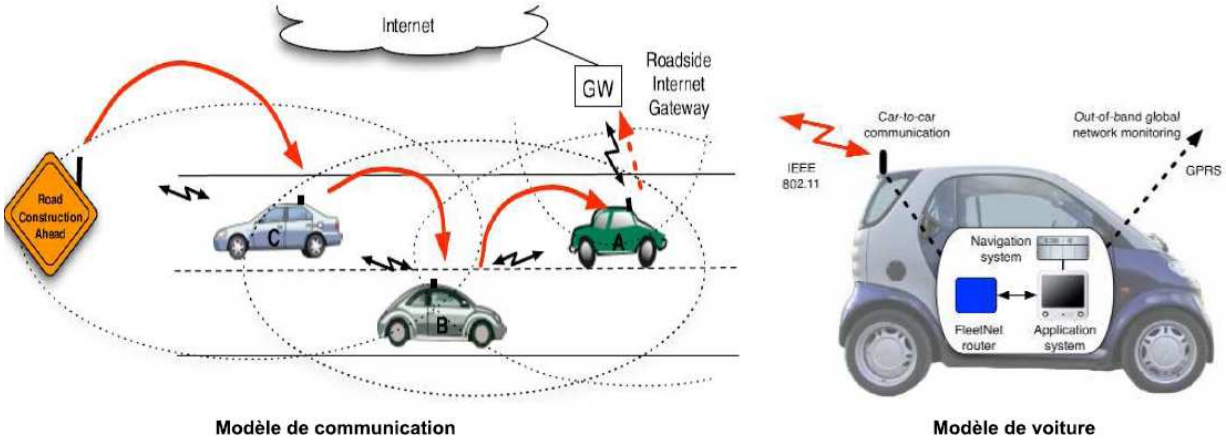


Figure 9: Architecture ad-hoc hybride FLEETNET [FESTAG04]

Des architectures ad-hoc hybrides ont également été choisies pour les réseaux véhiculaires dans l'optique première de l'extension de la zone de couverture des services, de l'optimisation du déploiement des stations de base ou des points d'accès et de l'adaptation à la forte dynamique des nœuds. Ainsi par exemple, le projet BAS (Business As uSual) [LI04] a développé un réseau véhiculaire ad-hoc hybride organisé autour de bus de transport public et de points d'accès disposés le long des routes pour fournir un accès à Internet (voir Figure 10). Afin que les passagers des bus puissent se connecter indépendamment de leur présence ou non dans la zone de couverture de l'infrastructure fixe, un protocole de routage géographique permettant d'accéder à l'infrastructure fixe par l'intermédiaire d'autres bus en mode ad-hoc, a été défini. À ce protocole, s'est également greffé un protocole de découverte de l'infrastructure fixe défini spécialement pour les bus situés en dehors de la zone de couverture de cette infrastructure.

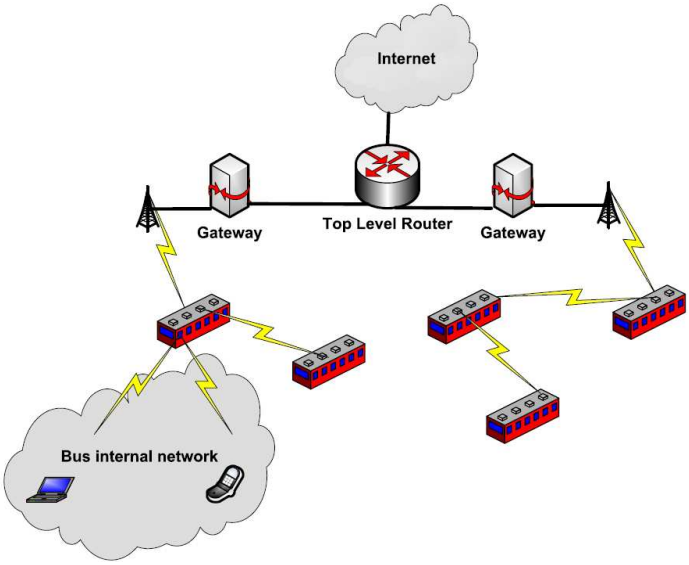


Figure 10: Réseau véhiculaire BAS

En plus des différents projets ci-dessus, notons qu'à travers le monde, divers autres projets sur les réseaux véhiculaires supposent des architectures de réseaux ad-hoc hybrides. C'est le cas notamment des projets européens COMeSafety [COMESAFE], COOPERS [COOPERS], CVIS [CVIS], GeoNet [GEONET] et SAFESPOT [SAFESPOT], du projet américain VII [VII], du projet ISO CALM [CALM], du projet ETSI ITS [ITS] pour ne citer que ceux là.

3.3.3. Approche de classification des architectures ad-hoc hybrides

L'étude des différentes architectures de réseaux ad-hoc hybrides nous a amené à identifier trois types d'architectures à savoir:

- *Les architectures ad-hoc intra-cellulaires* dans lesquelles les communications entre des terminaux et l'infrastructure fixe se font en mode ad-hoc alors même que ces terminaux sont dans la zone de couverture (*i.e.* à un saut) de cette infrastructure fixe. Un des principaux objectifs de ce type d'architecture est d'accroitre les performances par la réutilisation spatiale. On remarquera que ce type d'architecture est généralement marqué par l'utilisation d'une technologie de type WWAN (Wireless Wide Area Network) pour les communications en mode infrastructure et d'une technologie de type WLAN (Wireless Local Area Network) pour les communications en mode ad-hoc. Les architectures MCN [ANAN01], C2C-CC [C2C-CC07] et FleetNet [FESTAG04] en sont des exemples.

- *Les architectures ad-hoc inter-cellulaires* dans lesquelles les communications en mode ad-hoc permettent à des terminaux situés dans la zone de couverture d'un point d'accès (ou d'une station de base) d'atteindre un

autre point d'accès (ou une autre station de base) dont la zone de couverture ne couvre pas ces terminaux. Un des principaux avantages de ce type d'architecture est l'équilibrage des charges entre les cellules. Les technologies mises en œuvre pour les différents modes de communication sont généralement les mêmes que celles utilisées dans le cas ad-hoc intra-cellulaire. Les architectures ICAR [WU01] et SOPRANO [ZADEH02] en sont des exemples.

- *Les architectures ad-hoc extra-cellulaires* dans lesquelles les communications en mode ad-hoc sont utilisées entre des terminaux situés en dehors de toute zone de couverture de l'infrastructure fixe. Un des principaux objectifs avec ce type d'architecture est l'extension de la zone de couverture des services. On remarquera que dans ce type d'architecture les communications en mode ad-hoc et en mode infrastructure utilisent généralement la même technologie; technologie qui le plus souvent est de type WLAN ou WMAN (Wireless Metropolitan Area Network). Les architectures SOPRANO [ZADEH02], HNA [ZOIC05], BAS [LI04] et C2C-CC [C2C-CC07] à travers sa composante WAVE [IEEE-802.11p] en sont des illustrations.

Dans chacun des scénarii architecturaux précédents, il peut être fait usage de nœuds relais dédiés ou de terminaux remplissant également des fonctions de relais en plus du traitement de leurs propres trafics. De plus, dans les architectures ad-hoc intra-cellulaires et ad-hoc inter-cellulaires plus spécifiquement, on peut identifier deux configurations possibles: (i) une configuration mono-mode dans laquelle les communications des terminaux se font exclusivement en mode ad-hoc et (ii) une configuration bi-mode dans laquelle les communications des terminaux peuvent être en mode ad-hoc ou en mode infrastructure. La Figure 11 illustre cette classification des architectures ad-hoc hybrides ainsi que les avantages caractérisant chacune des principales classes.

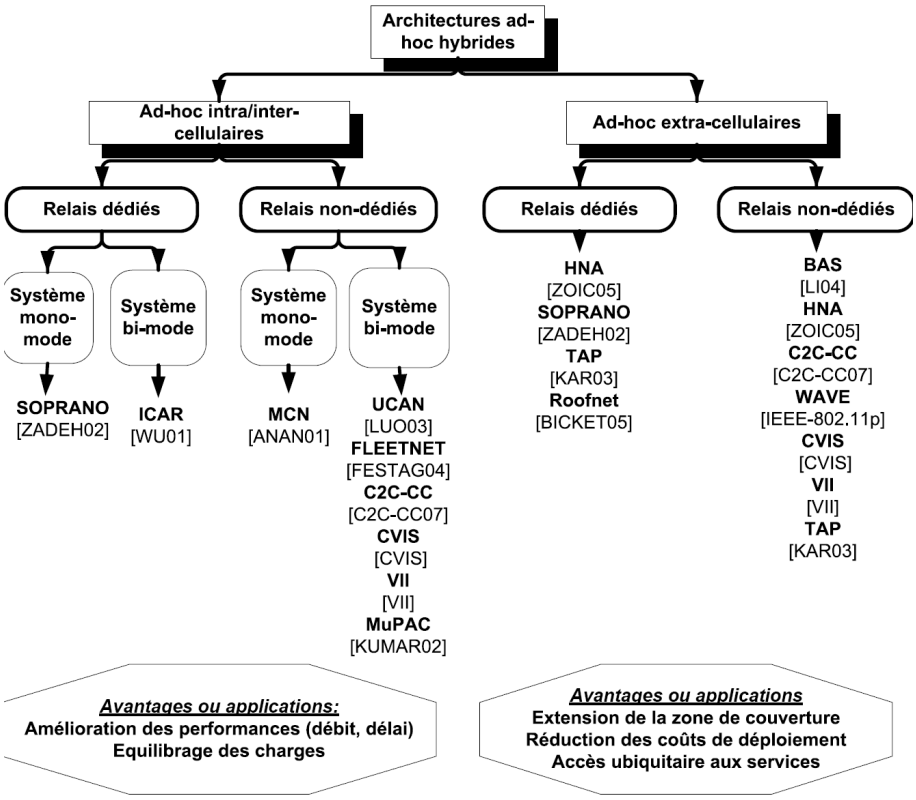


Figure 11: Classification des architectures de réseaux ad-hoc hybrides

4. Conclusion

Bien que les réseaux véhiculaires diffèrent quelque peu des réseaux sans fil traditionnels, notamment par leur potentiel énergétique, il est intéressant de constater que ces réseaux n'ont encore pu voir le jour sur le marché que dans des architectures à infrastructure. Cette tendance confirme la nécessité de s'atteler au développement des réseaux véhiculaires ad-hoc hybrides si l'on souhaite voir se matérialiser l'important potentiel applicatif des VANETs. En effet, les réseaux ad-hoc hybrides apparaissent comme une option crédible permettant de tirer parti concomitamment des avantages applicatifs et des caractéristiques des réseaux à infrastructure et des réseaux ad-hoc mais aussi d'engranger des gains de performance (*e.g.* débit, délai, optimisation de l'exploitation des ressources radio, etc.) et des avantages de la rationalisation du déploiement des points d'accès ou des stations de base. Cette perspective que présentent les réseaux ad-hoc hybrides est de nature à assurer des débouchés commerciaux au concept des communications ad-hoc et ainsi garantir des déploiements substantiels. Les projets actuellement en cours sur les réseaux véhiculaires ne s'y trompent pas puisqu'ils s'inscrivent en grande majorité dans un contexte architectural ad-hoc hybride même si les applications commerciales les plus porteuses (*i.e.* applications non liées à la sécurité routière) sont encore très peu prises en compte. Les réseaux

ad-hoc hybrides et en particulier leur déclinaison dans les réseaux véhiculaires restent donc un champ d'investigation prometteur appelant encore de nombreux investissements.

C'est dans ce contexte, que nous inscrivons les travaux de cette thèse dans une architecture des réseaux véhiculaires ad-hoc hybrides; architecture que nous instancions sur le plan technologique dans les réseaux véhiculaires DSRC (Dedicated Short Range Communications) [DSRC] dont le standard en cours de développement IEEE 802.11p [IEEE-802.11p] spécifie les couches physique et liaison de données pour les communications véhiculaires. En nous situant ainsi dans des réseaux s'appuyant sur une technologie de type WLAN, nous anticipons une généralisation de ces derniers, portée par le coût relativement faible que promet l'opération des services sur ces réseaux par rapport aux réseaux de type WWAN (*e.g.* 3G). Il est par ailleurs attendu que la généralisation de ces réseaux soit aussi portée par des incitations publiques dans l'optique du renforcement de la sécurité routière. De plus, le concept ad-hoc hybride appliqué aux réseaux DSRC permet d'étendre la zone de couverture des services, de favoriser l'accès ubiquitaire à ces derniers et de réduire les coûts de déploiement de l'infrastructure fixe.

Dans le chapitre qui va suivre nous nous intéresserons à la sécurité dans les WLANs actuels et en particulier dans les réseaux IEEE 802.11. Nous passerons ensuite en revue la sécurité dans le contexte spécifique des réseaux véhiculaires.

Chapitre 1.2. Sécurité des Réseaux Sans Fil et des Réseaux Véhiculaires

1. Introduction

Les réseaux locaux sans fil IEEE 802.11 constituent de nos jours le standard des WLANs le plus largement déployé et utilisé à travers le monde. Les contextes d'utilisation de ces réseaux sont divers et vont principalement du cadre domestique, aux lieux publics (*e.g.* gares, hôtels, restaurants, etc.) à travers notamment des HotSpots, en passant par le cadre du travail. Poussés précipitamment sur le marché, les WLANs 802.11 n'ont pu intégrer des mécanismes de sécurité robustes qu'après la déferlante des attaques dont ces réseaux ont fait l'objet et la prise de conscience progressive de l'étendue des vulnérabilités dans leur conception initiale. Dans le contexte des réseaux véhiculaires où un consensus technologique semble se dégager autour du standard DSRC/IEEE 802.11p pour les déploiements à venir, il est urgent de tirer les leçons des premiers déploiements des WLANs et donc d'éviter que la sécurité ne soit pensée, une fois de plus, a posteriori.

La sécurité des réseaux véhiculaires est donc aujourd'hui un enjeu majeur dont il faut se saisir pour garantir la plus large adoption possible de ces réseaux aussi bien par les usagers de la route dont on attend l'utilisation que les opérateurs dont on attend le déploiement. Cette sécurité s'inscrit dans un contexte particulier marqué, comme souligné dans le chapitre précédent, par une forte dynamique des nœuds avec des pointes de vitesse pouvant atteindre 200 Km/h, une aggravation de l'instabilité de la propagation radio, une connectivité intermittente, une topologie dynamique mais contrainte par celle des routes, un réseau potentiellement très étendu appelant une administration nécessairement hétérogène, un potentiel énergétique important, etc. En adjonction à cette liste non exhaustive, il faut certainement compter avec la nature des applications ou des services qui y sont opérés et qui sont susceptibles d'induire des exigences de sécurité différenciées à l'image de la dichotomie du modèle de communication induite par les applications. Tout ce contexte, pris dans sa globalité, crée pour la sécurité des réseaux véhiculaires de nombreuses possibilités d'investigation dont on ne peut pourtant pas encore dire, à l'aune des contributions actuelles, qu'elles soient pleinement explorées.

Dans ce chapitre nous présenterons la sécurité du standard de facto des WLANs, à savoir celui des WLANs IEEE 802.11. Nous aborderons en particulier les attaques possibles dans ces réseaux, les objectifs de sécurité généraux dans ces réseaux, et les différents mécanismes de sécurité qui y sont en vigueur ou qui peuvent être y utilisés. Forts de cette analyse, nous nous investirons plus spécifiquement dans la sécurité des réseaux véhiculaires. Nous ouvrirons une parenthèse particulière sur la nature des services mis en œuvre dans ces

réseaux avant de présenter des exemples d'attaques dans ces réseaux ainsi qu'une taxonomie correspondante. Il sera ensuite possible de mettre en évidence les principales exigences et défis de sécurité dans ces réseaux puis de présenter quelques contributions dans ce domaine.

Pour ce qui est de la structure organisationnelle du reste de ce chapitre, nous commencerons dans la section 2 par présenter la sécurité des WLANs 802.11. Dans la section 3 il sera question de la sécurité des réseaux véhiculaires. La section 4 quant à elle conclura le chapitre.

2. La sécurité des réseaux sans fil: Cas des WLANs IEEE 802.11

Nous nous intéressons dans cette section à la sécurité des WLANs 802.11 dans le mode infrastructure. Au-delà de sa suprématie dans les déploiements actuels, ce mode est le plus pertinent pour l'opérateur réseau et le contexte spécifique des travaux de cette thèse. Nos commencerons par présenter des exemples d'attaques dans ces réseaux, puis s'en suivront les objectifs de sécurité généraux dans ces réseaux et enfin les solutions et contributions actuelles.

2.1.Quelques exemples d'attaques

Alors que la sécurité des WLANs à infrastructure pose relativement moins de défis techniques que celle des réseaux ad-hoc (en raison notamment de la présence d'un point fixe par lequel tous les trafics du réseau sans fil transitent et à partir duquel tous les mécanismes de contrôle sont appliqués), les WLANs à infrastructure ont pourtant fait l'objet avec leur développement exponentiel, d'innombrables attaques qui constituent encore aujourd'hui une menace sérieuse pour ceux qui utilisent ces réseaux et ceux qui les opèrent. Parmi les attaques les plus saillantes, on distingue:

- *L'écoute des communications* (en anglais, *eavesdropping* ou *sniffing* ou *snooping*): Dans ce type d'attaque, le nœud malveillant ou l'entité malveillante écoute le trafic du réseau dans l'espoir d'en extraire ou d'en déduire des informations de valeur. Ces informations sont très variées et peuvent par exemple concernées la localisation des points d'accès, leurs SSIDs (Service Set IDentifiers), des statistiques sur l'activité du réseau, les identifiants et les mots de passe des utilisateurs du réseau, les données (*e.g.* courriers, fichiers, etc.) transmises, etc. [IAW03] Cette attaque est facilitée par la nature du canal radio où les transmissions se font par diffusion.

- *L'accès non-autorisé*: Cette attaque consiste à accéder aux services du réseau sans en avoir les droits ou les privilèges. L'accès gratuit à Internet est la principale motivation de ceux qui mènent ce type d'attaque dans

les WLANs 802.11. Cette attaque est plus largement connue et répertoriée sous les appellations anglaises "war driving", "war walking", ou "war flying". [AUE05]

- *L'attaque par l'homme du milieu* (en anglais, *Man-In-The-Middle "MITM" attack*): Dans cette attaque l'entité malveillante injecte/modifie le trafic entre une station cliente légitime et un point d'accès légitime en se faisant passer tour à tour pour ces derniers. Les attaques par usurpation d'identités menées par des entités malveillantes sur le protocole ARP (Address Resolution Protocol) ou sur les paquets EAP (Extensible Authentification Protocol) de notification de succès de l'authentification en vue de faire transiter les trafics par elles, sont des exemples courants d'attaques de type MITM.

- *Le vol de session* (en anglais, *Session hijacking*): Dans ce type d'attaque, l'entité malveillante essaie de prendre le contrôle d'une session en cours ou de réactiver une session passée généralement en usurpant l'identité ou les privilèges du détenteur légitime de la session. Cette attaque peut par exemple se traduire par l'envoi d'une trame MAC 802.11 de dés-association (*i.e.* 802.11 MAC Disassociate) par une entité malveillante se faisant passer pour un point d'accès. Lorsqu'une telle trame est reçue par la station cliente victime, cette dernière abandonne de bonne foi la session en cours. L'entité malveillante peut ainsi récupérer cette session en se faisant passer cette fois-ci pour la station cliente victime.

- *Le rejeu* (en anglais, *Replay attack*): Dans cette attaque, l'entité malveillante retransmet/rejoue les paquets d'une session antérieure. C'est par exemple le cas lorsque l'attaquant rejoue les paquets d'authentification d'une session authentifiée passée dans le but d'accéder au réseau et à ses services.

- *La constitution de points d'accès voyous* (en anglais, *Rogue APs "Access Points"*): Cette attaque consiste pour l'entité malveillante, à se déclarer comme point d'accès. Lorsqu'une authentification mutuelle appropriée n'est pas mise en œuvre, cette attaque peut conduire des stations clientes légitimes à s'associer au point d'accès intrus et ainsi exposer leurs privilèges et autres données sensibles.

- *Le déni de service* (en anglais, *Denial of Service "DoS"*): Ce type d'attaque regroupe l'ensemble des actions malveillantes au niveau applicatif ou au niveau des couches inférieures visant à empêcher la fourniture régulière des services dans le réseau. Le brouillage du canal radio pour bloquer les transmissions, l'injection massive de paquets visant à épuiser les ressources des terminaux ou du réseau ou encore l'exploitation des vulnérabilités des protocoles en sont quelques exemples. La multiplicité des formes que peuvent prendre ces attaques fait qu'elles sont parmi les plus difficiles à contrer.

2.2. Objectifs généraux de sécurité

La sécurisation des communications dans les WLANs comme dans les réseaux filaires passent par la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs de sécurité généraux. Ces objectifs, lorsqu'ils sont suivis, peuvent concourir à établir des contre-mesures efficaces à l'immense majorité des attaques dans ces réseaux. On peut citer principalement parmi ces objectifs:

- *L'authentification*: Cet objectif de sécurité permet aux entités du réseau de s'assurer de la bonne identité ou du bon droit des entités avec lesquelles elles communiquent. Ainsi par exemple, l'infrastructure fixe peut avoir l'assurance que les stations clientes sont bien celles qu'elles prétendent être et inversement ou qu'elles ont bien les droits qu'elles prétendent avoir et inversement. La réalisation de cet objectif de sécurité va donc mettre en échec toutes les attaques procédant par des usurpations d'identité ou de rôle.

- *La non-répudiation*: Cet objectif de sécurité permet de prouver l'origine des données. Il est donc atteint lorsque tout émetteur de message dans le réseau ne peut nier avoir émis ledit message. Ainsi la non-répudiation va permettre d'identifier les entités malveillantes qui seraient tentées de commettre des actes répréhensibles pour ensuite ne pas les reconnaître. Cet objectif est essentiel dans les transactions commerciales en ligne, les opérations électroniques de facturation et plus généralement dans toutes les communications sensibles.

- *La confidentialité*: Cet objectif de sécurité garantit la non-divulgation des données transmises dans le réseau, à des parties non autorisées. La réalisation de cet objectif doit être systématique chaque fois que des données que l'on considère comme sensibles sont transmises; et ce, qu'il s'agisse de données des couches applicatives ou de données des couches inférieures.

- *L'intégrité*: Cet objectif de sécurité permet de s'assurer que les communications ne sont pas modifiées ou altérées par des entités non-autorisées. Ainsi, toute manipulation de données est détectée et les paquets correspondants invariablement rejetés. Il est cependant important de noter que dans les réseaux sans fil, un défaut d'intégrité n'est pas toujours synonyme de manipulation. En effet, bien des altérations sont le fait des conditions de propagation radio.

- *La disponibilité*: Cet objectif de sécurité garantit que toute entité autorisée puisse accéder aux ressources du réseau avec une qualité de service adéquate. La réalisation de cet objectif passe donc par l'élimination ou la réduction des effets des attaques de type DoS. Cela étant dit, la très grande variété des attaques par déni de

service dans les réseaux sans fil, fait qu'il est certainement bien plus difficile d'atteindre cet objectif que les autres objectifs.

Il est important de relever que les objectifs de sécurité généraux précédents peuvent revêtir des degrés d'importance divers selon le contexte spécifique d'utilisation des WLANs. Ainsi, un contexte militaire mettra en avant le fort besoin d'authentification, de confidentialité et d'intégrité alors qu'une utilisation commerciale grand public nécessitera de se focaliser sur l'authentification et la disponibilité des services. Il est donc indispensable d'adapter chaque solution à son contexte d'utilisation à travers une analyse approfondie intégrant toutes les spécificités contextuelles.

2.3. Solutions et contributions

Les solutions de sécurité dans les WLANs à infrastructure sont pour l'essentiel des solutions de déploiement (*i.e.* des solutions ayant fait l'objet d'une standardisation). Ces solutions s'articulent autour de 2 principales composantes que sont l'authentification et la gestion des clés. C'est ensuite à partir de ces 2 composantes qu'est amorcée la réalisation des principaux objectifs de sécurité (*e.g.* confidentialité, intégrité, etc.). Les organismes de standardisation comme l'IEEE et l'IETF ont dans cet esprit, développé des architectures et des protocoles de sécurité pour l'authentification et la gestion des clés dans les WLANs. Ces solutions peuvent être répertoriées suivant 2 catégories, à savoir, les solutions de la couche 2 qui sont intimement liées à la technologie correspondante et les solutions des couches supérieures moins dépendantes des technologies de la couche 2. Très logiquement donc, l'IEEE à l'origine des WLANs 802.11, a développé des solutions au niveau de la couche 2 du modèle de référence des réseaux alors que l'IETF s'est attaché à développer des solutions au niveau des couches supérieures. Les solutions de la couche 2 bien que dépendantes de la technologie correspondante sont réputées procurer, lorsqu'elles sont bien conçues, un niveau de sécurité plus élevé que celui des couches supérieures. En effet, les solutions de la couche 2 vont en général prévenir l'accès aux couches supérieures (*e.g.* couches IP, transport, session, etc.) et donc à l'immense majorité des services du réseau tant que l'authentification n'est pas réalisée avec succès. De manière générale, plus une solution de sécurité est élevée dans la pile réseau, plus le spectre des services accessibles est grand et donc plus celui des attaques possibles l'est aussi.

2.3.1. Solutions et contributions de la couche 2

Dans cette section nous passons en revue les solutions développées au sein de l'IEEE ainsi que quelques contributions annexes de la littérature.

- *L'architecture IEEE 802.1X*

L'architecture IEEE 802.1X [IEEE-802.1X] fixe un cadre effectif pour la réalisation de l'authentification des stations clientes, le contrôle de leur trafic vers le réseau protégé (*i.e.* l'infrastructure fixe dans le cas des WLANs) et la gestion des clés dans les LANs comme dans les WLANs de la famille IEEE 802. Cette architecture suppose l'utilisation du protocole d'authentification générique EAP (Extensible Authentication Protocol) [EAP] et supporte à ce titre toute la diversité de ses méthodes (*e.g.* OTP, CHAP, TLS, etc.). Le contrôle d'accès mis en œuvre par l'architecture 802.1X est basé sur la définition de ports logiques. Cette architecture spécifie en outre 3 entités logiques que sont: le Supplicant (*i.e.* la station cliente), l'Authenticator (*i.e.* le point d'accès) et l'AS (Authentication Server) qui est en général un serveur RADIUS (Remote Authentication Dial In User Service) ou Diameter. Il est également défini sous l'acronyme EAPoL (EAP Over LAN), un protocole dédié au transport des paquets EAP entre le Supplicant et l'Authenticator.

Les échanges initiaux commencent par une demande de connexion du Supplicant à l'Authenticator. L'Authenticator active alors un port ne permettant que le transit des paquets EAP vers l'AS; tous les autres trafics étant bloqués jusqu'à l'authentification réussie du Supplicant. Ce port que l'on dit non-contrôlé est nommé Uncontrolled Port. Une fois l'authentification achevée, l'AS informe l'Authenticator du succès ou de l'échec de cette authentification. En cas de succès, ce dernier active un port permettant au Supplicant d'accéder au réseau protégé. Ce port que l'on dit contrôlé est nommé Controlled Port.

Il est à noter que les concepts logiques définis dans l'architecture 802.1X peuvent être déclinés dans des scénarios de déploiement très divers. Ainsi par exemple, il peut exister plusieurs Authenticators dans le réseau, l'AS et l'Authenticator peuvent être séparés ou co-localisés, l'AS peut être complètement distribué à des fins d'équilibrage de charge, etc. La Figure 1 illustre l'architecture IEEE 802.1X et ses concepts logiques. La Figure 2 présente quant à elle la pile EAP dans le contexte 802.1X.

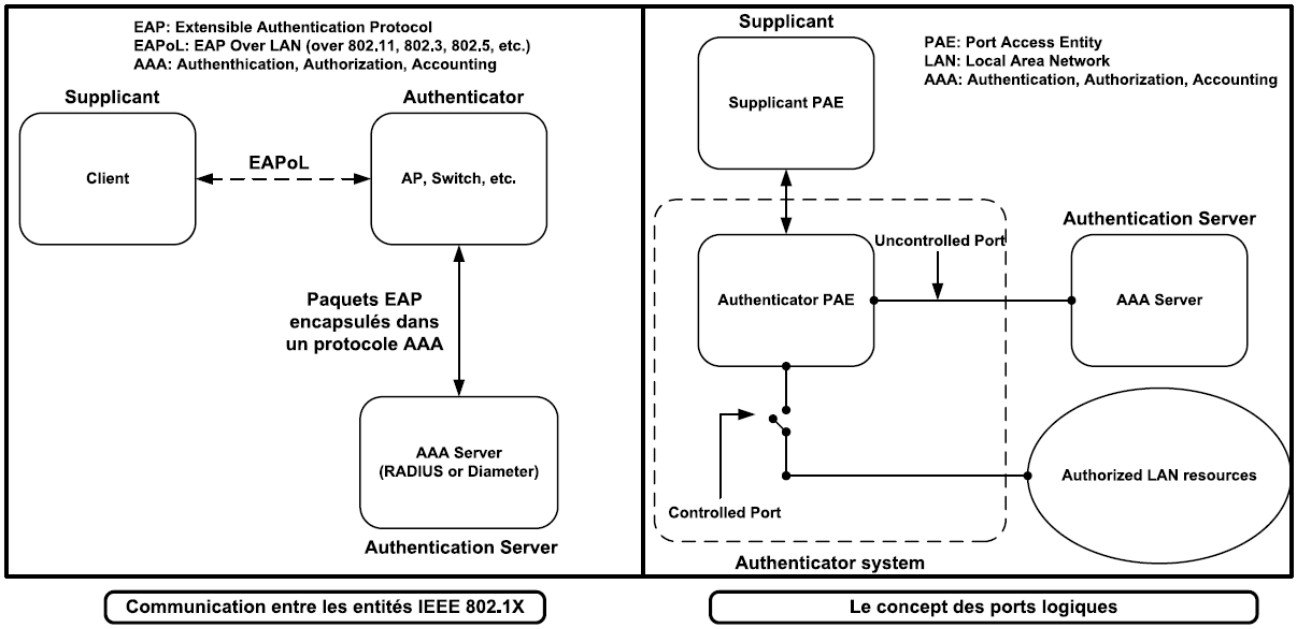
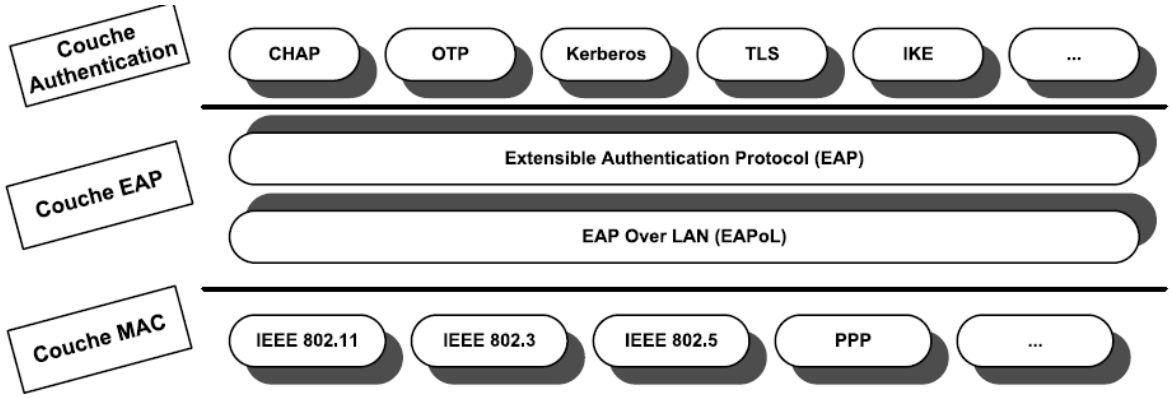


Figure 1: Architecture IEEE 802.1X



CHAP: Challenge Handshake Authentication Protocol

OTP: One Time Password

TLS: Transport Layer Security

IKE: Internet Key Exchange

PPP: Point to Point Protocol

Figure 2: Pile EAP dans l'architecture IEEE 802.1X

Sans spécifier la façon dont l'authentification est réalisée ou la façon dont les clés et les algorithmes cryptographiques sont définis, l'architecture 802.1X va donc principalement permettre l'acheminement de l'ensemble des données y afférentes. S'agissant plus spécifiquement des clés de chiffrement, le système 802.1X en distingue deux types: les clés de session qui sont partagées entre chaque Supplicant et l'Authenticator, et les clés de groupe qui le sont entre l'ensemble des Supplicants et l'Authenticator. Toutes ces clés sont renouvelées

aussi régulièrement que nécessaire afin de limiter les possibilités de leur compromission. Quant à l'authentification proprement dite, elle est déterminée à travers le choix d'une méthode EAP qui peut relever de l'authentification à clé secrète (*e.g.* Pre-Shared Key (EAP-PSK) [EAP-PSK], Lightweight Extensible Authentication Protocol (LEAP) [CISC02], Kerberos (EAP-Kerberos) [EAP-KER], Secure Remote Password (EAP-SRP) [EAP-SRP]), de l'authentification à clé publique (*e.g.* Transport Layer Security (EAP-TLS) [EAP-TLS]) ou encore de l'authentification à base de tunnel (*e.g.* Protected EAP (PEAP) [PALE04], EAP-Tunneled TLS (EAP-TTLS) [FUNK08]).

Au titre des faiblesses ou des limites du standard 802.1X, on relèvera, au-delà de l'absence de protection des paquets EAPoL qui crée des opportunités d'attaques par injection ou modification, l'inopérance de l'architecture correspondante dès lors que le Supplicant et l'Authenticator ne partagent pas le même support de transmission (*i.e.* ne sont pas sur un même lien).

- *Le standard IEEE 802.11i*

Le standard IEEE 802.11i [IEEE-802.11i] aujourd'hui intégré dans [IEEE-802.11] comprend principalement 3 composantes organisées en 2 plans. Sur le plan inférieur, sont introduits les algorithmes cryptographiques TKIP (Temporal Key Integrity Protocol) et CCMP (Counter mode with CBC-MAC "Cipher Block Chaining – Message Authentication Code" Protocol). Ces algorithmes qui permettent d'assurer l'intégrité et la confidentialité des données, viennent en remplacement du système WEP (Wired Equivalent Privacy) qui était utilisé jusque là et dont les vulnérabilités étaient plus que notoires [ARBA02] (*e.g.* il était désormais possible avec des analyseurs de trafic comme AirSnort ou WEPcrack de collectionner des messages chiffrés et de déduire en quelques heures la clé de chiffrement). Sur le plan supérieur, le standard 802.11i reprend l'architecture IEEE 802.1X de contrôle d'accès à base de ports logiques. L'architecture 802.1X donne au standard 802.11i un cadre de mise en œuvre de l'authentification et de la distribution des clés; cadre qui faisait défaut dans la spécification initiale des WLANs 802.11. À la différence du système WEP, où l'authentification et la protection des données étaient confondues, dans le standard 802.11i il y a une séparation claire entre le processus d'authentification et la protection des données qui interviennent en des temps et lieux différents. Ce sont donc ces 3 composantes (*i.e.* TKIP, CCMP, 802.1X) qui prises ensemble permettent de constituer des réseaux sécurisés robustes (en anglais, *Robust Security/Secure Network "RSN"*).

Dans ces RSNs, les paramètres de sécurité sont négociés entre chaque station cliente et le point d'accès. Pour ce faire, des structures de données appelées RSN IE (RSN Information Element) et contenant les paramètres de sécurité du réseau sont échangées. Cette négociation confère aux RSNs, une flexibilité suffisante pour permettre à chaque organisation de définir et d'appliquer dans son WLAN sa propre politique de sécurité. À titre d'illustration, une station cliente configurée pour utiliser l'algorithme CCMP peut en outre être instruite de s'associer ou de ne pas s'associer à un point d'accès utilisant l'algorithme TKIP pour ses messages de Broadcast.

Dans ce système, chaque point d'accès diffuse ses paramètres de sécurité (*i.e.* RSN IEs) à travers des balises appelées Beacons. Le point d'accès peut également annoncer ces paramètres dans un message *ProbeResponse* transmis en Unicast en réponse à une requête *ProbeRequest* émise par une station cliente. Les principaux paramètres de sécurité annoncés par les points d'accès concernent: (i) les suites cryptographiques relatives aux algorithmes assurant la protection des messages de Broadcast, (ii) les suites cryptographiques relatives aux algorithmes assurant la protection des messages Unicast, et (iii) les protocoles d'authentification et de gestion des clés. Une fois informée des paramètres de sécurité supportés dans le réseau, la station cliente choisit parmi ces paramètres, ceux qu'elle supporte et qui sont compatibles avec sa propre politique de sécurité. Ce choix est convoyé à l'intention du point d'accès dans la trame *AssociateRequest*. Si le choix effectué par la station cliente n'est pas conforme à la liste des protocoles communiquée par le point d'accès, l'association au réseau lui est refusée à travers une notification d'échec d'association contenue dans une trame *AssociationResponse*. Les messages échangés jusqu'ici entre le point d'accès et la station cliente sont non-protégés. La négociation pourra toutefois être authentifiée à l'issue de l'authentification - réussie - lors de l'échange des clés dans les messages *EAPoL-key*.

Les clés échangées à travers les messages *EAPoL-key* dans le standard 802.11i, sont issues d'une double hiérarchie des clés que sont: la hiérarchie des clés de protection du trafic Unicast (en anglais, *Pairwise Key Hierarchy*) et la hiérarchie des clés de protection du trafic de Broadcast (en anglais, *Group Key Hierarchy*). Ces 2 hiérarchies et les échanges de messages *EAPoL-key* sont illustrés sur les Figures 3 et 4 respectivement. Ces échanges de clés sont appelés dans la terminologie 802.11i, 4-Way Handshake (en raison des 4 messages qui le constituent) et Group Key Handshake pour les clés Unicast et Broadcast respectivement. Lors du 4-Way Handshake, plusieurs fonctions sont remplies: (a) le Supplicant et l'Authenticator s'assurent que l'un et l'autre possèdent bien la clé secrète maîtresse appelée PMK (Pairwise Master Key), (b) les clés temporaires utilisées pour la protection du trafic entre le Supplicant et l'Authenticator sont établies, (c) les paramètres de sécurité négociés sont authentifiés, (d) le premier échange de clés de groupe (*i.e.* le premier Group Key Handshake) est réalisé, et (e) les clés utilisées pour protéger les éventuels échanges ultérieurs de clés de groupe (*i.e.* les éventuels Group Key Handshake ultérieurs) sont obtenues. Il est à noter que le Group Key Handshake est dissocié du 4-Way Handshake uniquement lorsque des mises à jour de clés de groupe interviennent après le 4-Way Handshake. Autrement les clés de groupe sont transmises à travers les messages 3 et 4 du 4-Way Handshake.

La racine de la hiérarchie des clés du trafic Unicast est la clé PMK qui est transmise par le serveur d'authentification au point d'accès. Lorsque la méthode d'authentification par secret partagé (en anglais, *Pre-Shared Key*) est utilisée entre la station cliente et le serveur d'authentification, le standard 802.11i définit un mécanisme permettant de dériver la clé PMK à partir de ce secret. Dans tous les cas, la clé PMK est dérivée aussi bien au niveau du Supplicant que de l'AS. Une fonction pseudo-aléatoire prenant en entrée la clé PMK ainsi que d'autres paramètres (e.g. les adresses MAC du Supplicant et de l'Authenticator, un nonce généré par le

Supplicant "Snonce", un nonce généré par l'Authenticator "Anonce", etc.) permet de dériver la clé PTK (Pairwise Transient Key). Cette clé PTK est elle-même divisée en 3 clés que sont: (i) la clé KCK (EAPOL-Key Confirmation Key) utilisée pour assurer l'authenticité de l'origine et l'intégrité des messages *EAPoL-key*, (ii) la clé KEK (EAPOL-Key Encryption Key) utilisée pour assurer la confidentialité des messages *EAPoL-key*, et (iii) la clé TK (Temporal Key) utilisée pour assurer la confidentialité du trafic de données.

La racine de la hiérarchie des clés de groupe (*i.e.* hiérarchie des clés du trafic de Broadcast) est constituée par la clé GMK (Group Master Key). Cette clé est générée de manière aléatoire par le point d'accès (*i.e.* l'Authenticator). Elle est utilisée pour dériver la clé GTK (Group Temporal Key) qui est ensuite transmise aux stations clientes. Cette dérivation se fait par application d'une fonction pseudo-aléatoire prenant en entrée la clé GMK et des paramètres comme l'adresse MAC de l'Authenticator et un nonce généré par ce dernier.

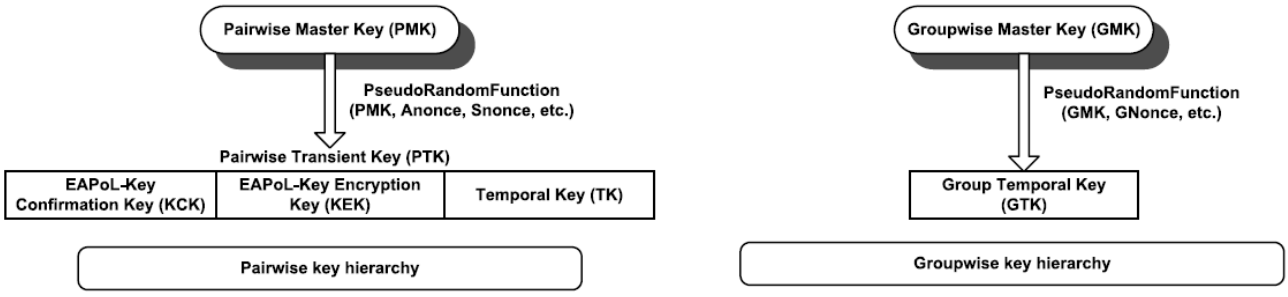


Figure 3: Hiérarchies des clés IEEE 802.11i

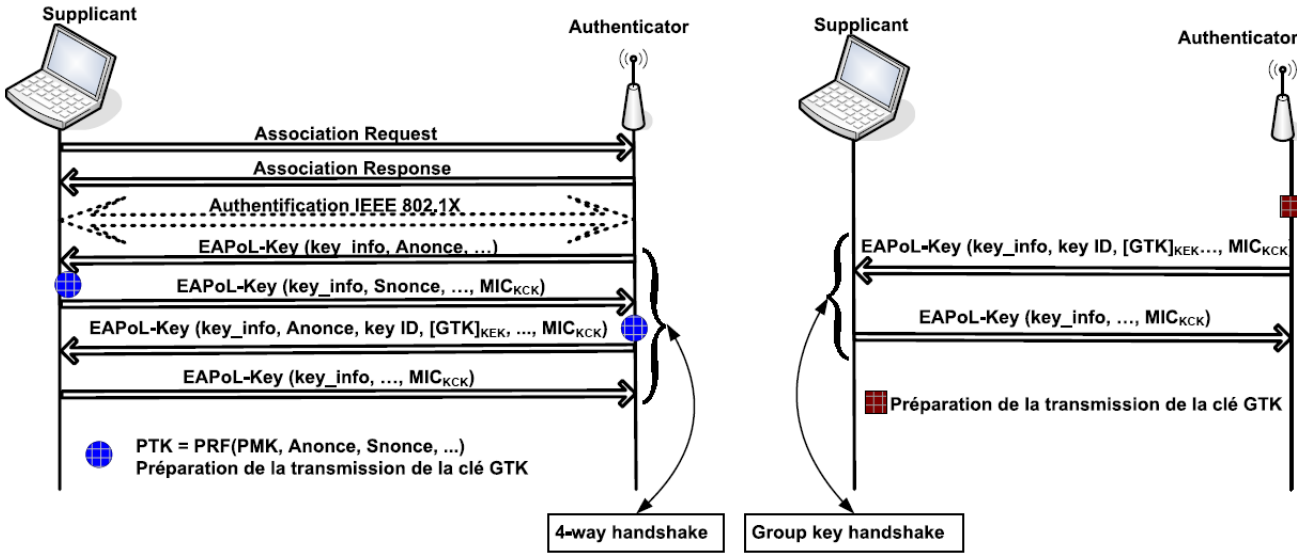


Figure 4: Dérivation et échange de clés IEEE 802.11i

Au rang des insuffisances du standard 802.11i on notera essentiellement les limites de la norme 802.1X (puisque 802.11i reprend cette dernière) avec ses messages non protégés et l'obligation pour le Supplicant et l'Authenticator d'être sur le même lien.

- *Contributions annexes*

Pour surmonter l'absence de protection des paquets EAPoL et toutes les attaques de type MITM ou DoS qu'elle entraine, il est proposé dans [MISH02], d'ajouter aux paquets de décision comme par exemple ceux transportant la notification du succès de l'authentification (*i.e.* EAP-Success), un code (*i.e.* MIC "Message Integrity Code" ou MAC "Message Authentication Code") permettant de s'assurer de leur authenticité et de leur intégrité. La clé utilisée pour générer ce code pourrait alors être une de clés générées par la méthode d'authentification EAP mise en œuvre. Une autre option recommandée dans cette analyse, est d'escamoter les notifications explicites de succès pour passer directement à l'échange de clés à travers les messages *EAPoL-key* qui eux sont mieux protégés.

L'analyse du 4-Way Handshake IEEE 802.11i réalisée dans [HE04] a permis de mettre en évidence des attaques possibles de type DoS à travers la falsification du premier message de cet échange (*i.e.* du 4-Way Handshake). Cette falsification est rendue possible puisque le premier message *EAPoL-key* du 4-Way Handshake ne bénéficie malheureusement pas de la protection (*i.e.* utilisation d'un MIC) qu'ont les messages *EAPoL-key* suivants. Les auteurs de cette analyse proposent en particulier diverses approches permettant de compliquer la tâche de l'attaquant.

Afin de rendre applicable la solution 802.11i dans des configurations ou la station cliente et le point d'accès ne sont pas sur le même lien (*i.e.* l'architecture du réseau est ad-hoc hybride), il est proposé dans [SHAE05] une approche de chiffrement et de gestion des clés 802.11i permettant à une station cliente après son association au point d'accès, de basculer en mode ad-hoc et de faire transiter de manière sécurisée son trafic vers le point d'accès par une autre station cliente. Bien qu'intéressante, cette contribution est toutefois limitée en ce qu'elle impose que l'association et la négociation des paramètres de sécurité 802.11i se fassent d'abord normalement avec le point d'accès avant tout basculement en mode ad-hoc. De plus, la solution proposée ne supporte qu'au plus une station relais entre la station cliente ayant basculé en mode ad-hoc et le point d'accès. D'autres contributions du même ordre ont été faites dans [MOU05] et [MOU06].

2.3.2. Solutions et contributions des couches supérieures

Les solutions et contributions passées en revue dans cette section sont dites des couches supérieures du fait qu'elles sont implémentées au niveau de la couche 3 (*i.e.* couche IP) ou des couches plus hautes. Les solutions les plus connues et les plus utilisées dans ce domaine sont standardisées au sein de l'IETF.

- *IPSec (IP Security)*

Parmi les solutions de niveau IP, nous avons la solution VPN (Virtual Private Network) IPSec (IP Security) [IPSEC] qui, même si elle n'avait initialement pas été conçue pour sécuriser les WLANs, est aujourd'hui une des plus répandues dans les WLANs d'entreprise. Sans rentrer dans les détails de l'architecture IPSec, on peut dire que cette solution arrive, lorsqu'elle est mise en œuvre de manière appropriée (*e.g.* choix approprié de la méthode d'authentification), à déjouer un grand nombre d'attaques répertoriées dans les WLANs et à apporter ainsi un niveau de sécurité élevé. On notera toutefois, au-delà de la complexité de mise en œuvre des associations de sécurité (*e.g.* multiplicité de paramètres et de combinaisons de paramètres), l'inopérance d'IPSec en l'absence d'un protocole de routage fiable lorsque les stations clientes sont à plus d'un saut IP du point d'accès: un état de fait qui n'est pas de nature à permettre l'utilisation d'IPsec dans des réseaux dynamiques souvent dépourvus de toute infrastructure de routage fiable. De plus, en supposant l'accès à nombre de services IP (*e.g.* DHCP, protocole de routage, etc.) et aux services des couches plus basses avant la mise en œuvre de l'authentification, IPSec créée des opportunités d'attaques contre ces services par des entités non-authentifiées.

- *PANA (Protocol for Carrying Authentication for Network Access)*

PANA (Protocol for Carrying Authentication for Network Access) [JAYA07] est un protocole en cours de développement au sein de l'IETF dédié à l'accès au réseau. Ce protocole assure le transport de l'authentification EAP (Extensible Authentication Protocol) [EAP] entre l'utilisateur et le réseau opérateur. Il ne spécifie donc pas la méthode d'authentification à utiliser mais en assure tout simplement le transport. Sa principale particularité est d'être mis en œuvre au-dessus des couches IP et UDP pour assurer l'indépendance par rapport aux couches inférieures, notamment la technologie physique utilisée à l'accès. PANA est conçu pour les réseaux filaires mais est aussi applicable dans les WLANs. Il est même utilisable dans certaines configurations ad-hoc hybrides de ces WLANs, notamment celles où le point d'accès relié à l'infrastructure fixe est séparé de la station cliente par plusieurs nœuds relais (voir Figure 5).

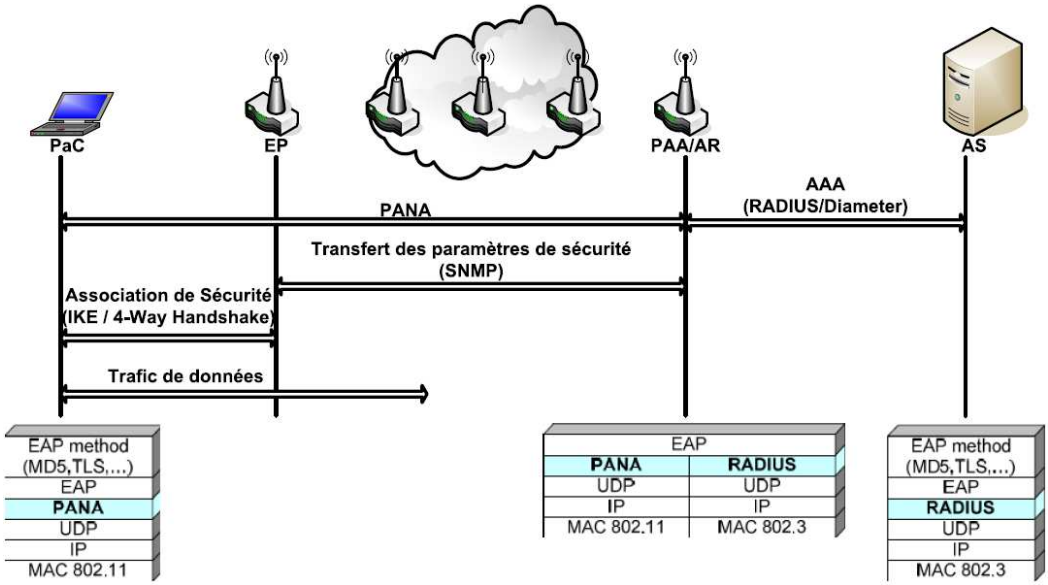


Figure 5: Exemple d'architecture PANA

PANA est exécuté entre le PaC (PANA Client) et le PAA (PANA Authentication Agent); ces 2 entités pouvant être à plusieurs sauts IP l'un de l'autre. Une autre entité appelée EP (Enforcement Point), éventuellement co-localisable avec le PAA, est chargée d'appliquer le contrôle d'accès. Afin de remplir efficacement ses fonctions, cette dernière entité ne peut être à plus d'un saut IP de la station cliente (*i.e.* PaC). Pour s'authentifier, le PAC doit d'abord découvrir l'adresse IP du PAA. Une fois cette adresse connue, l'authentification a lieu avec le serveur d'authentification (*i.e.* l'AS) à travers le PAA; le PAA et l'AS pouvant par ailleurs être co-localisés. Après l'authentification réussie du PAC, les attributs de sécurité du PAC sont transférés du PAA vers l'EP avec lequel une association de sécurité est établie (voir Figure 5).

Même si PANA apporte une certaine flexibilité de déploiement dans les WLANs (*e.g.* plusieurs sauts IP possibles entre le client (*i.e.* PaC) et point d'accès (*i.e.* PAA)), il reste que le premier nœud opéré du réseau, soit l'EP, est nécessairement fixe et ne peut être à plus d'un saut IP de la station cliente, ce qui rend PANA inapplicable dans un contexte dynamique où des stations clientes ne seraient pas sur le même lien que l'EP. De plus comme IPSec, PANA suppose l'accès avant l'authentification à bien des services des couches inférieures (couches MAC, réseau, transport, etc.).

- *Portails captifs*

D'autres solutions implémentées sur des couches encore plus hautes fleurissent chez les opérateurs de HotSpots. Ces solutions dont le principal attrait est la facilité de mise en œuvre sont pourtant très peu fiables. C'est le cas notamment des portails captifs qui autorisent l'accès jusqu'à la couche application avant toute authentification. Dans ces systèmes, le serveur d'authentification n'est généralement pas authentifié de

l'utilisateur. Quant à l'authentification de l'utilisateur, elle se fait en entrant un mot de passe sur une page Web. Une fois authentifié, l'adresse MAC ou l'adresse IP de l'utilisateur est inscrite dans une liste utilisée par l'AP pour contrôler les accès. Il suffit donc dans un tel système d'usurper l'adresse d'une station cliente authentifiée pour accéder au réseau. Il n'est même pas besoin de faire mention ici de toutes les possibilités d'attaques sur l'ensemble de la pile protocolaire offertes aux entités non-authentifiées.

- *Contributions annexes*

Une contribution visant à utiliser PANA dans des réseaux sans fil multi-sauts a été faite dans [CHEI06]. Les auteurs de ces travaux utilisent PANA pour permettre à des stations clientes d'un réseau ad-hoc d'accéder en multi-sauts aux services du réseau à infrastructure. Cette contribution s'affranchit en particulier de la nécessité d'avoir l'EP sur le même lien que le PaC. Ce faisant, cette proposition augmente la vulnérabilité de l'architecture PANA puisque toute la partie du réseau entre le PaC et l'EP est totalement incontrôlée. De plus, dans un tel contexte bien des options de sécurité de l'architecture PANA (*e.g.* utilisation des associations de sécurité de la couche 2) sont rendues caduques.

Des solutions d'authentification et de sécurité de niveau IP dans une architecture ad-hoc hybride sont proposées dans [ZHAN02] et [CARB04]. Les principes généraux de ces solutions sont soit de déléguer les fonctions du point d'accès ou du serveur d'authentification à certaines stations clientes (*i.e.* utilisation du concept de serveur mandataire ou de Proxy) dans un contexte d'utilisation de la cryptographie à clé publique, soit lorsqu'il n'y a pas de délégation, de fonder la sécurité du réseau sur celle du routage entre les stations clientes et le point d'accès. Ces solutions ont tout naturellement les faiblesses de leur choix d'implémentation (*i.e.* couches hautes).

3. La sécurité des réseaux véhiculaires

La sécurité des réseaux véhiculaires est encore aujourd'hui un champ d'investigation assez peu exploré. Nous présentons dans cette section un panorama des attaques, des enjeux et des contributions dans ce domaine. Mais avant, il est utile de revenir, au-delà des caractéristiques générales des réseaux véhiculaires (en termes de mobilité, de connectivité et de topologie) dont nous avons fait état dans le Chapitre 1.1, sur les caractéristiques applicatives de ces réseaux.

3.1. Caractéristiques applicatives

Il est attendu que les réseaux véhiculaires soient l'instrument de la fourniture d'une très grande variété d'applications au rang desquelles 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 suivant 2 grandes classes à savoir:

- *Les applications ITS (Intelligent Transportation System)*: Ce sont des applications liées à la sécurité routières (*i.e.* des applications impactant 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 l'accidentologie routière et d'améliorer les conditions de circulation. Ces applications ont constitué dans les différents travaux de recherche et projets gouvernementaux menés à travers le monde, le fondement premier du concept de réseau véhiculaire. Du point de vue du modèle de communication, on relève dans les applications ITS, une prééminence très prononcée du Broadcast ou du Multicast sur les autres formes de communication. Cette prééminence est bien sûr liée à la nature même de ces applications où les transmissions se font presque toujours à l'intention de tous ou d'un groupe. Parmi les exemples d'applications cités précédemment, les applications dites ITS pourront être: la conduite coopérative, l'aide aux dépassements de véhicules, les alertes accident, ralentissement, déviation, travaux, intempéries, etc.

- *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. Si ces applications ont émergées conceptuellement à la suite des applications ITS, leur mise en œuvre concrète a en revanche pris le pas sur les premières. Cette avance est principalement due à la préexistence d'un certain nombre d'infrastructures sur lesquelles ces applications sont déployées et à leur potentiel commercial beaucoup plus important. S'agissant du modèle de communication de ces applications, il n'est pas surprenant, compte tenu de leur accès plus discriminant, de constater la prééminence de l'Unicast. 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 Internet, les paiements automatiques, etc.

3.2. Attaques dans les réseaux véhiculaires

Nous donnons dans cette section, une classification générique des attaques recensées ou à venir dans les réseaux véhiculaires. Nous illustrons ensuite cette classification par quelques exemples concrets.

3.2.1. 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 dont certaines pourront même relever du terrorisme. A partir de la taxonomie introduite dans [RAYA05], nous définissons 4 grandes déclinaisons pour toute attaque dans ces réseaux:

- *Interne ou Externe*: Une attaque est dite interne si elle est instiguée 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 illégitime. 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 instiguée 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. A contrario, dans une attaque passive, l'attaquant ne fait qu'écouter et collecter le trafic pour une éventuelle utilisation malveillante ultérieure.

- *Indépendante ou Coordonnée*: 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 dessein se concertent pour la mener.

3.2.2. Exemples d'attaques

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

- *Attaque sur l'intimité numérique*: Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou 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 chaîne de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaîne de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat, etc. Au-delà des chaînes de caractères, l'empreinte radio de la victime peut également être utilisée: on parle alors d'attaque de la couche physique. La Figure 6 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*.

- *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 7 et 8 illustrent ce cas de figure. Sur la Figure 7 un attaquant diffuse des informations de trafic erronées et sur la Figure 8 des attaquants indiquent 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 7 est *Interne* ou *Externe*, *Intentionnelle*, *Active* et *Indépendante* alors que celle de la Figure 8 est *Interne* ou *Externe*, *Intentionnelle*, *Active* et *Coordonnée*.

- *Usurpation d'identité ou de rôle*: Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Figure 9 illustre un cas d'usurpation d'identité. L'attaque illustrée peut être *Interne* ou *Externe*, *Intentionnelle*, *Active* et *Indépendante*.

- *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 10 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*.

- *Ecoute 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 11 illustre une telle attaque dans laquelle l'attaquant espionne une transaction commerciale, typiquement un paiement électronique, en vue d'en extraire un mot de passe. Cette attaque peut être *Interne* ou *Externe*, *Intentionnelle*, *Passive* et *Indépendante*.

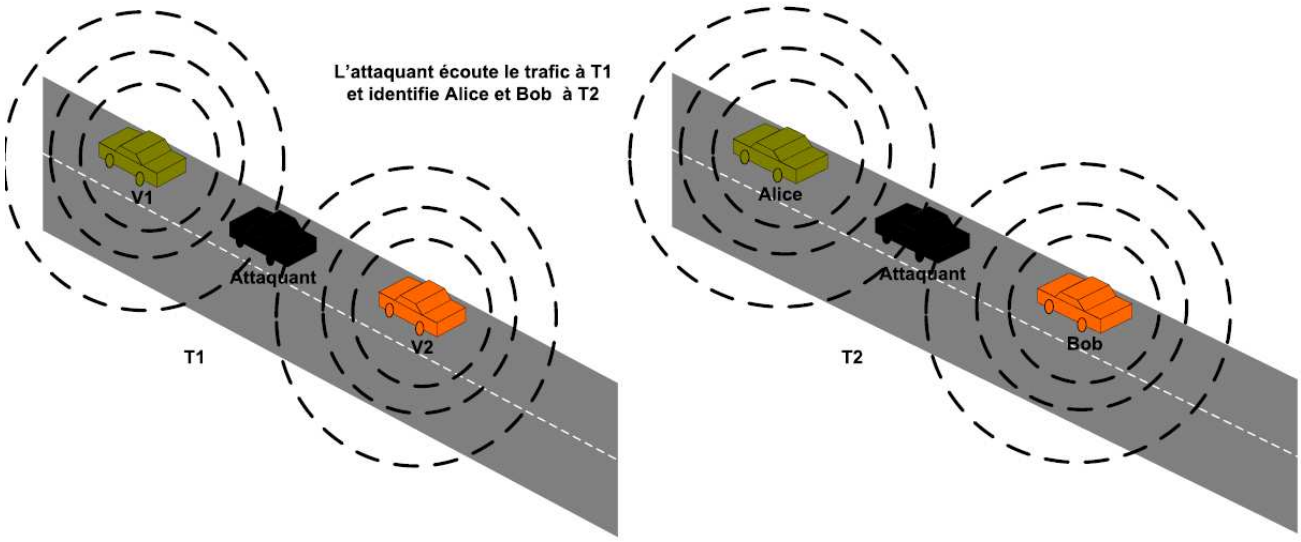


Figure 6: Identification non autorisée

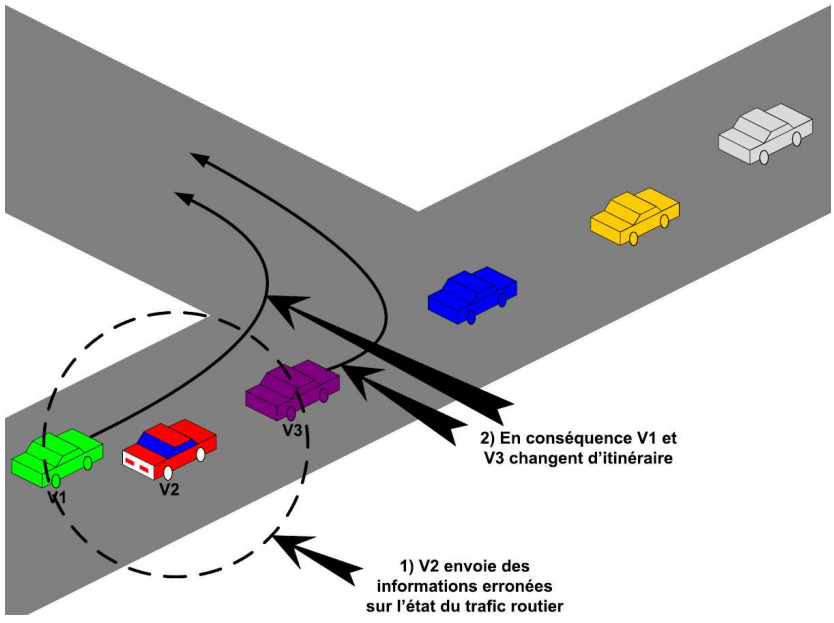


Figure 7: Injection d'informations de trafic erronées

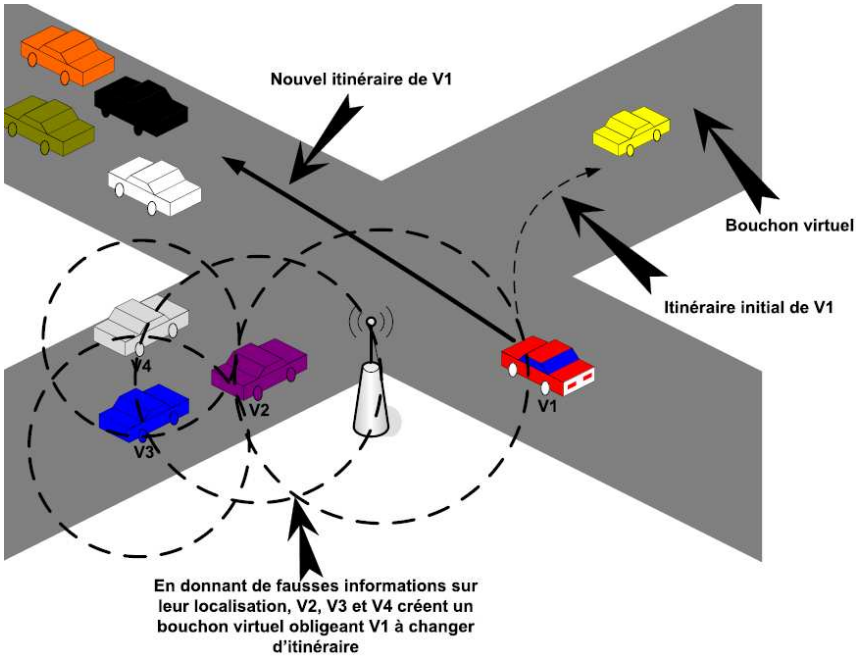


Figure 8: Fausses déclarations de localisation

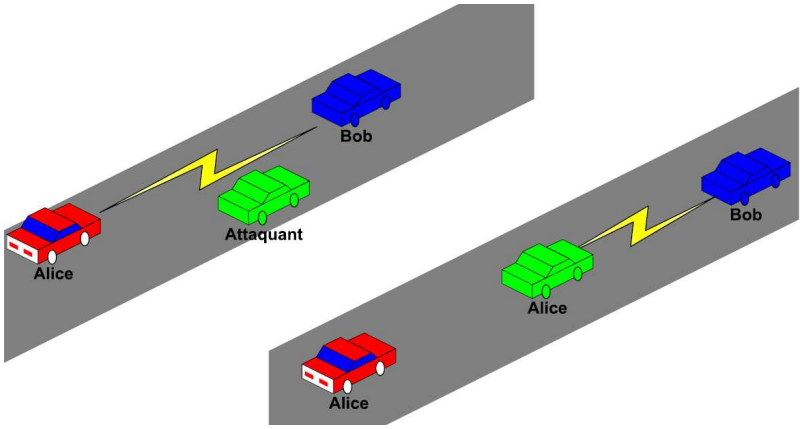


Figure 9: Usurpation d'identité

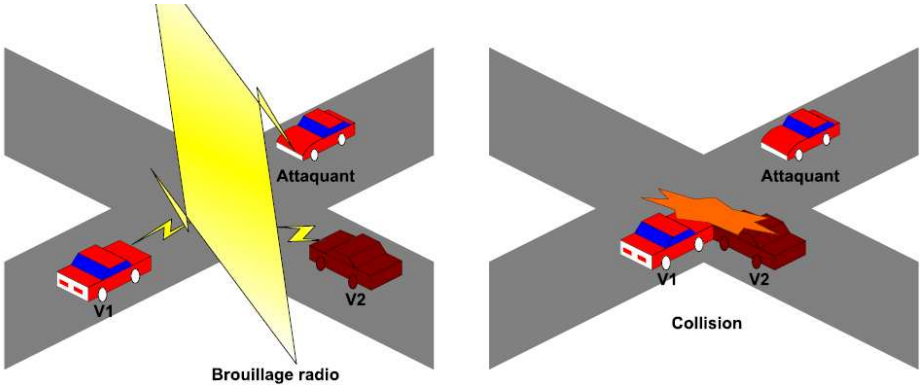


Figure 10: Déni de service par brouillage du canal radio

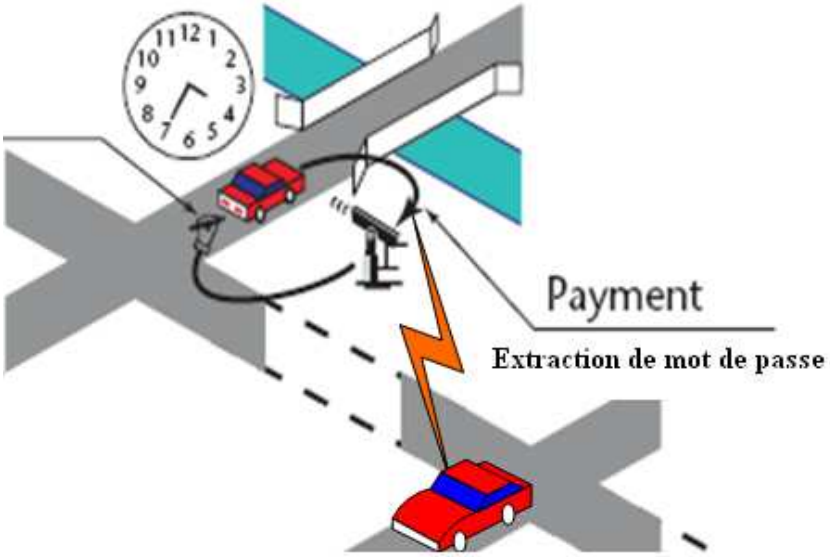


Figure 11: Extraction du mot de passe d'une transaction commerciale

3.3. Exigences et défis de sécurité

Nous présentons dans cette section les principales exigences de sécurité ainsi que les défis qui se posent à la sécurité dans un contexte d'opération des services ITS et non-ITS dans les réseaux véhiculaires. Ces exigences et ces défis sont définis pour être pris en compte aussi bien dans la conception architecturale de ces réseaux que dans la conception des protocoles de sécurité, des algorithmes cryptographiques et des implémentations matérielles et logicielles mis en œuvre dans ces réseaux. Au rang de ces exigences et défis de sécurité, on peut citer:

- *La confidentialité*: Les applications ITS ne peuvent atteindre leur objectif de prévention et de réduction des accidents de la route que si le maximum - si ce n'est la totalité - des véhicules coopèrent étroitement à leur

mise en œuvre. Il n'est donc, dans ce contexte, pas question de discriminer l'accès aux informations diffusées dans le réseau suivant que le véhicule est authentifié ou non. L'application du principe de confidentialité aux services ITS serait en effet contre-productive dans la mesure où les véhicules non authentifiés et donc ne pouvant déchiffrer ces services, feraient courir, du fait de leur non-information, un risque important d'accident aux véhicules authentifiés qui eux, peuvent déchiffrer ces services. A la différence donc des services non-ITS qui ont une vraie vocation commerciale et peuvent de ce fait appliquer la confidentialité pour assurer l'accès discriminé aux services, les services ITS doivent impérativement être accessibles à tous les véhicules du réseau qu'ils soient authentifiés ou non; et ce, dans l'intérêt de la sécurité de tous.

- *L'authentification de la source*: Une des principales restrictions, dans un contexte d'opération des services ITS, réside dans l'obligation pour toute entité générant et diffusant des messages ITS, d'y adjoindre une preuve d'authenticité (*e.g.* une signature). Cette restriction est faite pour éviter que des entités malveillantes ou non authentifiées puissent générer et diffuser des messages ITS sans qu'il soit possible d'en vérifier l'authenticité. Cette exigence de sécurité ne vaut que pour les services ITS dans la mesure où ils sont les seuls qui soient quasi-exclusivement régis par le modèle de transmission en Broadcast ou en Multicast.

- *La non-répudiation*: En raison de l'impact que peuvent avoir les applications ITS sur la sécurité des biens et des personnes, il est indispensable que toute entité générant ou modifiant des messages ITS soit toujours identifiable avec certitude. En d'autres termes, cette entité, après avoir émis un message, ne doit pas pouvoir ensuite nier cette action. Assurer la non-répudiation pour les services ITS, va donc éliminer toute possibilité pour une entité malveillante d'injecter des informations erronées et de causer éventuellement des accidents sans être confondue. S'agissant de la mise en œuvre de la non-répudiation, la signature numérique qui est majoritairement utilisée pour réaliser l'authentification entre des parties étrangères - l'une à l'autre - sans qu'il soit besoin de recourir à une entité de confiance en ligne, peut aussi la garantir. Pour ce faire, une signature doit être systématiquement ajoutée aux messages générés ou modifiés. A la différence des services ITS qui se distinguent par une exigence forte de non-répudiation, les services non-ITS peuvent s'en passer dans la plupart des cas; à l'exception notable de certains services non-ITS sensibles comme par exemple ceux impliquant des paiements.

- *L'authentification mutuelle, l'autorisation et le contrôle d'accès*: La nature commerciale ou transactionnelle des services non-ITS fait qu'il est nécessaire, plus qu'ailleurs, d'y appliquer le principe de l'authentification mutuelle, que ce soit entre les véhicules et l'opérateur réseau ou entre les véhicules uniquement. C'est en effet de cette authentification mutuelle que découle la mise en œuvre de l'autorisation et du contrôle d'accès. Par ailleurs, l'authentification mutuelle dont l'objet est d'assurer que les entités en communication sont bien

celles qu'elles prétendent être ou qu'elles ont bien les privilèges qu'elles prétendent détenir, va permettre de mettre en échec les attaques impliquant des usurpations de rôle ou d'identité. Une approche simple de mise en œuvre de l'authentification peut consister à utiliser des clés de groupe symétriques (en anglais, *Symmetric group keys*). Cette approche bien que facile à mettre en œuvre ne peut concerner malheureusement qu'un très petit nombre de véhicules placés sous la même autorité. Pour des déploiements à grande échelle, cette approche présente 2 inconvénients majeurs: (i) il suffit de compromettre un nœud pour compromettre la sécurité de tout le réseau et (ii) les nœuds ayant la clé peuvent se faire passer les uns pour les autres; ce qui empêche toute confidentialité et non-répudiation. Une autre approche d'authentification peut consister à utiliser des clés symétriques individuelles (en anglais, *Symmetric pairwise keys*) au lieu des clés de groupe. Seulement cette approche souffre d'une non-scalabilité intrinsèque puisque le nombre de clés à gérer augmente de manière linéaire avec le nombre de nœuds du réseau. Reste donc la cryptographie à clé publique qui, dans le contexte des réseaux véhiculaires, est seule à pouvoir permettre la réalisation de l'authentification tout en satisfaisant les exigences de scalabilité, de non-répudiation et de confidentialité. S'agissant du problème de la performance de la cryptographie à clé publique, il se pose moins dans le contexte des réseaux véhiculaires où des capacités matérielles importantes peuvent être attendues. De plus, avec les avancées réalisées ces dernières années dans le domaine de la cryptographie à clé publique, des choix avisés d'algorithmes peuvent permettre de réaliser des niveaux de performance élevés.

- *L'intimité numérique*: La sensibilité des individus quant à la préservation de leur intimité allant grandissante, il faudra leur assurer dans le contexte des réseaux véhiculaires, aussi bien pour les services ITS et que les services non-ITS, une forme d'anonymat et de non-traçabilité. Si l'anonymat est un concept simple garantissant la non-identification, la non-traçabilité est quant à elle un concept plus étendu recoupant diverses notions. Par exemple, violer la non-traçabilité d'un utilisateur U peut consister à répondre aux questions suivantes: (i) U communique avec qui ? (ii) U envoie quoi ? (iii) U utilise quelle application ? (iv) U se trouve où ? Et où va-t-il ? etc. Dans tous les cas, il est évident que l'anonymat et la non-traçabilité ne peuvent qu'être partiels; et ce, dans la mesure où l'exigence de non-répudiation doit également être garantie. De plus, les obligations légales de traçabilité et d'interception qu'ont les opérateurs vis-à-vis de l'autorité judiciaire doivent également être honorées. En définitive, la préservation de l'intimité numérique (*i.e.* anonymat et non-traçabilité) des utilisateurs du réseau véhiculaire ne peut être applicable que vis-à-vis des autres utilisateurs du réseau ou plus généralement vis-à-vis de toute autre entité autre que les opérateurs de ces réseaux et l'autorité judiciaire. La préservation de l'intimité numérique dans des environnements ouverts et dynamiques comme ceux des réseaux véhiculaires est d'autant plus complexe, que des éventuelles solutions, qui n'existent pas encore à ce jour, doivent aborder le problème de manière holistique en intégrant cette préservation dans toutes les phases de conception de ces réseaux et à tous les niveaux de la pile protocolaire.

- *Les contraintes temps réel*: Une des caractéristiques importantes des applications ITS est leur caractère temps réel et leur sensibilité aux délais. Il est par exemple montré dans [YAN04] que le délai de transmission critique d'un message ITS est de l'ordre de *100* ms. Il importe donc que les mécanismes de sécurité mis en œuvre dans les réseaux véhiculaires ne soient pas de nature à contrevenir à ces contraintes. Puisqu'il est attendu que les véhicules exécutant les services ITS, aient à faire plus de vérification de signatures que de génération de signatures, on peut par exemple choisir en priorité un crypto-système à clé publique rapide en vérification et n'ayant pas de très mauvaises performances en génération. Si on néglige les temps de calcul - ce que l'on peut légitimement faire puisque les véhicules sont supposées embarquer d'importantes ressources de calcul - alors on devra choisir en priorité le crypto-système à clé publique le plus compact et donc, induisant le moins de délai possible à la transmission. Dans tous les cas, le choix des mécanismes de sécurité à mettre en œuvre doit être optimisé pour tenir compte du défi posé par les contraintes temps réel des services ITS.

- *La cohérence des données*: Le caractère sensible des applications ITS impose que la cohérence des informations transmises dans le réseau soit garantie. Il est en effet souhaitable que des informations erronées, même lorsqu'elles proviennent d'entités régulièrement authentifiées dans le réseau, puissent être détectées. Il est tout à fait possible qu'une entité légitime puisse devenir malveillante en tentant d'influer sur le trafic routier ou en essayant de causer des accidents. Divers mécanismes permettant d'avoir une certaine assurance de la cohérence des informations ont été proposés. C'est par exemple le cas de ceux qui consistent à corréler l'information initiale avec les informations reçues d'autres sources en s'appuyant sur un système de réputation ou de recommandation. D'autres approches consistent à rechercher une explication plausible à l'information reçue à partir d'un modèle de connaissance du réseau [GOL04].

- *L'intégrité*: Cette exigence de sécurité apporte l'assurance que les données transmises ne sont pas altérées. Elle s'applique aussi bien aux services ITS qu'aux services non-ITS. Elle est en pratique mise en œuvre de manière concomitante avec l'authenticité.

- *La disponibilité*: Les services du réseau véhiculaire, qu'il s'agisse des services ITS ou non-ITS, doivent être disponibles en toute circonstance pour les véhicules légitimes les sollicitant. Pour assurer cette continuité du service, le réseau véhiculaire doit pouvoir résister le plus possible aux attaques de déni de service (*e.g.* brouillage du canal radio, saturation des ressources du réseau, comportements non coopératifs, etc.). La très grande diversité des attaques de déni de service, fait de la disponibilité un des enjeux de sécurité les plus complexes. Cela étant, l'exigence de disponibilité peut être mise en œuvre en implémentant par exemple des solutions contre les comportements non coopératifs (*e.g.* surveillance du réseau, système de réputation,

etc.), contre les brouillages ou surcharges des canaux radio (*e.g.* basculement entre canaux, radio cognitive, etc.), et plus généralement contre toutes les attaques de type DoS les plus importantes.

- *La forte mobilité*: La forte dynamique des nœuds des réseaux véhiculaires constitue un défi majeur à relever dans la conception des mécanismes de sécurité à mettre en œuvre dans ces réseaux. Si les plateformes embarquées dans les véhicules peuvent être assimilées, du point de vue du potentiel énergétique et des capacités de calcul, aux stations fixes du réseau filaire, il reste qu'à la différence de ces stations fixes, elles sont plus contraintes dans leur connectivité et leur débit. C'est une des raisons pour lesquelles la plupart des protocoles de sécurité des réseaux filaires s'avèrent inadaptés dans les réseaux véhiculaires où il est davantage besoin de protocoles compacts dont l'exécution est rapide. Ainsi par exemple dans des protocoles comme SSL/TLS, DTLS, WTLS on préférera à la place du légendaire crypto-système RSA [RSA78], l'utilisation du crypto-système NTRU [NTRU] pour sa rapidité d'exécution et plus encore du crypto-système ECC (Elliptic Curve Cryptography) [ECC87] pour son caractère compact. Dans les systèmes cryptographiques symétriques, on pourra également préférer aux protocoles DES et 3DES, le protocole AES pour sa relative rapidité et son niveau de sécurité supérieur. Des optimisations visant à accroitre la rapidité d'exécution peuvent également être faites par un choix avisé des implémentations matérielles ou logicielles des algorithmes cryptographiques. Il peut être aussi utile dans cette quête de rapidité, de définir des politiques de chiffrement qui soient fonction de la nature des données à chiffrer. Ainsi par exemple, il ne sera pas nécessaire de chiffrer tous les paquets d'un flux vidéo mais uniquement certains paquets essentiels au visionnage du flux. Adapter des protocoles de sécurité aux réseaux véhiculaires peut aussi se traduire par un choix avisé de la couche transport sur laquelle ces protocoles sont implémentés. Ainsi par exemple, au protocole TLS (Transport Layer Security) [TLS] dont l'implémentation est faite au dessus de TCP (Transmission Control Protocol) - un protocole de transport fiable inadapté dans un contexte de transmission erratique -, il sera préféré le protocole DTLS (Datagram TLS) [DTLS] qui lui, est implémenté sur UDP (User Datagram Protocol), un protocole de transport plus tolérant aux pertes.

Alors que le défi de la forte mobilité s'impose à tous les services des réseaux véhiculaires, on relève toutefois que ces services appellent des exigences de sécurité plus ou moins différentes. La Figure 12 illustre cet état de fait en soulignant les similitudes et les différences entre les principales exigences et les principaux défis de sécurité dans les réseaux véhiculaires.

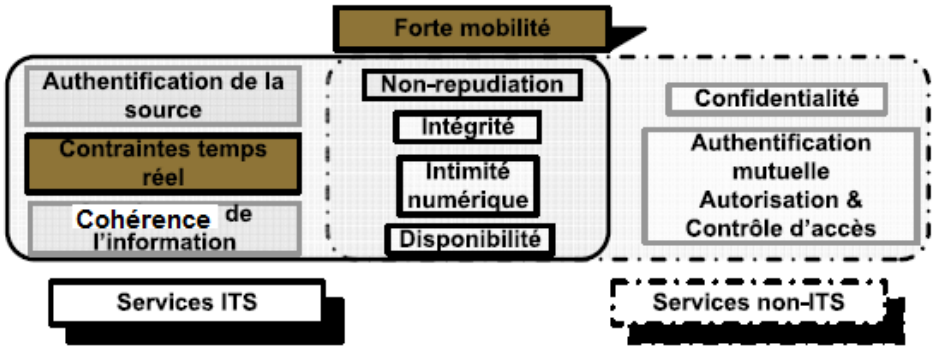


Figure 12: Principaux défis et exigences de sécurité des réseaux véhiculaires

3.4. Solutions et contributions

La sécurité spécifique 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. Les principaux travaux dans ce domaine sont pour l'essentiel axés sur la sécurité des services ITS. Ce faisant, ils ne donnent pas de perspective globale intégrant à la fois la sécurité des services ITS et la sécurité des services non-ITS.

Dans [ZAR02], il est proposé une architecture de sécurité pour les services ITS dans les réseaux véhiculaires. Cette architecture suppose une architecture réseau dépourvue de toute infrastructure de routage et ne s'appuyant que sur des communications en Broadcast à sens unique des stations de base vers les véhicules. La sécurité des échanges est assurée par des signatures dont les clés sont fournies par une PKI (Public Key Infrastructure). De plus, les contraintes temps réels des services ITS sont prises en compte dans les mécanismes de sécurité mis en œuvre. Cette proposition souffre cependant de nombreuses faiblesses dont son modèle de communication restrictif (*i.e.* le sens de la communication se fait uniquement des stations de base vers les véhicules), l'absence de prise en compte des problématiques d'intimité et des problématiques d'opérateurs (*e.g.* authentification avec l'opérateur ou le fournisseur de service, sécurité des services non-ITS, etc.). Toutes ces faiblesses ne permettent pas d'envisager la solution proposée dans une perspective de déploiement.

L'intimité numérique dans un contexte d'opération des services ITS est plus spécifiquement traitée dans [HUB04]. Il y est introduit une métrique pour l'intimité appelée entropie d'anonymisation. Des recommandations pour l'utilisation de la cryptographie à clé publique ainsi que des recommandations de mécanismes de vérification de la localisation sont également faites. Le principal intérêt de ces travaux est d'introduire des mécanismes notamment des mécanismes d'anonymisation utilisables par extension dans la plupart des services des réseaux véhiculaires.

Dans [BLUM04] une architecture de sécurité comprenant une PKI, un système de détection d'intrusion (en anglais, *Intrusion Detection System "IDS"*) et une infrastructure de routage sécurisée, est proposé pour les VANETs. Bien que ces travaux s'efforcent de prendre en compte les exigences de sécurité des services ITS et

des services non-ITS, les mécanismes proposés restent assez éloignés des problématiques opérateurs puisque n'envisageant prioritairement que des réseaux ad-hoc purs.

Les travaux réalisés dans [RAYA05] et [RAYA07] proposent un modèle d'analyse des attaques dans les réseaux véhiculaires ainsi qu'une architecture de sécurité pour les services ITS. Une PKI, des clés publiques anonymes et divers protocoles de révocation des certificats sont spécifiés. Ces contributions souffrent toutefois de ne pas s'inscrire dans un contexte de réseau opéré - ce qui occulte toute perspective de déploiement par des opérateurs - et plus encore, 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 [MOU06], une architecture de sécurité opérateur s'appuyant sur une PKI et le protocole EAP-Kerberos est étudiée. Cette architecture dont l'objet premier est de permettre la fourniture sécurisée de services non-ITS dans un réseau véhiculaire, ambitionne également de sécuriser les applications ITS. Une des insuffisances de cette contribution est l'absence de prise en compte de la mobilité dans la définition des associations de sécurité avec les points d'accès (*i.e.* les services sont constamment interrompus puisque de nouvelles associations de sécurité doivent être définies chaque fois qu'un véhicule change de point d'accès).

Dans le cadre du projet NOW (Network On Wheels) [NOW], les études publiées dans [GERL07], introduisent une architecture de sécurité pour les communications véhiculaires et en particulier les services ITS. Cette architecture intègre diverses composantes dont une composante pour l'enregistrement des véhicules, une composante pour la certification, une composante pour la révocation des certificats, une composante pour l'authentification, une composante pour la gestion de l'intimité et en particulier des pseudonymes, une composante pour la gestion de l'intégrité des données, une composante pour l'évaluation de la cohérence des informations, etc. Au-delà de cette contribution architecturale d'intégration, il est proposé dans [HAR08] 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. De manière générale, les solutions développées dans le cadre de ces travaux et plus largement dans le cadre du projet NOW intéressent davantage des réseaux véhiculaires spontanés que des réseaux véhiculaires opérés.

A l'image du projet NOW, des travaux sur la sécurité des réseaux véhiculaires sont également menés dans le consortium C2C-CC (Car2Car Communication Consortium) [C2C-CC], le projet SEVECOM (SEcure VEhicular COMmunications) [SEVECOM] et le groupe de travail IEEE P1609.2 [IEEE-P1609.2]. Tous les efforts menés dans ces différentes structures fondent la sécurité des réseaux véhiculaires sur l'utilisation des PKIs et des signatures numériques. Cependant, ils ne s'intéressent bien souvent qu'à la sécurité des applications ITS; le rôle de l'opérateur en tant que fournisseur de services et pilier de la confiance et de la sécurité, étant la plupart du temps ignoré.

3.5. Discussion

Arrivé au terme de la présentation de la sécurité dans les réseaux véhiculaires, il est intéressant de constater la diversité des exigences de sécurité qui s'y déclinent. On note par exemple la possibilité pour tous les véhicules du réseau d'accéder aux services ITS, alors que les services non-ITS ne seront généralement accessibles que des utilisateurs ayant souscrit un abonnement. On constate malheureusement à l'aune des efforts actuels qu'une vision architecturale globale intégrant la sécurité des services ITS et celle des services non-ITS fait défaut. En effet la plupart des contributions dans le domaine de la sécurité des réseaux véhiculaires ne traitent que de la sécurité des services ITS. Nous pensons pourtant que les services non-ITS, sans être à l'origine du concept des réseaux véhiculaires, constituent du fait de leur potentiel commercial, une des incitations les plus fortes au déploiement de ces réseaux.

En résumé, nous pensons que la sécurité des réseaux véhiculaires, au-delà de l'adaptation aux caractéristiques de mobilité, de connectivité, de topologie et d'échelle de ces réseaux, doit pouvoir se décliner en toute transparence aussi bien pour les services ITS que les services non-ITS. Dans cette déclinaison nous entendons donner une position centrale de mise en œuvre à l'opérateur afin de hâter l'avènement de ces réseaux. Pour ce faire, il est par exemple nécessaire de définir de nouveaux mécanismes d'authentification avec l'opérateur - compatibles avec des réseaux hautement dynamiques s'appuyant sur une technologie de type WLAN comme la technologie 802.11p [IEEE-802.11p] - à partir desquels va être fondée la sécurité de l'ensemble des services du réseau. De tels mécanismes ne sont aujourd'hui répertoriés dans aucune des contributions que nous avons explorées.

4. Conclusion

Nous avons présenté dans ce chapitre les attaques et les mécanismes de sécurité mis en œuvre dans les réseaux sans fil et en particulier dans les WLANs 802.11. Des insuffisances dans ces mécanismes ont été constatées, notamment leur inadéquation dans des environnements dynamiques où les stations clientes ne sont pas toujours nécessairement sur le même lien ou à un saut du premier nœud fixe opéré, leur propension à laisser libre accès à nombre de services du réseau lorsqu'ils sont implémentés sur les couches hautes, etc. Des contributions visant à pallier ces insuffisances ont été aussi relevées. Ces contributions restent toutefois peu flexibles (*e.g.* association directe préalable entre la station cliente et le premier nœud opéré, pas plus de 2 sauts entre la station cliente et ce nœud) ou alors tendent à altérer le niveau de sécurité du réseau (*e.g.* insécurité de la partie du réseau entre la station cliente et le premier nœud opéré, impossibilité de la mise en œuvre des associations de sécurité de la couche 2).

Nous intéressant plus spécifiquement à la sécurité des réseaux sans fil dans le contexte des réseaux véhiculaires, nous avons montré à travers le prisme de leurs caractéristiques spécifiques - notamment leurs caractéristiques applicatives - 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. Ces différents défis et exigences de sécurité ont été passés en revue en mettant chaque fois en lumière quelques pistes susceptibles de concourir à leur mise en œuvre. S'agissant des contributions dans ce domaine, nous avons noté de manière générale l'absence d'un modèle de sécurité global intégrant les problématiques de sécurité de l'ensemble des services des réseaux véhiculaires (*i.e.* services ITS et services ITS). De plus, ces contributions ne s'inscrivent généralement pas dans un schéma architectural d'opérateur de réseau ou de service et par conséquent n'adressent pas les problématiques associées. C'est ainsi par exemple que la problématique essentielle de l'authentification pour l'accès au réseau et aux services, est bien souvent ignorée. Nous pensons pourtant qu'investir les opérateurs dans les prochaines générations des réseaux véhiculaires (*e.g.* DRSC/802.11p) en leur donnant la possibilité d'y opérer aussi bien des services purement commerciaux que des services ITS, est un élément incitatif susceptible d'accélérer la concrétisation et le déploiement de ces réseaux.

C'est donc dans ce contexte que nous allons définir dans le chapitre qui va suivre, des architectures et des protocoles pour l'authentification dans les réseaux véhiculaires opérés s'appuyant sur une technologie de type WLAN. Ces architectures et ces protocoles sont conçus pour seoir à l'ensemble des caractéristiques spécifiques de ces réseaux.

Partie II

Chapitre 2.1. Architectures et Protocoles pour l'Authentification dans les Réseaux Véhiculaires

1. Introduction

L'adoption et le déploiement des réseaux véhiculaires aussi bien par les acteurs de l'industrie automobile que par les opérateurs réseaux passent par le développement de mécanismes de sécurité appropriés assurant en particulier l'authentification et l'autorisation des entités communicantes. Ainsi, seules les entités dont la légitimité est démontrée peuvent avoir accès aux ressources et aux services du réseau. Du point de vue de l'opérateur réseau, l'authentification est une étape centrale dans le processus d'autorisation d'accès aux services et dans l'établissement de la sécurité des communications dans le réseau. Dans ce contexte, rester en droite ligne des exigences de sécurité (dans les réseaux véhiculaires) illustrées dans le Chapitre 1.2 et donc tenir compte de la diversité de ces exigences, impose que la nature des services auxquels l'accès est demandé soit prise en compte dès la phase d'authentification.

Comme souligné dans l'étude des contributions existantes dans le domaine de la sécurité des réseaux véhiculaires, les efforts de recherche ont surtout porté sur la sécurité des applications/services ITS (Intelligent Transportation System) et/ou sur des architectures de réseaux véhiculaires ad-hoc isolés. Cette vision architecturale restrictive du réseau ne permet pas d'envisager les problématiques AAA (Authentication, Autorisation, Accounting) avec l'opérateur réseau ou le fournisseur de service dans le contexte particulier des réseaux véhiculaires marqué par une forte dynamique des nœuds du réseau, une connectivité intermittente, une grande étendue du réseau, une diversité des modèles et des enjeux de sécurité suivant la typologie des services, etc. Ce faisant, les opportunités de déploiement portées par les services commerciaux et plus globalement par les services non-ITS, s'en trouvent annihilées alors même qu'elles constituent un des leviers les plus puissants pour pousser à la mise en œuvre de l'infrastructure réseau sous-jacente.

Pour répondre aux défis précités dans la perspective du déploiement des réseaux véhiculaires opérés, nous présentons dans ce chapitre une architecture de sécurité fondée sur la différenciation entre les services ITS et les services non-ITS et augmentée de protocoles réalisant l'authentification et la délivrance de lettres de créance. Nous illustrons un modèle d'authentification et de délivrance des lettres de créance novateur s'appuyant sur un transport multi-sauts des paquets, implémenté au dessus de la couche 2 du modèle de référence des réseaux. Notre solution comprend globalement 4 composantes à savoir:

- Une architecture réseau illustrant les rôles et fonctions des différentes entités qui la constituent.
- Une infrastructure de confiance et de sécurité traduisant différentes relations de confiance et de sécurité entre les entités qui la constituent.
- Un protocole d'authentification et de délivrance des lettres de créance baptisé AUCRED (AUthentication and CREDentials delivery protocol).
- Un protocole de transport multi-sauts des paquets d'authentification nommé EGEMO (EAP Geographic and positioning Encapsulation for Multi-hOp transport).

Pour ce qui est de l'organisation de la suite de ce chapitre, nous commencerons par présenter dans la section 2 les principales exigences de sécurité ainsi que les défis que notre solution se propose d'adresser ou tout au moins de tenir compte. Dans la section 3, nous présenterons notre solution proprement dite, à savoir les architectures et les protocoles associés pour l'authentification. Enfin, la section 4 conclura le chapitre.

2. Exigences de sécurité et défis à relever

L'ambition de notre solution pour l'authentification est d'intégrer ou de tenir compte d'un certain nombre d'exigences de sécurité susceptibles de seoir, dans une perspective de déploiement, au contexte particulier des communications véhiculaires, aux utilisateurs et aux opérateurs. Ainsi, nous avons retenu les principales exigences de sécurité suivantes:

- *Authentification mutuelle et autorisation*: L'accès aux ressources et aux services du réseau ne doit se faire qu'à l'issue de l'authentification mutuelle entre le client (*i.e.* le véhicule) et le serveur d'authentification (*i.e.* le serveur AAA) de l'opérateur. De plus, le client doit pouvoir obtenir du serveur AAA, les autorisations nécessaires à la jouissance des services dont l'accès est discriminé suivant la nature des souscriptions engagées auprès de l'opérateur.

- *Sécurité des données d'authentification*: Les données d'authentification ne requièrent pas systématiquement une assurance de confidentialité sauf lorsque des clés secrètes ou des données dévoilant l'intimité sont transmises. Les paquets d'authentification seront par conséquent convoyés en clair dans le réseau la majeure partie du temps. En revanche, il est indispensable de mettre en œuvre un contrôle d'intégrité sur les données d'authentification de manière à parer à toute modification ou altération malveillante.

- *Intimité numérique (*en anglais, *privacy)*: L'exigence de préservation de l'intimité numérique recouvre les concepts de non-traçabilité et de préservation de l'anonymat. Ces concepts constituent une exigence de sécurité essentielle dans les réseaux véhiculaires. Ils doivent cependant être conditionnels afin qu'il soit

possible de les lever pour satisfaire les requêtes judiciaires, les réglementations liées aux interceptions légales ou encore l'exigence de non-répudiation de certaines applications. En tout état de cause, il est exclu que l'intimité numérique d'un utilisateur du réseau véhiculaire puisse être mise à mal par d'autres utilisateurs du réseau ou des entités extérieures au réseau. Les mécanismes d'authentification doivent donc dans ce contexte être mis en œuvre en assurant au mieux l'anonymat et la non-traçabilité de chaque client vis-à-vis d'entités extérieures ou d'autres clients.

En raison des caractéristiques particulières des réseaux véhiculaires (forte mobilité, étendue potentielle du réseau, nature des services mis en œuvre, etc.) notre solution est en outre tenue de relever un certain nombre d'exigences ou de défis qui s'expriment en termes de:

- *Contraintes temps réel*: Au-delà des services non-ITS, les réseaux véhiculaires sont surtout appelés à opérer des services ITS, lesquels présentent des contraintes temps réel évidentes dont il est important de tenir compte dès la phase d'authentification. En effet, si on considère que les services ITS comme les autres services, ne peuvent être opérés qu'à l'issue du processus d'authentification, alors il importe que ce processus soit aussi rapide que possible pour permettre l'opération des services ITS sensibles comme les services d'alerte. Pour ce faire, le processus d'authentification doit recourir aux crypto-systèmes à la fois compacts et rapides mais aussi s'appuyer sur des choix généraux de conception les moins couteux possibles en termes de latence.

- *Haute disponibilité*: Cette qualité peut être traduite en termes d'exigence de sécurité ou encore de défi à relever dans le contexte spécifique des réseaux véhiculaires. Du point de vue de la sécurité, l'exigence de haute disponibilité assure que la solution proposée soit résistante aux attaques de type déni de service (en anglais, *Denial of Service (DoS)*) orchestrées par une ou plusieurs entités malveillantes. Il peut s'agir par exemple d'attaques visant à épuiser les ressources du serveur d'authentification et donc rendre inopérant l'accès aux ressources et aux services du réseau. Assurer la haute disponibilité dans le contexte spécifique des réseaux véhiculaires marqué par une forte mobilité des nœuds et une étendue potentielle considérable, suppose aussi que soit relevé le défi de permettre au plus grand nombre de véhicules de s'authentifier (et donc d'accéder aux ressources et services du réseau) efficacement indépendamment de leur localisation. Si on considère par exemple des réseaux véhiculaires caractérisés par une portée de transmission relativement réduite, relever le défi de la haute disponibilité peut se traduire par des choix architecturaux de communication permettant aux véhicules situés au-delà de la portée de transmission des points d'accès, de pouvoir néanmoins communiquer avec ces derniers. De tels choix peuvent s'avérer d'autant plus incontournables que l'on suppose un déploiement restreint des points d'accès et que par conséquent les

véhicules seront la plupart du temps en dehors de la zone de couverture des points d'accès qu'à l'intérieur de cette zone de couverture.

La Figure 1 résume et illustre les principales exigences de sécurité ainsi que les défis généraux que notre solution se propose d'intégrer.

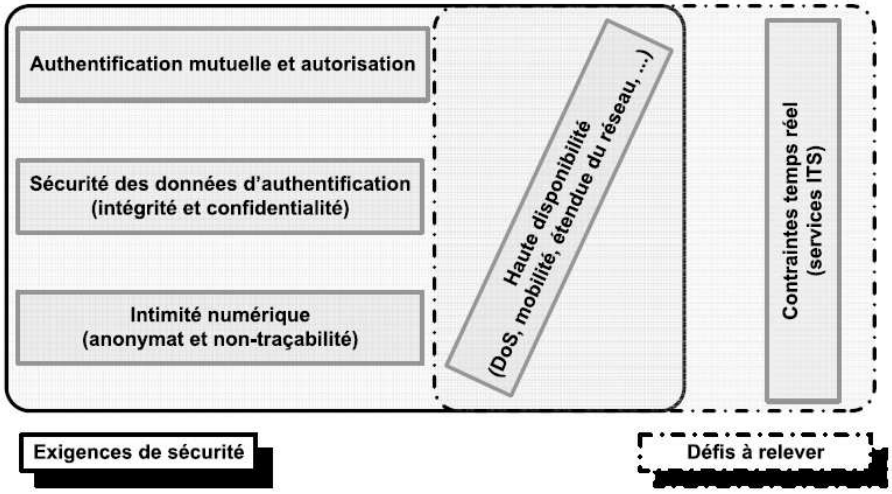


Figure 1: Exigences de sécurité et défis à relever

3. Architectures et protocoles pour l'authentification

Notre solution pour l'authentification s'inscrit dans un contexte où tout véhicule désireux d'accéder aux ressources et aux services du réseau passe obligatoirement par une phase d'authentification avec le serveur de l'opérateur; et ce, en vue d'obtenir des lettres de créance qui l'autoriseront à accéder effectivement à ces ressources et services. A la différence des travaux existants, notre contribution vise à promouvoir le déploiement des réseaux véhiculaires en intégrant en particulier le modèle d'affaire (en anglais, *business model*) des opérateurs réseaux (*e.g.* fourniture et contrôle des services depuis l'infrastructure, prépondérance des services non-ITS, etc.) mais aussi, la nécessité de fournir des services ITS en conformité avec les aspects réglementaires et légaux édictés par l'autorité publique et relatifs à ces services. Dans les sous-sections qui vont suivre, nous commencerons par présenter notre architecture réseau ainsi que les rôles des différentes entités qui la constituent. Nous introduirons ensuite de manière successive, l'infrastructure de confiance et de sécurité, le protocole d'authentification et de délivrance des lettres de créance et enfin le protocole assurant le transport multi-sauts sécurisé des paquets d'authentification.

3.1. Architecture du réseau

Nous considérons une architecture réseau dans laquelle les véhicules communiquent avec les points d'accès de l'opérateur sur un ou plusieurs sauts selon que ces véhicules se trouvent à l'intérieur ou en dehors de la zone de couverture des points d'accès. De manière plus précise et conformément à la classification donnée dans le Chapitre 1.1, notre architecture est de la catégorie des réseaux sans fil hybrides avec mode ad-hoc extra cellulaire. En effet, dans cette architecture le mode de communication ad-hoc est mis en œuvre essentiellement à l'extérieur de la cellule (*i.e.* la zone de couverture d'un point d'accès). Pour reprendre dans notre contexte la terminologie du Car-to-Car Communication Consortium (C2C-CC) [C2C-CC07], on dira que la communication entre les véhicules et l'infrastructure de l'opérateur (en anglais, *Vehicle-to-Infrastructure (V2I) communication*) ou la communication entre les On Board Units (OBUs) embarqués dans les véhicules et les Road-Side Units (RSUs) qui représentent les points d'accès, est uni ou multi-sauts. Ainsi comme illustré par la Figure 2, on distingue principalement dans notre architecture réseau trois entités que sont:

- *Les OBUs*: Ces entités sont embarquées dans les véhicules et constituent leur plateforme de communication. Ils peuvent à ce titre être sources ou destinations de trafic de données ou de contrôle. Ils peuvent de plus, relayer le trafic d'autres OBUs de manière à leur assurer une connectivité avec l'infrastructure fixe en particulier lorsque ces derniers ne sont pas dans la zone de couverture de cette infrastructure.

- *Les RSUs*: Ces entités représentent les points d'accès (en anglais, *Access Points (APs)*) et font partie de l'infrastructure fixe. Ils sont gérés par l'opérateur et font le lien entre les OBUs et le reste de l'infrastructure fixe ou d'autres réseaux.

- *Le serveur d'authentification (*en anglais, *AAA (Authentication, Authorization, Accounting) Server (AS)*): Cette entité réside dans l'infrastructure d'accès de l'opérateur et est directement contrôlée et administrée par ce dernier. Elle authentifie les OBUs et délivre à ceux-ci les lettres de créance nécessaires pour accéder aux ressources et aux services du réseau. Dans la pratique, elle peut interagir avec d'autres autorités (*e.g.* autorités de certification, en anglais, *Certification Authorities (CAs)*) intervenant dans le processus de validation des lettres de créance initiales fournies par l'OBU au moment de son authentification. Par souci de simplification, nous considèrerons néanmoins que toutes ces autorités forment avec l'AS une même et unique entité.

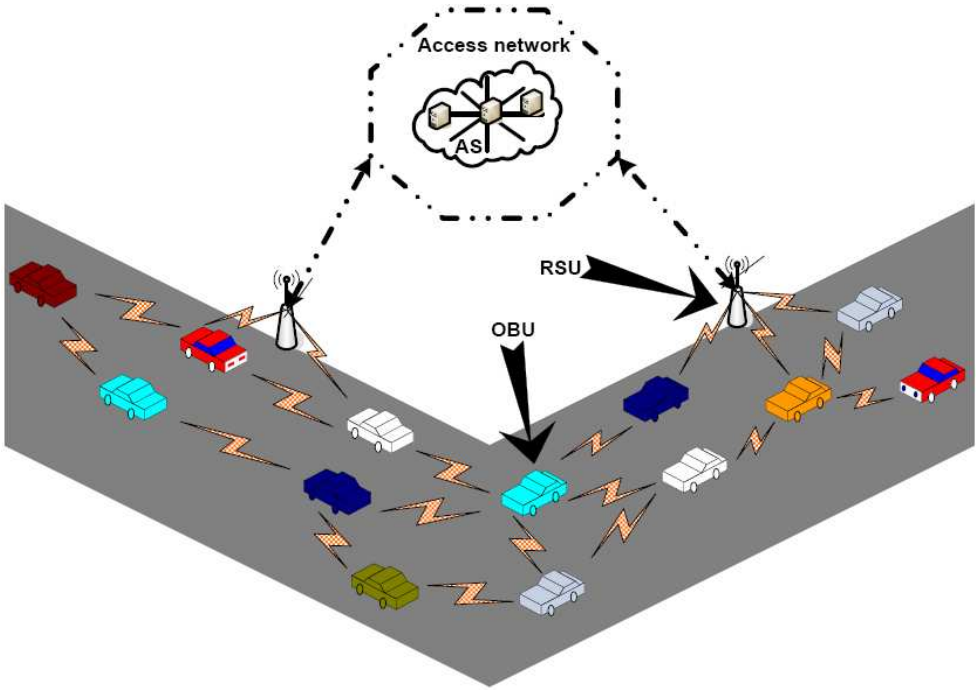


Figure 2: Architecture du réseau

Ce choix architectural du réseau (*i.e.* autorisant des communications multi-sauts) est un des éléments visant à relever le défi de la haute disponibilité. De plus, l'accroissement virtuel de la portée de transmission des RSUs permet à l'opérateur de déployer ces derniers avec la plus grande optimalité (*i.e.* en réduisant de manière considérable le nombre de RSUs nécessaires à la couverture d'une zone).

3.2. Infrastructure de confiance et de sécurité

3.2.1. Description générale de l'infrastructure

En raison de l'impact direct que peuvent avoir les services ITS sur la sécurité physique des biens et surtout des personnes, il importe que ces services à l'image des services d'ordre public soient régis par une autorité publique. L'autorité publique est donc dans ce contexte la source de confiance pour les services ITS. Elle délivre à cet effet, des lettres de créance aux opérateurs et aux véhicules. Ces lettres de créance valent agrément pour les opérateurs; ce qui les autorise à déployer des services ITS avec la confiance des véhicules. Quant aux lettres de créance fournies aux véhicules par l'autorité publique, elles leur permettent de participer activement à la mise en œuvre des services ITS par la génération, la modification et la diffusion des messages liés à ces services. Autrement dit, dans le modèle que nous définissons tout véhicule ne participera à la mise en œuvre des services ITS et de manière générale ne traitera les messages ITS diffusés dans un réseau donné que si l'opérateur de ce

réseau dispose d'un agrément de l'autorité publique, soit des lettres de créance correspondantes. De la même façon, un véhicule ne sera admis à participer à la mise en œuvre des services ITS, que si ce véhicule démontre à l'opérateur du réseau la possession de lettres de créance délivrées par l'autorité publique.

S'agissant des services non-ITS, nous considérons qu'ils doivent être régis par le modèle de confiance auquel sont soumis des réseaux opérés actuels (*e.g.* GSM, 3G, etc.). En d'autres termes, c'est l'opérateur ou le fournisseur de service qui constitue la source de confiance et qui définit en toute indépendance les rapports de confiance entre les éléments du réseau. L'opérateur ou le fournisseur de service va donc enregistrer les abonnements des véhicules et va de manière concomitante leur délivrer les lettres de créance nécessaires pour accéder aux services non-ITS pour lesquels ils ont souscrit.

Pour mettre en œuvre, le plus efficacement et scalable possible, le modèle de confiance que nous venons de concevoir pour les services ITS et non-ITS, nous définissons une infrastructure de confiance et de sécurité basée sur le concept d'infrastructure à clé publique (en anglais, *Public Key Infrastructure (PKI)*). En conséquence, les lettres de créance dont nous avons fait état jusqu'ici sont réifiées en certificats à clé publique (en anglais, *Public Key Certificate (PKC)*). Dans cette nouvelle infrastructure, on distingue trois entités symboliques (illustrées par la Figure 3), à savoir:

- *Une autorité publique des transports (*en anglais, *Public Transportation Authority "PTA")*: Cette entité délivre aux opérateurs et aux véhicules des certificats associés de manière exclusive aux services ITS; nous parlerons de certificats ITS. Les certificats ITS délivrés aux véhicules se distinguent des certificats ITS délivrés aux opérateurs par leur anonymisation. En effet, à la différence des certificats à clé publique classiques, les certificats délivrés aux véhicules ne portent pas l'identification de leur sujet. Dans ces certificats, l'identification du porteur est remplacée par un pseudonyme. Ainsi, le porteur n'est identifiable que par la PTA qui, pour ce faire, croise sa base de données des porteurs avec le numéro de série du certificat[1]. Les certificats délivrés par la PTA aux opérateurs et aux véhicules vont permettre à ces derniers d'établir les rapports de confiance nécessaires (notamment au moment de l'authentification initiale entre le véhicule et l'opérateur) pour opérer les services ITS. Les certificats ITS sont délivrés hors-ligne aux opérateurs et aux véhicules par un circuit administratif similaire à celui des cartes d'immatriculation. Le cycle de vie de ces certificats et leur politique de délivrance sont entièrement contrôlés par la PTA. Ces certificats, du fait de leur durée de validité relativement importante (*e.g.* validité annuelle) sont dits long-terme ou persistants. On notera cependant qu'outre l'échéance de validité, ces certificats peuvent être rendus invalides suite à une action de révocation décidée par la PTA. En dehors des cas de révocation, les véhicules sont tenus d'initier le renouvellement de leurs certificats à échéance de leur durée de validité.

[1] Le numéro de série d'un certificat est réputé unique parmi l'ensemble des numéros de série des certificats délivrés par une même autorité de certification.

- *Un opérateur réseau (*en anglais, *Network Operator (NO))*: Comme la PTA, cette entité délivre des certificats anonymes aux véhicules. Elle délivre en particulier, par des canaux ou pour des usages différents, trois types de certificats anonymes. Le premier type correspond aux certificats associés aux services non-ITS - on parlera de certificats non-ITS - et délivrés aux véhicules ou utilisateurs ayant engagé une souscription pour accéder à ces services. Ces certificats non-ITS sont délivrés hors-ligne avec une durée de validité conséquente (*e.g.* validité annuelle). Ils sont donc dits long-terme ou persistants. Les deuxième et troisième types de certificats délivrés par le NO sont associés aux services ITS et non-ITS respectivement. Ces certificats comme le premier type de certificats, sont anonymes mais, contrairement à ces derniers, sont délivrés en ligne et avec une durée de validité réduite (*e.g.* quelques minutes ou quelques heures). Ils sont donc dits temporaires ou volatiles. Alors que les certificats non-ITS persistants sont utilisés pour établir les rapports de confiance (notamment au moment de l'authentification initiale entre le véhicule et le NO) avant la fourniture des services non-ITS, les certificats ITS et non-ITS volatiles sont utilisés au cours des réauthentifications successives mais aussi et surtout au moment de la mise en œuvre de la sécurité et du contrôle d'accès aux services ITS et non-ITS. Les certificats volatiles suivant le type de service auquel ils sont associés vont donc par exemple être utilisés pour assurer l'authenticité de l'origine des messages ITS (*i.e.* signature des messages ITS par la source), mettre en œuvre les protocoles de sécurité de la couches IP (*e.g.* IPsec) et des couches supérieures (*e.g.* TLS, DTLS, etc.) et plus généralement réaliser l'authentification entre les véhicules ainsi que la sécurisation de leurs communications lors de l'exécution des services.

- *Les véhicules*: Tous les véhicules sont chacun porteur d'un certificat ITS anonyme persistant. Les véhicules ayant en outre souscrit un abonnement auprès du NO, sont en plus chacun porteur d'un certificat non-ITS anonyme persistant. Nous supposons également chaque véhicule en possession des certificats des différentes autorités (*i.e.* PTA, NO) lui ayant délivré les certificats dont il est porteur.

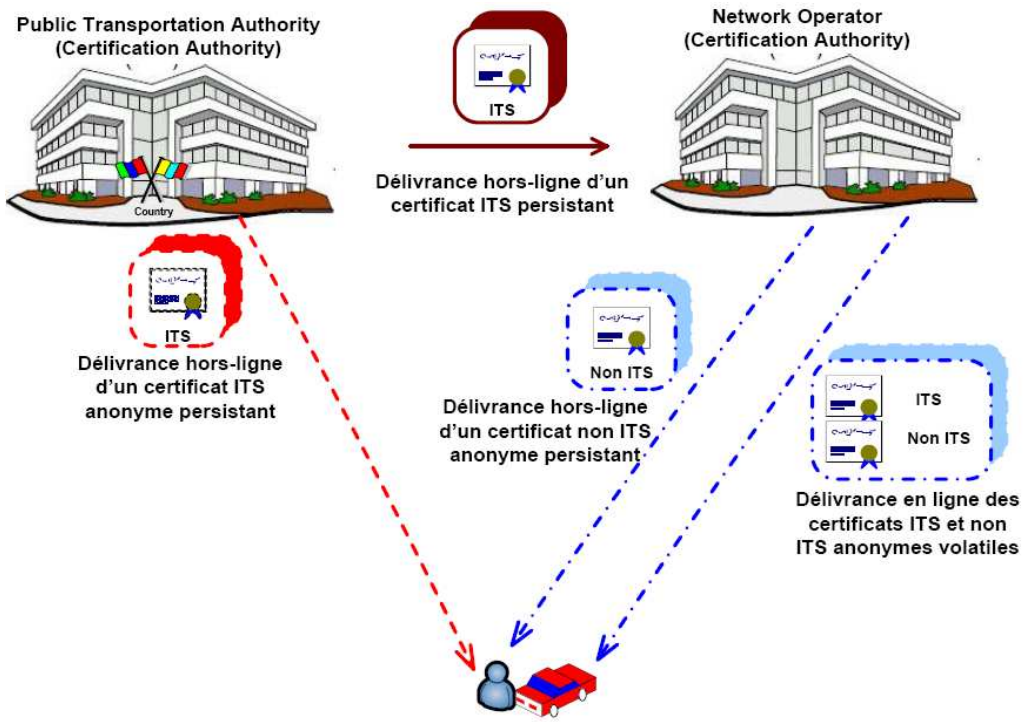


Figure 3: Infrastructure de confiance et de sécurité

3.2.2. Eléments de l'infrastructure pour la haute disponibilité et les contraintes temps réel

Compte tenu de la forte mobilité dans les réseaux véhiculaires, relever le défi de la haute disponibilité et des contraintes temps réel passe par des interactions (*i.e.* échanges de messages) aussi rapides que possible. Pour atteindre cet objectif, nous recourons en priorité aux standards cryptographiques à clé publique (en anglais, *Public Key Cryptography Standards (PKCS)*) les plus compacts et pas forcément à ceux ayant le temps d'exécution le plus court. En effet, plus que les capacités de calcul (*i.e.* ressources processeurs), la ressource radio dans les réseaux véhiculaires est considérée comme plus rare et donc plus coûteuse. A la différence des petits terminaux, les véhicules grâce à leur taille conséquente, peuvent embarquer d'importantes capacités énergétiques et de calcul. En revanche, les plateformes de communication embarquées dans les véhicules en mobilité sont soumises à d'importantes contraintes radio (*e.g.* multi-path fading, shadowing, path loss, etc.) [OISHI06] qui imposent que les paquets soient de taille réduite pour assurer des transmissions rapides et efficaces. Il est donc clair que les PKCS retenus pour l'infrastructure de confiance et de sécurité doivent en priorité être les plus compacts. Cela étant dit, il ne sera tout de même pas totalement inutile de s'assurer que leurs temps d'exécution restent acceptables.

C'est dans ce contexte que nous avons retenu le PKCS ECC (Elliptic Curve Cryptosystems) [ECC87] dont on peut déduire depuis le Tableau 1 [LENS01] et le Tableau 2 [CSI02] qu'il est nettement supérieur en termes de niveau de sécurité par bit et de taille de signature et de donnée chiffrée (*i.e.* signature et donnée chiffrée plus

compactes) respectivement, au PKCS RSA (Rivest, Shamir, Adleman) [RSA78] qui est actuellement le plus répandu dans les PKIs. Plus concrètement, le Tableau 1 illustre les équivalences de niveau de sécurité suivant la taille de clé entre les algorithmes symétriques et les PKCS ECC et RSA alors que le Tableau 2 présente les tailles de données chiffrées de ces PKCS obtenues avec 22 octets de données ainsi que les tailles de signatures de ces mêmes PKCS obtenues avec la fonction de hachage SHA-1 (Secure Hash Algorithm number 1).

Tableau 1: Equivalences de niveau de sécurité suivant la taille de clé [LENS01]

Taille de clé symétrique (bits)	*Taille de clé ECC (bits)*	*Taille de clé RSA (bits)*
80	163	1024
112	233	2240
128	283	3072
192	409	7680
256	571	15360

Tableau 2: Comparaison entre ECC et RSA suivant les tailles de signatures et de données chiffrées [CSI02]

Equivalence de niveau de sécurité	*Taille de signature ECC avec SHA-1 (octets)*	*Taille de signature RSA avec SHA-1 (octets)*	*Taille de donnée (22 octets) chiffrée avec ECC (octets)*	*Taille de donnée (22 octets) chiffrée avec RSA (octets)*
ECC 113 = RSA 512	30	64	73	64
ECC 131 = RSA 768	34	96	77	96
ECC 160 = RSA 1024	42	128	83	128
ECC 283 = RSA 2048	72	256	115	256
ECC 409 = RSA 4096	102	512	147	512

Quant aux temps d'exécution (*i.e.* capacités de calcul consommées), le Tableau 3 [JANS04] illustre pour le PKCS ECC de meilleures performances générales même si on relève la supériorité du PKCS RSA dans le temps de vérification de signature. Il est à noter que ces performances sont obtenues à partir d'une plateforme Intel P4 cadencée à 2 GHz et embarquant une RAM de 512 MB. L'algorithme SHA-1 est utilisé pour générer et vérifier les signatures à partir un fichier texte de 100 KB.

Tableau 3: Comparaison entre ECC et RSA suivant les temps d'exécution [JANS04]

Equivalence de niveau de sécurité	*Temps de génération de clé ECC (s)*	*Temps de génération de clé RSA (s)*	*Temps de génération de signature ECC (s)*	*Temps de génération de signature RSA (s)*	*Temps de vérification de signature ECC (s)*	*Temps de vérification de signature RSA (s)*
ECC 163 = RSA 1024	0.08	0.16	0.15	0.01	0.23	0.01
ECC 233 = RSA 2240	0.18	7.47	0.34	0.15	0.51	0.01
ECC 283 = RSA 3072	0.27	9.80	0.59	0.21	0.86	0.01
ECC 409 = RSA 7680	0.64	133.90	1.18	1.53	1.80	0.01

ECC 571 = RSA 15360	1.44	679.06	3.07	9.20	4.53	0.03

Une alternative au PKCS ECC aurait pu être le PKCS NTRU [NTRU]. En effet, le PKCS NTRU est un concurrent des PKCS ECC et RSA qui présente des performances en termes de temps d'exécution nettement meilleures que celles de ces derniers. Cependant, compte-tenu du contexte particulier des réseaux véhiculaire où le caractère compact des PKCS est privilégié, l'option NTRU est écartée. Les limites du PKCS NTRU sont en effet illustrées par le Tableau 4 [NTRU] duquel on peut aisément relever que pour un même niveau de sécurité, les tailles de la clé publique NTRU et des données chiffrées avec NTRU sont largement supérieures à celles de ses concurrents dont notamment le PKCS ECC que nous avons retenu pour notre infrastructure de confiance et de sécurité. Notons que les temps d'exécution du Tableau 4 sont obtenus depuis une plateforme Intel P3 cadencée à 800 MHz.

Tableau 4: Comparaison des PKCS NTRU, RSA et ECC pour un même niveau de sécurité [NTRU]

	NTRU 251	*RSA 1024*	*ECC 163*
Clé publique (bits)	2008	1024	164
Clé privée (bits)	251	1024	163
Taille du bloc à chiffrer	160	702	163
Taille du bloc chiffré	2008	1024	163
Vitesse de chiffrement (blocs/s => Mbps)	22727 => 3.6	1280 => 0.90	458 => 0.075
Vitesse de déchiffrement (blocs/s => Mbps)	10869 => 1.7	110 => 0.077	702 => 0.11

On notera de manière générale que, pris ensemble, les différents temps d'exécution des algorithmes présentés dans chacun des tableaux ci-dessus traduisent une tendance susceptible d'être généralisée. En revanche, chaque temps d'exécution d'un algorithme pris séparément ne reflète qu'une implémentation particulière ainsi que les caractéristiques matérielles et logicielles de la plateforme sur laquelle cet algorithme s'exécute.

3.2.3. Eléments de l'infrastructure pour l'intimité numérique

Au-delà du défi de la haute disponibilité dont nous venons de dévoiler un des moyens mis en œuvre (*i.e.* choix du PKCS ECC) pour le relever, on notera aussi l'utilisation des certificats anonymes et des certificats volatiles pour éliminer ou réduire les risques d'exposition de l'identité et de traçabilité des utilisateurs aux fins de préserver leur intimité numérique. En effet, à l'issue de l'authentification initiale entre le véhicule et l'opérateur à l'aide des certificats persistants, le véhicule se voit délivrer des certificats volatiles qui vont être renouvelés chaque fois pendant les réauthentifications successives. Dans ce contexte, si l'anonymat peut être considéré comme garanti du fait de l'utilisation de pseudonymes dans tous les certificats, le niveau de non-

traçabilité est quant à lui fonction de la fréquence de renouvellement des certificats volatiles et donc, fonction de la fréquence de réauthentification. Dans une architecture réseau à infrastructure (*i.e.* la communication entre le véhicule et le point d'accès de l'opérateur se fait sur un unique saut), on peut considérer que la réauthentification et donc le renouvellement des certificats volatiles se fasse chaque fois que le véhicule rencontre un nouveau point d'accès (*i.e.* le véhicule entre dans la zone de couverture de ce dernier). Cette fréquence de réauthentification du réseau à infrastructure, ramenée à notre architecture réseau multi-sauts (*i.e.* la communication entre le véhicule et le point d'accès de l'opérateur peut se faire sur plus d'un saut), constitue un minimum pour assurer un niveau satisfaisant de non-traçabilité. On peut en effet s'attendre, dans une architecture réseau multi-sauts, à ce que les véhicules se ré-authentifient avant d'avoir rencontré le prochain point d'accès (*i.e.* avant d'être effectivement entré la zone de couverture de ce dernier) et donc, que ces véhicules aient une fréquence de réauthentification supérieure à celle qu'ils pourraient avoir dans une architecture réseau à infrastructure.

Considérant toutes ces observations, nous définissons un coefficient de non-traçabilité dont les valeurs sont comprises entre -1 et 1, la valeur médiane 0 correspondant au niveau de non-traçabilité satisfaisant minimal, lui-même associé à la fréquence de réauthentification décrite précédemment pour une architecture réseau à infrastructure (*i.e.* la réauthentification est initiée chaque fois que le véhicule entre dans la zone de couverture d'un nouveau point d'accès). Plus précisément, on dit que le coefficient de non-traçabilité a la valeur satisfaisante minimale (*i.e.* 0), lorsque l'intervalle de réauthentification ou de renouvellement des certificats volatiles est égal à la durée que met un véhicule pour parcourir la distance qui sépare les entrées de zone de couverture de 2 points d'accès consécutifs. En dessous de 0, le coefficient de non-traçabilité est dit médiocre avec -1 comme valeur la plus faible. A partir et au dessus de 0, le coefficient de non-traçabilité est dit satisfaisant avec 1 comme valeur maximale. Pour un véhicule donné, le coefficient de non-traçabilité est défini comme suit:

$$F_{non-trac}(\mathrm{Re}\,authInt) = \begin{cases} 1 - \dfrac{\mathrm{Re}\,authInt * S}{(InterAPDist)} & Si \quad \mathrm{Re}\,authInt \le {(InterAPDist)}/{S} \\ \dfrac{(InterAPDist)}{\mathrm{Re}\,authInt * S} - 1 & Sinon \end{cases} \qquad (1)$$

Où $F_{non\text{-}trac}$ est le coefficient de non-traçabilité du véhicule, *ReauthInt* l'intervalle de réauthentification ou de renouvellement des certificats volatiles du véhicule, *S* la vitesse moyenne du véhicule et *InterAPDist* la distance moyenne entre les points d'accès. La Figure 4 illustre les données de distance utilisée dans l'Equation 1 mais

aussi la portée de transmission des points d'accès (représentée par *R*) supposée constante et identique pour tous les points d'accès dans le réseau.

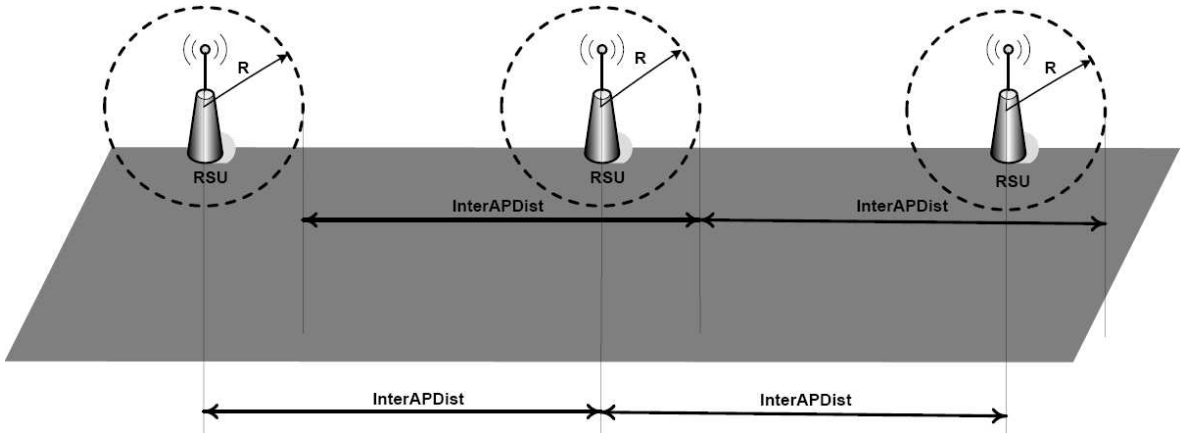


Figure 4:Données de distance pour le calcul du coefficient de non-traçabilité

On notera de manière générale qu'un accroissement du coefficient de non-traçabilité est synonyme d'une fréquence de renouvellement des certificats volatiles plus élevée soit d'un intervalle de réauthentification plus court. On peut aussi aisément relever qu'un intervalle de réauthentification trop court sera susceptible d'entraîner une charge de trafic trop importante dans le réseau. Il faudra donc dans la pratique calibrer l'intervalle de réauthentification pour obtenir un coefficient de non-traçabilité satisfaisant qui induise une charge de trafic acceptable dans le réseau.

3.3. Le protocole AUCRED (AUthentication and CREdential Delivery protocol)

La Figure 5 illustre les 3 principales phases du processus d'accession au réseau tel que nous l'envisageons dans le contexte de notre architecture réseau. La phase 1 correspond à l'exécution d'un protocole de découverte visant à localiser le RSU et obtenir ses caractéristiques ou ses propriétés en termes notamment de mécanismes de sécurité supportés. La phase 2 est la phase d'authentification proprement dite entre l'OBU et l'AS. La phase 3 correspond quant à elle à l'exécution d'un protocole pour établir une association de sécurité entre l'OBU et le RSU. Il est important de noter que nous ne nous intéresserons dans cette thèse et plus particulièrement dans cette section, qu'à la phase la plus cruciale dite d'authentification ou phase 2.

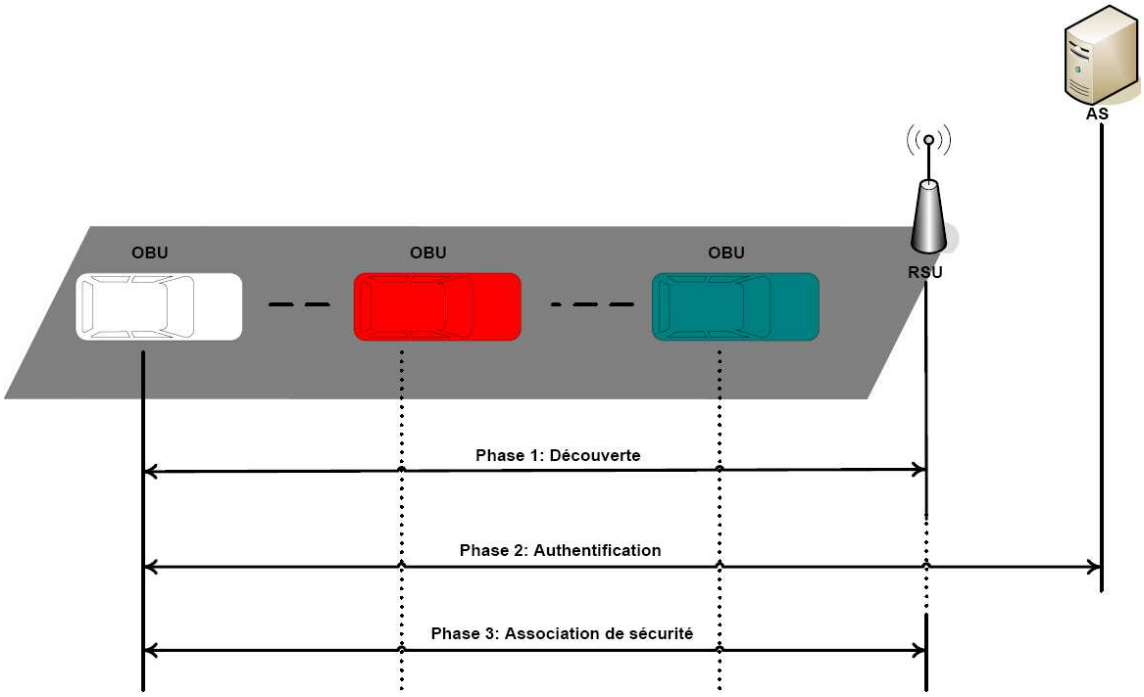


Figure 5: Les principales phases du processus d'accession au réseau

C'est donc dans ce contexte que nous définissons le protocole AUCRED dont l'exécution est précisément attendue à la phase 2 du processus d'accession au réseau. Le protocole AUCRED va en effet permettre de réaliser l'authentification mutuelle entre l'AS et les OBUs (à partir des certificats persistants) ainsi que la délivrance des certificats volatiles à ces derniers. Les mécanismes d'authentification mis en œuvre par le protocole AUCRED sont dérivés de ceux du protocole Transport Layer Security (TLS) [TLS] dont nous reprenons ici le formalisme. Le protocole AUCRED doit donc à ce titre être appréhendé comme une extension du protocole TLS. La Figure 6 et la Figure 7 illustrent les échanges de messages du protocole AUCRED dans des cas d'exécution réussie (*i.e.* authentification réussie) entre l'OBU et l'AS. Plus précisément, la Figure 6 correspond à une exécution complète du protocole alors que la Figure 7 correspond à la réauthentification, soit à la forme abrégée du protocole. Ces figures ne représentent pas le RSU et les éventuels OBUs intermédiaires puisque ces derniers n'interviennent pas dans la logique interne du protocole AUCRED (*i.e.* ils n'interprètent pas les messages AUCRED).

Les mécanismes d'authentification mis en œuvre par le protocole AUCRED étant appréhendés comme une extension de ceux de TLS, ces mécanismes sont donc en pratique la résultante de l'ajout de nouveaux messages ou de la modification des messages existants du protocole TLS. Les nouveaux messages et les messages de TLS ayant fait l'objet d'une modification ou d'une extension sont suivis d'un astérisque sur les Figures 6 et 7.

3.3.1. Echanges de messages du protocole AUCRED lors de l'authentification initiale

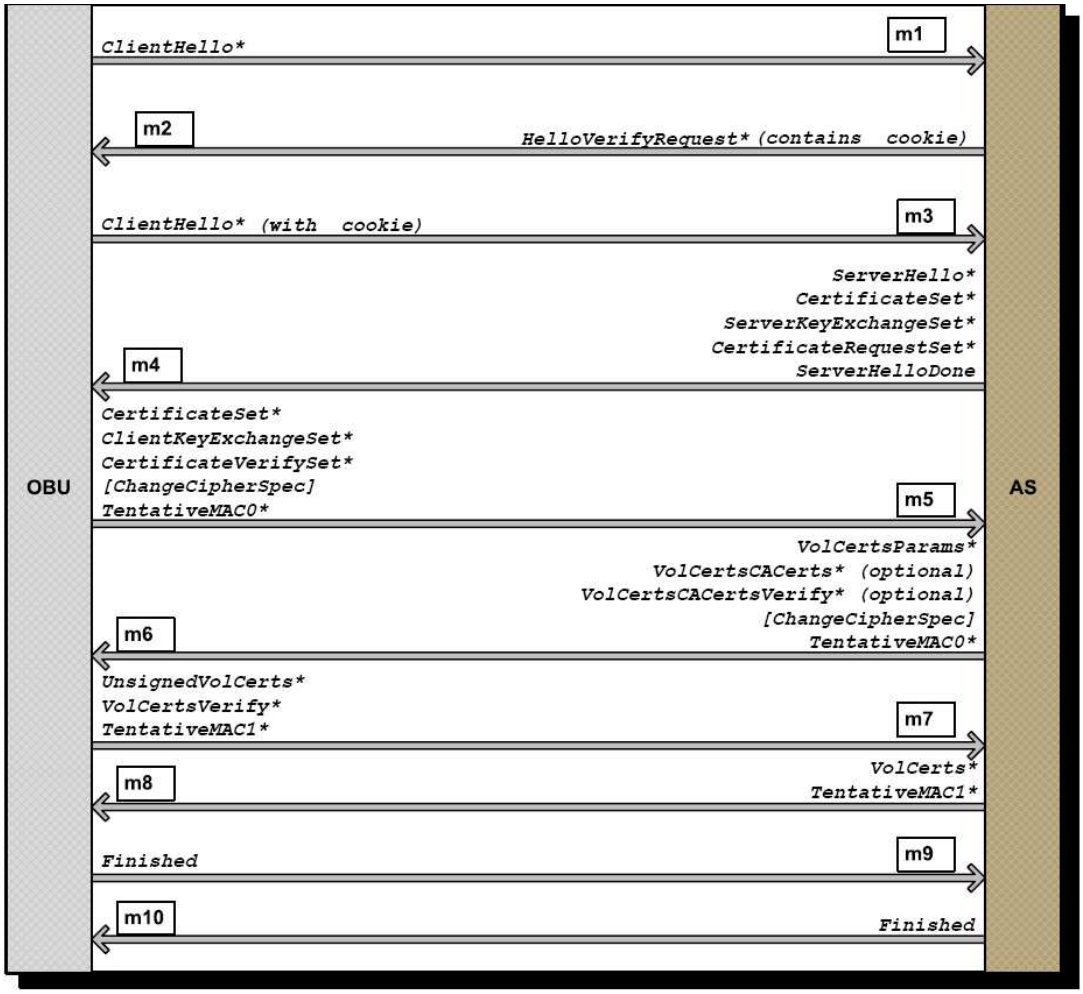


Figure 6: Echanges de messages AUCRED lors de l'authentification initiale

Au début de cet échange (voir Figure 6), l'OBU envoie:

- Un message *ClientHello* (*m1* sur la figure) contenant entre autres la version du protocole, la liste des algorithmes cryptographiques préférés et un nonce[2] produit à partir d'un générateur de nombres aléatoires. A la différence du message *ClientHello* classique de TLS, ce message comporte également une extension indiquant que l'exécution en cours est bien celle du protocole AUCRED. Cette extension indique aussi les types de service pour lesquels l'authentification et la délivrance des certificats volatiles vont être faites. Les types de service indiqués peuvent correspondre aux services ITS ou aux services non-ITS séparément, ou encore aux 2 types de service simultanément.

L'AS répond par:

- Un message *HelloVerifyRequest* (*m2* sur la figure) contenant un témoin (en anglais, *Cookie*) que l'OBU doit obligatoirement retourner à l'AS pour lui prouver qu'il est bien celui qu'il prétend. L'envoi de ce message évite à l'AS de réserver des ressources à ce stade du processus d'authentification, l'objet ici étant de contrer les attaques de type DoS menées par des OBUs malveillants ayant usurpé l'identifiant d'autres OBUs. Ce message ainsi que son principe d'utilisation sont dérivés du protocole Datagram Transport Layer Security (DTLS) [DTLS].

L'OBU ayant reçu le message *HelloVerifyRequest* répond par:

- Un message *ClientHello* (*m3* sur la figure) contenant les mêmes données que le *ClientHello* initial avec en plus le Cookie contenu dans le message *HelloVerifyRequest*.

L'AS ayant reçu le nouveau ClientHello et après s'être assuré de la validité du Cookie contenu dans ce dernier message, répond par:

- Un groupe de messages (*m4* sur la figure) contenant:

  - Un message *ServerHello* comprenant entre autres la version du protocole, un identifiant de session auto-généré, les algorithmes cryptographiques supportés et un nonce produit à partir d'un générateur de nombres aléatoires. Comme le message *ClientHello* reçu précédemment, ce message comporte aussi une extension indiquant que l'exécution en cours est bien celle du protocole AUCRED. Cette extension spécifie également les types de service supportés (ITS ou non ITS ou les 2).

  - Un message *CertificateSet* contenant pour chaque type de service, le certificat correspondant de l'AS. Ce message contient pour chaque certificat de l'AS, la chaîne éventuelle des certificats nécessaires à sa validation. Le message *CertificateSet* se distingue du message *Certificate* classique de TLS, en ce qu'il est à même de convoyer plusieurs certificats de l'AS (*i.e.* plusieurs messages *Certificate* classiques de TLS). L'intérêt de ce message se révèle lorsque l'AS authentifie l'OBU pour les services ITS et non-ITS simultanément. Dans ce cas en effet, l'AS doit présenter plus d'un certificat à savoir son certificat ITS et son certificat non-ITS.

  - Un message *ServerKeyExchangeSet* qui spécifie (dans le cas où le ou les certificats de l'AS ne le feraient pas) la ou les informations cryptographiques (*e.g.* une ou plusieurs clés publiques)

[2] Le nonce est utilisé pour parer aux attaques de re-jeu.

que doit utiliser l'OBU pour chiffrer la clé PMS[3] (PreMaster Secret). Le message *ServerKeyExchangeSet* se distingue du message *ServerKeyExchange* classique de TLS, en ce qu'il est à même de convoyer typiquement, plus d'une clé publique (*i.e.* plusieurs messages *ServerKeyExchange* classiques de TLS). L'intérêt d'une telle structure se révèle lorsque l'AS authentifie l'OBU pour les services ITS et non-ITS simultanément. Dans ce cas en effet, l'AS peut indiquer dans le message *ServerKeyExchangeSet* 2 clés publiques (une ITS et l'autre non-ITS) qui vont être utilisées pour chiffrer séparément le PMS 2 fois. On notera que lorsque le message *ServerKeyExchangeSet* est utilisé (*i.e.* lorsque les clés publiques des certificats de l'AS ne sont pas utilisés pour chiffrer le PMS), chaque clé publique est accompagnée d'une signature réalisée avec la clé privée correspondante, comme c'est également le cas dans le message *ServerKeyExchange* classique de TLS.

- Un message *CertificateRequestSet* qui spécifie à l'intention de l'OBU et pour chaque type de service, les types de certificat et les autorités de certifications acceptées par l'AS. A la différence donc du message *CertificateRequest* classique de TLS, le message *CertificateRequestSet* peut convoyer plusieurs catégories d'autorités de certification et de types de certificat. Plus concrètement, le message *CertificateRequestSet* peut comprendre plusieurs messages *CertificateRequest* classiques de TLS. Lorsque par exemple l'AS authentifie l'OBU pour les services ITS et non-ITS simultanément, il présente à travers le message *CertificateRequestSet*, deux messages *CertificateRequest* classiques de TLS; soit un pour les services ITS et un autre pour les services non-ITS.

- Un message *ServerHelloDone* qui met fin à la séquence des messages du *ServerHello* (*i.e.* la séquence courante).

L'OBU après s'être assuré de la validité du groupe de message précédent (*m4* sur la figure) répond par:

- Un groupe de messages (*m5* sur la figure) contenant:

  - Un message *CertificateSet* comprenant pour chaque type de service indiqué dans les messages *ClientHello* et *ServerHello*, le certificat correspondant de l'OBU. Ce message a les mêmes caractéristiques que le message *CertificateSet* envoyé par l'AS. Il se distingue donc du message *Certificate* classique de TLS de la même manière.

[3]Il est à noter que la clé PMS est la clé racine allant servir à dériver toutes les autres clés secrètes de la session qui va être établie.

- Un message *ClientKeyExchangeSet* transportant le PMS[4] (PreMasterSecret) chiffré. Si l'authentification se fait pour un seul type de service (*i.e.* ITS ou bien non-ITS) alors le PMS est chiffré avec la clé publique de l'AS correspondant à ce service. Cette clé publique est celle du certificat correspondant de l'AS ou bien celle indiquée dans le message *ServerKeyExchangeSet* et correspondant au type de service considéré. Dans le cas où l'authentification se fait pour les deux types de service simultanément (*i.e.* ITS et non-ITS), alors le PMS est chiffré séparément deux fois, la première fois avec la clé publique de l'AS correspondant aux services ITS et la deuxième fois avec la clé publique de l'AS associée aux services non-ITS. Le message *ClientKeyExchangeSet* contient dans ce cas deux résultats de chiffrement du PMS. Contrairement donc au message *ClientKeyExchange* classique de TLS, le message *ClientKeyExchangeSet* peut contenir plus d'un résultat de chiffrement. En d'autres termes, il peut contenir plusieurs messages *ClientKeyExchange* classiques de TLS.

- Un message *CertificateVerifySet* contenant les signatures de l'OBU construites sur tous les messages échangés jusqu'ici avec l'AS à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même (*i.e. CertificateVerifySet*). A la différence donc du message *CertificateVerify* classique de TLS, le message *CertificateVerifySet* peut convoyer plus d'une signature. Cela arrive en particulier lorsque le protocole AUCRED est exécuté pour les deux types de service simultanément (*i.e.* ITS et non-ITS). Dans ce cas en effet, le message *CertificateVerifySet* va contenir deux signatures, à savoir, une signature générée avec la clé privée du certificat ITS et l'autre générée avec la clé privée du certificat non-ITS. Le message *CertificateVerifySet* comme le message *CertificateVerify* classique de TLS, permet à l'AS d'effectivement authentifier l'OBU.

- Un message *ChangeCipherSpec* utilisé comme un signal pour notifier à l'AS le changement de la politique de chiffrement. En effet une fois ce message envoyé, les enregistrements[5] (en anglais, *records*) suivants envoyés par l'OBU sont chiffrés et authentifiés avec les clés et algorithmes négociés avec l'AS. Ce message est le même et a donc exactement la même fonction que le message *ChangeCipherSpec* classique de TLS. On notera que ce message, à la différence de tous les autres messages échangés entre l'OBU et l'AS ne fait pas partie de la famille des messages dits de *Handshake* ou tout simplement du sous-protocole de TLS appelé

[4] On notera que la clé PMS est générée de manière aléatoire par l'OBU. Cette clé est transmise à l'AS et est utilisée par les 2 parties pour générer la clé secrète commune MS (Master Secret).

[5] Un enregistrement peut contenir un groupe de messages comme illustré sur les figures représentant les échanges de messages entre l'OBU et l'AS. La constitution des enregistrements est régie par un sous-protocole de TLS appelé *record protocol*.

Handshake protocol. Le message *ChangeCipherSpec* est au contraire associé à un sous-protocole éponyme.

- Un message *TentativeMAC0* contenant une empreinte de hachage MAC (Message Authentication Code) construite sur tous les messages dits de *Handshake* échangés jusqu'ici avec l'AS à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même (*i.e. TentativeMAC0*). C'est en particulier la clé MS (Master Secret) elle-même dérivée de la clé PMS qui est utilisée dans cette construction. Si le message *TentativeMAC0* a la même structure et le même principe de construction que le message *Finished* classique de TLS, il n'en a cependant pas tout à fait les mêmes fonctions. Du point de vue des fonctions remplies, ces messages sont similaires dans la mesure où tous les deux permettent de confirmer l'agrément sur les clés et algorithmes négociés en réalisant un contrôle d'intégrité et en authentifiant les messages échangés. En revanche, à la différence du message *Finished* classique de TLS, le message *TentativeMAC0* ne signale aucunement la fin du processus d'authentification et encore moins le début de l'échange des données applicatives sous le régime des algorithmes et clés négociés. On notera qu'à ce stade d'exécution dans le protocole TLS classique, c'est le message *Finished* qui est envoyé en lieu et place du message *TentativeMAC0* dans le cas présent.

L'AS après avoir vérifié et validé le groupe de messages précédent (*m5* sur la figure) envoie:

- Un groupe de messages (*m6* sur la figure) comprenant:
  - Un message *VolCertsParams* contenant pour chaque type de service, les paramètres cryptographiques (*e.g.* algorithme ou standard de clé publique, taille de clé, etc.) que doit utiliser l'OBU pour générer le certificat volatile non signé correspondant. Notons que générer un certificat non signé peut correspondre à générer tout simplement un couple de clés (clé publique, clé privée).
  - Un message *VolCertsCACerts* contenant pour chaque type de certificat volatile à délivrer (*i.e.* ITS, non-ITS) le certificat correspondant de l'autorité de certification ainsi que la chaine éventuelle des certificats nécessaires à la validation du certificat de cette autorité. Dans le cas de notre infrastructure de confiance et de sécurité, cette autorité de certification n'est rien d'autre que le NO (*i.e.* l'AS dans l'architecture réseau). Ce message a la même structure que le message *CertificateSet* envoyé précédemment par l'AS et par l'OBU. On notera cependant que

ce message est optionnel dans la mesure où il n'est pas envoyé lorsque l'OBU est supposé déjà détenir les certificats qui serviront à signer les certificats volatiles.

- Un message *VolCertsCACertsVerify* contenant les signatures réalisées à l'aide des certificats qu'utilise l'AS pour délivrer (*i.e.* signer) les certificats volatiles. Lorsque par exemple l'authentification se fait simultanément pour les services ITS et non-ITS, ce message contient 2 signatures à savoir une signature réalisée avec le certificat qu'utilise l'AS pour signer les certificats volatiles ITS et une autre signature réalisée avec le certificat qu'utilise l'AS pour signer les certificats volatiles non-ITS. Les signatures incluses dans ce message sont construites sur tous les messages dits de *handshake* échangés jusqu'à présent avec l'OBU à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et du message courant (*i.e. VolCertsCACertsVerify*). Le message *VolCertsCACertsVerify* a exactement la même structure que le message *CertificateVerifySet*. Sa fonction est d'attester la possession par l'AS des clés privées qui vont être utilisées pour signer les certificats volatiles. En d'autres termes, le rôle de ce message est de permettre à l'OBU d'authentifier les certificats qu'il reçoit et qui vont être utilisés par l'AS pour signer les certificats volatiles. Le message *VolCertsCACertsVerify* est optionnel dans la mesure où il n'existe que si le message optionnel *VolCertsCACerts* est lui-même présent.

- Un message *ChangeCipherSpec* utilisé pour notifier à l'OBU l'entrée en vigueur de la politique de chiffrement négociée. Une fois ce message envoyé, les enregistrements suivants envoyés par l'AS sont chiffrés et authentifiés avec les clés et algorithmes négociés avec l'OBU. Ce message a donc la même structure et la même fonction que celui envoyé précédemment par l'OBU.

- Un message *TentativeMAC0* contenant une empreinte de hachage MAC[6] (Message Authentication Code) construite sur tous les messages dits de *Handshake* échangés jusqu'ici avec l'OBU à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même (*i.e. TentativeMAC0*). Ce message permet de réaliser un contrôle d'intégrité et d'authentifier les messages échangés jusqu'ici avec l'OBU. Il reprend à ce titre les mêmes principes que le message *TentativeMAC0* envoyé précédemment par l'OBU.

Après avoir reçu, vérifié et validé le groupe de messages précédent (*m6* sur la figure), l'OBU chiffre (sous le régime des algorithmes cryptographiques négociés) et envoie:

- Un groupe de messages (*m7* sur la figure) comprenant:

  - Un message *UnsignedVolCerts* contenant pour chaque type de service, le certificat volatile non signé correspondant. Les certificats contenus dans ce message ne portent que leurs clés publiques et sont dépourvus de toute signature. Les messages *CertificateSet* et *UnsignedVolCerts* sont quasi-identiques dans leur structure. Ils ne diffèrent en effet que par l'absence dans la structure du message *UnsignedVolCerts*, de la chaîne de certificats (pour chaque type de service) que peut comporter le message *CertificateSet*. Seuls les certificats volatiles non signés sont donc présents dans le message *UnsignedVolCerts*.

  - Un message *VolCertsVerify* contenant les signatures réalisées à partir des certificats volatiles non signés générés par l'OBU. Ce message a la même structure et quasiment le même principe de construction que le message *CertificateVerifySet*. Le message *CertificateVerifySet* ne diffère du message *VolCertsVerify* que dans la mesure où ce dernier n'est construit que sur les messages dits de *handshake* n'ayant pas encore été signés par l'OBU (*i.e.* n'ayant pas été utilisés dans la construction du message *CertificateVerifySet* que l'OBU a précédemment envoyé). Comme avec le message *CertificateVerifySet*, la construction du message *VolCertsVerify* se fait également à l'exclusion à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même (*i.e. VolCertsVerify*). La fonction de ce message est d'attester auprès de l'AS la possession par l'OBU des clés privées associées aux certificats volatiles non signés. Autrement dit, ce message permet à l'AS d'authentifier les certificats volatiles non signés dont la signature lui est demandée.

  - Un message *TentativeMAC1* dont la structure et la fonction sont identiques au message *TentiveMAC0*. Ce message diffère toutefois du message *TententativeMAC0* dans son principe de construction puisqu'il n'est construit que sur les messages dits de *Handshake* échangés avec l'AS et n'ayant pas encore été hachés par l'OBU (*i.e.* n'ayant pas été utilisés dans la construction du message *TentativeMAC0* que l'OBU a précédemment envoyé). Comme avec le message *TentativeMAC0*, la construction du message *TentativeMAC1* se fait également à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même.

L'AS ayant reçu, déchiffré et validé le groupe de messages précédent (*m7* sur la figure), chiffre (sous le régime des algorithmes cryptographiques négociés) et envoie :

[6] Correspond à une fonction de hachage sécurisée ou construite en utilisant une clé secrète.

- Un groupe de messages (*m8* sur la figure) comprenant:

  - Un message *VolCerts* contenant pour chaque type de service, le certificat volatile signé correspondant. Les certificats contenus dans ce message sont générés par l'AS et les clés publiques présentes dans les certificats volatiles non signés reçus précédemment de l'OBU y sont reportées. Tous les autres paramètres des certificats présents dans ce message dont par exemple les paramètres d'anonymisation (*e.g.* pseudonymes) sont déterminés par l'AS. Ce message a exactement la même structure que le message *UnsignedVolCerts*. Ainsi, seuls les certificats volatiles signés sont présents dans le message *VolCerts*. Il est à noter que le contenu des certificats volatiles n'est accessible durant tout le processus de délivrance que par l'OBU et l'AS (les messages révélant ce contenu étant tous chiffrés); ce qui réduit d'autant les risques d'association entre les certificats persistants et les certificats volatiles et par conséquent renforce la non-traçabilité de l'OBU.

  - Un message *TentativeMAC1* dont la structure, le principe de construction et la fonction sont identiques au message *TentiveMAC1* précédemment reçu de l'OBU. Il n'est donc construit que sur les messages dits de *Handshake* échangés avec l'OBU et n'ayant pas encore été hachés par l'AS (*i.e.* n'ayant pas été utilisés dans la construction du message *TentativeMAC0* que l'AS a précédemment envoyé). La construction de ce message se fait aussi à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même.

Après avoir reçu, déchiffré et validé le groupe de messages précédent (*m8* sur la figure), l'OBU chiffre (toujours sous le régime des algorithmes cryptographiques négociés) et envoie:

- Un message *Finished* (*m9* sur la figure) ayant la même structure, la même fonction mais un principe de construction légèrement modifié par rapport au message *Finished* classique de TLS. Ce message annonce en effet la fin réussie du processus d'authentification (*i.e.* la fin réussie du protocole AUCRED). Il diffère du message *Finished* classique de TLS dans la mesure où il n'est construit que sur les messages dits de *Handshake* échangés avec l'AS et n'ayant pas encore été hachés par l'OBU (*i.e.* n'ayant pas été utilisés dans la construction des messages *TentativeMAC0* et *TentativeMAC1* que l'OBU a précédemment envoyé). Comme le message *Finished* classique de TLS, la construction ce message se fait à l'exclusion des 2 premiers messages (*i.e.* premier *ClientHello* et *HelloVerifyRequest*) et de lui-même.

Ayant reçu, déchiffré et validé le message précédent (*m9* sur la figure), l'AS chiffre (toujours sous le régime des algorithmes cryptographiques négociés) et envoie:

- Un message *Finished* (*m10* sur la figure) qui confirme à l'OBU la fin réussie du processus d'authentification. Ce message reprend la syntaxe et le principe de construction du message *Finished* précédemment envoyé par l'OBU.

3.3.2. Echanges de messages du protocole AUCRED lors de la réauthentification

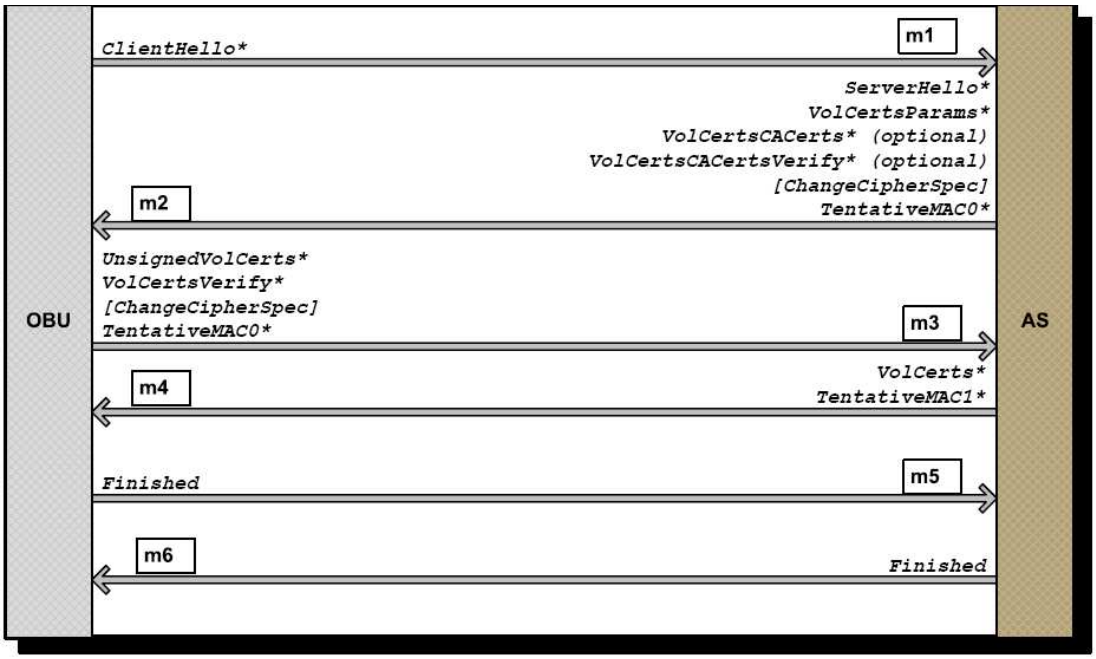


Figure 7: Echanges de messages AUCRED lors de la réauthentification

Le cas de la réauthentification correspond à la forme abrégée du protocole AUCRED (Figure 7). Les messages utilisés ici sont donc un sous ensemble de ceux utilisés au moment de l'authentification initiale. Ces messages reprennent généralement les mêmes syntaxes, les mêmes sémantiques et les mêmes principes de construction que ceux utilisés lors de l'authentification initiale. En résumé, l'OBU envoie au moment de la réauthentification un message *ClientHello* contenant en plus des paramètres utilisés lors de l'authentification initiale, l'identificateur de la session initiale (*i.e.* l'identificateur de session généré par l'AS dans le message *ServerHello* au moment de l'authentification initiale). Cet identificateur permet à l'AS de retrouver le contexte d'authentification de l'OBU dont en particulier la clé MS. L'AS répond ensuite par un message *ServerHello* contenant aussi ce même identificateur de session. La suite des échanges est ensuite abrégée après que les 2 parties ont dérivé un nouveau contexte de session en calculant notamment une nouvelle clé secrète commune MS obtenue en hachant la clé MS de la session initiale avec les nouveaux nonces échangés entre les 2 parties. Comme au moment de l'authentification initiale, la nouvelle clé MS est utilisée par les 2 parties pour dériver

toutes les autres clés secrètes de la session. Cette démarche de réalisation est équivalente à la démarche de reprise de session dans le protocole TLS classique.

3.3.3. Exemple

Nous introduisons ici un exemple d'exécution du protocole AUCRED notamment dans sa version complète (*i.e.* celle correspondant à l'authentification initiale). Cet exemple donne une vue simplifiée du protocole tout mettant en évidence les formes cryptographiques les plus importantes. Ici, l'OBU s'authentifie pour un seul type de service (*e.g.* services ITS) et n'est pas supposé déjà détenir le certificat utilisé par l'AS pour délivrer le certificat volatile correspond au service pour lequel il s'authentifie. De plus, l'OBU et l'AS sont supposés détenir le certificat utilisé par l'autorité de certification pour délivrer les certificats persistants associés au type de service considéré.

Dans cet exemple, l'OBU est assimilé au client tandis que l'AS est assimilé au serveur. Ainsi, dans le formalisme que nous utilisons, les données propres ou générées par l'OBU sont préfixées par "*c*-" alors que les données propres ou générées par l'AS sont préfixées par "*s*-". Ces données peuvent être des certificats, des clés publiques, des clés privées, etc. Les données communes générées par les 2 parties (*e.g.* clé MS) ne sont en revanche pas préfixées. On relèvera aussi que les accolades (*i.e.* "{}") qui entourent certains messages ou groupe de messages signifient que ces messages sont protégés et en particulier chiffrés avec les algorithmes et clés nouvellement négociés. Pour le reste, nous avons:

- La fonction de signature représentée par "$Sign_{Cert}$ *(PrivKey,* $data_1$*, ...,* $data_n$*)*" où *Cert* est le certificat utilisé, *PrivKey* la clé privée correspondant à ce certificat et $data_1$, …, $data_n$ les données à signer.
- La fonction de chiffrement à clé publique représentée par "$Encrypt_{Cert}$ *(PubKey,* $data_1$*, ...,* $data_n$*)*" où *Cert* est le certificat utilisé, *PubKey* la clé publique correspondant à ce certificat et $data_1$, …, $data_n$ les données à chiffrer.
- La fonction de hachage ordinaire (*i.e.* non sécurisée ou n'utilisant pas de clé secrète) est représentée par "*Hash(* $data_1$*, ...,* $data_n$*)*" où $data_1$, …, $data_n$ sont les données à hacher.
- La fonction de hachage MAC (Message Authentication Code) représentée par "*HMAC(Secret,* $data_1$*, ...,* $data_n$*)*" où *Secret* est la clé secrète utilisée par la fonction et $data_1$, …, $data_n$ les données à hacher. On notera qu'à la place de la fonction de hachage MAC classique, on peut substituer une fonction pseudo-aléatoire obtenue par itération et combinaison de plusieurs fonctions de hachage MAC. La fonction pseudo-aléatoire est généralement utilisée dans l'expansion des clés secrètes aux fins de dériver d'autres clés ou de valider les clés utilisées pour réaliser la dérivation [TLS]. Dans le cas présent, la fonction pseudo-aléatoire n'est utilisée que dans une optique de validation. Elle est en conséquence représentée dans notre exemple d'instanciation par la fonction "*PRF(Secret, Label, Hash(*$data_1$*, ...,* $data_n$*))*" où *Secret* est la clé secrète utilisée, *Label* une chaîne de caractère normalisée et $data_1$, …, $data_n$ les données à hacher.

Compte tenu des descriptions du protocole faites dans les sous sections précédentes, les autres éventuels symboles utilisés dans l'exemple illustré par la Figure 8 se comprennent aisément.

Figure 8: Exemple d'exécution du protocole AUCRED

3.3.4. Hiérarchie des clés du protocole AUCRED

Tel que défini, le protocole AUCRED est une extension du protocole TLS. Il en reprend donc logiquement la même hiérarchie des clés. Ainsi, la clé MS est dérivée de la clé PMS et les clés de sessions (*i.e.* clés utilisées pour la protection des données) sont dérivées de la clé MS. Plus précisément, la clé MS est dérivée en une clé Key Block (KB) qui est ensuite partitionnée pour obtenir les clés de session dont les vecteurs d'initialisation font également partie. La Figure 9 illustre cette hiérarchie des clés ainsi que leur calcul. La fonction pseudo-aléatoire est utilisée dans ce contexte pour dériver les clés. Sa forme générale est alors comme suit: "*PRF(Secret, Label, Seed)*" où *Secret* est la clé secrète utilisée, *Label* une chaîne de caractère normalisée et *Seed* une donnée aléatoire. La notation "*PRF-X*" correspond à une application de la fonction pseudo-aléatoire générant un résultat sur "*X*" octets.

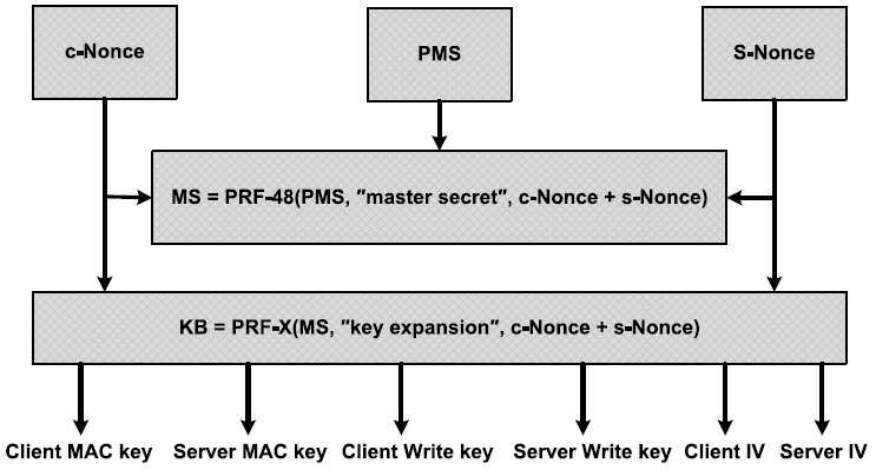


Figure 9: Hiérarchie des clés AUCRED [TLS]

3.3.5. Propriétés du protocole AUCRED

Le protocole AUCRED étant défini sur la base du protocole TLS [TLS], il en reprend assez naturellement les principales propriétés de sécurité. Des mécanismes ont toutefois été ajoutés au protocole AUCRED pour tenir compte du contexte spécifique des réseaux véhiculaires et pallier certaines vulnérabilités. De plus, AUCRED reprend tous les principes édictés par l'infrastructure de confiance et de sécurité que nous avons définie pour les réseaux véhiculaires opérés.

Dans un contexte où l'attaquant ou l'entité malveillante dispose de ressources matérielles conséquentes, est capable d'intercepter, de modifier, de rejouer ou de supprimer des messages, mais est incapable de remettre en cause les fondements des algorithmes cryptographiques (*e.g.* inversion de fonction de hachage, prédiction du résultat d'un générateur de nombres aléatoires, etc.) et d'obtenir les clés secrètes par des moyens autres que ceux dont il dispose, le protocole AUCRED assure:

- *L'authentification mutuelle entre l'AS et l'OBU et la délivrance des lettres de créance à ce dernier*: Cette fonction est réalisée pour chaque type de service auquel l'OBU souhaite accéder. Plus précisément, pour un type de service donné, l'AS authentifie l'OBU et s'assure de ses droits d'accès pour ce type de service. L'OBU authentifie ensuite l'AS et s'assure que ce dernier est bien l'entité qu'il prétend (*i.e.* l'entité investie des privilèges idoines pour le type de service considéré). Au moment de la délivrance des certificats volatiles, l'OBU authentifie l'autorité de certification en charge de la délivrance de ces certificats volatiles. Nous rappelons que dans un souci de simplification cette autorité de certification est assimilée à l'AS. Cette autorité de certification (*i.e.* l'AS) authentifie ensuite le certificat volatile non signé (ou la clé publique correspondante) que lui présente l'OBU avant de le lui délivrer; et ce, sans avoir à prendre connaissance de

la clé privée associée au certificat volatile. Il est cependant à relever que c'est bien l'autorité de certification (*i.e.* l'AS) qui détermine les caractéristiques du couple de clés que l'OBU doit générer. Au-delà de toutes ces propriétés, l'authentification mutuelle réalisée ici permet d'éliminer d'emblée toutes les attaques par l'Homme du milieu (en anglais, *Man In The Middle*). On notera également que pour éviter des exécutions multiples et potentiellement coûteuses dans un environnement très dynamique, le protocole AUCRED permet en une seule exécution, de réaliser l'authentification mutuelle et la délivrance des lettres de créance pour plusieurs types de service.

- *La négociation des suites cryptographiques et la dérivation des clés*: En reprenant le modèle de négociation TLS, le protocole AUCRED tire profit de la foultitude des options négociables (*e.g.* méthode d'obtention des certificats, méthode de compression, etc.) et apporte par la même occasion la garantie de son évolutivité. Les algorithmes devenus vulnérables par exemple pourront facilement être exclus des options de la négociation alors que les nouveaux algorithmes ou de nouveaux mécanismes pourront être supportés. De plus, en reprenant le modèle de dérivation et de mise à jour dynamique des clés de TLS, le protocole AUCRED assure la non-réutilisation des clés et la construction d'une hiérarchie des clés robuste.

- *L'intégrité des messages d'authentification*: Aucune entité extérieure à l'AS et à l'OBU en cours d'authentification ne peut tirer partie d'une modification des messages d'authentification puisqu'ils sont protégés par une fonction de hachage sécurisée à travers notamment les messages *TentativeMAC0*, *TentativeMAC1* et *Finished*.

- *La confidentialité de certains messages d'authentification*: Cette propriété ne devient effective entre l'OBU et l'AS qu'après l'envoie du message *ChangeCipherSpec*. Cette fonction, sans être essentielle à la sécurité du protocole AUCRED, permet toutefois de renforcer la non-traçabilité des OBUs - par rapport aux autres OBUs ou autres entités - en limitant les risques d'association entre leurs certificats persistants et leurs certificats volatiles notamment au moment de l'authentification initiale. Le contenu des certificats volatiles est en effet chiffré durant tout le processus de délivrance.

- *La protection contre le rejeu*: Cette propriété est également héritée du protocole TLS. Elle permet à l'AS et à l'OBU de détecter les tentatives de rejeu des messages d'authentification visant à obtenir des privilèges indus par la reproduction d'une session légitime passée. Cette protection est mise en œuvre par l'utilisation de générateurs pseudo-aléatoires pour produire des nonces qui sont ensuite utilisés dans la dérivation des clés servant à protéger (via des fonctions de hachage sécurisées notamment) les messages d'authentification. Compte tenu de l'utilisation de ces aléas, l'entité malveillante à l'origine du rejeu ne peut être en mesure de dériver les bonnes clés.

- *La protection contre les attaques par dictionnaire*: Les attaques par dictionnaire procèdent par le test de mots de passe contenus dans un dictionnaire dans l'optique de trouver le bon mot de passe permettant d'accéder aux privilèges convoités. L'utilisation systématique des certificats et par conséquent la non-utilisation de mots de passe ou de secrets partagés dans le processus d'authentification permet de prémunir le protocole AUCRED contre ce type d'attaque.

- *La réauthentification rapide*: Cette fonction correspond à la forme abrégée du protocole AUCRED. Le nombre de messages échangés est réduit, de nouvelles clés de session sont dérivées et de nouvelles lettres de créance sont délivrées à l'OBU. Compte tenu de la forte dynamique des réseaux véhiculaires et des contraintes temps réel induites par certains services à l'instar des services ITS, l'exécution de cette forme du protocole devra être privilégiée une fois l'authentification initiale réalisée.

- *L'indépendance des sessions*: La garantie de cette propriété vient de la dérivation de clés maitresses (*i.e.* clés MS) distinctes pour les différentes sessions; qu'il s'agisse de sessions correspondant aux authentifications initiales ou de sessions correspondant aux réauthentifications. En supposant la non-compromission des clés maîtresses et la non-inversibilité des fonctions de hachage utilisées pour dériver les clés de chiffrement à partir des clés maitresses, même la compromission des clés de chiffrement ne permet pas de remonter jusqu'aux clés maitresses et de remettre ainsi en cause l'indépendance des sessions. Dans ces conditions, les sessions successives d'un OBU peuvent être considérées comme parfaitement étanches entre elles et a fortiori avec les sessions d'autres OBUs. Cette propriété du protocole AUCRED procède de la même démarche que celle du protocole TLS classique.

- *La protection contre des attaques de type déni de service (DoS)*: A l'image de la variante Datagram Transport Layer Security (DTLS) [DTLS] du protocole TLS, le protocole AUCRED met en œuvre une technique à base de *Cookie* visant à parer aux attaques menées par des OBUs malveillants initiant des requêtes d'authentification sans jamais avoir l'intention de les poursuivre. Ces OBUs malveillants commencent généralement par usurper les adresses d'autres OBUs. En envoyant ensuite massivement des requêtes d'authentification, ils épuisent les ressources de l'AS ou utilisent ce dernier comme amplificateur ou relais d'attaque vers les OBUs dont ils ont initialement usurpé les adresses. Lors de l'authentification initiale, l'obligation qui est faite à chaque OBU de retourner le *Cookie* (envoyé par l'AS à travers le message *HelloVerifyRequest*) avant toute réservation de ressource et poursuite du protocole, limite fortement ce type d'attaque.

3.3.6. Scénario d'exécution et d'implantation du protocole AUCRED

Conformément à l'architecture réseau que nous avons définie en section 3.1, le protocole AUCRED est destiné à être mis en œuvre dans des configurations où le nombre de sauts entre le RSU et l'OBU peut être non seulement supérieur à 1 mais peut aussi varier au cours d'une même exécution. Une telle flexibilité est de nature à seoir à la forte dynamique des véhicules et par là même, à conférer au processus d'authentification une plus grande disponibilité et efficacité. La Figure 10 présente des exemples de configuration réseau dans lesquels le protocole AUCRED peut être amené à s'exécuter.

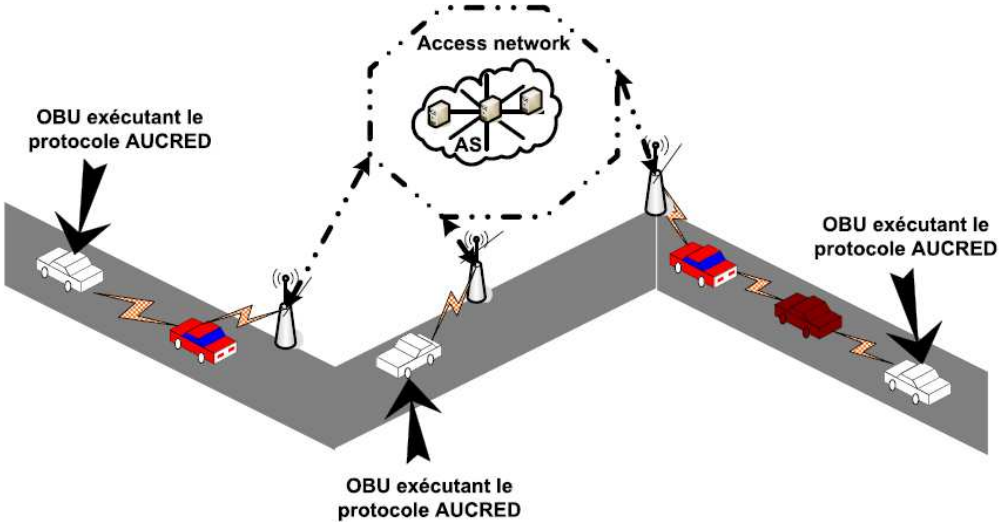


Figure 10: Exemples de configuration réseau pour l'exécution AUCRED

Afin de restreindre l'accès à la couche 3 (*i.e.* couche IP) et aux couches supérieures avant l'exécution réussie de l'authentification, nous avons tout logiquement choisi d'implanter le protocole AUCRED entre la couche 2 (*i.e.* couche liaison de données) et la couche 3 du modèle de référence des réseaux. Ce choix de conception, tout en conférant un niveau de sécurité élevé, permet de rendre les échanges de messages potentiellement plus rapides notamment par la réduction de leurs tailles et la suppression des traitements induits par la couche 3 et les couches supérieures.

Pour réaliser cette implantation du protocole AUCRED, nous avons opté de passer par un protocole d'authentification générique susceptible d'embarquer AUCRED en tant que nouvelle méthode. En définissant le protocole AUCRED comme méthode d'un protocole générique, il devient possible d'utiliser d'autres méthodes du même protocole ou de définir de nouvelles méthodes du protocole sans avoir à remettre en cause l'ensemble de la pile protocolaire. C'est dans cette optique que nous avons retenu le protocole EAP (Extensible Authentication Protocol) [EAP] qui est en effet un protocole d'authentification générique et qui plus est assez répandu dans les réseaux. Par ailleurs, AUCRED étant défini comme une extension de TLS, son encapsulation dans EAP et la hiérarchie des clés correspondante ne sont plus à définir puisque cette encapsulation et cette

hiérarchie sont régies par le même standard EAP-TLS [EAP-TLS]. De plus, l'expérience d'implantation du protocole EAP entre les couches 2 et 3 est illustrée dans nombre de standards de réseaux sans fil (*e.g.* [IEEE-802.16] [IEEE-802.11]).

Cependant, à la différence des standards précédents (*i.e.* [IEEE-802.16] [IEEE-802.11]) qui mettent en œuvre le protocole EAP dans des réseaux sans fil n'autorisant qu'un unique saut entre le terminal et le point d'accès, notre solution s'inscrit dans un contexte architectural beaucoup plus flexible pouvant autoriser plus d'un saut. Il est donc nécessaire afin de rendre le protocole EAP opérant entre les couches 2 et 3, de définir un nouveau protocole permettant de transporter les paquets EAP indifféremment sur un ou plusieurs sauts. Ce nouveau protocole est présenté ci-après.

3.4. Le protocole EGEMO (EAP Geographic and positioning Encapsulation for Multi-hOp transport)

3.4.1. Description générale

Le protocole EGEMO est dédié au transport entre les couches 2 et 3 des paquets EAP; et ce, sur un ou plusieurs sauts dans un environnement hautement dynamique. Il permet en particulier à chaque OBU d'initier le processus d'authentification indépendamment du fait d'être à l'intérieur ou à l'extérieur de la zone de couverture du RSU. Pour ce faire, EGEMO utilise les informations de mobilité et les positions géographiques des OBUs et des RSUs qui sont dans ce contexte supposés embarquer un système de positionnement à l'instar du GPS (Global Positioning System) ou du futur système Galileo. Ces systèmes de positionnement permettent en outre de synchroniser temporellement les nœuds du réseau. Il est à noter que l'utilisation de ces systèmes pour l'acheminement des données dans les réseaux véhiculaires est assez largement acceptée comme étant la démarche la plus appropriée [HAR08] contrairement aux autres démarches fondées sur la topologie du réseau; topologie que l'on sait extrêmement volatile dans le cas des réseaux véhiculaires. Toutefois, à la différence des nombreux protocoles de routages géographiques (utilisant ces systèmes) qui ont été conçus pour les réseaux véhiculaires [FUB02] [FESTAG04], le protocole EGEMO possède des propriétés spécifiques convenant davantage au trafic d'authentification, à notre infrastructure de confiance et de sécurité et de manière générale aux exigences et défis de sécurité que nous avons définis. Ainsi, le protocole EGEMO est :

- *Dédié au transport des paquets d'authentification EAP*: EGEMO est conçu et optimisé pour le trafic d'authentification EAP dont il épouse les principales caractéristiques. C'est par exemple parce que EAP est un protocole de type *lockstep* (*i.e.* protocole de type requête-réponse ou protocole ne pouvant émettre de nouveau paquet avant la réception de l'accusé de réception du paquet précédent) qu'il n'est pas utile d'assurer

l'ordonnancement des paquets dans le protocole EGEMO lui-même devenu un protocole de type *lockstep*. EGEMO ne saurait donc a priori être utilisé pour le transport de tout type de trafic.

- *Sans état*: Il ne nécessite aucune construction de tables de routage ou de chemins et par conséquent aucun échange de messages de contrôle pour les maintenir. Cette propriété est particulièrement adaptée à un environnement hautement mobile où le voisinage des nœuds est en perpétuel renouvellement.

- *Basé sur l'acheminement par Broadcast plutôt que par Unicast*: Les messages à acheminer (*i.e.* les paquets EAP) sont diffusés de proche en proche jusqu'à leur destination. L'impact de la perte d'un lien qui est une phénomène très attendu dans les réseaux véhiculaires, est ainsi fortement réduit. De plus, il n'est pas nécessaire de disposer d'une infrastructure de routage et encore moins d'accéder aux services de la couche IP ou des couches supérieures avant l'authentification complète. C'est cette méthode d'acheminement par diffusion qui confère au protocole EGEMO la propriété d'être sans état. On notera que ce principe d'acheminement diffère de l'inondation classique par l'utilisation des coordonnées géographiques qui permettent d'éviter à l'ensemble des nœuds du réseau de participer à la diffusion des messages.

- *Caractérisé par un relayage opportuniste des paquets*: Tout OBU recevant un paquet dont il n'est pas destinataire est susceptible de le relayer (*i.e.* rediffuser) s'il estime utile de le faire pour atteindre efficacement la destination. Les nœuds amenés à participer au relayage d'un paquet ne peuvent donc être prédéterminés puisque la décision de relayer est prise de manière indépendante par chaque nœud. Pour un nœud donné, cette décision dépendra par exemple de sa position à ce moment là et de la connaissance qu'il aura du trafic dans le réseau.

- *Caractérisé par un acheminement multi-chemins*: En effet, le paquet faisant l'objet d'un acheminement peut arriver au nœud destinataire par plus d'un chemin. Cette propriété accroit la fiabilité de l'acheminement des paquets et permet en particulier de limiter l'impact des attaques de type DoS menées par des nœuds égoïstes (en anglais, *selfish nodes*) se refusant à relayer les paquets dont ils ne sont pas destinataires ou par des nœuds malveillants visant à faire dysfonctionner le réseau en jetant systématiquement tous les paquets. Il est à noter que l'acheminement multi-chemins et ses propriétés de fiabilité et de robustesse découlent du relayage opportuniste des paquets.

- *Sécurisé*: Le protocole EGEMO encapsule le paquet EAP via l'ajout d'un certain nombre de champs qui sont mis à jour par les nœuds relais au fur et à mesure de l'acheminement. Pour assurer la sécurité (*i.e.* l'authentification de la source et l'intégrité) de ces champs supplémentaires ainsi que celle du paquet EAP, le protocole EGEMO implémente un schéma de signature saut-par-saut (en anglais, *hop-by-hop signature*)

réputé convenir aux protocoles dont certains des champs sont modifiés par les nœuds relais. En d'autres termes, chaque nœud recevant un paquet EGEMO doit en vérifier la signature et le cas échéant relayer le paquet après avoir généré une nouvelle signature. Ces signatures sont construites à partir des certificats persistants ou volatiles des nœuds du réseau. Ainsi donc, toute injection ou altération des paquets par une entité externe (*i.e.* ne possédant pas les certificats appropriés) est détectée et de plus, une entité autorisée (*i.e.* possédant les certificats appropriés) menant la même action malveillante, peut être tracée par sa signature.

L'intégration des protocoles AUCRED et EGEMO permet d'obtenir une nouvelle pile EAP illustrée par la Figure 11. Le protocole AUCRED en tant que méthode d'authentification est situé au niveau de la couche authentification alors que les protocoles EAP et EGEMO sont situés au niveau de la couche EAP. Conformément aux exigences et aux défis de sécurité qui ont été définis, la couche EAP et la couche authentification sont effectivement implantées entre les couches 2 et 3 du modèle de référence des réseaux. La conception modulaire de ces protocoles permet d'envisager leur mise en œuvre sur diverses technologies radio dont en particulier les technologies DSRC (Dedicated Short Range Communications) [DSRC] conçues spécifiquement pour les communications véhiculaires.

La Figure 12 précise les couches traversées au niveau de chaque élément du réseau lors du processus d'authentification depuis l'OBU désireux de s'authentifier jusqu'à l'AS. Cette figure illustre en particulier un cas d'authentification sur 3 sauts (entre l'OBU et le RSU) mais qui reste généralisable quelque soit le nombre de sauts. Ce cas d'authentification intègre les protocoles AUCRED, EAP et EGEMO et est mis en œuvre sur la technologie radio DSRC pour ce qui est de la partie sans fil du réseau et sur la technologie IEEE 802.3 pour ce qui est de la partie filaire du réseau. A l'image de ce qui se pratique dans les architectures WLAN classiques, les paquets EAP sont transportés dans le réseau filaire (*i.e.* entre le RSU et l'AS) par des protocoles AAA tels que Remote Authentication Dial In User Service (RADIUS) ou Diameter.

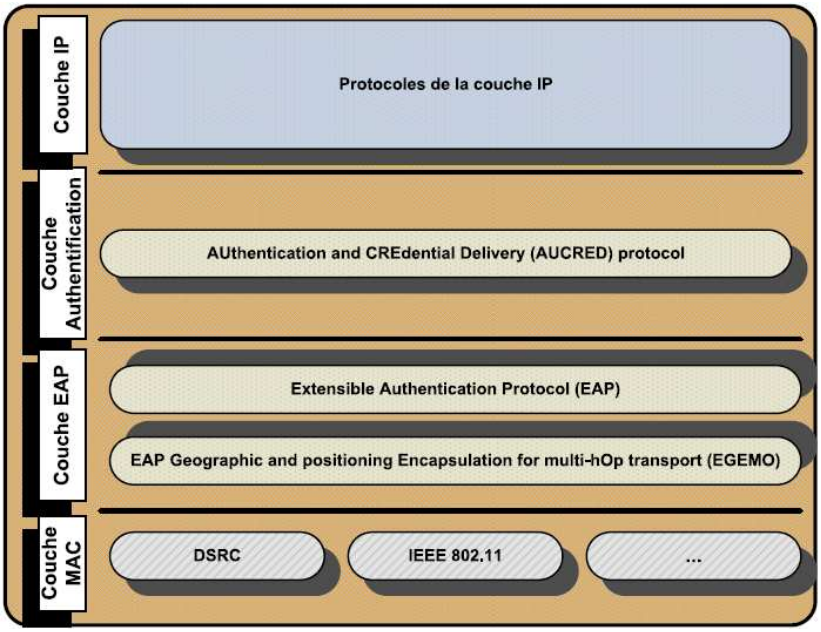


Figure 11: Pile EAP avec les protocoles AUCRED et EGEMO

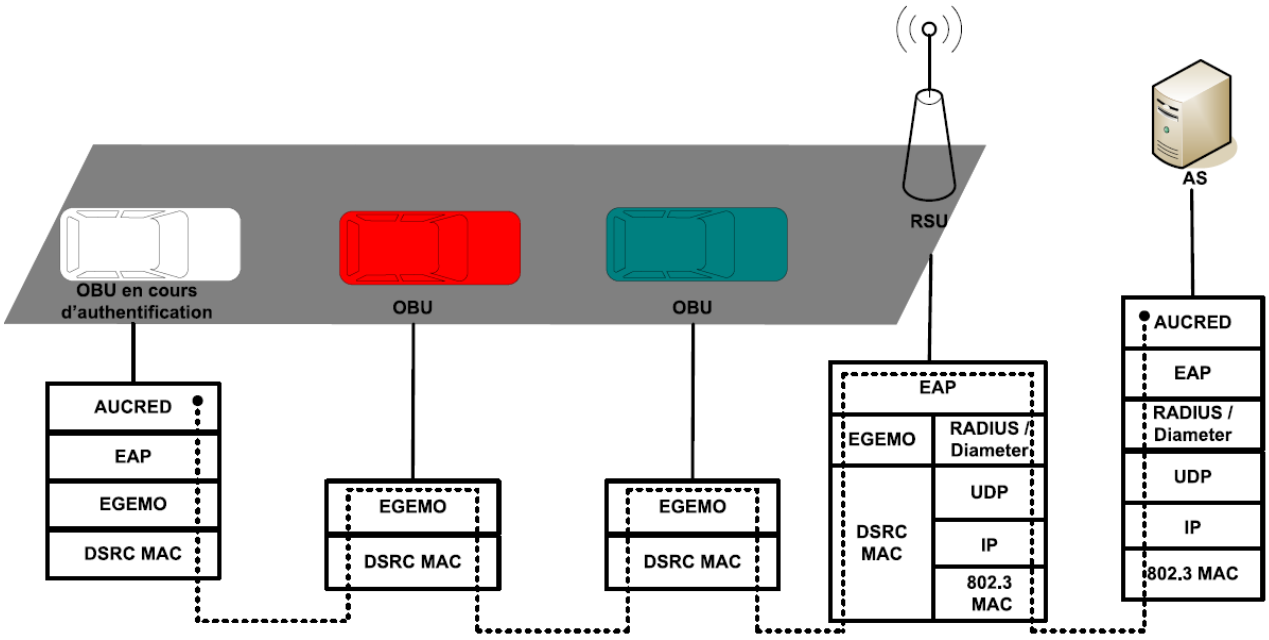


Figure 12: Couches (de la pile protocolaire) traversées lors de l'authentification entre OBU et AS

3.4.2. Format des paquets EGEMO

La Figure 13 représente le format général d'un paquet EGEMO ainsi que les tailles en octets de ses principaux champs.

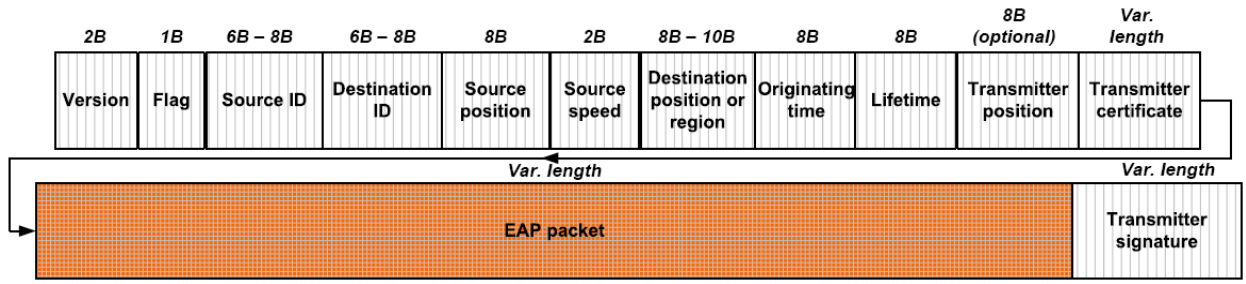


Figure 13: Format d'un paquet EGEMO

Parmi les principaux champs du paquet, on distingue:

- *Version* qui spécifie la version du protocole

- *Flag* utilisé pour spécifier l'absence ou la présence des champs optionnels (*e.g. Transmitter position*) ou pour contrôler les tailles de certains des champs dont les leurs sont variables (*e.g. Source ID, Destination ID, Destination position or region, Transmitter certificate, Transmitter signature*).

- *Source ID* pour identifier le nœud source de manière unique dans le réseau.

- *Destination ID* pour identifier le nœud destination de manière unique dans le réseau. Ce champ tout comme le champ précédent (*i.e. Source ID*) peut être dérivé d'une adresse MAC codée sur 6 ou 8 octets.

- *Source Position* contenant la position géographique courante de la source du paquet. Cette position est utilisée par la destination pour déterminer la région géographique dans laquelle se trouve la source (si celle-ci est mobile) au moment de lui envoyer une réponse.

- *Source speed* contenant la vitesse courante de la source. Cette valeur est utilisée par la destination pour approximer la vitesse de la source de manière à déterminer ensuite la région géographique dans laquelle se trouve cette source au moment de lui envoyer une réponse.

- *Originating time* qui indique l'heure à laquelle le paquet a été généré à la source. Ce champ est utilisé pour contrôler la date d'expiration du paquet. Il sert également d'estampille temporelle.

- *Lifetime* contenant une valeur de temps précisant la durée de validité du paquet.

- *Destination position or region* qui est un champ à contenance variable permettant de localiser géographiquement la destination. Il contient la position géographique de la destination si cette dernière est fixe. En revanche, si la destination est mobile, ce champ contient en plus de la dernière position géographique connue de cette destination, le rayon de mobilité de cette même destination. Le rayon de mobilité correspond à la distance maximale que pourra avoir parcouru la destination depuis la communication de sa dernière position géographique jusqu'à la réception du paquet courant. Ce rayon délimite une région géographique en forme de cercle dont le centre est la dernière position géographique connue. L'utilisation d'une région géographique en forme de cercle permet de localiser la destination quelque soit la direction qu'elle aura prise depuis la communication de sa dernière position géographique. Considérons un OBU nommé O et un RSU nommé R.; O envoie un paquet EGEMO à R et en réponse, R s'apprête à générer et à transmettre un paquet EGEMO à l'intention de O. On se place dans le pire cas en considérant que le paquet de réponse, une fois émis par R, arrivera à destination à la limite de sa durée de validité. Dans ces conditions, R détermine le rayon de mobilité de O au moment de la génération du paquet de réponse comme suit:

$$MobilityRadius = SourceSpeed_O * \left((CurrentTime - OriginatingTime_O) + Lifetime_R \right) \quad (2)$$

Où $SourceSpeed_O$ est la valeur contenue dans le champ éponyme du paquet EGEMO envoyé par O (*i.e.* la vitesse de O), *CurrentTime* est le temps courant, $OriginatingTime_O$ est la valeur contenue dans le champ éponyme du paquet EGEMO envoyé par O (*i.e.* l'heure de génération du paquet envoyé par O), $Lifetime_R$ est la valeur contenue dans le champ éponyme du paquet EGEMO que s'apprête à envoyer R (*i.e.* la durée de validité du paquet de réponse que R s'apprête à envoyer).

- *Transmitter position* qui est un champ optionnel indiquant la position géographique du nœud qui transmet le paquet. Ce champ est omis lorsque c'est la source du paquet qui transmet ce dernier. Dans ce cas en effet, la position du nœud qui transmet est la même que la position de la source du paquet contenue dans le champ *Source position*. Il est à noter que le champ *Transmitter position* permet de contrôler le relayage des paquets en assurant par exemple que des nœuds très proches (*i.e.* couvrant plus ou moins la même zone de couverture) ne diffusent pas inutilement à tour de rôle le même paquet.

- *Transmitter certificate* contenant le certificat du nœud qui transmet le paquet. Ce certificat indique si son porteur peut l'utiliser pour générer des signatures sur les paquets EGEMO, auquel cas, les algorithmes utilisés sont précisés. Ce certificat est utilisé par les nœuds qui reçoivent le paquet pour en vérifier la signature. La taille de ce champ varie en fonction des standards cryptographiques considérés.

- *EAP packet* contenant le paquet EAP proprement dit. La taille de ce champ est fonction de la charge utile du paquet EAP.

- *Transmitter signature* contenant une signature produite sur le condensat de l'ensemble des autres champs du paquet. Cette signature est générée par le nœud qui transmet le paquet. Sa taille est fonction des standards cryptographiques utilisés.

3.4.3. Les algorithmes EGEMO

Le protocole EGEMO est exécuté dans les OBUs et les RSUs aussi bien à la réception d'un paquet du protocole EAP destiné à la couche 2 qu'à la réception d'un paquet de la couche 2 destiné au protocole EAP. Le principe de cette mise en œuvre transparaît de l'implantation du protocole EGEMO dans la pile EAP (voir la Figure 11). Les algorithmes qui fondent le protocole EGEMO supposent la connaissance par tous les OBUs des identités ou adresses des RSUs ainsi que leurs coordonnées géographiques. Les mécanismes qui président à l'acquisition de cette connaissance ne sont pas traités dans cette thèse. On notera cependant que ces mécanismes peuvent être dynamiques (*i.e.* connaissance acquise via un protocole réseau de découverte) ou statiques (*i.e.* connaissance pré-implantée dans les OBUs). Les algorithmes EGEMO supposent également l'exécution de l'authentification via le RSU géographiquement le plus proche de l'OBU à l'initiative de l'authentification. La Figure 14 donne une vue globale des principales fonctions qui sous-tendent ces algorithmes au niveau de l'OBU et du RSU.

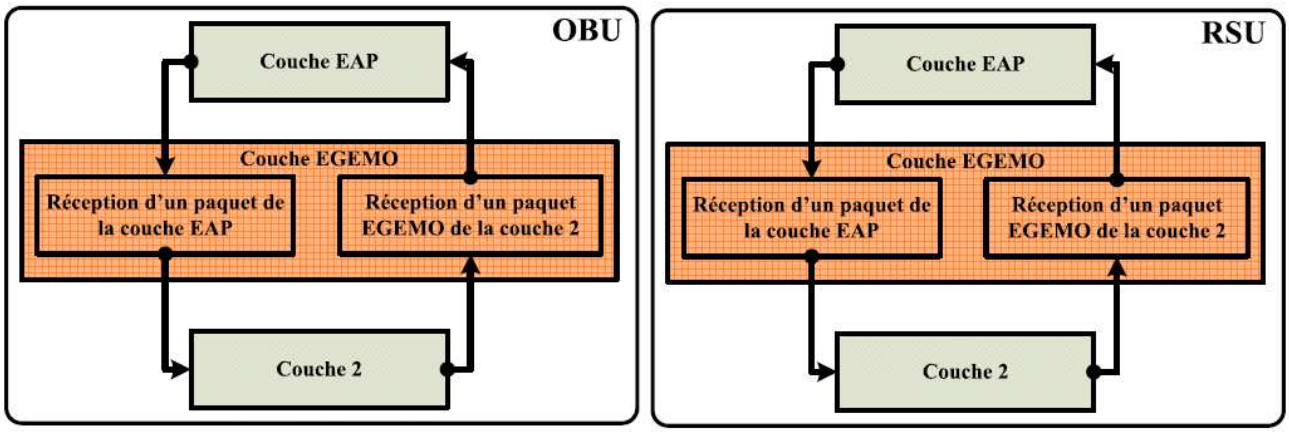


Figure 14: Vue globale des fonctions EGEMO au niveau de l'OBU et du RSU

Plus en détail, ces fonctions sont comme suit:

- *Réception (dans un OBU) d'un paquet provenant du protocole EAP et destiné à la couche 2*

Cette fonction est activée chaque fois qu'un paquet EAP est transmis au protocole EGEMO. En cas d'initialisation d'une nouvelle session EAP, le RSU destinataire sélectionné par l'OBU est celui qui est géographiquement le plus proche sinon c'est le RSU de la session courante qui est choisi. Le paquet est ensuite encapsulé dans un paquet EGEMO puis est transmis à la couche 2 pour diffusion. Cette opération d'encapsulation et de transmission à la couche 2 est répétée chaque fois que le temps d'attente[7] limite défini pour recevoir le paquet de réponse expire. Il est à noter que la réception du paquet de réponse est détectée par la présence d'un paquet dans la mémoire tampon de réception gérée par le protocole EGEMO et affectée au stockage temporaire des paquets dont la charge utile est à remonter au protocole EAP. En raison de la caractéristique *lockstep* du protocole EAP et donc du protocole EGEMO, cette mémoire tampon ne peut contenir pour une session donnée et à un moment donné, qu'au plus un paquet EGEMO et ce paquet transporte nécessairement la réponse au paquet EAP en cours de transmission par le protocole EGEMO. Notons également qu'en plus du temps d'attente avant retransmission, il est également défini un nombre maximum de retransmissions au bout duquel le paquet EAP est abandonné.

Comme l'illustre la Figure 15, l'organigramme de la fonction de réception dans un OBU d'un paquet provenant du protocole EAP, s'organise en un état d'attente, un évènement correspondant à la réception d'un paquet EAP, 4 tests conditionnels et 8 actions assurant la sélection du RSU destinataire, la construction du paquet EGEMO, sa transmission à la couche 2 et la gestion des retransmissions.

[7] Ce temps d'attente limite est généralement appelé *Retransmisssion Time-Out (RTO).*

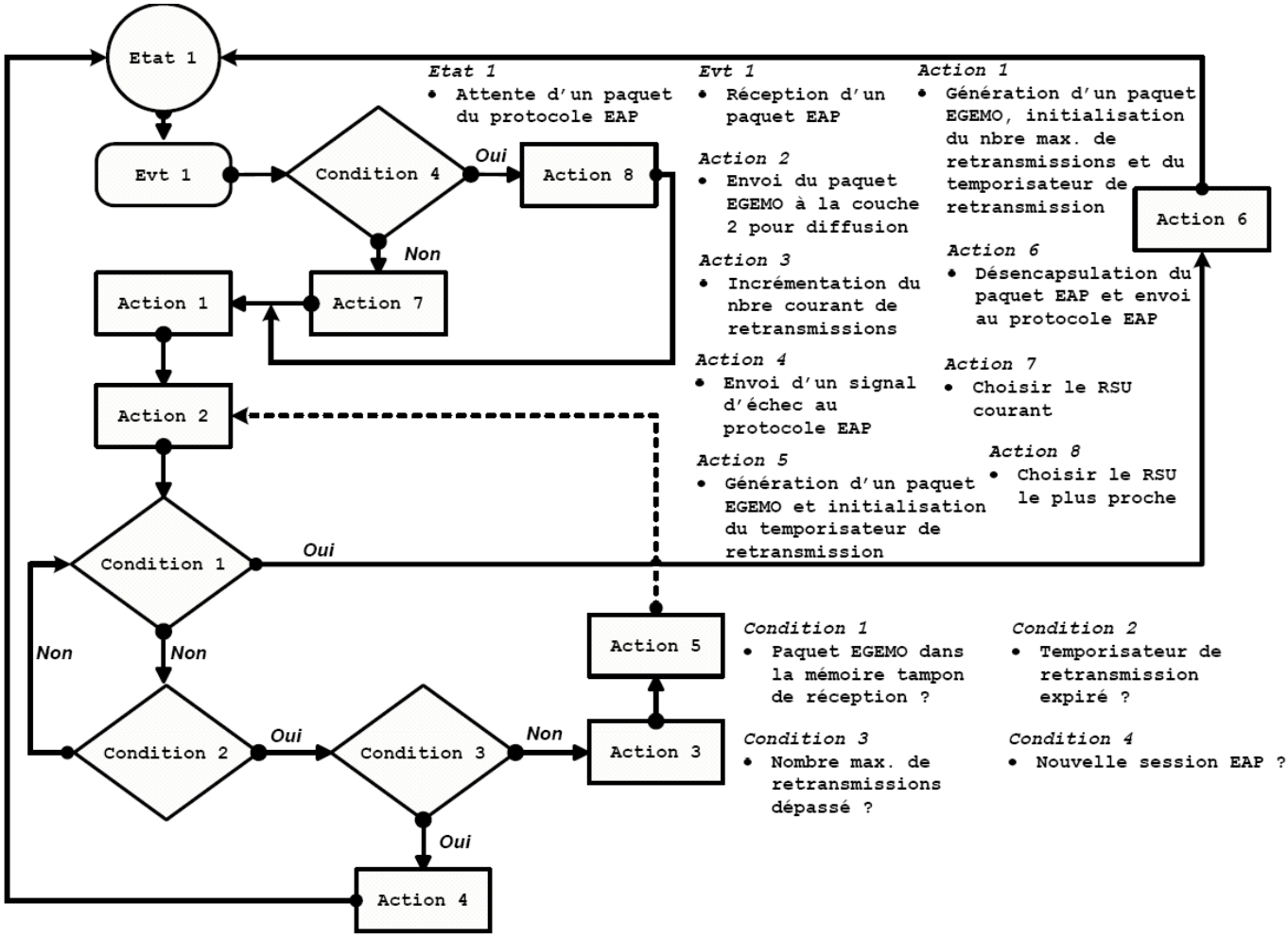


Figure 15: Réception dans un OBU d'un paquet provenant du protocole EAP et destiné à la couche 2

- *Réception (dans un OBU) d'un paquet EGEMO provenant de la couche 2*

Cette fonction est exécutée chaque fois qu'un paquet EGEMO est remonté par la couche 2. Lorsque le paquet reçu est à destination de l'OBU (*i.e. Destination ID = OBU ID*), le paquet est stocké dans la mémoire tampon de réception (en attendant d'être remonté au protocole EAP) après la mise en œuvre d'une série de tests visant à s'assurer que la duré de validité du paquet n'a pas expiré, que l'estampille temporelle du paquet est différente et n'est pas antérieure à l'estampille du dernier paquet reçu de la même source (ce test permet de s'assurer que le paquet correspond à l'état le plus récent du protocole) et que la validité du contenu de chacun des champs du paquet (*e.g.* certificat, signature) est vérifiée. Si les tests précédents sont tous vérifiés alors que l'OBU n'est pas destinataire du paquet (*i.e. Destination ID ≠ OBU ID*), alors le paquet est mis à jour et est retransmis à la couche 2 pour diffusion (*i.e.* le paquet est relayé) après la mise en œuvre de tests supplémentaires. Ces tests supplémentaires permettent notamment de s'assurer que l'OBU est dans la zone géographique délimitée par le rayon de mobilité de la destination ou que l'OBU est plus proche de la destination que ne l'est le dernier

émetteur du paquet. Ces derniers tests permettent de ne sélectionner prioritairement pour relayer les paquets que les OBUs les mieux placés géographiquement. Pour illustrer, si *T* est l'OBU qui vient de diffuser le paquet EGEMO, *C* l'OBU qui le reçoit, *D* l'OBU à qui le paquet est destiné, $MobRad_D$ le rayon de mobilité de *D*, *Distance (X, Y)* la fonction de distance entre 2 nœuds *X* et *Y*, alors on dira que *C* est dans la zone géographique délimitée par le rayon de mobilité de *D* si:

$$Distance(C,D) \leq MobRad_D \quad (3)$$

On dira également que *C* est plus proche de la destination *D* que ne l'est *T* si:

$$Distance(C,D) < Distance(T,D) \quad (4)$$

Il est à noter que dans la fonction *Distance (X, Y)*, *X* et *Y* représentent les coordonnées géographiques respectives des entités *X* et *Y*.

La Figure 16 illustre l'organigramme de la fonction de réception d'un paquet EGEMO provenant de la couche 2 au niveau d'un OBU. Cet organigramme s'organise en un état d'attente, un évènement correspondant à la réception d'un paquet EGEMO, 6 tests conditionnels et 3 actions aboutissant soit à la transmission du paquet à la couche 2 pour diffusion, soit à son stockage temporaire dans la mémoire tampon de réception, soit à son abandon.

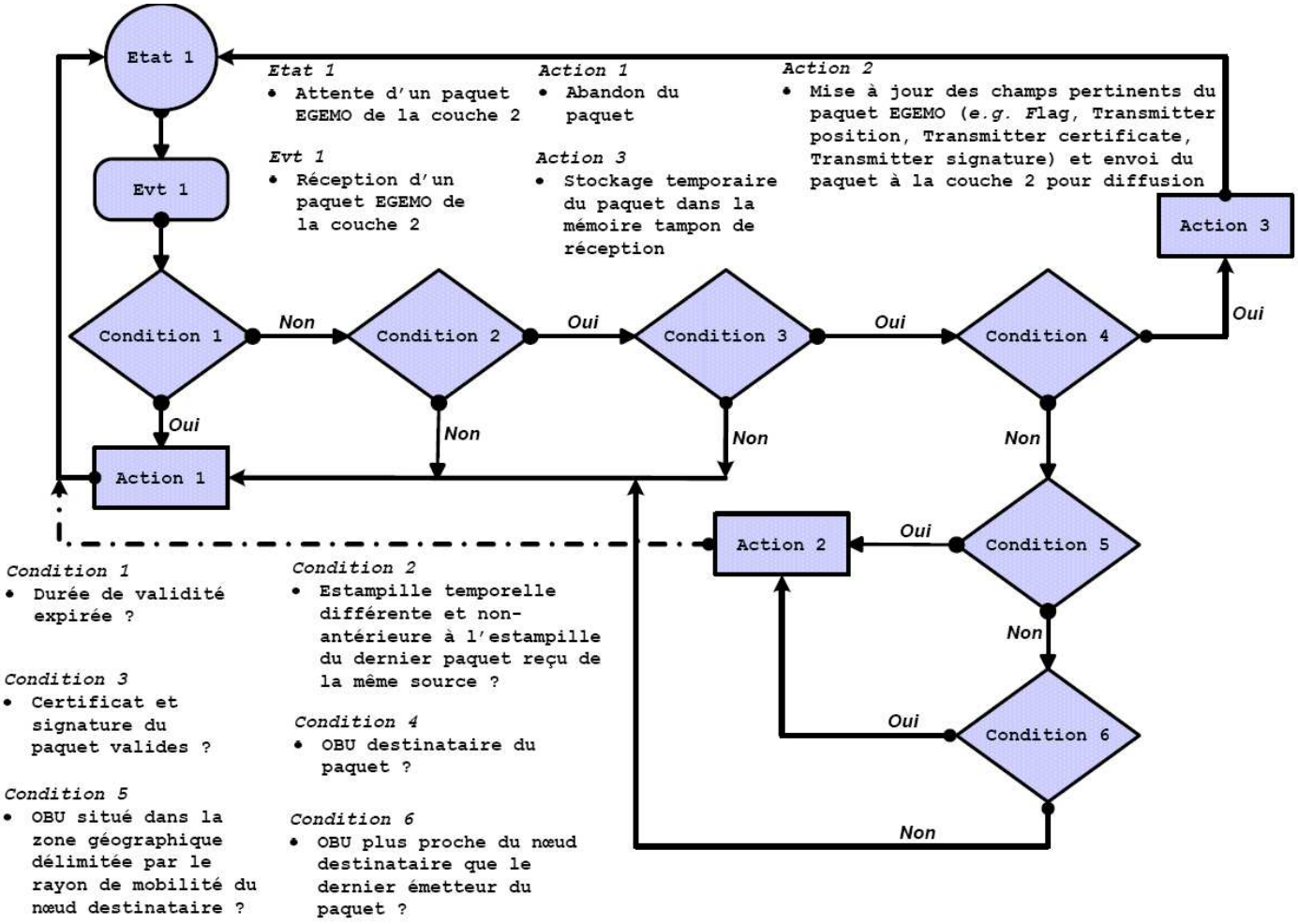


Figure 16: Réception dans un OBU d'un paquet EGEMO provenant de la couche 2

- *Réception (dans un RSU) d'un paquet EGEMO provenant de la couche 2*

Contrairement à la fonction de réception du même nom dans un OBU, cette fonction ne donne jamais lieu à la retransmission du paquet reçu (*i.e.* transmission du paquet à la couche 2 après mise à jour des champs EGEMO) puisque le RSU durant la phase d'authentification ne peut être que destinataire de paquet; ce qui lui enlève toute vocation à relayer les paquets EGEMO. Plus concrètement, le paquet reçu n'est traité que dans la mesure où il est destiné au RSU. Dans ce cas, le paquet est stocké dans la mémoire tampon de réception de la session courante (en attendant d'être remonté au protocole EAP) après la mise en œuvre des tests visant à s'assurer que la duré de validité du paquet n'a pas expiré, que l'estampille temporelle du paquet est différente et n'est pas antérieure à l'estampille du dernier paquet reçu de la même source (ce test permet de s'assurer que le paquet correspond à l'état le plus récent du protocole) et que la validité du contenu de chacun des champs du paquet (*e.g.* certificat, signature) est vérifiée. De plus, lorsque tous ces tests sont vérifiés, le RSU sauvegarde dans le contexte de la session en cours, les coordonnées géographiques ainsi que les informations de mobilité de la

source du paquet. Ces données vont être utilisées par le RSU pour évaluer le rayon de mobilité de l'OBU et construire le prochain paquet EGEMO à destination de cet OBU.

La fonction de réception (dans un RSU) d'un paquet EGEMO provenant de la couche 2 est illustrée par la Figure 17. Cet organigramme s'organise en un état d'attente, un évènement correspondant à la réception d'un paquet EGEMO, 4 tests conditionnels et 2 actions aboutissant soit au stockage temporaire du paquet dans la mémoire tampon de réception de la session soit à l'abandon du paquet.

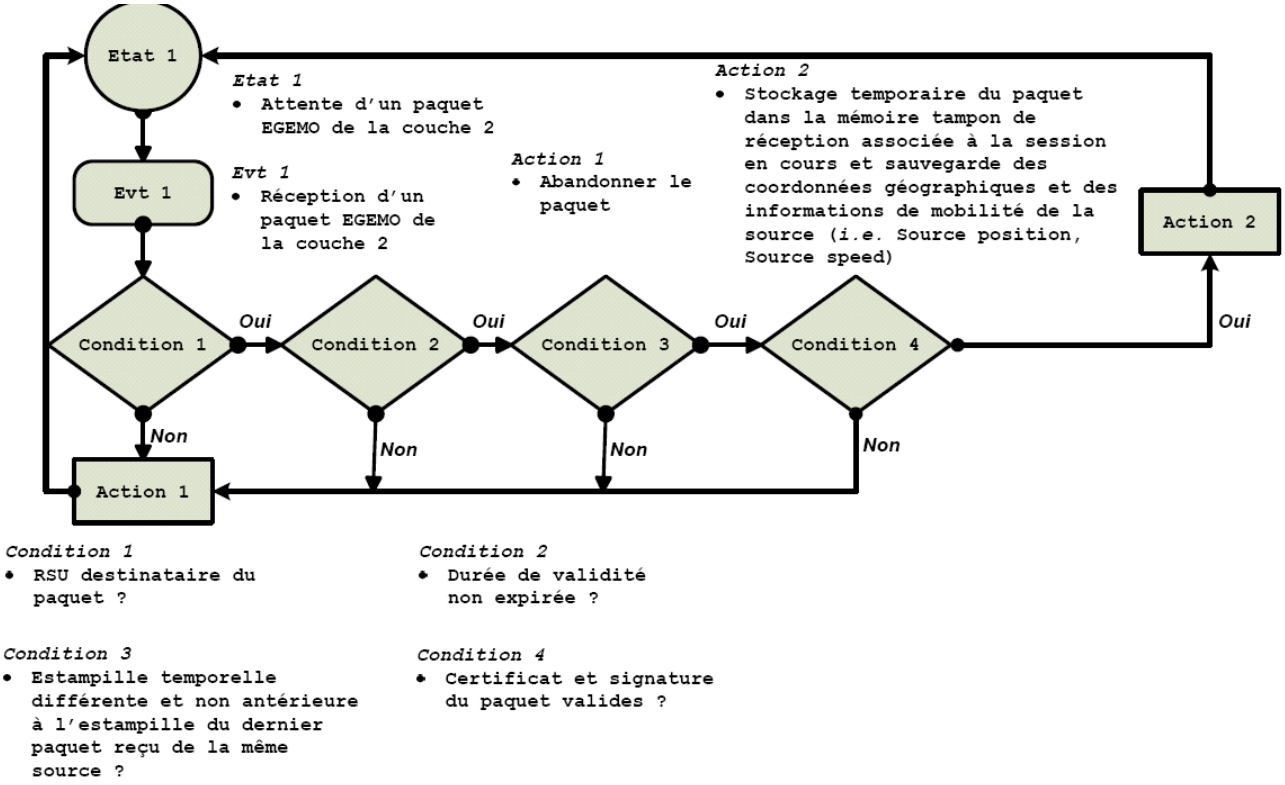


Figure 17: Réception dans un RSU d'un paquet EGEMO provenant de la couche 2

- *Réception (dans un RSU) d'un paquet provenant du protocole EAP et destiné à la couche 2*

Cette fonction ne diffère de la fonction du même nom dans un OBU que dans la mesure où le RSU n'initie pas de session et par conséquent n'a pas à déterminer ou sélectionner un OBU destinataire; ce dernier étant connu à l'avance du fait de la réception antérieure d'un premier paquet initiant le processus d'authentification. Compte tenu de la mobilité de l'OBU destinataire, cette fonction donne lieu au calcul d'un rayon de mobilité.

Comme dépeint sur la Figure 18, l'organigramme de la fonction de réception dans un RSU d'un paquet provenant du protocole EAP, s'organise en un état d'attente, un évènement correspondant à la réception d'un paquet EAP, 3 tests conditionnels et 7 actions assurant le calcul du rayon de mobilité de la destination, la construction du paquet EGEMO, sa transmission à la couche 2 et la gestion des retransmissions.

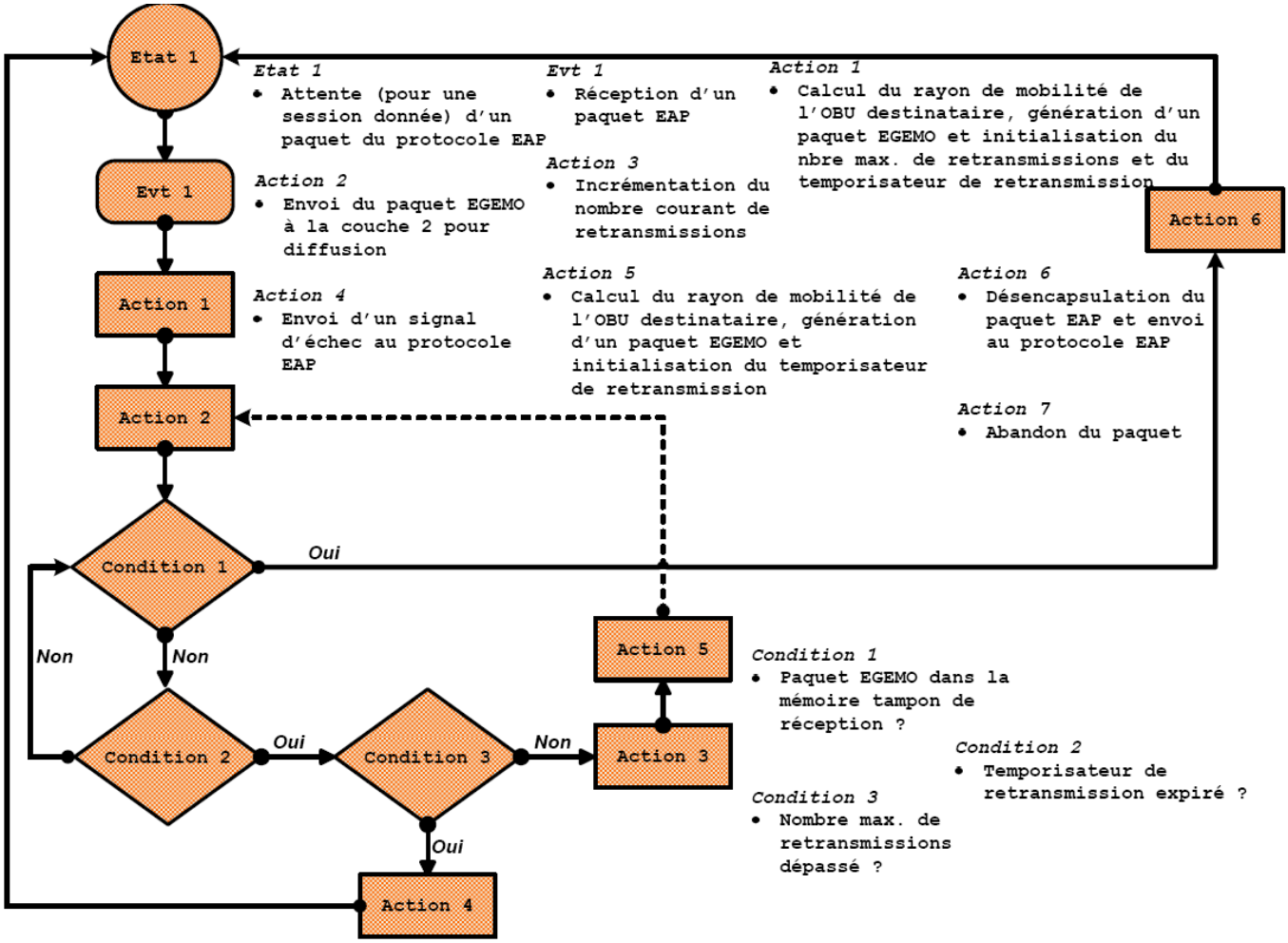


Figure 18: Réception dans un RSU d'un paquet provenant du protocole EAP et destiné à la couche 2

4. Conclusion

Les architectures et protocoles introduits dans ce chapitre constituent une des toutes premières contributions adressant la problématique d'authentification pour l'accès au réseau et aux services dans les réseaux véhiculaires opérés. Cette contribution comprend globalement une architecture réseau, une infrastructure de confiance et de sécurité, un protocole d'authentification et de délivrance des lettres de créance (AUCRED) et un protocole de transport multi-sauts des paquets d'authentification (EGEMO). En prenant en compte les modèles et les contraintes de sécurité spécifiques aux services ITS et aux services non-ITS, cette contribution répond aux préoccupations de l'opérateur dans sa démarche de fourniture du plus grand nombre possible de services à valeur ajoutée dans ces nouveaux types de réseaux. De plus, nos architectures et protocoles ont été définis pour convenir à la forte dynamique des réseaux véhiculaires (*e.g.* architecture réseau flexible, transport opportuniste

et multi-chemins des paquets d'authentification, etc.) tout en conférant un niveau élevé aussi bien du point de vue de la sécurité du réseau (*e.g.* accès restrictif aux services IP et couches supérieures, mécanisme anti-DoS à base de *Cookie* dans le protocole d'authentification, transport opportuniste et multi-chemins des paquets d'authentification pour contrer des attaques DoS par non-coopération etc.) que du point de vue de la préservation de l'intimité numérique des utilisateurs (*e.g.* certificats anonymes, certificats volatiles, coefficient de non-traçabilité, etc.). Il est à noter que l'évolutivité de notre solution par rapport aux contextes cryptographiques futurs est assez largement garantie par les mécanismes de négociation que nous avons voulus consubstantiels au protocole d'authentification. Notons enfin que la claire identification des différents modules de notre solution, de même que celle des couches réseau qu'elle impacte, lui confère la possibilité d'être mise en œuvre sur des technologies de communication diverses.

Nos architectures et protocoles ayant été conceptuellement définis et détaillés, il ne reste désormais plus qu'à évaluer leurs performances du point de vue réseau. Nous avons à cet effet choisi de mener une évaluation par le biais des simulations. C'est toute la substance du chapitre qui va suivre.

Chapitre 2.2. Simulations et Analyse des Performances

1. Introduction

Après avoir défini les architectures et protocoles pour l'authentification, il s'agit dans ce chapitre d'en évaluer les performances par le biais des simulations. Pour ce faire, le logiciel de simulation GrooveNet [MAN06] est utilisé. Ce logiciel est un outil de simulation libre dédié aux communications véhiculaires. Les communications IVC (Inter-Vehicular Communications) et RVC (Road-to-Vehicle Communications) y sont modélisées, de même que la topographie réelle des routes, le système de positionnement GPS et divers autres modèles dont les modèles d'itinéraire et de mobilité. Une présentation et une documentation complètes du simulateur GrooveNet peuvent être trouvées en ligne sur [GROOVENET].

Bien que le simulateur GrooveNet contienne déjà un certain nombre de modèles indispensables à la modélisation des communications véhiculaires, il a été nécessaire de le compléter en ajoutant un modèle de couche physique plus réaliste et plus en ligne avec la norme IEEE 802.11p [IEEE-802.11p] dont on admet qu'elle est la base de la couche radio DSRC (Dedicated Short Range Communications) [DSRC]. L'approche d'implémentation de cette nouvelle couche physique dans l'outil GrooveNet est la même que celle suivie par [YUN05]. Dans cette approche, la détermination de la probabilité d'erreur lors de la transmission d'un paquet tient compte de la position des entités communicantes (*e.g.* vue directe (LOS) ou indirecte (NLOS)), de leur environnement de communication, des interférences et de nombreux autres paramètres (dont certains sont spécifiques au standard IEEE 802.11p) comme la puissance de transmission, le codage canal, etc. Il est à noter qu'à la date de rédaction de ce mémoire la norme IEEE 802.11p est encore en cours de finalisation à l'IEEE. Une présentation du modèle de communication DSRC est faite dans le Chapitre 2.4.

Au-delà de l'implémentation d'une nouvelle couche physique, nous avons implémenté notre solution proprement dite, soit essentiellement les protocoles EAP, AUCRED et EGEMO. Afin de comparer notre solution avec le modèle d'authentification EAP classique sur un saut, nous avons également implémenté le protocole EAP Over LAN (EAPoL) [IEEE-802.1X] en l'adaptant au contexte des communications véhiculaires dans lequel on exclut par exemple l'association explicite entre OBU et RSU [C2C-CC07]. Le fait que la technologie EAPoL soit une technologie pour le transport des paquets EAP au niveau de la couche 2 tout comme l'est la technologie EGEMO, justifie son choix pour cette analyse comparative.

Une fois les modèles et protocoles précédents implémentés, il a été possible de réaliser de nombreuses simulations de notre solution (*i.e.* EGEMO) ainsi que de l'authentification classique sur un saut (*i.e.* EAPoL). Ces simulations ont été menées suivant diverses densités d'OBUs et de RSUs.

S'agissant de l'organisation de ce chapitre, nous commencerons par présenter en section 2, les scénarios de simulation ainsi que les métriques de performance que nous avons retenues. Dans la section 3, nous présenterons les résultats des simulations et procèderons à l'analyse des performances proprement dite. Enfin, la section 4 conclura le chapitre.

2. Scénarios de simulation et métriques de performance

2.1. Scénarios de simulation

Nous considérons pour nos simulations une circulation (rapide) en agglomération avec une vitesse des OBUs variant uniformément entre *46* km/h et *72* km/h (*i.e.* entre *12.77* m/s et *20* m/s) et ayant comme moyenne *59.4* km/h (*i.e. 16.5* m/s). Les OBUs et les RSUs embarquent un système GPS leur fournissant une horloge globale ainsi que les données de positionnement en temps réel. Nous supposons dans ces simulations que les RSUs et en particulier leurs positions géographiques et leurs identifiants sont connus de tous les OBUs. Cette pré-connaissance qu'ont les OBUs leur permet de toujours initier le processus d'authentification via le RSU géographiquement le plus proche.

Au niveau de la couche radio des OBUs et des RSUs, le codage canal le plus robuste est choisi (*i.e.* BPSK1/2 (Binary Phase Shift Keying avec un taux de redondance à *50%*)) avec un débit physique à *6* Mbps. La puissance de transmission est fixée à *20* dBm (*i.e. 100* mW) et tous les nœuds sont équipés d'antennes omnidirectives ayant une taille d'environ *1.65* m. Toutes les communications se font sur le 5ème canal radio. La fréquence centrale de ce canal est de *5.9* GHz et sa largeur de bande est de *10* MHz. La portée de transmission des OBUs et des RSUs est limitée à *200* m.

S'agissant de la topologie de l'environnement de simulation, elle peut être considérée comme linéaire, la largeur des routes étant négligeable par rapport à la portée de transmission des nœuds du réseau. La longueur de la route utilisée dans nos simulations est fixée à *6* km. Notre évaluation porte sur 2 densités de RSUs, chacune de ces densités étant choisie de manière à rendre possible des communications multi-sauts entre OBUs et RSUs dès le premier paquet initiant le processus d'authentification. Le premier cas de densité correspond à 3 RSUs répartis le long de la route suivant une distribution d'un RSU tous les *2* km. Quant au 2ème cas de densité, il correspond à 2 RSUs répartis le long de la route suivant une distribution d'un RSU tous les *4* km. Ces scénarios de densité des RSUs sont illustrés par la Figure 1.

Il convient de relever qu'une densité de RSUs est reconnue permettre des communications multi-sauts entre OBUs et RSUs dès le premier paquet initiant le processus d'authentification, si cette densité est telle que la distance moyenne inter-RSUs est supérieure à 2 fois la portée de transmission des nœuds (*i.e.* supérieure à *400* m dans notre cas précis) en supposant bien entendu que les OBUs s'authentifient toujours via le RSU le plus proche et que les portées de transmission de tous les nœuds sont égales. Ainsi, sous les mêmes hypothèses, une densité de RSUs rendra impossible toute communication multi-sauts dès le premier paquet initiant le processus d'authentification si elle est telle que la distance moyenne inter-RSUs est inférieure ou égale à 2 fois la portée de transmission des nœuds (*i.e.* inférieure ou égale à *400* m dans notre scénario précis). En effet dans ce dernier cas, les OBUs sont nécessairement et de manière permanente dans la zone de couverture d'au moins un RSU.

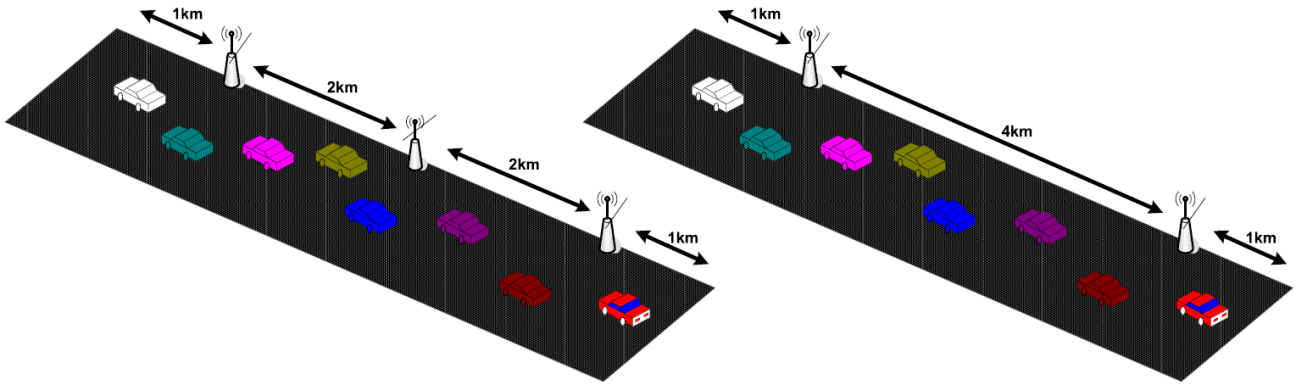


Figure 1: Densités de RSUs considérées pour les simulations

Pour ce qui est de la densité des OBUs, nous avons retenu jusqu'à 6 scénarios de densité correspondant à autant de distributions poissonnièmes:

- La première distribution de Poisson suppose un temps moyen d'inter-arrivées de *12* s, soit un taux moyen d'arrivées de *1/12*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *200* m.

- La deuxième distribution de Poisson suppose un temps moyen d'inter-arrivées de *9* s, soit un taux moyen d'arrivées de *1/9*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *150* m.

- La troisième distribution de Poisson suppose un temps moyen d'inter-arrivées de *6* s, soit un taux moyen d'arrivées de *1/6*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *100* m.

- La quatrième distribution de Poisson suppose un temps moyen d'inter-arrivées de *3* s, soit un taux moyen d'arrivées de *1/3*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *50* m.

- La cinquième distribution de Poisson suppose un temps moyen d'inter-arrivées de *1.5* s, soit un taux moyen d'arrivées de *2/3*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *25* m.

- La sixième et dernière distribution de Poisson suppose quant à elle un temps moyen d'inter-arrivées de *0.6* s, soit un taux moyen d'arrivées de *5/3*, ce qui correspond, en considérant une vitesse moyenne des OBUs de *16.5* m/s, à une distance moyenne inter-OBUs de *10* m.

Du point de vue de la sécurité nous considérons dans nos simulations l'utilisation par la PTA et par le NO d'une infrastructure PKI 1-tiers. En conséquence, la longueur de la chaine de certificats que présente l'OBU ou l'AS au moment de l'authentification est toujours égale à 1. Autrement dit, la validation d'un certificat par l'OBU ou par l'AS ne requiert aucun certificat intermédiaire; étant entendu que l'entité validatrice est déjà en possession de la clé publique du certificat racine ayant servi à délivrer le certificat à valider. Conformément aux préconisations de notre infrastructure de confiance et de sécurité, nous considérons l'utilisation du PKCS (Public Key Cryptographic Standard) ECC 163 (*i.e.* ECC avec une taille de clé de 163 bits). En conséquence, l'utilisation des algorithmes Elliptic Curve Digital Signature Algorithm (ECDSA) et Elliptic Curve Integrated Encryption Scheme (ECIES) est supposée pour la signature et le chiffrement respectivement. Les algorithmes SHA-1et MD5 sont quant à eux utilisés pour les opérations de hachage. Pour ce qui est de la préservation de l'intimité numérique, nous considérons pour l'ensemble de nos simulations un coefficient de non-traçabilité de *0.5*; soit, si on suppose une vitesse moyenne des OBUs de *16.5 m/s*, un intervalle de réauthentification de *61 s* pour la première configuration des RSUs (*i.e.* distance inter-RSUs de *2 km*) et un intervalle de réauthentification de *121 s* pour la deuxième configuration des RSUs (*i.e.* distance inter-RSUs de *4 km*) (voir Equation 1 dans le Chap 2.1 pour les calculs).

Dans nos simulations les traitements cryptographiques proprement dits sont négligés puisque les OBUs sont suffisamment robustes pour embarquer de grandes quantités d'énergie et des processeurs performants de manière à permettre cette simplification. En revanche, les bits supplémentaires induits par l'utilisation des algorithmes cryptographiques sont pris en compte. Les tailles de ces bits sont déduites pour l'essentiel de [CSI02] et de [TLS]. Nos simulations portent donc davantage sur les communications réseau que sur les traitements processeurs.

Notons enfin que les résultats obtenus pour chaque scénario considéré (*i.e.* chaque densité d'OBUs et chaque densité de RSUs) sont des moyennes calculées chacune sur 20 simulations. La durée d'une simulation dans ce contexte est fixée à *900* s. Le Tableau 1 résume les paramètres de nos simulations.

Tableau 1: Principaux paramètres de simulation

Authentification EGEMO		***Authentification EAPoL***	
Paramètre	**Valeur**	**Paramètre**	**Valeur**
Durée de validité d'un paquet EGEMO	2 s	*Durée de validité d'un paquet EAP*	2 s
Temporisateur de retransmission (RTO)	2 s	*Temporisateur de retransmission (RTO)*	2 s
Nombre maximum de retransmissions	3	*Nombre maximum de retransmissions*	3
Authentification EGEMO et Authentification EAPoL			
Paramètre		**Description ou Valeur**	
PKCS		ECC 163 – Architecture PKI 1-tiers	
Coefficient de non-traçabilité ($F_{non-trac}$)		0.5	
Topologie		6 Km en topologie linéaire	
Densités de RSUs		1 RSU tous les 2 Km, 1 RSU tous les 4 Km	
Taux d'arrivée des OBUs (nombre d'OBUs par seconde)		1/12, 1/9, 1/6, 1/3, 2/3, 5/3	
Mobilité		Vitesse des OBUs uniformément variée (12.77 m/s – 20 m/s) - Vitesse moyenne de 16.5 m/s	
Couche MAC		DSRC CSMA CW_{Min} 15 Time Slot 13 us SIFS Time 32 us	
Couche Radio		Fréquence centrale 5.9 GHz Largeur de bande 10 MHz Antenne omnidirective de 1.65 m de hauteur Puissance de transmission 100 mW (20 dBm) Modulation OFDM BPSK ½ Portée de transmission 200 m Débit physique 6 Mbps	
Nombre de simulations et durée de chaque simulation		20 simulations (de 900 s chacune) par scénario (*i.e.* par densité de RSUs, densité d'OBUs et approche d'authentification)	

2.2. Métriques de performance

Nous avons défini une dizaine de métriques de performance aux fins d'analyser les résultats de nos simulations. Nous distinguons à cet effet:

- *Le taux de succès de l'authentification*: Ce taux est le rapport entre le nombre de requêtes d'authentification se soldant par un succès (*i.e.* réception du message EAP-Success) et le nombre total de requêtes (*i.e.* requêtes se soldant ou ne se soldant pas par un succès). Autrement dit, ce taux dénote le pourcentage de succès d'authentification des OBUs. Il peut également traduire un certain niveau de sécurité ou de confiance dans le réseau.

- *Le délai d'authentification*: Ce délai correspond au temps écoulé entre la transmission par un OBU d'un paquet initiant le processus d'authentification et la notification du succès de l'authentification.

- *Le taux d'Overhead imputable aux authentifications réussies*: Ce taux est le rapport entre le nombre de paquets transmis dans le réseau et ayant abouti à des succès d'authentification et le nombre total de paquets transmis (*i.e.* paquets ayant abouti ou n'ayant pas abouti à des succès d'authentification). Cette métrique illustre l'efficacité de l'authentification par rapport à l'Overhead généré dans le réseau. Plus la valeur de cette métrique est importante, plus le processus d'authentification est considéré comme efficace par rapport à l'Overhead généré dans le réseau.

- *Le taux de perte d'une authentification réussie*: Ce taux est le rapport entre le nombre de paquets perdus entre un OBU désireux de s'authentifier et un RSU et le nombre total de paquets transmis par les 2 nœuds lors du processus d'authentification. Ce taux de perte porte sur les authentifications ayant abouti au succès.

- *Le niveau de sollicitation de l'AS*: Cette métrique correspond au nombre de paquets EAP traités par l'AS. Elle traduit le taux d'occupation de l'AS.

- *Le taux de retransmission d'une authentification réussie*: Ce taux correspond au pourcentage de paquets retransmis par rapport à l'ensemble des paquets transmis entre un OBU et un RSU au cours du processus d'authentification. Ce taux est calculé exclusivement en référence aux authentifications ayant abouti au succès.

- *Le taux de retransmission inutile d'une authentification réussie*: Ce taux est le rapport entre le nombre de retransmissions inutiles et le nombre total de transmissions entre un OBU et un RSU au cours du processus d'authentification. Il est à noter qu'une retransmission est dite inutile si la réception à la destination du paquet retransmis ne modifie pas ou ne fait pas évoluer l'état du protocole d'authentification. C'est le cas lorsqu'un paquet EAP est reçu alors qu'il avait déjà été reçu et traité précédemment.

- *Le taux de perte dû à un défaut de connectivité*: Ce taux correspond au pourcentage de paquets perdus en raison d'un défaut de connectivité (*i.e.* absence d'OBU relais) par rapport à l'ensemble des paquets générés dans le réseau.

- *Le nombre de sauts d'une tentative d'authentification*: Cette métrique illustre le nombre de sauts (entre un OBU et un RSU) que traversent les paquets lors du processus d'authentification; que ce processus se solde ou non par un succès.

- *Débit du trafic d'authentification*: Cette métrique traduit le débit induit dans le réseau par le trafic lié au processus d'authentification. Elle est le rapport entre la somme des tailles des paquets d'authentification générés dans le réseau durant toute la simulation et la durée de cette simulation.

Dans notre analyse des performances, les métriques introduites ci-dessus sont illustrées sur les différentes courbes sous forme de moyennes. Ces moyennes sont obtenues sur chaque simulation puis sur l'ensemble des simulations du scénario considéré (*i.e.* densité d'OBUs et densité de RSUs considérées).

2.3. Analyse des performances

Comme introduit dans la présentation des scénarios de simulation, nous considérons 2 hypothèses principales dans notre analyse à savoir une même portée de transmission pour tous les nœuds du réseau et des densité de RSUs telles que la distance inter-RSUs est supérieure à 2 fois la portée de transmission des nœuds (*i.e.* des communications multi-sauts sont possibles dès le premier paquet initiant le processus d'authentification). Les conclusions et observations générales que nous déduirons de notre analyse, sont donc à mettre en correspondance avec ces hypothèses.

Les analyses de l'évolution des différentes métriques de performance que nous avons définies sont répertoriées suivant les métriques ou les groupes de métriques comme suit:

- *Taux de succès de l'authentification*

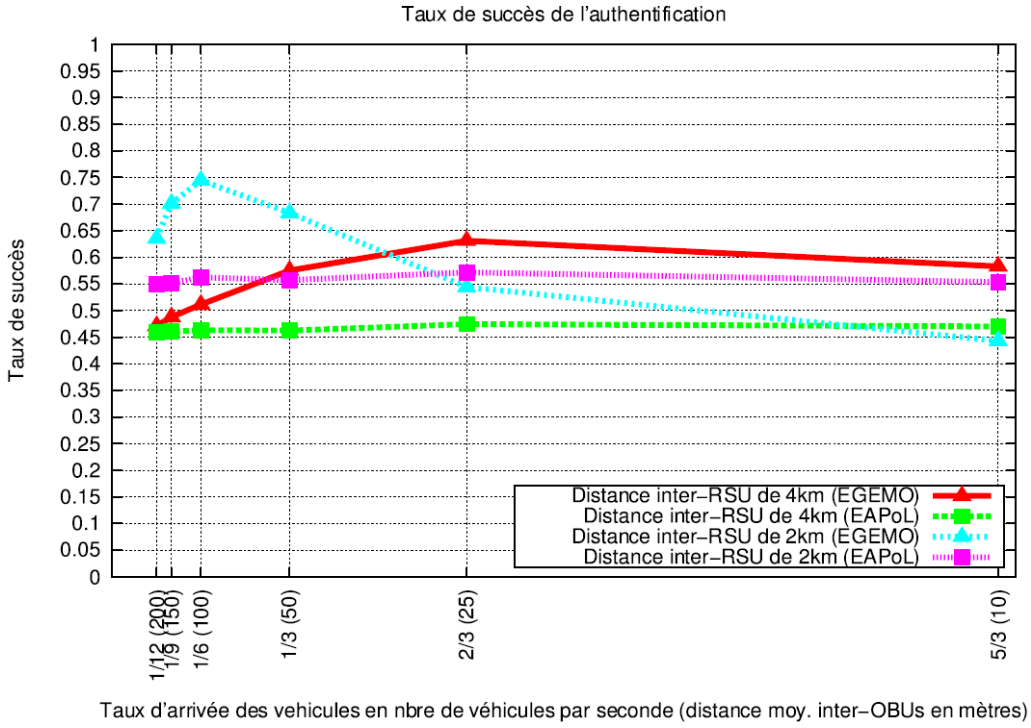


Figure 2: Taux de succès de l'authentification

Comme on peut le voir sur la Figure 2, notre solution (*i.e.* EGEMO) par rapport à l'approche classique (*i.e.* EAPoL) permet d'améliorer sensiblement le taux de succès de l'authentification pour des configurations de RSUs et d'OBUs bien choisies. Dans les cas où notre approche se montre plus avantageuse, l'amélioration du taux de succès est en moyenne de *15%* et *7%* notamment lorsque la distance inter-RSUs vaut 10 fois la portée de transmission (*i.e. 2 km* sur la figure) et 20 fois la portée de transmission (*i.e. 4 km* sur la figure) respectivement. Avec notre solution, l'amélioration du taux de succès de l'authentification a donc tendance à augmenter lorsque la densité des RSUs augmente et à diminuer lorsque cette dernière régresse. On peut donc s'attendre à ce que l'amélioration du taux de succès de l'authentification par rapport au schéma d'authentification classique soit supérieure à *15%* pour les cas de densités de RSUs plus fortes (*i.e.* lorsque la distance inter-RSUs est inférieure à 10 fois la portée de transmission et donc à *2 km* dans le cas précis de nos simulations) et inférieure à *7%* pour les cas de densités de RSUs moindres (*i.e.* lorsque la distance inter-RSUs est supérieure à 20 fois la portée de transmission et donc à *4 km* dans le cas précis de nos simulations).

Au-delà des configurations où notre approche se montre supérieure en termes de taux de succès, on note toutefois que notre solution n'apporte pas amélioration et tend même à dégrader le taux de succès pour les densités d'OBUs trop importantes. C'est notamment le cas sur la Figure 2, lorsque la distance inter-RSUs vaut *2 km* et que la distance moyenne inter-OBUs est inférieure ou égale à *25 m.*

En définitive, si l'augmentation de la densité des RSUs est susceptible d'augmenter la pertinence de notre solution par rapport à l'approche classique d'authentification, il est néanmoins impératif de s'assurer que l'importance de la densité des OBUs, ne soit pas de nature à dégrader les taux de succès de l'authentification.

Au vu de l'évolution du taux de succès de l'authentification (avec notre solution) qui augmente puis décroit avec l'augmentation de la densité des OBUs, nous sommes en mesure de déduire une heuristique mathématique susceptible d'anticiper la densité des OBUs la plus favorable (*i.e.* correspondant au pic du taux de succès de l'authentification avec notre solution) au-delà de laquelle le taux de succès commence à se dégrader au point d'être éventuellement moins important que le taux de succès obtenu avec le schéma d'authentification classique. En d'autres termes, cette heuristique permet d'obtenir la densité des OBUs au-delà de laquelle il n'est pas recommandé d'utiliser notre solution étant entendu que des densités d'OBUs plus fortes aboutissent à la dégradation du taux de succès de l'authentification. L'Equation 1 donne une représentation possible de cette heuristique[1]. La distance inter-OBUs en deçà de laquelle il n'est pas recommandé de mettre en œuvre notre solution ($InterOBUDist_{Rec\text{-}AuthSucc}$ exprimée en mètres) y est déterminée en fonction de la distance inter-RSUs considérée (*InterRSUDist* exprimée en mètres) et de la portée de transmission des nœuds du réseau (*Range* exprimée en mètres).

$$InterOBUDist_{Rec-AuthSucc} = \frac{Range}{2^{\left(\frac{2*InterRSUDist-10*Range}{10*Range}\right)}} \quad (1)$$

Ainsi, conformément à cette heuristique et à l'évolution du taux de succès de l'authentification observable sur la Figure 2, lorsque la distance inter-RSUs vaut *2000 m* avec une portée de transmission à *200 m*, le taux de succès de l'authentification commence à se dégrader à partir du moment où la distance inter-OBUs passe en dessous de *100 m*. De même, lorsque la distance inter-RSUs vaut *4000 m* avec une portée de transmission à *200 m*, le taux de succès de l'authentification commence à se dégrader à partir du moment où la distance inter-OBUs passe en dessous de *25 m*.

De manière générale, en choisissant avec attention la densité des RSUs et les densités d'OBUs à ne pas dépasser, notre solution permet d'augmenter de manière sensible les taux de succès de l'authentification par rapport à l'approche classique d'authentification et par conséquent d'accroître le nombre d'OBUs authentifiés et donc la confiance, la sécurité et la disponibilité des services dans le réseau.

- *Niveau de sollicitation de l'AS*

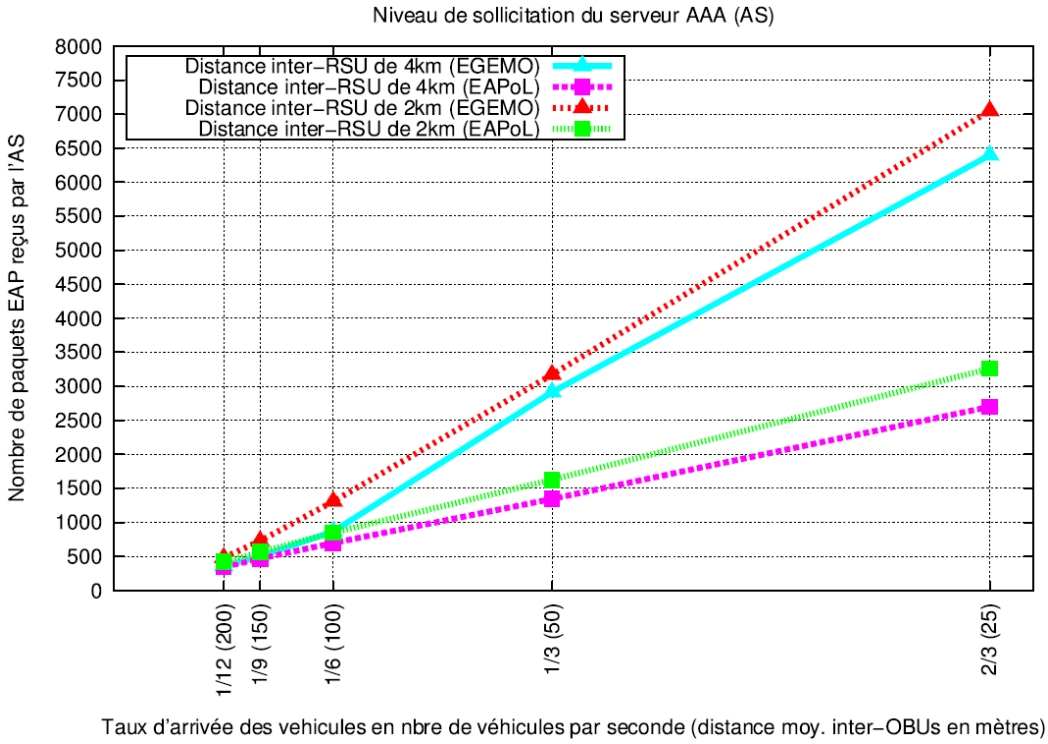


Figure 3: Niveau de sollicitation de l'AS

Comme on pouvait s'y attendre et comme l'illustre la Figure 3, notre solution conduit à un taux d'occupation plus important de l'AS par rapport au schéma d'authentification classique sur un saut. Le niveau d'occupation plus élevé de l'AS ne traduit pas nécessairement une augmentation du nombre d'OBUs réussissant à s'authentifier. En effet, l'évolution des courbes de la Figure 2 et de la Figure 3 ne sont pas exactement les mêmes puisqu'on peut remarquer sur la première une baisse du taux de succès de l'authentification dans les cas de très fortes densités d'OBUs sans que cela ne se traduise par une baisse de la sollicitation de l'AS sur la deuxième. Nous avons donc dans ce cas, beaucoup d'OBUs atteignant l'AS avec une latence telle qu'ils multiplient les retransmissions mais sans jamais arriver au bout du processus d'authentification, probablement à cause du dépassement du nombre maximum de retransmissions autorisées induit lui-même par la congestion dans le réseau.

On peut aussi remarquer que lorsque la distance inter-OBUs est égale à la portée de transmission (*i.e. 200 m* dans le cas de nos simulations), le niveau d'occupation de l'AS avec notre solution est sensiblement le même que le niveau d'occupation obtenu avec le schéma d'authentification classique sur un saut. En effet, lorsque la distance inter-OBUs est supérieure ou égale à la portée de transmission, la connectivité entre les OBUs est extrêmement faible, voire inexistante et par conséquent les communications avec les RSUs se font

[1] Les heuristiques présentées dans cette thèse, comme leur appellation l'indique, ont été déduites de manière empirique (*i.e.* par simple observation des résultats des simulations). Elles ne peuvent à ce titre que traduire des estimations. Elles n'ont en conséquence, aucun caractère absolu; et ce, d'autant que d'autres formes de représentation sont tout à fait possibles.

essentiellement sur un saut comme dans le schéma d'authentification classique. Les densités d'OBUs répondant à ces caractéristiques correspondent à ce que nous appelons ici les cas limites de connectivité.

- *Délai d'authentification, Taux de perte d'une authentification réussie et Taux de perte dû à un défaut de connectivité*

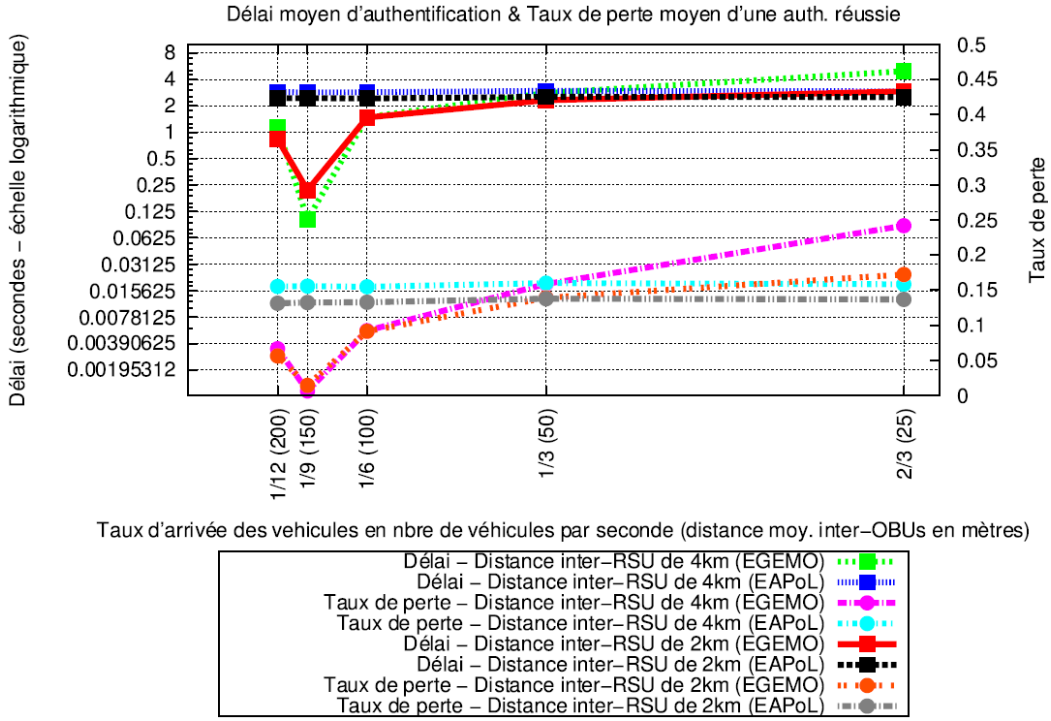


Figure 4: Délai d'authentification et Taux de perte d'une authentification réussie

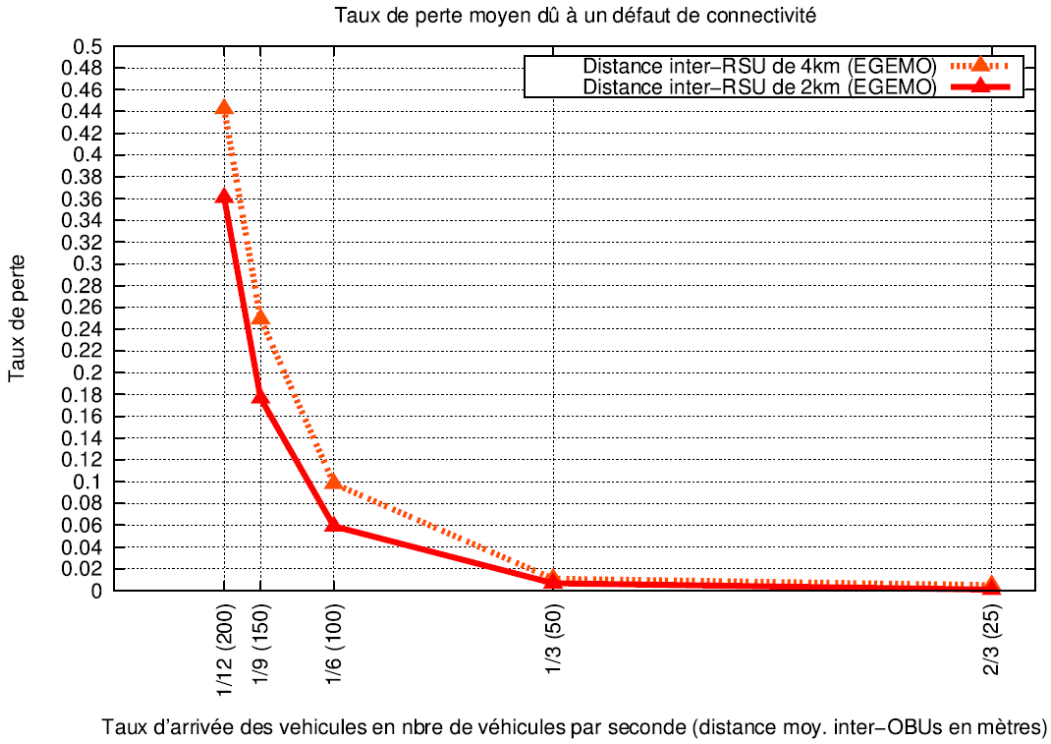


Figure 5: Taux de perte dû à un défaut de connectivité

Comme le montre la Figure 4 l'évolution du délai d'authentification se calque sur celle du taux de perte d'une authentification réussie. Cette figure illustre en particulier des délais d'authentification et des taux de perte élevés et quasi-constants dans le cas de l'authentification classique sur un saut. En revanche on observe, qu'avec notre solution, les délais peuvent être jusqu'à 10 ou 20 fois inférieures à ceux obtenus avec le schéma d'authentification classique notamment lorsque la distance inter-OBUs est supérieure ou égale au ¼ de la portée de transmission (*i.e. distance inter-OBUs >= 50 m* dans le cas de nos simulations). On note donc que ces délais tendent à augmenter avec la densité des OBUs et à terme finissent par dépasser les délais obtenus dans le cas de l'authentification classique.

Le mouvement d'augmentation des délais avec le renforcement de la densité des OBUs ne s'applique cependant pas aux cas de faibles densités correspondant aux cas limites de connectivité. En effet, dans les cas limites de connectivité (*i.e. distance inter-OBUs >= 200 m* dans le cas de nos simulations), la densité des OBUs bien que faible, présente des délais anormalement élevés. Ces délais élevés sont dus à des pertes importantes de paquets liées à un défaut de connectivité. Cet état de fait est illustré par la Figure 5 où on observe des taux de perte liés à un défaut de connectivité plus importants lorsque la densité des OBUs est faible.

En revenant à la Figure 4, on observe également que les délais d'authentification les plus bas sont obtenus lorsque la distance inter-OBUs vaut environ ¾ la portée de transmission (*i.e. distance inter-OBUs =150 m* dans le cas nos simulations). Et pour cause, cette densité correspond à une distribution particulièrement optimale des OBUs puisque les aires de communication de ces OBUs se recouvrent juste assez pour permettre des

communications multi-sauts. Ce recouvrement optimal des aires de communication, limite les interférences entre OBUs, de même que les collisions de paquets. On peut dire de manière générale qu'avec la mise en œuvre de notre solution, les densités d'OBUs trop faibles causent d'importantes pertes dues à des défauts de connectivité, ce qui peut produire des délais d'authentification assez voisins des délais obtenus avec le modèle classique d'authentification sur un saut. En revanche, les densités d'OBUs élevées sont à l'origine de nombreuses collisions et interférences qui impactent significativement les délais d'authentification.

Compte-tenu de toutes ces observations, il est possible de déduire des heuristiques mathématiques permettant, lorsque notre solution est mise en œuvre, d'anticiper les densités d'OBUs présentant les délais les plus compétitifs comparativement à l'approche d'authentification sur un saut. Ainsi, si l'on souhaite obtenir avec notre solution la meilleure performance (en termes de délais et de taux de perte) par rapport au modèle classique d'authentification, alors la distance moyenne inter-OBUs dans le réseau doit être voisine de $InterOBUDist_{Best-Delay}$ (donnée en mètres) exprimée ci-après en fonction de la portée de transmission des nœuds du réseau (*Range* donnée en mètres).

$$InterOBUDist_{Best-Delay} = \frac{3}{4} * Range \quad (2)$$

De manière plus large, si l'on souhaite obtenir avec notre solution des performances (en termes de délais et de taux de perte) compétitives par rapport au schéma d'authentification classique, alors on peut recommander que la distance moyenne inter-OBUs dans le réseau ne soit pas inférieure à $InterOBUDist_{Rec-Delay}$ (donnée en mètres) exprimée ci-après en fonction de la portée de transmission des nœuds du réseau (*Range* donnée en mètres).

$$InterOBUDist_{Rec-Delay} = \frac{1}{4} * Range \quad (3)$$

- *Taux d'Overhead imputable aux authentifications réussies, Nombre de sauts d'une tentative d'authentification et Débit du trafic d'authentification*

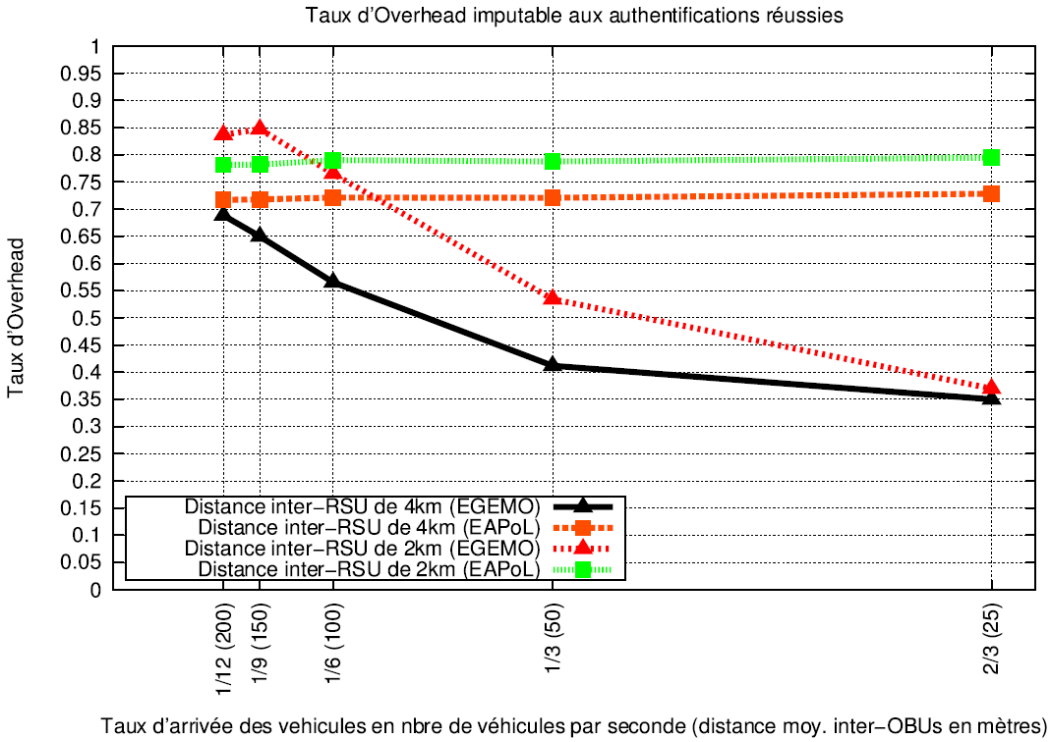


Figure 6: Taux d'Overhead imputable aux authentifications réussies

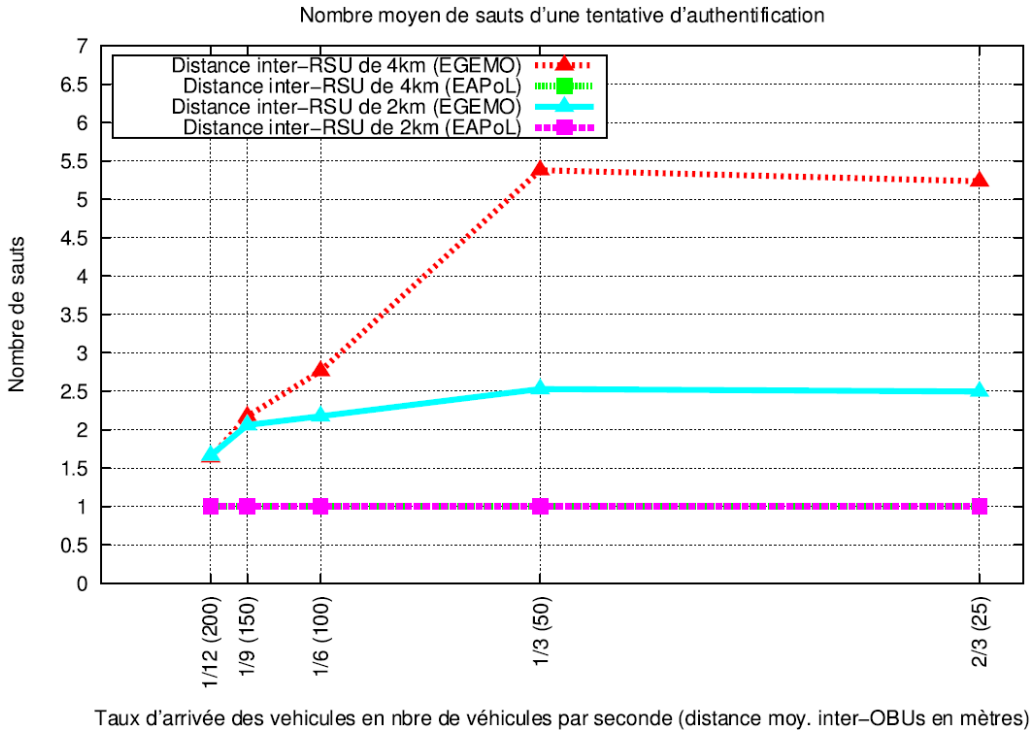


Figure 7: Nombre de sauts d'une tentative d'authentification

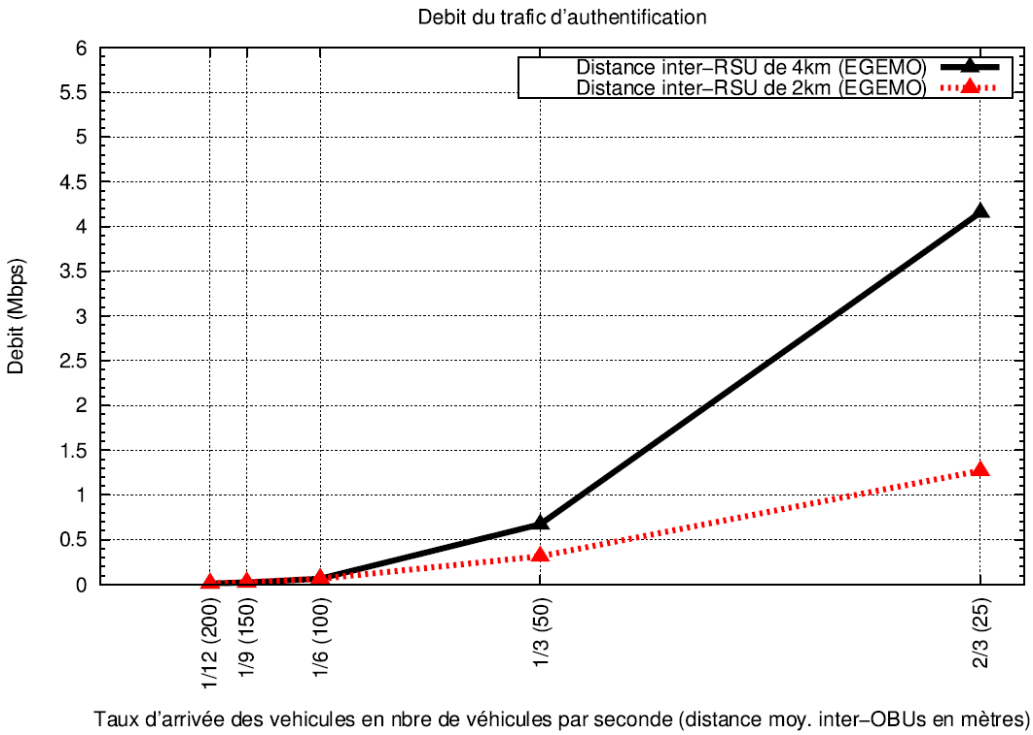


Figure 8: Débit du trafic d'authentification

La Figure 6 illustre l'évolution du taux d'Overhead imputable aux authentifications réussies. Nous rappelons qu'un taux élevé traduit une grande efficacité de l'authentification par rapport à l'Overhead généré dans le réseau alors qu'un taux faible est synonyme d'une moindre efficacité. L'observation de la Figure 6 permet de noter une efficacité de l'authentification élevée et quasi-constante dans le cas du modèle classique d'authentification sur un saut. En revanche, la mise en œuvre de notre solution conduit généralement à une efficacité moindre notamment lorsque la densité des OBUs est élevée et/ou la densité des RSUs est faible.

Ces résultats réservés sont assez largement dus au nombre de sauts entre OBU et RSU (lors d'une tentative d'authentification) qui, avant de se stabiliser, tend à augmenter lorsque la densité des OBUs augmente et/ou la densité des RSUs baisse. Cette évolution du nombre de sauts est observable sur la Figure 7. Plus précisément, l'augmentation du nombre de sauts détériore l'efficacité de l'authentification par rapport à l'Overhead généré dans le réseau, en ce qu'elle fait croître avec le mécanisme de retransmission, le nombre de paquets générés dans le réseau pour des OBUs qui n'arriveront pourtant pas à s'authentifier. Il est en effet attendu que les OBUs ne réussissant pas à s'authentifier soient à l'origine de plus de retransmissions que les OBUs réussissant à s'authentifier.

Nonobstant les résultats réservés de notre solution quant à l'efficacité par rapport à l'Overhead généré dans le réseau, on note toutefois que cette moindre performance ne constitue pas un handicap majeur puisque le débit induit par le trafic d'authentification, illustré par la Figure 8, reste acceptable si on considère que la capacité maximale du réseau est en $\theta\ (W(An)^{1/2})$ où W est le débit physique du canal radio, A l'aire occupée par les

nœuds du réseau et *n* le nombre de nœuds dans le réseau [GUP00]. On relève en particulier sur cette figure que le débit induit par le trafic d'authentification augmente lorsque la densité des OBUs augmente et/ou que la densité des RSUs baisse.

- *Taux de retransmission d'une authentification réussie et Taux de retransmission inutile d'une authentification réussie*

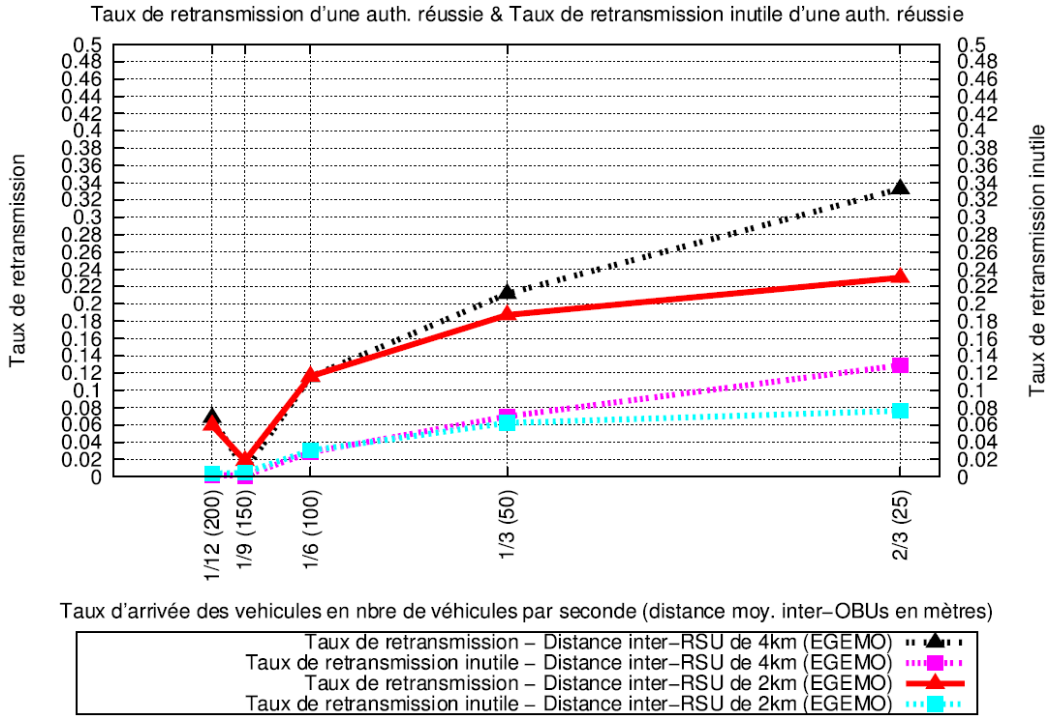


Figure 9: Taux de retransmission et de retransmission inutile d'une authentification réussie

L'analyse de ces taux ne porte que sur notre modèle d'authentification, l'objectif ici étant d'en observer l'évolution pour ensuite envisager des pistes susceptibles d'optimiser le mécanisme de retransmission. Le but n'est donc pas de faire une analyse comparative des 2 modèles d'authentification par rapport à ces taux. Il est de toute façon attendu que les taux de retransmission et de retransmission inutile soient quasi-constants dans le cas de l'authentification classique sur un saut. Pour ce qui est de notre modèle d'authentification, les taux de retransmission et de retransmission inutile correspondants sont illustrés par la Figure 9. On peut y observer, hormis pour la densité correspondant au cas limite de connectivité (*i.e. distance inter-OBUs = 200 m*), que le taux de retransmission d'une authentification réussie, tend à augmenter avec le renforcement de la densité des OBUs. On observe dans le même temps que lorsque la densité des OBUs augmente, une part non négligeable (*e.g.* jusqu'à *13%* dans le cas de nos simulations) des paquets transmis correspond en fait à des retransmissions inutiles. Toutes ces observations amènent à penser qu'au lieu d'utiliser une valeur fixe pour le temporisateur de

retransmission, on pourrait optimiser les retransmissions en faisant croître la valeur du temporisateur avec l'augmentation de la densité des OBUs. On pourrait ainsi non seulement réduire le taux de retransmission mais aussi réduire l'Overhead généré dans le réseau sans pour autant affecter les taux de succès et les délais d'authentification.

3. Conclusion

Au terme de la présentation des performances comparées de notre solution et de l'approche classique d'authentification sur un saut, il ressort de manière générale que notre solution présente de meilleures performances puisque permettant une authentification à la fois, plus efficiente, plus robuste et plus scalable pour peu que les densités de RSUs et d'OBUs soient calibrées avec intelligence. Pour aider à cet effort de calibrage, nous avons dérivé à la lumière des résultats des simulations, des principes et des heuristiques concourant à borner les densités de RSUs et d'OBUs présentant les résultats les plus favorables. Par exemple, si on considère le taux de succès de l'authentification comme étant la métrique de performance essentielle, alors pour obtenir une amélioration du taux de succès de plus de *15%* par rapport au modèle classique d'authentification (*i.e.* EAPoL), il convient de choisir une densité des RSUs telle que la distance inter-RSUs est inférieure à 10 fois la portée de transmission des nœuds tout en veillant à ce que la distance moyenne inter-OBUs dans le réseau ne soit pas inférieure à $InterOBUDist_{Rec\text{-}AuthSucc}$ (voir Equation 1). Si le délai d'authentification est la métrique privilégiée, alors il faut s'assurer que la distance moyenne inter-OBUs dans le réseau ne soit pas inférieure à $InterOBUDist_{Rec\text{-}Delay}$ (voir Equation 2) et idéalement qu'elle soit voisine de $InterOBUDist_{Best\text{-}Delay}$ (voir Equation 3).

Si notre modèle d'authentification présente des avantages certains suivant les densités de RSUs et d'OBUs bien précises, il reste tout de même qu'à la différence des densités de RSUs, les densités d'OBUs ne peuvent être totalement anticipées dans des conditions réalistes de circulation. Il convient donc à partir d'une densité de RSUs judicieusement choisie, d'améliorer les performances de notre modèle d'authentification de manière à le rendre pertinent sur des spectres plus larges de densités d'OBUs. Au regard de l'analyse des performances présentée dans ce chapitre, cette amélioration peut passer par une reproduction virtuelle des densités d'OBUs ayant présenté les résultats les plus favorables. Cette reproduction virtuelle des densités d'OBUs les plus favorables peut se faire en ajustant les algorithmes de transport EGEMO (*e.g.* un OBU ne sera désormais éligible pour relayer un paquet d'authentification que si en plus des tests conditionnels classiques du protocole EGEMO, cet OBU est au moins à une distance *d* de l'OBU émetteur, *d* étant un seuil de distance inter-OBUs en deçà duquel il est établi que les performances régressent) ou encore en distribuant/déléguant les fonctions de l'AS à des OBUs authentifiés dès qu'un seuil de densité d'OBUs au-delà duquel les performances se dégradent, est dépassé. Une autre approche d'amélioration des performances peut consister à augmenter les capacités radio

disponibles pour le trafic d'authentification; en particulier par la mise à contribution de la diversité des canaux DSRC. Toutes ces pistes d'amélioration de notre modèle d'authentification sont l'objet des chapitres suivants.

Chapitre 2.3. Optimisation du Transport de l'Authentification

1. Introduction

L'analyse des performances de notre solution initiale a permis d'observer une augmentation non négligeable de la bande passante consommée par le trafic d'authentification; augmentation, couplée à une assez faible efficacité du processus d'authentification par rapport à l'Overhead généré dans le réseau notamment lorsque la densité des OBUs augmente. Même si cette augmentation de la bande passante consommée et cette faible efficacité par rapport à l'Overhead généré dans le réseau ne sont en rien fatales compte tenu de la capacité maximale réalisable dans le réseau, il convient en raison de la rareté de la ressource radio d'optimiser notre solution de manière à réduire le trafic induit par le processus d'authentification (notamment dans les cas de forte densité d'OBUs pour lesquels le trafic d'authentification tend à exploser) tout en préservant les performances les plus importantes du processus d'authentification dont en premier lieu la disponibilité.

L'optimisation de la bande passante consommée dans le réseau et l'amélioration de l'efficacité du processus d'authentification passent par l'optimisation du protocole assurant le transport de l'authentification, soit celle du protocole EGEMO. Il s'agit en particulier d'ajuster le protocole EGEMO de manière à réduire le nombre de paquets générés dans le réseau au moment de l'authentification. Plus précisément, nous ajoutons à la série de tests visant à décider de la rediffusion ou non d'un paquet EGEMO, des tests supplémentaires dont l'objectif est de restreindre le nombre d'OBUs susceptibles de relayer le paquet. Cette restriction est mise en œuvre en émulant des densités d'OBUs réputées suffisamment fortes pour assurer la connectivité entre les OBUs et en même temps suffisamment faibles pour éviter une trop grande contention pour l'accès au canal ou de trop nombreuses interférences et collisions. Il est à noter qu'une contention aigue pour l'accès au canal ou des interférences et collisions trop importantes sont à l'origine de multiples retransmissions qui concourent à augmenter la bande passante consommée et à réduire l'efficacité du processus d'authentification.

Une fois notre approche d'optimisation du transport de l'authentification introduite, nous en évaluons la pertinence et les performances par rapport à la solution initiale. Comme dans le chapitre précédent, cette évaluation est conduite par des simulations et en particulier avec le simulateur GrooveNet [MAN06] dans lequel la solution initiale et l'approche d'optimisation du transport EGEMO ont été implémentées.

Pour ce qui est de l'organisation de ce chapitre, nous commencerons par présenter en section 2, la description de notre approche d'optimisation du transport de l'authentification. Dans la section 3, nous introduirons les

simulations et l'analyse des performances. Cette section présentera en particulier les scénarios de simulation ainsi que les métriques de performance. Les résultats des simulations et l'analyse des performances proprement dite seront ensuite présentés. Enfin, la section 3 conclura le chapitre.

2. Description de l'optimisation du transport de l'authentification

L'optimisation pour réduire la bande passante consommée par le trafic d'authentification et améliorer l'efficacité du processus d'authentification par rapport à l'Overhead repose sur deux principes essentiels que sont:

- *Le relayage probabiliste des paquets*: L'objet de ce principe est de favoriser le relayage des paquets EGEMO par les OBUs les plus éloignés du nœud duquel les paquets ont été reçus. Ainsi, plus un OBU est éloigné du nœud duquel il reçoit un paquet, plus la probabilité pour qu'il relaie ce paquet est grande. Inversement, plus un OBU est proche du nœud duquel il reçoit un paquet, plus la probabilité pour qu'il relaie ce paquet est faible. Le fondement de ce principe est de limiter les relayages de paquets dont la contribution pour atteindre la destination est quasi-nulle. En effet, un OBU relayant un paquet reçu d'un autre nœud dont il est géographiquement très proche, ne permet pas de réaliser un gain substantiel dans le processus d'acheminement du paquet vers la destination. Ceci est en particulier vrai si on considère la même portée de transmission pour tous les nœuds du réseau. Dans cette hypothèse en effet, un OBU très proche d'un autre nœud émettant un paquet à relayer, couvre sensiblement la même aire de communication que cet autre nœud. Le relayage du paquet par l'OBU dans ce contexte s'avère donc inopportun.

- *Le relayage différé des paquets*: L'objet de ce principe est de limiter le relayage des paquets EGEMO par des OBUs séparés du nœud ayant transmis le paquet par une distance inférieure à une distance minimale définie. Cette distance minimale correspond à une densité seuil d'OBUs au-delà de laquelle le réseau connaît de trop grandes perturbations. De manière générale, la définition de cette distance minimale permet de reproduire virtuellement des densités d'OBUs suffisamment fortes pour assurer la connectivité entre les OBUs et en même temps suffisamment faibles pour éviter une trop grande contention pour l'accès au canal ou de trop nombreuses interférences et collisions. Plus concrètement, le principe du relayage différé consiste à introduire, lorsque l'OBU est séparé du nœud ayant transmis le paquet par une distance inférieure à la distance minimale définie, un temps d'attente dédié à l'écoute du réseau et précédant la prise de décision du relayage du paquet. Ce temps d'attente qui est supérieur ou égal à la durée de transmission du paquet à relayer, permet à l'OBU d'éventuellement recevoir un ou plusieurs autres exemplaires du paquet en attente. Dans tous les cas, au bout de l'épuisement de ce temps d'attente, le paquet n'est relayé que si l'OBU n'a reçu

aucun autre exemplaire de ce même paquet provenant d'un autre nœud situé à proximité. En effet, si tel n'était pas le cas (*i.e.* réception par l'OBU d'au moins un autre exemplaire du paquet provenant d'un autre nœud situé à proximité) l'OBU et le nœud ayant transmis le paquet couvriraient sensiblement la même aire de communication; ce qui rendrait le gain du relayage par l'OBU dans le processus d'acheminement du paquet vers la destination, quasi-nul.

Les principes d'optimisation du protocole EGEMO sont mis en œuvre dans les OBUs et plus spécifiquement dans l'algorithme de réception d'un paquet EGEMO provenant de la couche 2. Cette mise en œuvre dans l'algorithme intervient juste avant la prise de décision de relayage d'un paquet (*i.e.* avant la mise à jour des champs pertinents et l'envoi du paquet à la couche 2 pour diffusion) et par conséquent, juste après la validation des tests conditionnels classiques du protocole EGEMO menant au relayage.

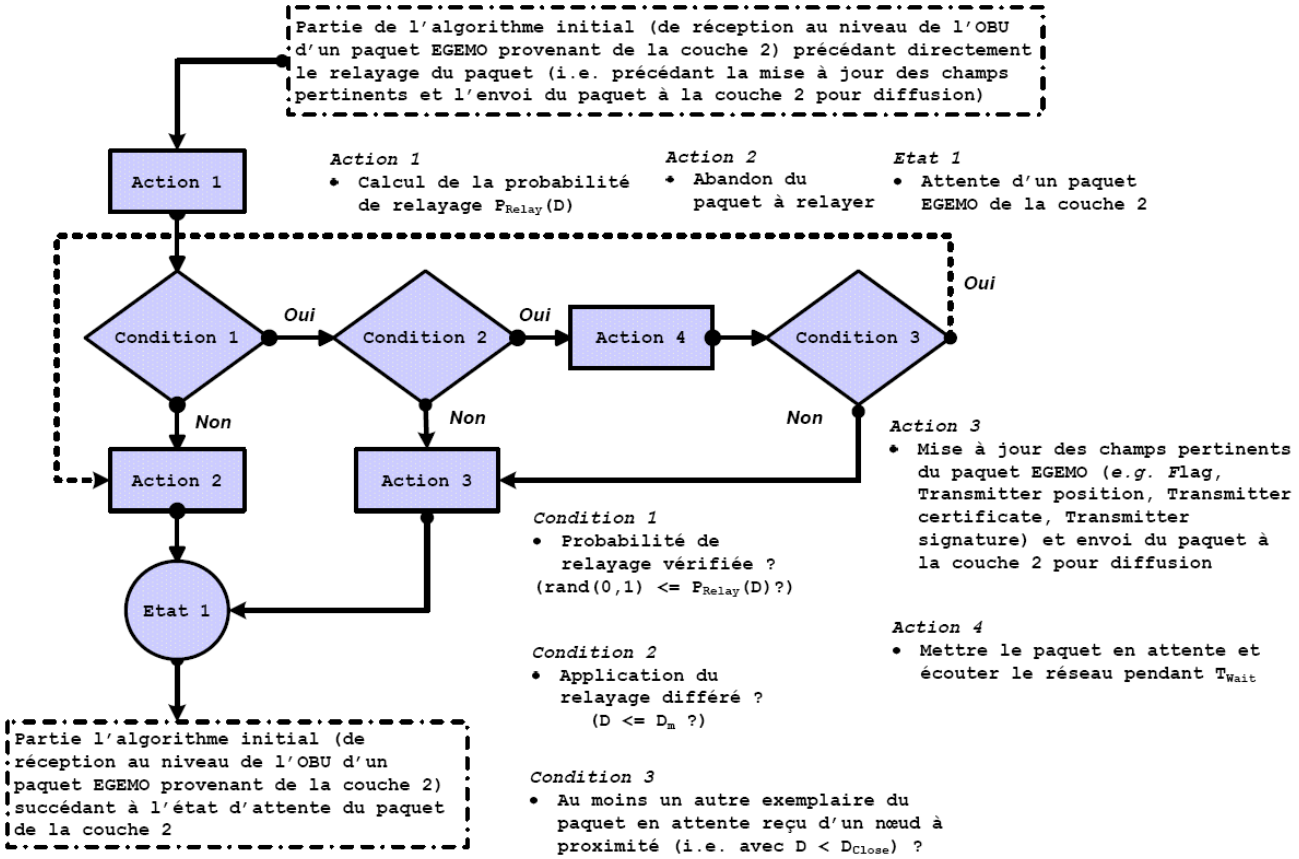


Figure 1: Optimisation du transport de l'authentification

La Figure 1 représente l'organigramme de la partie de l'algorithme mettant en œuvre nos principes d'optimisation. Ainsi, après avoir validé les tests conditionnels classiques du protocole EGEMO menant au relayage, l'OBU décide dans un premier temps et conformément au principe du relayage probabiliste, de relayer

le paquet avec une probabilité $P_{relay}(D)$ qui augmente lorsque la distance qui sépare l'OBU du nœud ayant transmis le paquet augmente. Cette probabilité de relayage est exprimée comme suit:

$$P_{\mathrm{Re}\,lay}(D) \;=\; 1-(1-D/Range)^{\alpha} \quad (1)$$

Où *Range* est la portée de transmission des nœuds du réseau, D ($0 \le D \le Range$) est la distance qui sépare l'OBU du nœud ayant transmis le paquet et α ($\alpha > 1$) est un exposant amplificateur. Notons que cet exposant amplificateur est utilisé pour faire converger plus ou moins rapidement la probabilité de relayage vers 1. Autrement dit, plus cet exposant est important, plus vite la probabilité de relayage convergera vers 1. Inversement, plus il est petit, moins vite la probabilité de relayage convergera vers 1. Cet exposant peut donc être utilisé pour faciliter (*i.e.* α grand) ou restreindre (*i.e.* α petit) la probabilité de relayage.

Lorsque la décision de poursuivre le processus de relayage est prise, l'OBU détermine s'il doit ou non appliquer le principe du relayage différé. Pour ce faire, il compare la distance D qui le sépare du nœud ayant transmis le paquet, à la distance minimale D_{min} correspondant à la densité seuil d'OBUs au-delà de laquelle le réseau connaît de trop grandes perturbations. Compte-tenu des analyses de performance réalisées dans le chapitre précédent, et selon que l'on opte pour une optimisation plus ou moins agressive du relayage, cette distance minimale peut correspondre respectivement au maximum (voir Equation 2) ou au minimum (voir Equation 3) des distances inter-OBUs recommandées pour les taux de succès et pour les délais d'authentification. Si en revanche on opte pour une optimisation médiane du relayage, cette distance minimale peut correspondre à la moyenne (voir Equation 4) des distances inter-OBUs recommandées pour les taux de succès et pour les délais d'authentification. Il est bien entendu ici que les Equations 2, 3 et 4 n'ont rien d'absolu et ne traduisent que des possibilités.

$$D_{\min} = MAX\left(InterOBUDist_{\mathrm{Re}\,c-AuthSucc}, InterOBUDist_{\mathrm{Re}\,c-Delay}\right) = MAX\left(\frac{Range}{2^{\left(\frac{2*InterRSUDist-10*Range}{10*Range}\right)}}, \frac{1}{4}*Range\right) \quad (2)$$

$$D_{\min} = MIN\left(InterOBUDist_{\mathrm{Re}\,c-AuthSucc}, InterOBUDist_{\mathrm{Re}\,c-Delay}\right) = MIN\left(\frac{Range}{2^{\left(\frac{2*InterRSUDist-10*Range}{10*Range}\right)}}, \frac{1}{4}*Range\right) \quad (3)$$

$$D_{\min} = \frac{InterOBUDist_{Rec-AuthSucc} + InterOBUDist_{Rec-Delay}}{2} = \frac{\frac{Range}{2^{\left(\frac{2*InterRSUDit-10*Range}{10*Range}\right)}} + \frac{1}{4} * Range}{2} \quad (4)$$

Si la distance *D* qui sépare l'OBU du nœud ayant transmis le paquet, est supérieure à la distance minimale définie D_{min}, alors le paquet est mis à jour et transmis à la couche 2 pour diffusion. En revanche, l'OBU est tenu d'appliquer le principe du relayage différé lorsque la distance *D* qui le sépare du nœud ayant transmis le paquet, est inférieure ou égale à la distance minimale définie D_{min}. Dans ce dernier cas (*i.e.* $D \leq D_{min}$), l'OBU se met à l'écoute du réseau pendant une durée au moins égale à $T_{Min\text{-}Wait}$. Cette durée minimale est définie comme suit:

$$T_{Min-Wait} = PacketSize / W \quad (5)$$

Où *PacketSize* est la taille du paquet à relayer et *W* est le débit de transmission sur le canal radio. Dans la pratique, le temps d'attente choisi vaut au moins deux fois le temps d'attente minimum défini ci-dessus. Ajoutons qu'il est utile d'augmenter le temps d'attente choisi, d'une durée aléatoire très petite afin d'éviter les effets d'une synchronisation possible entre les transmissions des nœuds ayant décidé de relayer le paquet à l'issue de leurs temps d'attente. Ainsi par exemple, si on suppose l'utilisation d'une couche MAC (Medium Access Control) DSRC/802.11p [IEEE-802.11p], le temps d'attente choisi peut être de la forme:

$$T_{Wait} = \lambda * T_{Min-Wait} + rand(0, CW) * T_{Slot} \quad (6)$$

Où λ est un facteur supérieur à 1 ($\lambda>1$), *CW* est la taille de la fenêtre de contention et T_{Slot} est la durée d'une tranche temporelle (en anglais, *time slot*).

Si à l'issue du temps d'attente, l'OBU a reçu d'un autre nœud situé à proximité, au moins un autre exemplaire du paquet en attente de relayage, alors le relayage du paquet en attente est abandonné et ce dernier est supprimé. Si en revanche l'OBU n'a reçu aucun autre exemplaire du paquet provenant d'un autre nœud situé à proximité, alors le paquet en attente est mis à jour et transmis à la couche 2 pour diffusion. On peut considérer dans ce contexte qu'un nœud est situé à proximité d'un OBU si la distance *D* qui les sépare est inférieure ou égale à une distance seuil de proximité D_{Close} nécessairement fonction de la portée de transmission des nœuds du réseau et inférieure à la distance minimale D_{min} définie plus haut. D_{Close} peut ainsi être de la forme:

$$D_{Close} = \mu * D_{\min} \quad (7)$$

Où μ est un facteur compris entre 0 et 1 ($0 < \mu < 1$).

Après avoir relayé le paquet ou abandonné le relayage, l'OBU revient à l'état d'attente d'un paquet EGEMO provenant de la couche 2. S'ensuit la partie de l'algorithme EGEMO initial succédant à cet état d'attente.

3. Simulations et analyse des performances

Après avoir implémenté notre approche d'optimisation du transport de l'authentification dans le simulateur GrooveNet [MAN06], il s'agit dans cette section d'en évaluer les performances par rapport à la solution initiale. Pour ce faire, nous commencerons, avant d'en arriver à l'analyse des performances proprement dite, par introduire les scénarios de simulation et les métriques de performance que nous avons retenus.

3.1. Scénarios de simulation et métriques de performance

Nous considérons sensiblement les mêmes scénarios de simulation que ceux de l'évaluation de la solution initiale dans le chapitre précédent. Une des seules différences par rapport au chapitre précédent réside dans l'utilisation avec l'évaluation présente, d'une seule densité de RSUs soit un RSU tous les *4* km. Le choix de cette densité suffit pour mettre en relief la pertinence de notre approche d'optimisation puisque des 2 densités considérées dans les scénarios du chapitre précédent, elle est celle ayant présenté les résultats les moins favorables. Ce scénario de densité des RSUs est illustré par la Figure 2. Pour ce qui est du cas spécifique de l'optimisation du transport de l'authentification, nous avons retenu dans nos simulations une approche d'optimisation médiane du relayage (*i.e.* la distance minimale D_{min} est calculée suivant l'Equation 4). Pour le reste, le Tableau 1 résume l'ensemble des paramètres de nos simulations.

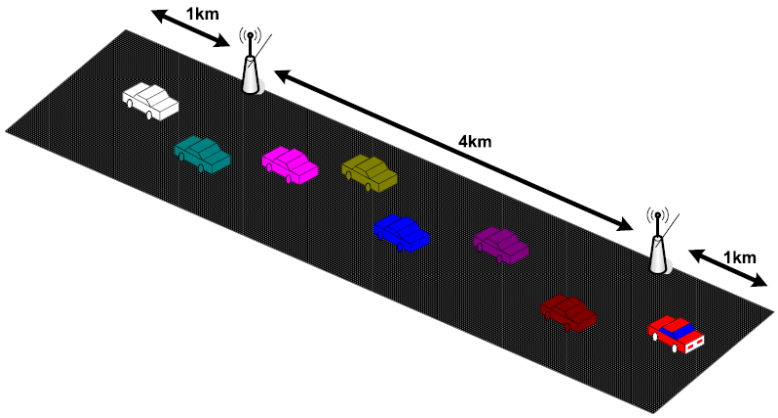


Figure 2: Densité de RSUs considérée pour les simulations

Tableau 1: Principaux paramètres de simulation

	Authentification EGEMO	***Authentification EGEMO optimisé***
Paramètre	**Valeur**	
Durée de validité d'un paquet EGEMO	2 s	
Temporisateur de retransmission (RTO)	2 s	
Nombre maximum de retransmissions	3	
PKCS	ECC 163 – Architecture PKI 1-tiers	
Coefficient de non-traçabilité ($F_{non\text{-}trac}$)	0.5	
Topologie	6 Km en topologie linéaire	
Densité de RSUs	1 RSU tous les 4 Km	
Taux d'arrivée des OBUs (nombre d'OBUs par seconde)	1/12, 1/9, 1/6, 1/3, 2/3	
Mobilité	Vitesse des OBUs uniformément variée (12.77 m/s – 20 m/s) - Vitesse moyenne de 16.5 m/s	
Paramètres d'optimisation	N/A	Exposant amplificateur $\alpha = 10$ Optimisation médiane (D_m suivant Equation 4) Facteur $\lambda = 2$ Facteur $\mu = 0.5$
Couche MAC	DSRC CSMA CW_{Min} 15 Time Slot 13 us SIFS Time 32 us	
Couche Radio	Fréquence centrale 5.9 GHz Largeur de bande 10 MHz Antenne omnidirective de 1.65 m de hauteur Puissance de transmission 100 mW (20 dBm) Modulation OFDM BPSK ½ Portée de transmission 200 m Débit physique 6 Mbps	
Nombre de simulations et durée de chaque simulation	20 simulations (de 900 s chacune) par scénario (*i.e.* par densité d'OBUs et approche d'authentification)	

S'agissant des métriques de performance, nous avons choisi d'illustrer plus particulièrement le taux d'Overhead imputable aux authentifications réussies et le débit du trafic d'authentification afin de mettre en exergue la pertinence de notre approche d'optimisation par rapport à la solution initiale. Nous avons également choisi de mettre en relief le taux de succès de l'authentification afin d'illustrer l'impact éventuel de notre approche d'optimisation sur la disponibilité de l'authentification. Ces 3 métriques étant les mêmes que celles définies dans le chapitre précédent, elles en reprennent en conséquence les mêmes modes de calcul.

3.2. Analyse des performances

A l'image de l'analyse des performances de notre solution initiale, nous faisons dans cette analyse des performances deux principales hypothèses à savoir une même portée de transmission pour tous les nœuds du réseau et des densité de RSUs telles que la distance inter-RSUs est supérieure à 2 fois la portée de transmission

des nœuds (*i.e.* des communications multi-sauts sont possibles dès le premier paquet initiant le processus d'authentification).

Les analyses de l'évolution des 3 métriques de performance qui ont été retenues sont répertoriées comme suit:

- *Taux d'Overhead imputable aux authentifications réussies et Débit du trafic d'authentification*

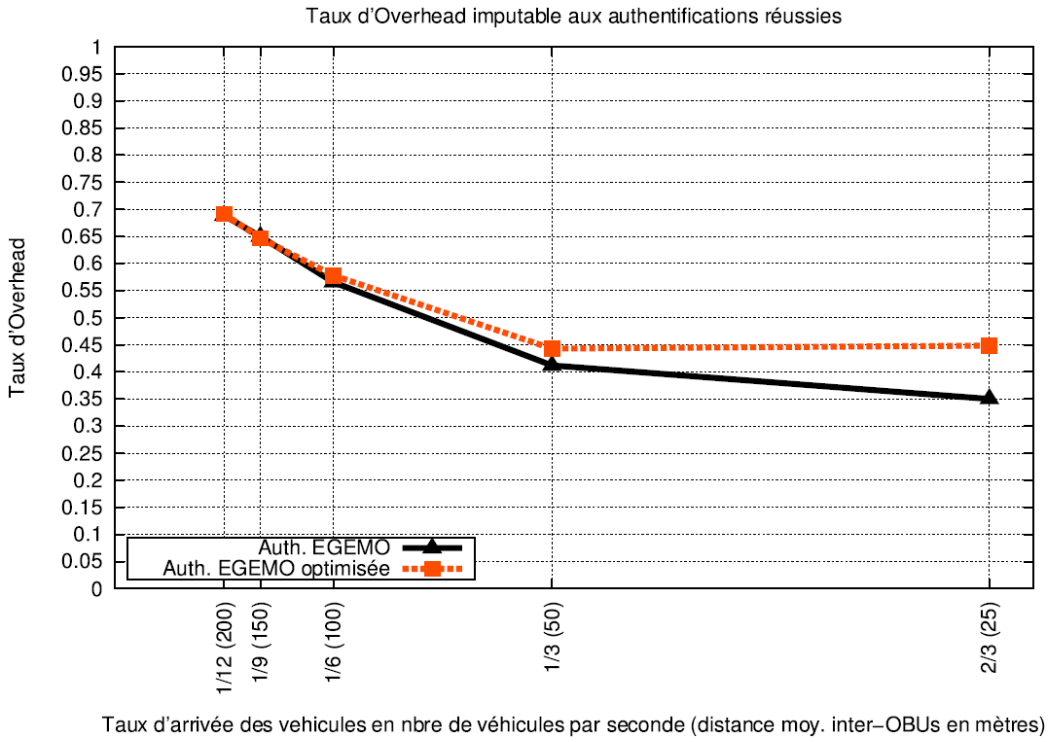


Figure 3: Taux d'Overhead imputable aux authentifications réussies

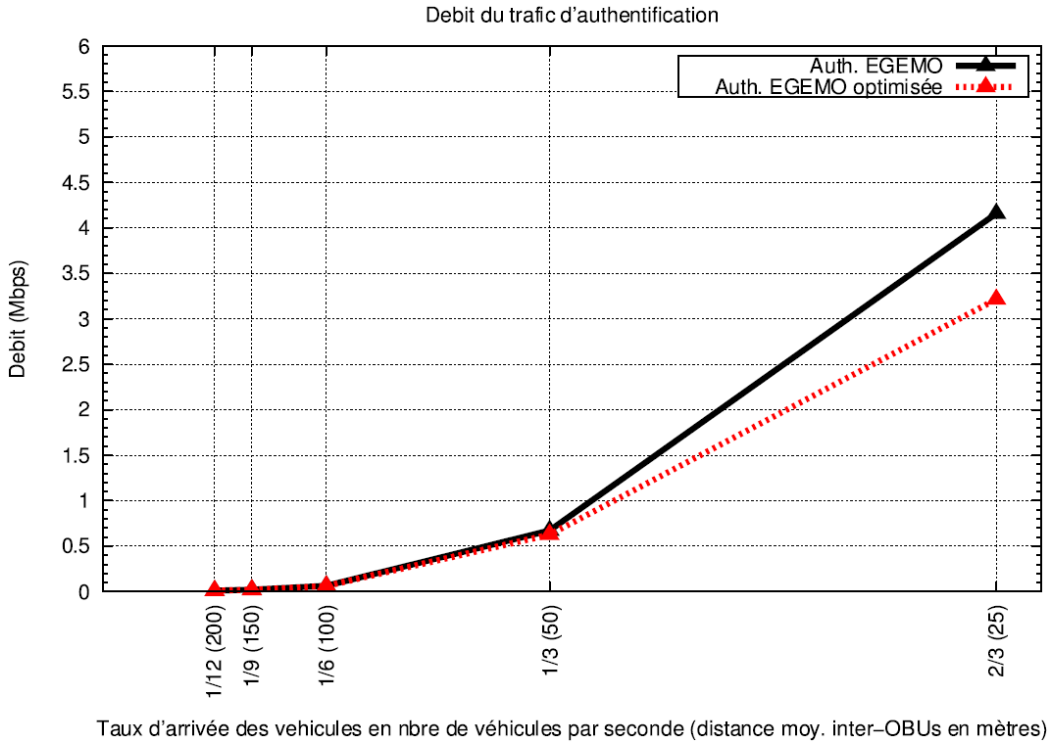


Figure 4: Débit du trafic d'authentification

Comme on peut le voir sur la Figure 3, la version optimisée du protocole EGEMO par rapport à la version initiale permet de freiner de manière sensible la chute de l'efficacité du processus d'authentification par rapport à l'Overhead généré dans le réseau. Rappelons qu'un taux élevé de l'Overhead traduit une grande efficacité de l'authentification par rapport à l'Overhead généré dans le réseau alors qu'un taux faible est synonyme d'une moindre efficacité. On note en particulier qu'avec la version optimisée du protocole EGEMO, l'amélioration de l'éfficacité de l'authentification est manifeste lorsque la densité des OBUs augmente. Plus précisément, l'amélioration de l'efficacité par rapport à la solution initiale va croissante avec l'augmentation de la densité des OBUs et atteint pour la plus forte densité d'OBUs simulée (*i.e.* distance moyenne inter-OBUs à *25* m) dans notre scénario, jusqu'à *10%.*

L'amélioration de l'efficacité du processus d'authentification que confère notre approche d'optimisation, rejaillit sur la bande passante consommée par l'authentification comme illustré sur la Figure 4. On note en effet sur cette dernière figure, une baisse sensible de la bande passante consommée dans le cas de la solution optimisée par rapport à la solution initiale. Comme dans le cas de l'amélioration de l'efficacité du processus d'authentification, la baisse de la bande passante consommée va croissante avec l'augmentation de la densité des OBUs. On obtient par exemple pour la plus forte densité simulée (*i.e.* distance moyenne inter-OBUs à *25* m) dans notre scénario, une baisse de la bande passante consommée de l'ordre de *1* Mbps par rapport à la solution initiale.

- *Taux de succès de l'authentification*

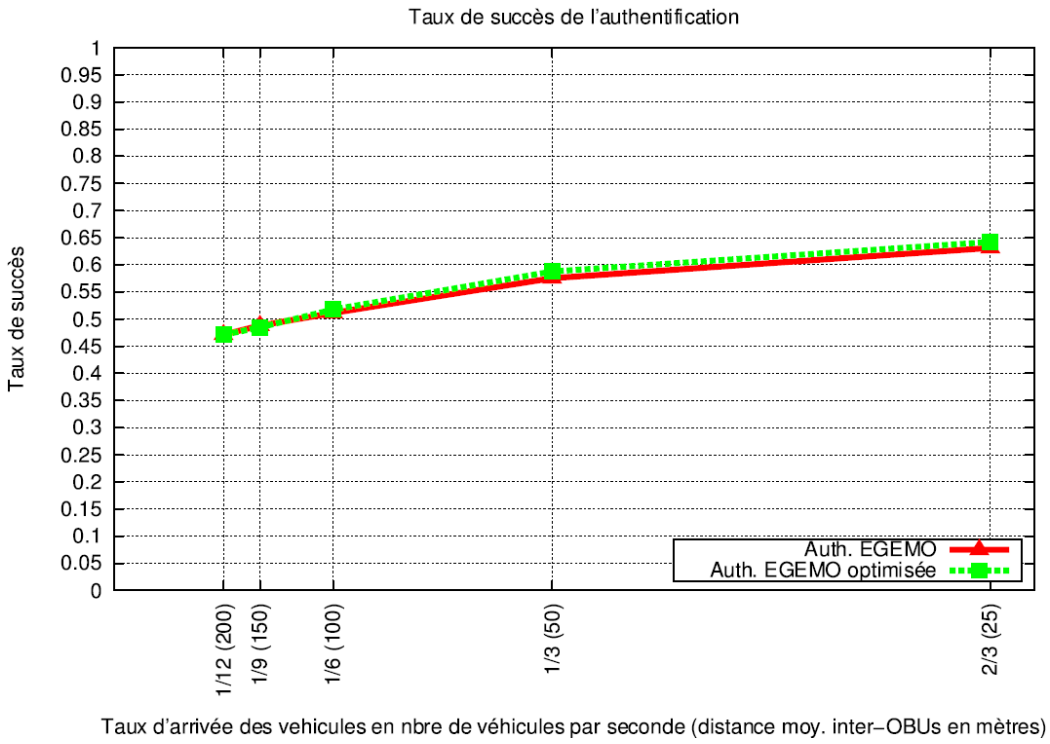


Figure 5: Taux de succès de l'authentification

Comme l'illustre la Figure 5, le taux de succès de l'authentification de la solution optimisée est en droite ligne de celui de la solution initiale. Cette absence de variation du taux de succès entre les 2 versions de l'algorithme confirme l'impact quasi-nul des mécanismes d'optimisation sur la disponibilité de l'authentification. En d'autres termes, nous obtenons avec l'algorithme EGEMO optimisé la même disponibilité de l'authentification qu'avec l'algorithme EGEMO initial et ce, tout en améliorant l'efficacité du processus d'authentification par rapport à l'Overhead généré dans le réseau et en réduisant de manière significative la bande passante consommée par l'authentification.

4. Conclusion

Compte-tenu de l'enjeu de rareté de la ressource radio dans les réseaux sans fil et des performances de notre solution initiale par rapport à cet enjeu, nous avons présenté dans ce chapitre une approche visant à optimiser le transport de l'authentification dans notre solution. Cette approche est conçue en respectant la philosophie de la solution initiale dont la pertinence est de convenir aux spécificités des réseaux véhiculaires dont en particulier la très forte dynamique des nœuds du réseau. En vue de réduire le nombre d'OBUs éligibles au relayage des

paquets d'authentification et donc de réduire le nombre de paquets émis dans le réseau, notre approche d'optimisation du transport de l'authentification met en œuvre deux principes essentiels que sont le relayage probabiliste et le relayage différé des paquets. Les simulations de la version initiale et de la version optimisée du protocole de transport de l'authentification confirment la pertinence de notre approche d'optimisation. En effet, la solution optimisée par rapport à la solution initiale, permet, tout en maintenant un niveau identique de disponibilité de l'authentification, d'améliorer l'efficacité du processus d'authentification par rapport à l'Overhead généré dans le réseau et de réduire la bande passante consommée par l'authentification. Comme anticipé, les améliorations observées gagnent en importance avec l'augmentation de la densité des OBUs. Ainsi, en permettant une utilisation parcimonieuse du spectre radio, notre approche d'optimisation assure l'exploitabilité de notre solution sur des éventails de densités d'OBUs plus importants.

On rappellera avant de mettre un terme à ce chapitre, que l'approche d'optimisation qui vient d'être présentée et étudiée s'inscrit dans un schéma global visant à améliorer les performances de notre solution pour l'authentification dans les réseaux véhiculaires. C'est dans ce même esprit que le chapitre qui suit introduira une approche de priorisation de l'authentification mettant à contribution la diversité des canaux radio DSRC.

Chapitre 2.4. Utilisation de la Diversité des Canaux DSRC

1. Introduction

Toutes les analyses de notre solution pour l'authentification dans les réseaux véhiculaires réalisées jusqu'ici, ont permis d'observer de meilleures performances générales et un potentiel certain par rapport au modèle classique d'authentification sur un saut. Cependant, il est attendu que les performances de notre approche de mise en œuvre de l'authentification soient mises à rude épreuve en présence de trafics d'autres services du réseau véhiculaire. L'objet de ce chapitre est donc d'anticiper cette perspective en présentant, dans le contexte technologique DSRC, une approche de priorisation du trafic d'authentification tirant le plus possible parti de la diversité des canaux radio.

Dans le contexte DSRC, l'authentification peut être assimilée à un service à l'image d'autres applications du réseau véhiculaire. Nous proposons toutefois d'attribuer un statut particulier au service d'authentification dans la mesure où nous entendons qu'il précède et conditionne l'accès aux ressources et aux autres services du réseau véhiculaire. Partant de là, nous proposons une approche de priorisation, qui, sans remettre en cause le modèle de priorité des services DSRC, réserve des conditions préférentielles pour la transmission des paquets d'authentification par rapport aux paquets d'autres services. Ces conditions préférentielles se traduisent par l'association de plusieurs canaux au service d'authentification et par le choix, au moment de la transmission des paquets d'authentification, du canal susceptible d'être le plus rapidement disponible pour la transmission des paquets d'authentification. L'approche de sélection du canal susceptible d'être le plus rapidement disponible se base sur une technique d'évaluation de l'état des canaux radio basée elle-même sur une interaction entre la couche assurant le transport de l'authentification (*i.e.* le protocole EGEMO dans notre cas) et la couche MAC (Medium Access Control) DSRC. En choisissant une technique d'évaluation locale et sans échange de messages de l'état des canaux, notre approche ne permet certes pas d'atteindre l'optimalité globale (réputée par ailleurs problème NP-complet [JAIN03]) mais s'avère intéressante à étudier dans le contexte des réseaux véhiculaires marqué par une forte dynamique des nœuds.

Une fois notre approche de priorisation de l'authentification et les différents scénarios de déploiement associés présentés, nous en évaluons les performances par rapport à l'approche naïve fondée sur une sélection aléatoire des canaux. Cette évaluation qui suppose un contexte de déploiement multi-interfaces, est conduite avec le simulateur GrooveNet [MAN06] dans lequel les différentes approches ont été implémentées.

D'un point de vue organisationnel, ce chapitre est structuré comme ainsi qu'il suit. Nous commencerons par présenter en section 2 le système DSRC de manière à appréhender son objet et son fonctionnement. Nous introduirons plus spécifiquement dans la section 3, les motivations des ajustements du modèle de DSRC que nous proposons. Dans la section 4, nous présenterons notre approche de priorisation de l'authentification. Nous discuterons ensuite en section 5 des différents scénarios de déploiement de notre solution. Dans la section 6, nous aborderons les simulations et l'analyse des performances. Enfin, la section 7 conclura le chapitre.

2. Présentation générale du système DSRC

Les réseaux véhiculaires permettent d'établir des communications entre véhicules dites IVC (Inter-Vehicle Communications) d'une part et entre véhicules et infrastructure dites RVC (Road-to-Vehicle Communications) d'autre part. DSRC (Dedicated Short Range Communications) [DSRC] regroupe un ensemble de technologies dédiées aux communications véhiculaires. Dans le système DSRC, chaque véhicule embarque un terminal de communication appelé OBU (On Board Unit) tandis que les terminaux fixes disposés le long des routes et constituant l'infrastructure sont appelés RSUs (RoadSide Units). Ainsi, au lieu de recourir à un dispositif spécifique pour chaque type d'application, on utilise les OBUs et les RSUs qui constituent le point d'entrée pour tout type d'application déployée dans les réseaux véhiculaires.

Le standard DSRC sous-tend une technologie de communication radio plus connue sous la norme IEEE 802.11p ou WAVE (Wireless Access for Vehicular Environments) [IEEE-802.11p]. Cette technologie radio offre des portées de transmission pouvant aller jusqu'à 1000 m. Elle est en outre définie dans la bande de fréquence des 5.9 GHz sur une largeur de bande totale de 75 MHz (5.850 GHz – 5.925 GHz). Cette largeur de bande est segmentée en 7 canaux de 10 MHz chacun. Ces canaux se répartissant fonctionnellement en 1 canal de contrôle et 6 canaux de service, chacun pouvant offrir des débits allant de 6 à 27 Mbps. Optionnellement, des canaux peuvent être configurés sur une largeur de bande de 20 MHz, ce qui permet d'obtenir des débits pouvant aller jusqu'à 54 Mbps. Le canal de contrôle est réservé à la transmission des messages de gestion du réseau (basculement entre canaux, annonces de services, etc.). Il est également utilisé pour transmettre des messages de très haute priorité à l'instar des certains messages critiques liés à la sécurité routière. Les 6 autres canaux sont quant à eux dédiés à la transmission des données des différents services annoncés sur le canal de contrôle.

A titre d'illustration, la Figure 1 et la Figure 2 présentent pour le standard DSRC respectivement, les débits et les portées de transmission et la bande de fréquence.

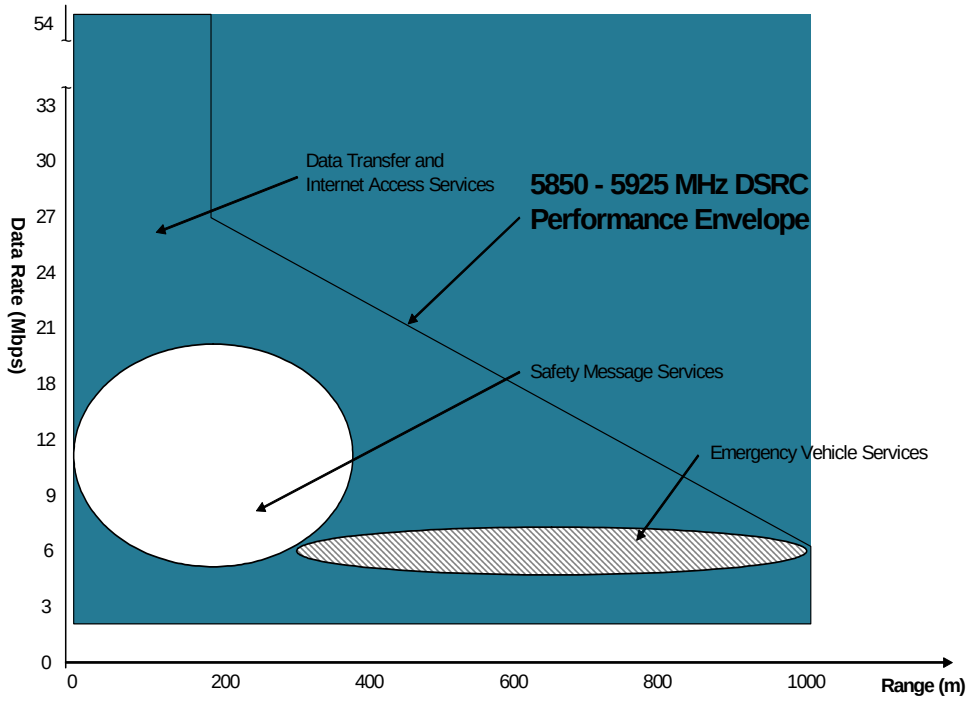


Figure 1: Débits et portées de transmission DSRC [DSRC]

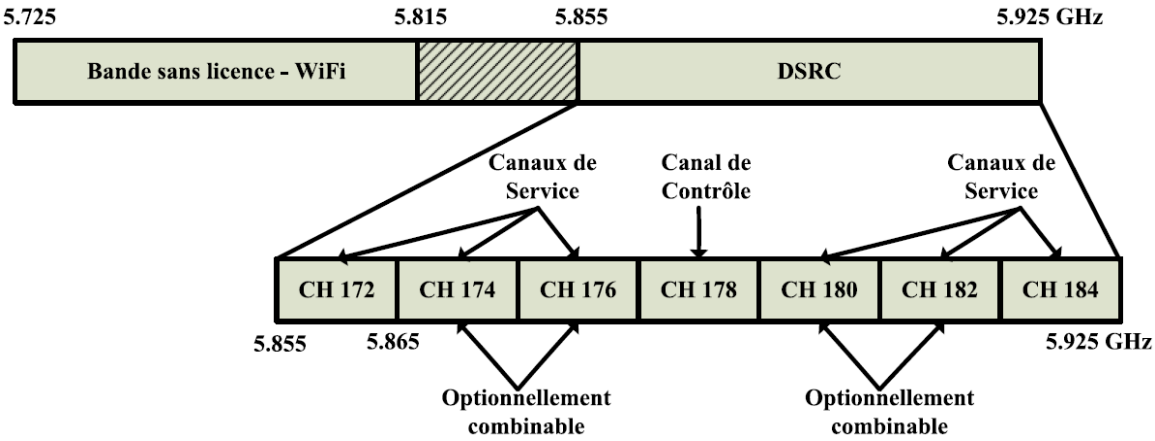


Figure 2: Bande de fréquence DSRC

De manière synthétique, on distingue dans le système DSRC 4 fonctions qui régissent l'accès aux services/applications et l'exécution de ces services/applications. Prises séparément, ces fonctions assurent:

- *L'enregistrement des applications/services*: Avant toute exécution, les applications du système doivent être enregistrées dans les OBUs et les RSUs. Cet enregistrement suppose l'affectation de paramètres comme l'AI (Application ID) ou encore la priorité de l'application.

- *La surveillance du canal de contrôle*: Les OBUs écoutent régulièrement le canal de contrôle à travers lequel ils reçoivent les annonces d'applications ou les messages critiques liés à la sécurité routière. Cette écoute du canal de contrôle est opérée au moins toutes les 100 ms.

- *Les annonces d'applications ou de services*: Les applications actives dans le système DSRC sont annoncées sur le canal de contrôle par les RSUs ou les OBUs; et ce, de manière périodique ou à la demande. Ces annonces sont faites à travers une table appelée PST (Provider Service Table). Cette PST contient, pour une application donnée, le canal sur lequel l'application est active ainsi que les paramètres liés à cette application (*e.g.* AI). Les annonces périodiques sont utilisées pour les applications toujours actives (*e.g.* péage autoroutier) alors que les annonces à la demande permettent de faire participer des nœuds à des applications dont l'activation est conditionnée par la production d'un ou plusieurs évènements (*e.g.* alerte accident).

- *L'initialisation et l'exécution des applications/services*: Les applications sont mises en route ou initialisées en mettant en correspondance l'AI enregistré localement et l'AI diffusé sur le canal de contrôle au travers de la PST. L'exécution ou l'échange des données applicatives se fait ensuite sur l'un des 6 canaux de service indiqué dans la PST. Le basculement de canal (*i.e.* canal de contrôle vers canal de service) lors de l'exécution d'une application, permet de préserver la bande passante du canal de contrôle qui reste ainsi pleinement dédié à la transmission des messages de gestion et des messages critiques.

La Figure 3 donne une vue simplifiée de l'organigramme mettant en œuvre des différentes fonctions régissant l'accès aux services/applications et l'exécution de ces services/applications dans le système DSRC.

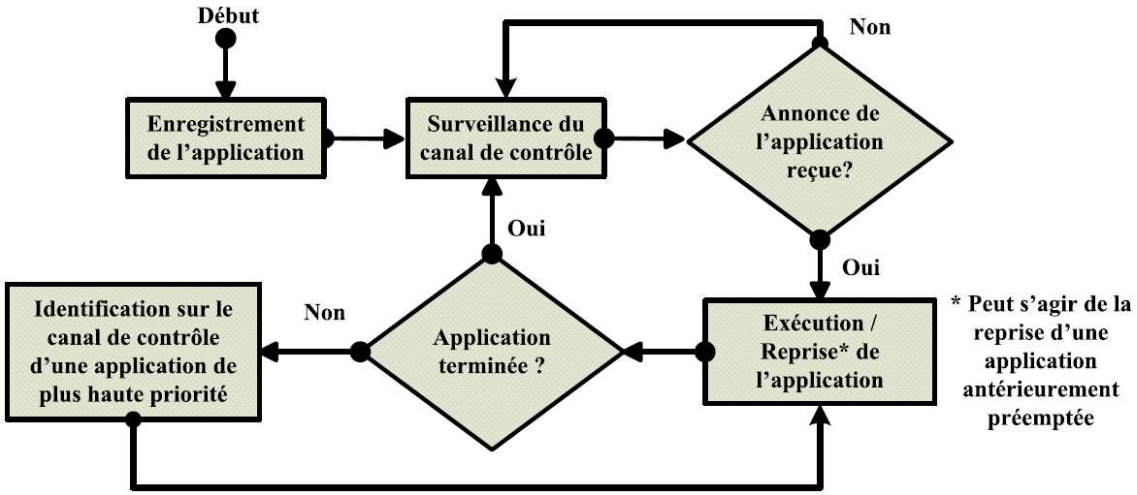


Figure 3: Accès et exécution des applications dans le système DSRC

3. Motivations de l'utilisation de la diversité des canaux DSRC pour le service d'authentification

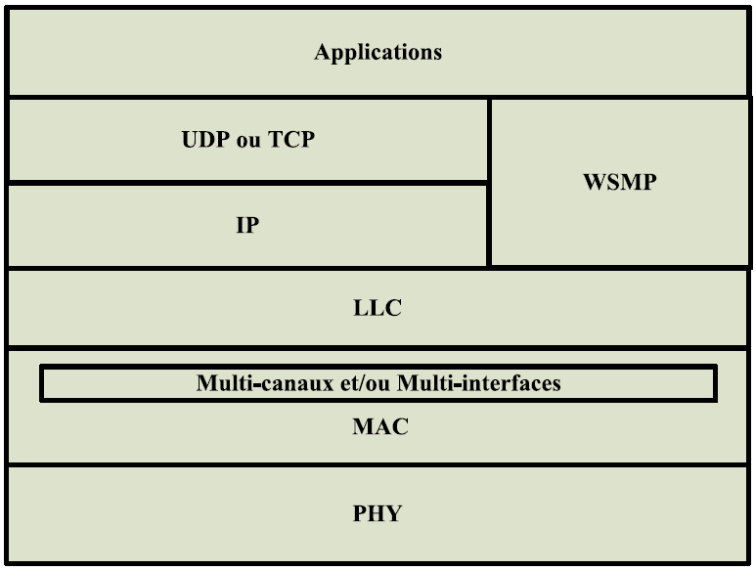
Dans le contexte des réseaux opérés, l'authentification en tant que fonction de gestion de l'accès au réseau et aux services, constitue la phase initiale précédant et conditionnant l'accès aux ressources et aux services. Le rôle de l'authentification est en particulier d'obtenir l'assurance que les entités communicantes sont bien ce qu'elles prétendent être. En d'autres termes, l'authentification garantit la véracité des identités ou des statuts des entités communicantes. L'authentification constitue à ce titre pour l'opérateur ou le fournisseur de service la pierre angulaire dans la mise en œuvre des architectures de sécurité des réseaux.

Ramenée au système DSRC, l'authentification avec l'opérateur réseau ou le fournisseur de service, constitue un service particulier qui se distingue singulièrement des services généraux des réseaux véhiculaires (*e.g.* alerte bouchon, payage électronique, navigation Internet, services P2P, etc.). En effet, ces derniers (*i.e.* services généraux) ne peuvent être opérés qu'après l'exécution complète et réussie du service d'authentification. Dans une telle configuration, au lieu de restreindre l'authentification à l'utilisation d'un seul canal comme le suggère le modèle DSRC, il convient afin d'en assurer la plus grande efficacité et robustesse, de mettre la diversité des canaux radio DSRC à son service. Plus concrètement, plusieurs canaux de service peuvent être utilisés pour la transmission des paquets d'authentification tandis que le canal de contrôle, réservé aux messages de gestion et aux messages critiques liés à la sécurité routière, reste épargné. Au-delà du renforcement de l'efficacité et de la robustesse du service d'authentification, l'utilisation intelligente au profit de l'authentification de plusieurs canaux de service fait rejaillir ces mêmes propriétés d'efficacité et de robustesse sur l'accès aux services généraux dont on sait qu'il est étroitement lié, dans les réseaux opérés, à la réussite du processus d'authentification.

C'est dans l'esprit de la mise à contribution intelligente de la diversité des canaux de service DSRC au profit du service d'authentification que nous présentons dans la section qui suit notre approche de priorisation de l'authentification.

4. Description de l'approche de priorisation de l'authentification

Notre approche de priorisation de l'authentification, consiste au niveau des OBUs ou des RSUs, à transmettre chaque paquet d'authentification sur le canal de service susceptible d'être le plus rapidement disponible, soit en d'autres termes celui qui est identifié comme étant le moins chargé. Pour ce faire, nous utilisons une nouvelle pile DSRC dans laquelle est ajouté le support optionnel des interfaces multiples[1] comme illustré par la Figure 4. Comme souligné dans les motivations de l'utilisation de la diversité des canaux DSRC, le canal de contrôle n'est pas utilisé pour la transmission des paquets d'authentification afin de préserver ses fonctions critiques de transmission des messages de gestion et des messages d'urgence liés à la sécurité routière.



WSMP: WAVE Short Message Protocol
UDP: User Datagram Protocol
TCP: Transmission Control Protocol
IP: Internet Protocol
LLC: Logical Link Control
MAC: Medium Access Control
PHY: PHYsical layer

Figure 4: Pile DSRC avec support optionnel d'interfaces multiples

[1] La mise en œuvre du support des interfaces multiples allant bien au-delà du sujet de cette thèse, nous ne la présenterons pas dans ce mémoire. Le lecteur intéressé peut cependant se référer à [ADYA04] pour avoir une approche de mise en œuvre possible.

La réalisation de notre approche de priorisation de l'authentification passe par la mise en œuvre de composantes ou de modules traduisant un mode opératoire, des fonctions spécifiques ou des options d'implémentation. Nous avons parmi ces composantes:

- *L'évaluation de l'état des canaux radio*

L'état des canaux radio est évalué localement par chaque nœud en mesurant pour chaque canal, la taille de la file de paquets (appartenant aux services de priorité supérieure ou égale à celle du service d'authentification) au niveau de la couche MAC et en écoutant chacun de ces canaux (en anglais, *channel sensing*). Plus prosaïquement, l'état d'un canal *i* recoupe la taille en bits de la file des paquets (appartenant aux services de priorité supérieure ou égale à celle du service d'authentification) en attente de transmission sur ce canal ($Length^i$) et l'état d'occupation courant du canal (libre ou occupé soit respectivement $Busy^i = 0$ ou $Busy^i = 1$).

En évitant des échanges de messages entre les nœuds du réseau, notre approche d'évaluation de l'état des canaux n'induit en conséquence aucun délai lié à ces échanges. De plus, une telle approche d'évaluation a le mérite de convenir aux environnements très mobiles à l'instar des réseaux véhiculaires dont on sait qu'ils sont marqués par une connectivité sujette à des variations telles qu'elles fausseraient systématiquement toute évaluation de l'état des canaux qui se ferait par des échanges de messages. Ajoutons qu'une évaluation locale de l'état des canaux, quand bien même elle ne permettrait pas d'approcher un résultat optimal à l'échelle de tout le réseau, reste la moins coûteuse et la plus adaptée au contexte mobile. Il est en effet démontré dans [JAIN03], qu'atteindre un résultat optimal à l'échelle du réseau est un problème d'optimisation globale réputé NP-complet. En d'autres termes, il est extrêmement couteux de trouver une solution qui approcherait, même de quelques facteurs, la solution optimale.

- *L'interaction inter-couches (en anglais, cross-layer interaction)*

Prioriser l'authentification passe par la mise en œuvre d'une interaction entre la couche assurant le transport du protocole d'authentification (*i.e.* le protocole EGEMO dans notre cas) et la couche MAC en charge de la gestion des canaux DSRC et/ou des interfaces multiples DSRC. La fonction de cette interaction est d'obtenir l'état des canaux radio en vue de sélectionner le canal susceptible d'être le plus rapidement disponible pour la transmission du paquet d'authentification. Plus concrètement, la couche transport du protocole d'authentification choisit parmi les canaux de service que l'on souhaite utiliser pour l'authentification, le canal sur lequel le paquet d'authentification doit être transmis. Pour ce faire, une requête sur l'état des canaux de service ciblés est transmise à la couche MAC qui en retour renvoie les différents états des canaux. La Figure 5 en donne une illustration simplifiée avec notamment la représentation des fonctions requête *GetServiceChannelsStatus()* et réponse *ReturnServiceChannelsStatus().*

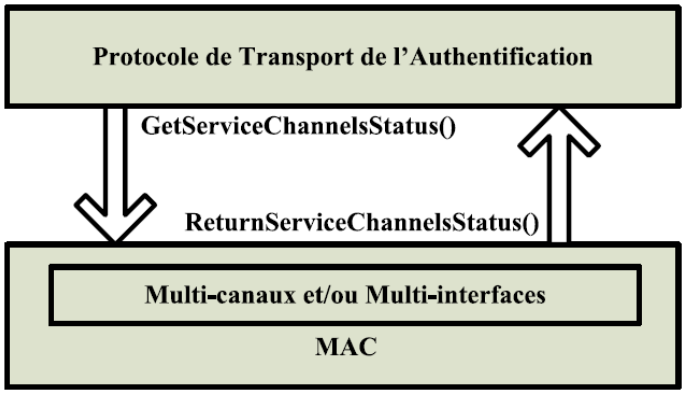


Figure 5: Interaction entre la couche transport de l'authentification et la couche MAC

- *Le transport des paquets d'authentification*

La couche assurant le transport du protocole d'authentification peut être implémentée directement au dessus de la couche 2 ou sur une couche supérieure (*e.g.* WSMP (WAVE "Wireless Access for Vehicular Environment" Short Message Protocol)) comme l'illustrent respectivement la Figure 6(b) et la Figure 6(a). Dans tous les cas, le protocole de transport de l'authentification doit être en mesure de déterminer le canal sur lequel chaque paquet d'authentification est transmis. Le format des paquets du protocole de transport de l'authentification comporte en conséquence un champ spécifique comportant des informations sur le canal sur lequel les couches inférieures doivent transmettre le paquet. Dans le cas de notre solution pour l'authentification, c'est le protocole EGEMO dont le scénario d'implémentation correspond à celui de la Figure 6(b), qui convoie ce champ.

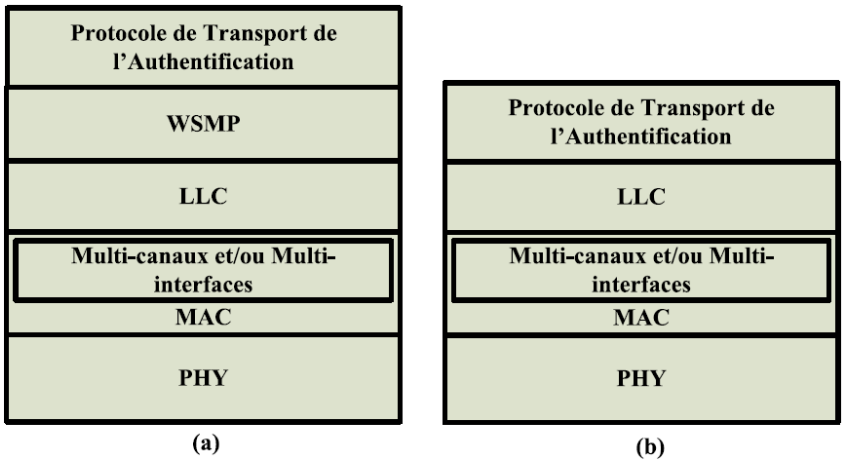


Figure 6: Scénarios d'implémentation du protocole de transport de l'authentification

- *La sélection du canal de transmission*

Lors du traitement au niveau du protocole de transport de l'authentification d'un paquet à transmettre, l'algorithme de sélection du canal de transmission illustré par l'organigramme de la Figure 7, amène à choisir en priorité, parmi les canaux de service que l'on souhaite utiliser, un canal sur lequel il n'y a aucune activité (*i.e.* le canal est libre ou son état d'occupation est à "libre") et dont la file des paquets (appartenant aux services de priorité supérieure ou égale à celle du service d'authentification) au niveau de la couche MAC est vide (*i.e.* la longueur de la file vaut 0). Si un tel canal n'existe pas, c'est un canal dont la file des paquets a la taille minimale qui est choisi. Nous supposons dans notre approche, qu'un canal est libre ou a son état d'occupation à "libre", si aucune activité ou aucune transmission de paquet n'a été détectée sur ce canal pendant au moins la durée maximale entre 2 transmissions de paquets. Si on suppose la saturation des files MAC dans un réseau DSRC/802.11p, la durée maximale T_{Max} entre 2 transmissions de paquets peut être exprimée comme suit:

$$T_{Max} = DIFS + CW_{\max} * T_{Slot} \quad (1)$$

Où *DIFS* (DCF "Distributed Coordination Function" Inter-Frame Spacing) est une durée de temps associée à la fonction de coordination distribuée de la norme 802.11p, CW_{max} est la taille maximale de la fenêtre de contention dans cette norme et T_{Slot} est la durée d'une tranche temporelle (en anglais, *time slot*) dans cette même norme.

On observe dans l'organigramme de la Figure 7 que lorsque le nombre de canaux de service éligibles pour la transmission d'un paquet d'authentification est supérieur à 1, le choix d'un canal parmi ces canaux éligibles se fait alors de manière équiprobable (*i.e.* chaque canal éligible a la même probabilité d'être choisi). L'implémentation de ces choix probabilistes utilise généralement des générateurs de nombres pseudo-aléatoires. Dans notre cas par exemple, il peut s'agir de segmenter la plage des réels bornée par 0 et 1, en sous-plages égales, le nombre de sous-plages étant égal au nombre de canaux éligibles. Chaque canal éligible se voit ensuite attribuer une sous-plage. Il suffit enfin de tirer grâce au générateur de nombres pseudo-aléatoires un réel compris entre 0 et 1. Le canal correspondant à la sous-plage à laquelle le nombre tiré (de manière pseudo-aléatoire) appartient est choisi.

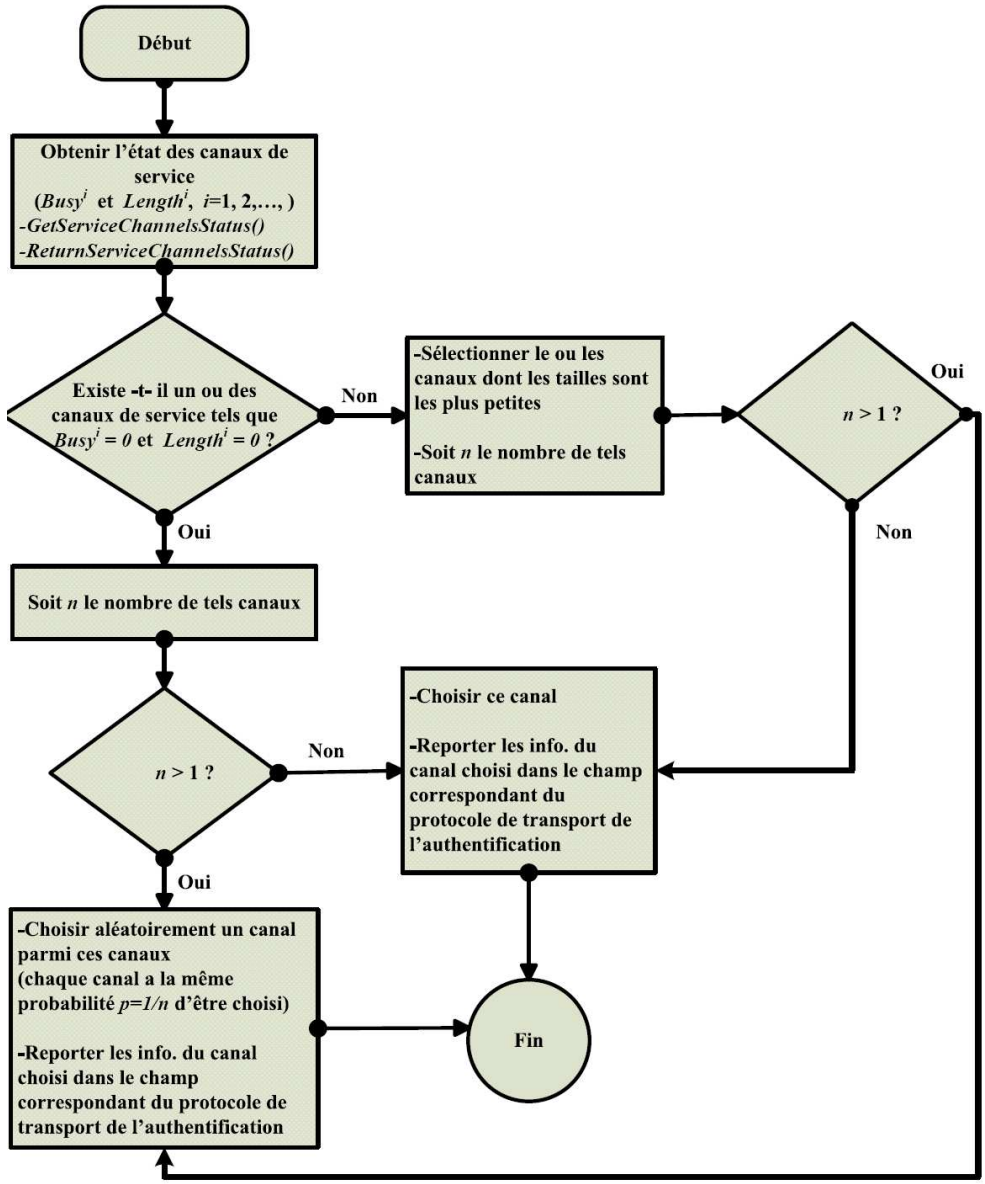


Figure 7: Algorithme de sélection du canal de transmission d'un paquet d'authentification

Il est à noter que dans le cas de notre solution pour l'authentification, l'algorithme de sélection du canal de transmission présenté ci-dessus, est mis en œuvre juste avant la construction du paquet EGEMO au niveau de l'OBU et du RSU mais aussi juste avant la mise à jour des champs du paquet EGEMO au niveau de l'OBU. En d'autres termes, l'algorithme de sélection est introduit au niveau de l'OBU et du RSU dans l'algorithme EGEMO de réception d'un paquet provenant du protocole EAP. De même, il est introduit au niveau de l'OBU dans l'algorithme EGEMO de réception d'un paquet provenant de la couche 2.

5. Scénarios de déploiement

Les principaux objectifs de notre approche de priorisation sont essentiellement le renforcement de l'efficacité et de la robustesse du processus d'authentification; et ce, même en présence de trafics de services tiers. Ce faisant notre approche pallie les limites de la technique antérieure basée sur l'utilisation d'un seul canal DSRC pour le service d'authentification. Cela étant dit, il est utile de relever que l'ampleur des avantages induits par notre approche de priorisation dépend étroitement des contextes de déploiement choisis; soit en d'autres termes du nombre d'interfaces mis en œuvre.

En effet, lorsque notre approche de priorisation est implémentée sur une unique interface DSRC, le service d'authentification bénéficie d'un allègement de la contention sur chacun des canaux et par conséquent d'une réduction potentielle des délais d'authentification (en particulier si on néglige les effets induits par la synchronisation des canaux dont notamment le basculement entre canaux). Suivant le même principe, les taux de succès de l'authentification, comparativement à ceux de la technique basée sur l'utilisation d'un seul canal, peuvent également être améliorés.

Les avantages potentiels attendus avec une unique interface sont cependant plus évidents et plus prononcés lorsque notre approche de priorisation est implémentée sur plusieurs interfaces DSRC. En effet, le service d'authentification bénéficie dans ce cas d'une bande passante plus étendue du fait des transmissions parallèles que rendent possible les interfaces multiples. Plus concrètement, un OBU relais recevant plusieurs paquets provenant potentiellement d'autant de sources différentes, peut les transmettre en parallèle et dans des conditions préférentielles sur plusieurs canaux de service. Les performances en termes de délai et de taux de succès de l'authentification sont donc beaucoup plus accrues.

On notera cependant que lorsque notre approche de priorisation est mise en œuvre sur un nombre d'interfaces inférieur au nombre de canaux de services que l'on souhaite associer au service d'authentification, alors il y a obligation d'utiliser en plus de la technique de priorisation, une méthode de synchronisation des canaux qui va permettre aux nœuds souhaitant communiquer de se retrouver sur le même canal pour pouvoir le faire. Pour s'affranchir du recours à une telle méthode, qui plus est, potentiellement très coûteuse en termes de ressources radio supplémentaires consommées et de délais dans un environnement très dynamique, notre approche de priorisation doit de préférence être déployée dans des configurations où le nombre de canaux de service associés au service d'authentification sur chaque nœud, est inférieur ou égal au nombre d'interfaces. En d'autres termes, chacun des canaux de service associés à l'authentification doit pouvoir se voir attribuer une interface radio de manière permanente.

6. Simulations et analyse des performances

Afin de conduire une évaluation comparative de notre solution et d'en démontrer la pertinence, nous avons implémenté (dans le simulateur GrooveNet [MAN06]) en plus de notre approche de priorisation, une approche naïve de sélection des canaux. A la différence de notre approche, l'approche naïve sélectionne les canaux de service sur lesquels doivent être transmis les paquets d'authentification de manière totalement aléatoire, chaque canal associé au service d'authentification ayant toutefois la même probabilité d'être sélectionné. Notons que l'optimisation du transport de l'authentification est active dans les différentes implémentations utilisées dans notre évaluation comparative. Avant de présenter l'analyse des performances proprement dite, nous introduisons d'abord ci-après les scénarios de simulation et les métriques de performance que nous avons retenus.

6.1. Scénarios de simulation et métriques de performance

Nous considérons sensiblement les mêmes scénarios de simulation que dans le chapitre précédent notamment en termes de densité des RSUs (voir Figure 8), de densité des OBUs, de mobilité, de topologie et de sécurité. Les seules différences résident dans l'association des 2 premiers canaux de service (*i.e. CH 172* and *CH 174*) au service d'authentification alors que le premier canal de service (*i.e. CH 172*) est également associé à un service P2P d'échange de fichiers entre les OBUs. De plus, chacun des 2 premiers canaux de service est associé à une interface distincte. Les simulations ont été conduites pour différents débits du service P2P. Suivant les simulations, chaque OBU génère un débit de *54* Kbps, *200* Kbps ou encore *2* Mbps. Nous faisons l'hypothèse qu'un même indice de priorité DSRC est affecté au service P2P et au service d'authentification (*i.e.* il n'y a pas de préemption entre les deux services). Pour le reste, le Tableau 1 résume l'ensemble des paramètres de nos simulations.

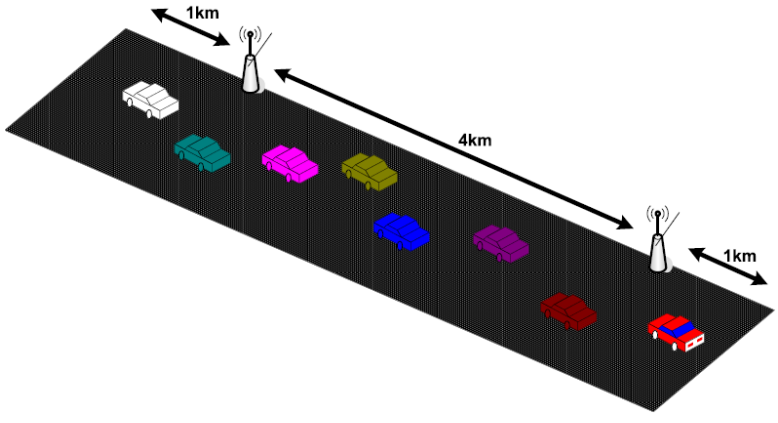


Figure 8: Densité de RSUs considérée pour les simulations

Tableau 1: Principaux paramètres de simulation

	Authentification EGEMO priorisée	***Authentification EGEMO non-priorisée (sélection aléatoire des canaux pour le service d'authentification)***
Paramètre	**Valeur**	
Durée de validité d'un paquet EGEMO	2 s	
Temporisateur de retransmission (RTO)	2 s	
Nombre maximum de retransmissions	3	
PKCS	ECC 163 – Architecture PKI 1-tiers	
Coefficient de non-traçabilité ($F_{non\text{-}trac}$)	0.5	
Topologie	6 Km en topologie linéaire	
Densité de RSUs	1 RSU tous les 4 Km	
Taux d'arrivée des OBUs (nombre d'OBUs par seconde)	1/12, 1/9, 1/6, 1/3	
Mobilité	Vitesse des OBUs uniformément variée (12.77 m/s – 20 m/s) - Vitesse moyenne de 16.5 m/s	
Associations "Service-Canal"	Authentification – Canaux CH 172 et CH 174 P2P – Canal CH 172	
Débits du service P2P	54 Kbps, 200 Kbps, 2 Mbps	
Paramètres d'optimisation du transport de l'authentification	Exposant amplificateur $\alpha = 10$ Optimisation médiane Facteur $\lambda = 2$ Facteur $\mu = 0.5$	
Couche MAC	DSRC CSMA CW_{Min} 15 Time Slot 13 us SIFS Time 32 us	
Couche Radio	2 canaux /interfaces (CH 172 et CH 174) Largeur de bande de chaque canal 10 MHz Antenne omnidirective de 1.65 m de hauteur Puissance de transmission 100 mW (20 dBm) Modulation OFDM BPSK ½ Portée de transmission 200 m Débit physique 6 Mbps	
Nombre de simulations et durée de chaque simulation	20 simulations (de 900 s chacune) par scénario (*i.e.* par densité d'OBUs, débit P2P et approche d'authentification)	

Nous avons choisi d'illustrer la pertinence de notre approche de priorisation au travers des 2 métriques de performance que sont le délai d'authentification et le taux de succès de l'authentification. Ces métriques à elles seules traduisent l'efficacité et la robustesse du processus d'authentification. Ces 2 métriques étant les mêmes que celles définies dans le Chapitre 2.2, elles en reprennent en conséquence les mêmes modes de calcul.

6.2. Analyse des performances

Les analyses du délai d'authentification et du taux de succès de l'authentification sont répertoriées comme suit:

- *Délai d'authentification*

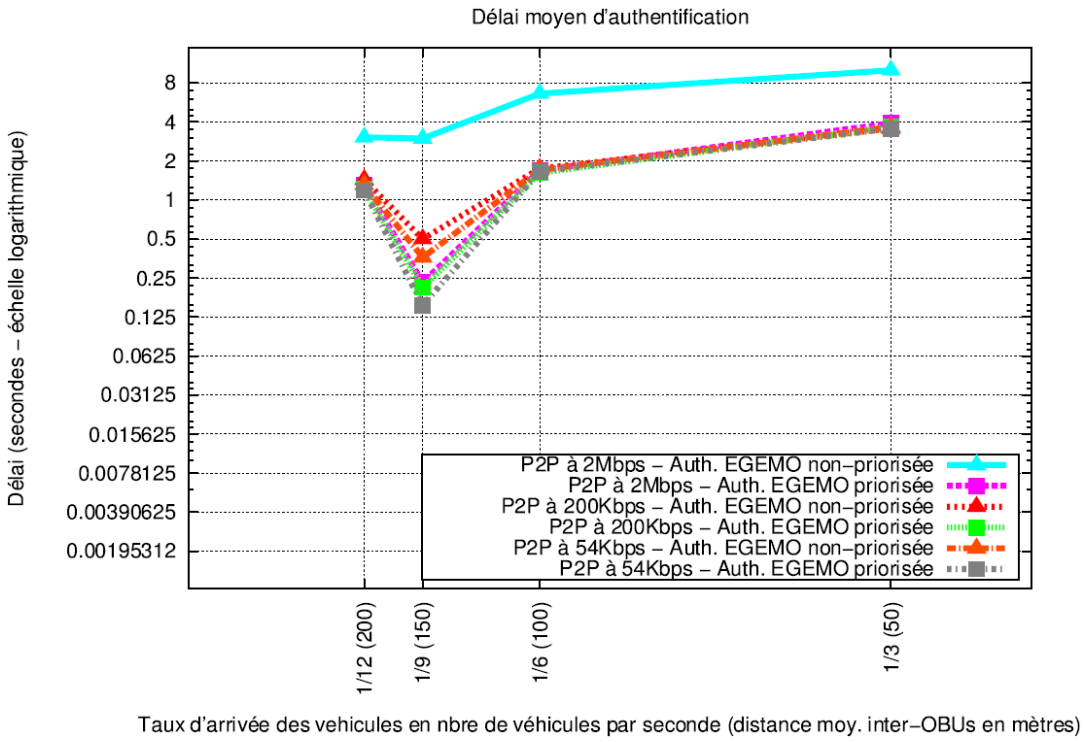


Figure 9: Délai d'authentification

La Figure 9 illustre l'évolution du délai d'authentification suivant différentes densités d'OBUs, différents débits du service P2P et selon que l'on utilise ou pas notre approche de priorisation de l'authentification. L'analyse de cette figure permet d'observer que notre approche de priorisation, même si elle permet d'obtenir des délais d'authentification relativement moindres, se différencie finalement assez peu du modèle de sélection aléatoire des canaux lorsque le débit des autres services (*i.e.* service P2P dans le cas présent) est relativement faible (*54* Kbps et *200* Kbps sur la figure). On note en revanche que lorsque le débit des autres services est relativement élevé (*2* Mbps pour le service P2P sur la figure), notre approche de priorisation permet de maintenir le délai d'authentification à un niveau bas pouvant être jusqu'à *10* fois inférieur (voir sur la figure lorsque la distance inter-OBUs = *150* m) au niveau obtenu lorsque notre approche de priorisation n'est pas mise en œuvre. A la lumière de ces résultats, on peut dire de manière générale que notre approche de priorisation permet, par l'obtention de délais d'authentification plus réduits, de rendre le processus d'authentification plus efficient en particulier lorsque ce dernier est en présence de services tiers très consommateurs de bande passante.

- *Taux de succès de l'authentification*

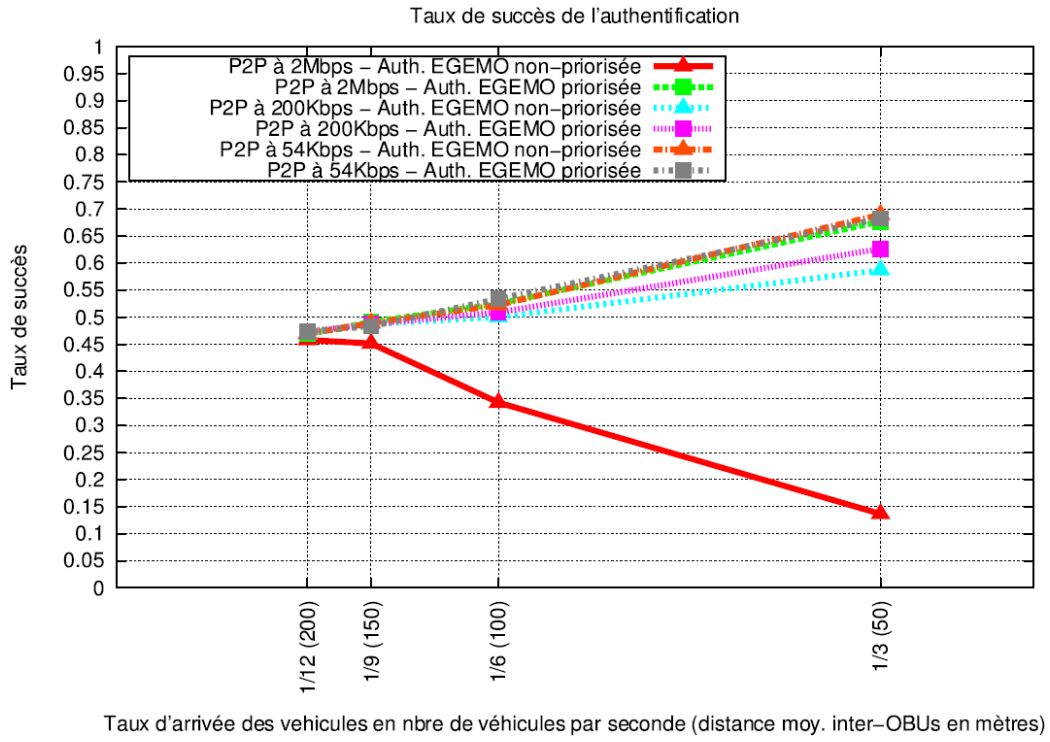


Figure 10: Taux de succès de l'authentification

La Figure 10 présente les variations du taux de succès de l'authentification suivant différentes densités d'OBUs, différents débits du service P2P et selon que notre approche de priorisation est mise en œuvre ou pas. Comme cela a été le cas pour le délai, on observe sur cette figure que l'écart entre le taux de succès obtenu avec notre approche de priorisation et celui obtenu avec l'approche dite naïve est d'autant plus fort que le débit des autres services est élevé. Ainsi par exemple le taux de succès de l'authentification est quasi-identique entre les deux approches lorsque le débit du service P2P ne vaut que *54* Kbps. En revanche lorsque ce débit augmente jusqu'à *2* Mbps par exemple, le taux de succès de l'authentification obtenu avec notre approche est maintenu aux environs de *70%* pour la plus forte densité d'OBUs simulée (*i.e.* distance inter-OBUs = *50* m), alors que dans le même temps il s'effondre à moins de *15%* avec l'approche naïve. Toutes ces observations dénotent la capacité de notre approche de priorisation à garantir la robustesse du processus d'authentification notamment en présence de service tiers gourmands en bande passante.

7. Conclusion

Compte-tenu du rôle particulier de l'authentification et de son impact sur l'accès aux services dans les réseaux opérés, nous avons présenté dans ce chapitre une approche de priorisation de l'authentification visant à garantir l'efficacité et la robustesse de l'authentification même en présence de services tiers dans le système DSRC. Cette

approche de priorisation met à contribution la diversité des canaux DSRC au travers d'une interaction entre la couche MAC et la couche assurant le transport de l'authentification; et ce, en vue de toujours sélectionner pour les paquets d'authentification le canal de service susceptible d'être le plus rapidement disponible. Nous avons pour ce faire défini une approche d'évaluation locale des canaux qui, loin de produire des résultats d'évaluation optimaux à l'échelle du réseau, reste néanmoins moins onéreuse et plus adaptée au contexte des réseaux véhiculaires marqué par une très forte dynamique des nœuds. De la discussion des options de déploiement de notre approche de priorisation de l'authentification, il ressort que les avantages attendus de notre solution ne peuvent véritablement prendre toute leur mesure que dans des configurations multi-interfaces où le nombre de canaux de service associés au service d'authentification est inférieur ou égal au nombre d'interfaces sur chaque nœud du réseau. L'analyse des performances qui a ensuite été conduite au travers des simulations confirme la pertinence de notre approche de priorisation en illustrant la capacité de cette dernière à garantir l'efficacité et la robustesse du service d'authentification notamment en présence de services tiers très consommateurs de bande passante. Il est cependant à noter que des simulations, non présentées ici, ont été faites pour des scénarios dans lesquels l'authentification utilise 6 canaux de service (*i.e.* le nombre maximum de canaux de service) et chaque nœud au moins 6 interfaces. Dans ces scénarios, l'amélioration des performances par rapport à celles des scénarios étudiés ici (*i.e.* 2 canaux de service pour l'authentification et 2 interfaces par nœud), est marginale, ce qui amène à penser que les gains de performance sont plafonnés et donc que la multiplication des canaux affectés à l'authentification ne se traduit pas nécessairement par des gains de performance substantiels.

Après la priorisation visant à renforcer les performances de notre solution pour l'authentification dans les réseaux véhiculaires, nous poursuivons dans la même optique d'amélioration des performances, en introduisant dans le chapitre qui va suivre une approche de distribution des fonctions de l'AS (AAA Server) à des OBUs du réseau déjà authentifiés.

Chapitre 2.5. Distribution de la Fonction d'Authentification

1. Introduction

Les analyses de performance de notre solution d'authentification dans le Chapitre 2.2, ont permis d'observer une dégradation du taux de succès de l'authentification et donc de la disponibilité de l'authentification dans les scénarios de forte densité d'OBUs. Ces analyses montrent également que les délais d'authentification ont tendance à augmenter avec le renforcement de la densité des OBUs, ce qui traduit une moindre efficacité du processus d'authentification. D'autres paramètres traduisant l'efficacité du processus d'authentification par rapport à l'utilisation de la ressource radio (*e.g.* taux d'Overhead imputable aux authentifications réussies) tendent également à se dégrader avec le renforcement de la densité des OBUs. Toutes ces tendances, observées dans les scénarios de forte densité d'OBUs et accentuées dans les scénarios de faible densité de RSUs, correspondent pourtant aux scénarios les plus attendus dans le contexte des réseaux véhiculaires.

Afin de corriger ou de freiner ces tendances à la dégradation qui impactent l'accès aux ressources et aux services du réseau, nous proposons de limiter le trafic d'authentification vers l'AS en distribuant ou en déléguant l'authentification (*i.e.* le rôle d'AS) en fonction de la densité des OBUs dans le réseau. Cette délégation de la fonction d'authentification qui est faite au profit des OBUs déjà authentifiés, est déclenchée par l'AS chaque fois qu'un seuil de densité d'OBUs est dépassé dans le réseau. Plus concrètement, à intervalles de temps réguliers, l'AS calcule le nombre seuil de requêtes d'authentification qu'il est censé recevoir pour une densité seuil d'OBUs donnée. Sur la base du même intervalle de temps, aussi appelé durée d'observation, l'AS met à jour le nombre de requêtes d'authentification qu'il a effectivement reçues. Le nombre seuil de requêtes d'authentification est calculé en intelligence avec les RSUs qui fournissent à l'AS des informations comme celles relatives à la mobilité des OBUs; informations obtenues via le protocole de transport de l'authentification, soit dans notre cas, le protocole EGEMO. Le maintien par l'AS du nombre seuil de requêtes et du nombre de requêtes effectivement reçues, lui permet au moment de l'authentification ou de la réauthentification d'un OBU et en particulier lorsque le nombre de requêtes d'authentification reçues est supérieur au nombre seuil de requêtes calculé, de traduire dans les paramètres des certificats volatiles de l'OBU, la délégation de la fonction d'authentification. L'OBU ainsi investi des privilèges de l'AS, intercepte dans l'intervalle de durée de validité de ses certificats volatiles, les requêtes d'authentification d'autres OBUs afin de réaliser les authentifications correspondantes. Ce faisant, le processus d'authentification des OBUs est relocalisé au plus près de ces derniers avec des effets d'amélioration

des performances sur la disponibilité et l'efficience de l'authentification mais aussi sur l'efficacité du processus d'authentification par rapport à l'utilisation de la ressource radio. Grâce à une telle distribution, le défi de l'accès ubiquitaire aux ressources et aux services du réseau, celui du déploiement optimum des RSUs et celui de la minimisation de la complexité matérielle des nœuds du réseau (*e.g.* utilisation d'une seule interface radio par nœud) peuvent être relevés.

Les analyses de performance réalisées à la suite de l'implémentation de la distribution de l'authentification dans le simulateur GrooveNet [MAN06] permettent de confirmer l'intérêt de notre démarche par rapport à la solution classique ne mettant pas en œuvre l'authentification distribuée. En effet, avec la distribution de l'authentification, des taux de succès et des délais d'authentification avantageux mais aussi une utilisation plus efficace de la ressource radio sont obtenus, notamment lorsque la densité des OBUs se renforce.

Pour ce qui est de la structuration de ce chapitre, nous commencerons en section 2 par décrire notre approche de distribution de l'authentification. Dans la section 3 nous aborderons les simulations et l'analyse des performances. Enfin la section 4 conclura le chapitre.

2. Approche de distribution de l'authentification

2.1. Description et formalisme

Notre approche de distribution de l'authentification s'inscrit dans le cadre des architectures et des protocoles présentés dans le Chapitre 2.1. Pour des raisons évidentes de sécurité, la distribution de l'authentification est entièrement contrôlée par l'AS. Ainsi, à l'occasion de l'authentification d'un OBU, l'AS lui délègue ses fonctions lorsqu'un certain seuil de densité d'OBUs dans le réseau est dépassé. Plus concrètement, l'OBU est investi des privilèges de l'AS lorsque le nombre de requêtes d'authentification reçues par l'AS sur un intervalle de temps appelé durée d'observation, dépasse le nombre de requêtes qu'aurait reçues l'AS pour une densité seuil d'OBUs encore appelée densité seuil d'OBUs de déclenchement de la distribution de l'authentification.

Les analyses réalisées dans le Chapitre 2.2 montrent que le taux de succès de l'authentification, indicateur par excellence de la disponibilité ou de la robustesse du processus d'authentification, commence à décliner lorsque la distance inter-OBUs moyenne dans le réseau est inférieure à $InterOBUDist_{Rec\text{-}AuthSucc}$:

$$InterOBUDist_{Rec-AuthSucc} = \frac{Range}{2^{\left(\frac{2*InterRSUDist-10*Range}{10*Range}\right)}} \quad (1)$$

Où *Range* est la portée de transmission des nœuds du réseau et *InterRSUDist* est la distance inter-RSUs moyenne dans le réseau. Ces analyses montrent en outre que le délai d'authentification, indicateur important de l'efficacité du processus d'authentification, tend à être moins compétitif que la solution d'authentification classique sur un saut, dès que la distance inter-OBUs moyenne dans le réseau est inférieure à $InterOBUDist_{Rec\text{-}Delay}$:

$$InterOBUDist_{Rec-Delay} = \frac{1}{4} * Range \quad (2)$$

Où *Range* est la portée de transmission des nœuds du réseau.

Dans ce contexte, la densité seuil d'OBUs de déclenchement de la distribution de l'authentification peut correspondre à une distance inter-OBUs seuil $InterOBUDist_{Thresh\text{-}Distrib}$, égale au minimum (voir Equation 3) ou au maximum (voir Equation 4) des distances inter-OBUs recommandées ci-dessus, selon que l'on opte respectivement, pour une distribution moins agressive ou plus agressive de la fonction d'authentification. Si en revanche on opte pour une distribution médiane de la fonction d'authentification, alors la densité seuil d'OBUs de déclenchement peut correspondre à une distance inter-OBUs seuil égale à la moyenne (voir Equation 5) des distances inter-OBUs recommandées ci-dessus.

$$InterOBUDist_{Thresh-Distrib} = MIN\left(InterOBUDist_{Rec-AuthSucc}, InterOBUDist_{Rec-Delay}\right) \quad (3)$$

$$InterOBUDist_{Thresh-Distrib} = MAX\left(InterOBUDist_{Rec-AuthSucc}, InterOBUDist_{Rec-Delay}\right) \quad (4)$$

$$InterOBUDist_{Thresh-Distrib} = \left(InterOBUDist_{Rec-AuthSucc} + InterOBUDist_{Rec-Delay}\right) / 2 \quad (5)$$

Avant d'arriver à la distribution de l'authentification proprement dite, chaque RSU (en plus de son activité ordinaire dans le processus d'authentification) maintient le nombre de paquets EGEMO reçus $NbPckt_{EGEMO}$ ainsi que la vitesse cumulative correspondante *CumulSpeed*. Cette vitesse cumulative n'est rien d'autre que la somme des vitesses extraites des paquets EGEMO reçus par le RSU. A titre d'illustration, si pendant un intervalle de temps donné un RSU reçoit *N* paquets EGEMO, alors la vitesse cumulative associée à ces paquets est comme suit:

$$CumulSpeed = \sum_{i=1}^{N} SourceSpeed_i \quad (6)$$

Où $SourceSpeed_i$ est la vitesse de l'OBU source du paquet EGEMO *i*.

A expiration d'une durée d'observation définie *T*, chaque RSU envoie à l'AS via un paquet RADIUS ou Diameter, le nombre de paquets EGEMO reçus et la vitesse cumulative correspondante. Le pseudo-code exécuté afin de mener à bien cette étape au niveau de la couche EGEMO de chaque RSU est présenté sur la Figure 1. Il est à noter que la réalisation à intervalles réguliers (*i.e.* sur des durées d'observation successives) de ces opérations permet l'adaptation de notre solution aux changements des conditions de circulation dans le réseau.

```
Pour tout (paquet EGEMO reçu) Faire
    Si (nouvelle période d'observation) Alors
        - Initialiser ou réinitialiser la vitesse cumulative et le
        nombre de paquets EGEMO reçus:
              CumulSpeed = NbPckt_EGEMO = 0
    Sinon
          - Mettre à jour la vitesse cumulative avec la
            vitesse de la source du paquet EGEMO reçu:
            CumulSpeed = CumulSpeed + SourceSpeed

          - Mettre à jour le nombre de paquets EGEMO reçus:
              NbPckt_EGEMO = NbPckt_EGEMO + 1
    Fsi
Fp

À (intervalle de temps T (Durée d'observation)) Faire
 - Envoyer CumulSpeed et NbPckt_EGEMO (via un paquet RADIUS ou
   Diameter) à l'AS
Fa
```

Figure 1: Pseudo-code du RSU pour le calcul et la restitution de la vitesse cumulative et du nombre de paquets EGEMO reçus

Au terme de la durée d'observation, une fois reçu de tous les RSUs, les nombres de paquets EGEMO que ces derniers ont reçus et les vitesses cumulatives correspondantes, l'AS peut désormais calculer la vitesse moyenne des OBUs dans le réseau et déduire ensuite le nombre seuil de requêtes d'authentification correspondant à la

densité seuil d'OBUs de déclenchement de la distribution de l'authentification; cette densité seuil d'OBUs étant elle-même associée à une distance seuil inter-OBUs déterminée suivant l'une des Equations 3 4 ou 5. La vitesse moyenne des OBUs (*Speed*) est déterminée par l'AS ainsi qu'il suit:

$$Speed = \frac{\sum_{k=1}^{L} CumulSpeed_k}{\sum_{j=1}^{L} NbPckt^{j}_{EGEMO}} \quad (7)$$

Où *L* est le nombre de RSUs ayant envoyé leurs nombres de paquets EGEMO reçus et les vitesses cumulatives correspondantes, $CumulSpeed_k$ est la vitesse cumulative associée aux paquets EGEMO reçus par le RSU *k*, $NbPckt^{j}_{EGEMO}$ est le nombre de paquets EGEMO reçus par le RSU *j*. Le nombre seuil de requêtes d'authentification ($AuthReq_{Thresh\text{-}Distrib}$) correspondant à la densité seuil d'OBUs de déclenchement de la distribution de l'authentification, est quant à lui déterminé par l'AS comme suit:

$$AuthReq_{Thresh-Distrib} = \frac{T}{\left(InterOBUDist_{Thresh-Distrib} / Speed \right)} = \frac{T * Speed}{InterOBUDist_{Thresh-Distrib}} \quad (8)$$

Où *T* est la durée d'observation, $InterOBUDist_{Thresh\text{-}Distrib}$ est la distance seuil inter-OBUs associée à la densité seuil d'OBUs de déclenchement de la distribution de l'authentification et *Speed* est la vitesse moyenne des OBUs dans le réseau.

Une fois le nombre seuil de requêtes d'authentification calculé, l'AS est désormais en mesure de décider notamment lors de l'authentification ou de la réauthentification d'un OBU, de la distribution ou non de la fonction d'authentification. Ainsi, à l'occasion de l'authentification ou de la réauthentification d'un OBU et avant de générer les paramètres des certificats volatiles dans le message AUCRED *VolCertsParams* du groupe de messages *m6* (lors de l'authentification initiale) ou du groupe de message *m2* (lors de la réauthentification) (voir Figure 2), l'AS compare le nombre de requêtes d'authentification effectivement mesuré (*AuthReqNb*) sur la dernière période d'observation au nombre seuil de requêtes ($AuthReq_{Thresh\text{-}Distrib}$) calculé sur cette même période. Si le nombre mesuré est supérieur au nombre seuil calculé (*i.e.* $AuthReqNb > AuthReq_{Thresh\text{-}Distrib}$) alors l'AS décide de déléguer la fonction d'authentification à l'OBU en cours d'authentification ou de réauthentification. Cette décision est notifiée dans les paramètres des certificats volatiles qu'envoie l'AS à l'OBU. Si on suppose à ce propos l'utilisation de la norme (de certificat) X.509v3 [PKIX] comme c'est le cas dans la plupart des implémentations récentes, alors les extensions standards *KeyUsage* et *ExtendedKeyUsage* qui renseignent sur l'utilisation qui doit être faite de la clé d'un certificat, peuvent être spécifiées dans le message *VolCertsParams*

de manière à autoriser l'utilisation des certificats volatiles de l'OBU en cours d'authentification ou de réauthentification, pour jouer le rôle de serveur d'authentification et délivrer des certificats volatiles à d'autres OBUs. Au terme de l'authentification ou de la réauthentification, l'OBU investi dispose donc de certificats volatiles signés par l'AS lui conférant au travers des champs *KeyUsage* et *ExtendedKeyUsage* les privilèges de l'AS. Notons en outre que la distribution de la fonction d'authentification par l'AS est mise en œuvre jusqu'à ce que le nombre de requêtes d'authentification reçues passe en dessous du nombre seuil de requêtes correspondant à la densité seuil d'OBUs de déclenchement de la distribution. Le pseudo-code présenté sur la Figure 3 synthétise les instructions exécutées par l'AS dans ce contexte.

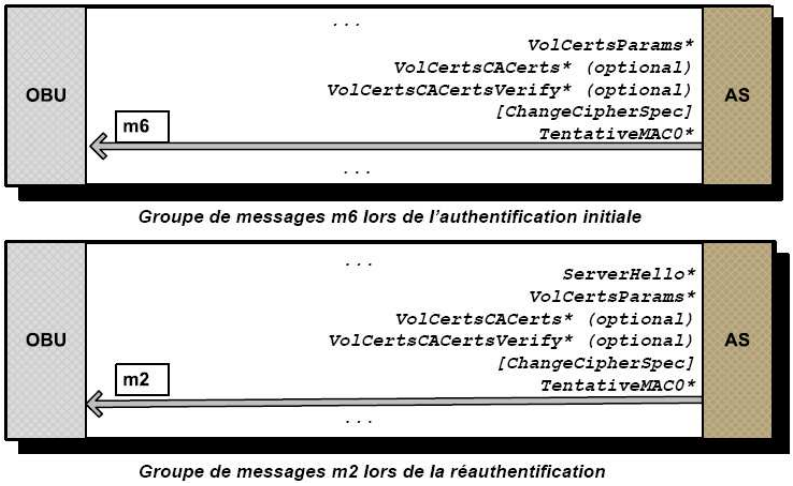


Figure 2: Groupes de messages AUCRED contenant le message *VolCertsParams*

```
Pour tout (paquet EAP reçu (via RADIUS ou Diameter) et correspondant à une
requête d'authentification)
Faire
    Si (nouvelle période d'observation) Alors
        - Réinitialiser le nombre de requêtes d'authentification:
                AuthReqNb = 0
    Sinon
        - Mettre à jour le nombre de requêtes d'authentification:
                AuthReqNb = AuthReqNb + 1
    Fsi
Fp

À (intervalle de temps T (Durée d'observation)) Faire
- Obtenir de tous les RSU^i (i=1..m) les nombres de paquets EGEMO traités
  ainsi que les vitesses cumulatives correspondantes:
      CumulSpeed_i, NbPckt^i_EGEMO (i=1..m)
- Calculer la vitesse moyenne des véhicules:
      Speed = (CumulSpeed_1+...+CumulSpeed_m) / (NbPckt^i_EGEMO+...+NbPckt^m_EGEMO)
- Calculer le nombre seuil de requêtes d'authentification pour la densité
  seuil d'OBUs associée à la distance seuil inter-OBUs InterOBUDist_Thresh-Distrib:
      AuthReq_Thresh-Distrib= (T * Speed)/ InterOBUDist_Thresh-Distrib
Fa

Pour tout (message AUCRED m5 (auth. initiale) ou m1 (réauth.) reçu d'un OBU)
Faire
    Si (AuthReqNb > AuthReq_Thresh-Distrib) Alors
        - Notifier le rôle d'AS dans les paramètres des certificats volatiles
        (sous-message VolCertsParams du message m6 (auth. initiale) ou m2
        (réauth.) ) et poursuivre normalement le processus
    Sinon
        - Poursuivre normalement le processus
    Fsi
Fp
```

Figure 3: Pseudo-code de l'AS pour la distribution de l'authentification

Dans notre schéma de distribution de l'authentification, l'OBU investi des privilèges de l'AS, au lieu de relayer vers le RSU les requêtes d'authentification qu'il reçoit d'autres OBUs, va directement y répondre et réaliser l'authentification en lieu et place de l'AS (voir Figure 4). Cet OBU investi exerce ses privilèges jusqu'à sa prochaine authentification ou réauthentification à l'issue de laquelle il devra acquérir de nouveaux certificats volatiles. Autrement dit, les privilèges accordés sont temporaires et ne durent que le temps de validité des certificats volatiles qui les confèrent. Il est à noter que dans notre solution, l'OBU investi n'est par défaut pas autorisé à déléguer de nouveau la fonction d'authentification. Cela étant dit, on peut parfaitement envisager que l'OBU investi puisse à son tour déléguer la fonction d'authentification s'il en est explicitement autorisé par l'AS dans les paramètres de ses certificats volatiles. Dans tous les cas, tout OBU n'accepte d'être authentifié par un autre OBU que si ce dernier lui présente des certificats volatiles dont les paramètres confèrent les privilèges de l'AS.

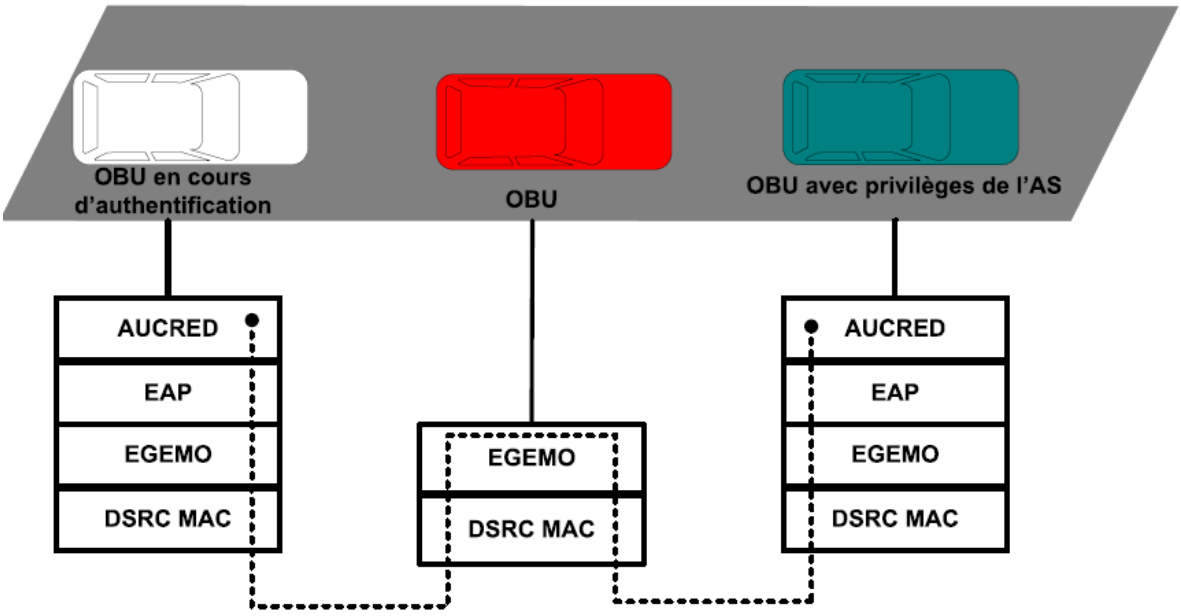


Figure 4: Authentification entre un OBU ordinaire et un OBU investi des privilèges de l'AS

2.1. Précautions de calcul

Dans la pratique, il convient de lisser la mesure du nombre de requêtes d'authentification ainsi que le calcul du nombre seuil de requêtes de manière à tenir compte de l'antériorité et à pondérer l'évolution de ces valeurs. Une telle pondération est nécessaire afin d'éviter que la volatilité des conditions de circulation routière ne se traduise par de trop gros écarts entre les valeurs mesurées ou calculées d'une période d'observation à l'autre. Pour ce faire, toute valeur calculée ou mesurée au bout de chaque période d'observation est pondérée come suit:

$$Val = \alpha * Val_{new} + (1-\alpha) * Val_{old} \quad (9)$$

Où α ($0 < \alpha < 1$) est le facteur de pondération, Val_{new} est la nouvelle valeur calculée ou mesurée sur la durée d'observation venant de s'écouler, Val_{old} est l'ancienne valeur calculée ou mesurée sur la durée d'observation précédant celle qui vient de s'écouler et *Val* est la valeur pondérée ou lissée.

3. Simulations et analyse des performances

Une fois notre approche de distribution de l'authentification greffée à la solution d'authentification initiale et implémentée dans le simulateur GrooveNet [MAN06], nous conduisons dans cette section, afin d'en démontrer la pertinence, une analyse comparative mettant en scène le cas où notre approche de distribution de l'authentification est mise en œuvre et le cas où elle ne l'est pas. Avant d'en arriver à l'analyse des performances proprement dite, nous commencerons ci-après par présenter nos scénarios de simulation ainsi les métriques de performance appelées à baliser notre analyse.

3.1. Scénarios de simulation et métriques de performance

Les scénarios de simulation que nous avons retenus ici sont assez proches de ceux utilisés dans le Chapitre 2.3, notamment en termes de densité de RSUs (voir Figure 5), de densité d'OBUs, de configuration radio (*e.g.* une seule interface radio par nœud), de mobilité, de topologie et de sécurité. Nous considérons toutefois dans le cas présent, 2 scénarios de trafic à savoir un premier cas où seul le service d'authentification est associé au canal de service considéré (canal *CH 180* avec fréquence centrale à *5.9* GHz) et un deuxième cas où un service P2P d'échange de fichiers à *200* Kbps (*i.e.* chaque OBU génère *200* Kbps de données) est associé au canal de service considéré en plus du service d'authentification. Le service P2P lorsqu'il est exécuté et le service d'authentification sont supposés avoir le même indice de priorité dans le système DSRC (*i.e.* il n'y a pas de préemption entre les deux services). Pour ce qui est de la distribution de l'authentification, les simulations la mettant en œuvre appliquent une distribution médiane soit un calcul de la distance seuil inter-OBUs de déclenchement de la distribution selon l'Equation 5. La durée d'observation et le facteur de pondération dans ces simulations sont quant à eux fixés à *30* s et *0.3* respectivement. Pour le reste, le Tableau 1 récapitule l'ensemble des paramètres de nos simulations.

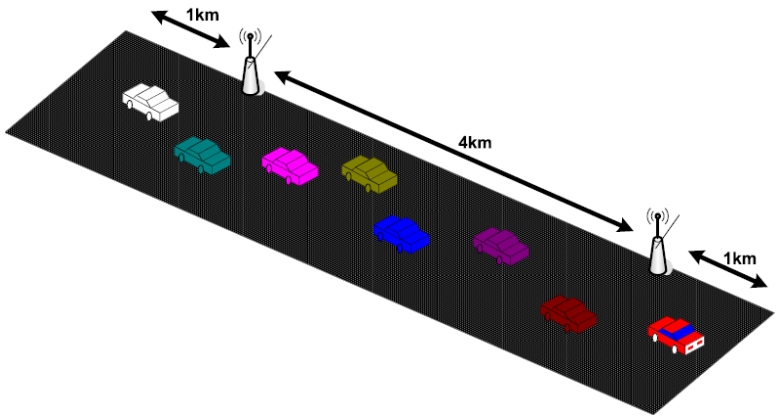


Figure 5: Densité de RSUs considérée pour les simulations

Tableau 1: Principaux paramètres de simulation

	Authentification EGEMO distribuée	***Authentification EGEMO non-distribuée***
Paramètre	**Valeur**	
Durée de validité d'un paquet EGEMO	2 s	
Temporisateur de retransmission (RTO)	2 s	
Nombre maximum de retransmissions	3	
PKCS	ECC 163 – Architecture PKI 1-tiers	
Coefficient de non-traçabilité ($F_{non\text{-}trac}$)	0.5	
Topologie	6 Km en topologie linéaire	
Densité de RSUs	1 RSU tous les 4 Km	
Taux d'arrivée des OBUs (nombre d'OBUs par seconde)	1/12, 1/9, 1/6, 1/3	
Mobilité	Vitesse des OBUs uniformément variée (12.77 m/s – 20 m/s) - Vitesse moyenne de 16.5 m/s	
Scénarios de trafic	Authentification – Canal CH 180 Authentification et P2P à 200 Kbps – Canal CH 180	
Paramètres d'optimisation du transport de l'authentification	Exposant amplificateur $\alpha = 10$ Optimisation médiane Facteur $\lambda = 2$ Facteur $\mu = 0.5$	
Paramètres pour la distribution de l'authentification	Distribution médiane (*InterOBUDist*$_{Thresh\text{-}Distrib}$ suivant Equation 5) Durée d'observation T = 30 s Facteur de pondération $\alpha = 0.3$	N/A
Couche MAC	DSRC CSMA CW_{Min} 15 Time Slot 13 us SIFS Time 32 us	
Couche Radio	Fréquence centrale 5.9 GHz (CH 180) Largeur de bande de chaque canal 10 MHz Antenne omnidirective de 1.65 m de hauteur Puissance de transmission 100 mW (20 dBm) Modulation OFDM BPSK ½ Portée de transmission 200 m Débit physique 6 Mbps	
Nombre de simulations et durée de chaque simulation	20 simulations (de 900 s chacune) par scénario (*i.e.* par densité d'OBUs, scénario de trafic et approche d'authentification)	

Pour mener notre analyse comparative et étayer la pertinence de la distribution de l'authentification, nous avons retenu 3 métriques de performance illustrant respectivement la disponibilité ou la robustesse du processus d'authentification, l'efficience de ce processus et le niveau d'efficacité de ce processus par rapport à l'utilisation des ressources radio. Ces métriques sont nommément: le taux de succès de l'authentification, le délai d'authentification et le taux d'Overhead imputable aux authentifications réussies. Ces 3 métriques sont conceptuellement les mêmes que celles définies dans les chapitres précédents. Elles en reprennent à ce titre les mêmes principes de calcul.

3.2. Analyse des performances

Les analyses comparatives de l'évolution des 3 métriques de performance retenues sont répertoriées et présentées successivement comme ci-après:

- *Taux de succès de l'authentification*

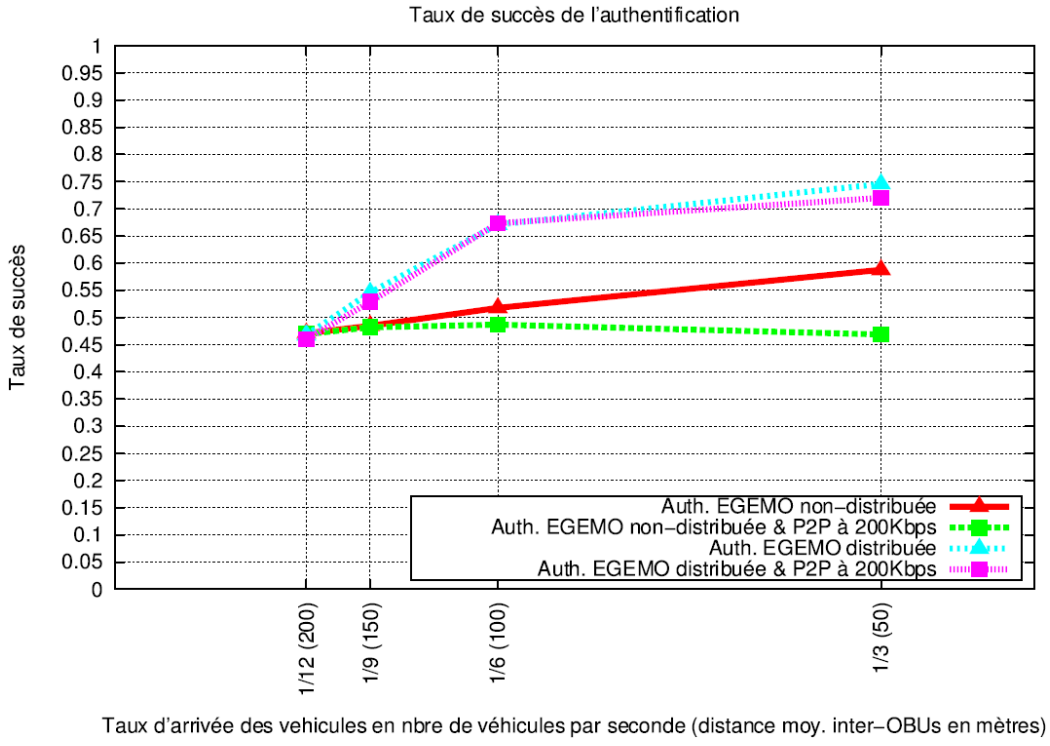


Figure 6: Taux de succès de l'authentification

La Figure 6 présente différentes évolutions du taux de succès de l'authentification suivant différents scénarios de densités d'OBUs, suivant que l'on adjoint ou pas au service d'authentification un service de P2P à *200* Kbps

et enfin suivant que l'on active ou pas la distribution de l'authentification. Comme attendu, on note sur cette figure et en particulier avec le renforcement de la densité des OBUs, une bien meilleure orientation du taux de succès de l'authentification avec l'authentification distribuée par rapport à l'authentification classique (*i.e* non-distribuée). Pour la plus forte densité simulée par exemple (*i.e.* distance inter-OBUs = *50* m), on observe que la distribution de l'authentification permet d'obtenir un taux de succès d'environ *75%*, ce qui traduit un gain de performance de l'ordre de *10%* à 25% selon respectivement que le service d'authentification opère seul sur son canal ou qu'il le partage avec un service P2P de même priorité à *200* Kbps. En d'autres termes et de manière plus générale, l'authentification distribuée, par rapport à l'authentification classique, améliore d'autant plus la disponibilité de l'authentification que la densité des OBUs est forte et que le débit des services de même priorité utilisant le même canal que le service d'authentification, tend à être important. Cette propriété de robustesse que reflète notre approche de distribution, est d'autant plus cruciale que notre solution pour l'authentification est appelée à être mise en œuvre dans des configurations qui sont parmi les plus attendues dans les réseaux véhiculaires, à savoir des configurations de forte densité d'OBUs avec une seule interface radio et un canal partagé entre le service d'authentification et d'autres services de même priorité.

- *Délai d'authentification*

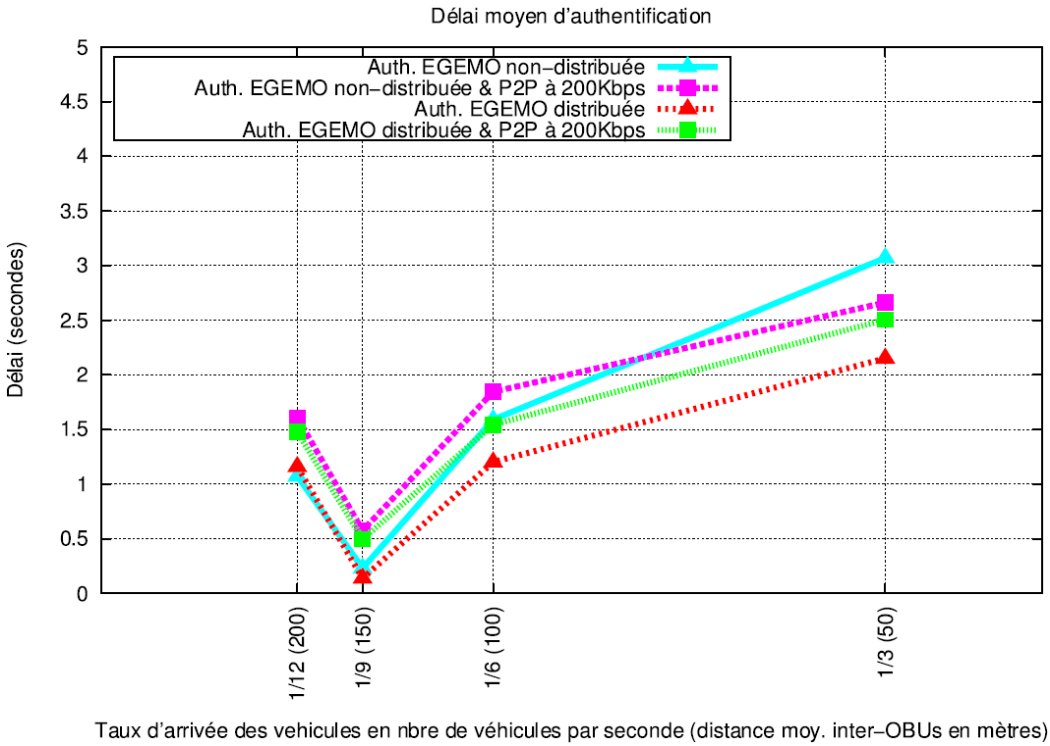


Figure 7: Délai d'authentification

Dans les mêmes conditions d'analyse que celles du taux de succès de l'authentification (*i.e.* divers scénarios de densités d'OBUs, partage et non-partage du canal de transmission entre le service d'authentification et un service P2P de même priorité à *200* Kbps, activation et non-activation de la distribution de l'authentification), la Figure 7 illustre les évolutions du délai d'authentification. On peut y relever qu'avec l'augmentation de la densité des OBUs, l'authentification distribuée, par rapport à l'authentification classique (*i.e.* non-distribuée), réduit les délais d'authentification. Pour les densités simulées les plus importantes par exemple (*e.g.* distance inter-OBUs = *100* m ou *50* m), ces réductions sont de l'ordre de *0.5* s lorsqu'il y a partage de canal et de *1* s lorsque le service d'authentification opère seul sur son canal. S'il est possible de conclure que la distribution de l'authentification améliore l'efficacité du processus d'authentification, il importe de noter toutefois que cette amélioration est inversement proportionnelle au débit des services de même priorité partageant le même canal que le service d'authentification. Partant de là, on peut parfaitement anticiper qu'une augmentation inconsidérée des débits des services de même priorité utilisant le même canal que le service d'authentification, ne faciliterait pas l'accès de la plupart des OBUs à l'AS, ce qui aurait l'effet mécanique de freiner et même bloquer la mise en œuvre de la distribution de l'authentification et par conséquent, d'anéantir tous les bénéfices escomptés. Il va sans dire que cet anéantissement serait encore plus marqué si les services utilisant le même canal que le service d'authentification, en plus d''une consommation inconsidérée de la bande passante, avaient des indices de priorité supérieurs.

- *Taux d'Overhead imputable aux authentifications réussies*

Comme le montre la Figure 8, alors qu'on obtient un taux d'Overhead maximal de *80%* et un taux minimal de *70%* avec la distribution de l'authentification, ces taux ne sont respectivement que de *70%* et *30%* sans la distribution. Rappelons qu'un taux élevé de l'Overhead traduit une grande efficacité de l'authentification par rapport à l'Overhead généré dans le réseau alors qu'un taux faible est synonyme d'une moindre efficacité. Plus précisément, on observe sur cette figure que l'authentification distribuée par rapport à l'authentification classique (*i.e.* non-distribuée) améliore sensiblement, avec le renforcement de la densité des OBUs, le taux d'Overhead imputable aux authentifications réussies et par conséquent l'efficacité du processus d'authentification quant à l'utilisation de la ressource radio. Cette amélioration est d'ailleurs d'autant plus prégnante que le débit des services de même priorité utilisant le même canal que le service d'authentification (*i.e.* service P2P dans notre cas) tend à être consistant. Ainsi par exemple, pour la densité d'OBUs simulée la plus importante (*i.e.* distance inter-OBUs = *50* m) le gain d'efficacité de l'authentification distribuée par rapport à l'authentification classique est de l'ordre de *40%* lorsque le service d'authentification partage son canal avec un service P2P de même priorité à *200* Kbps et *30%* lorsque le service d'authentification opère seul sur son canal. Cette tendance à l'amélioration qui tend à se renforcer avec l'augmentation de la densité des OBUs et l'appréciation du débit des services de même priorité utilisant le même canal que le service d'authentification,

confirme l'adéquation de l'authentification distribuée à ces scénarios dont la récurrence dans les réseaux véhiculaires est hautement probable.

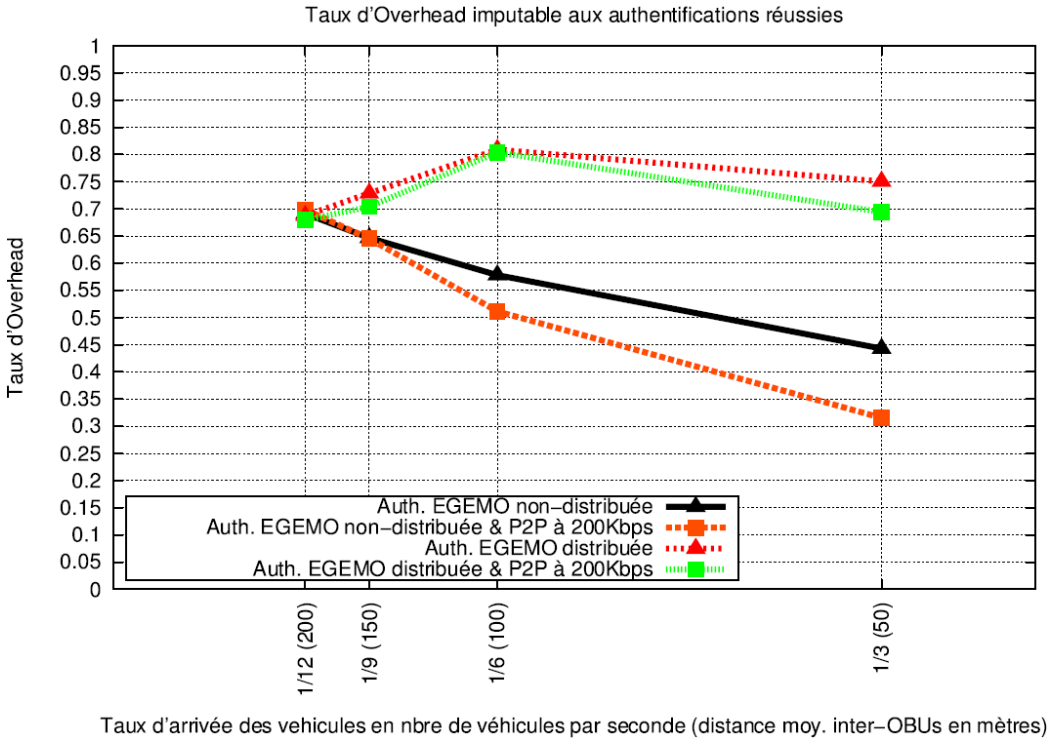


Figure 8: Taux d'Overhead imputable aux authentifications réussies

4. Conclusion

Nous avons présenté dans ce chapitre une approche de distribution de l'authentification tendant à relocaliser la fonction d'authentification (*i.e.* le service fourni par l'AS) au plus près des OBUs désirant s'authentifier pour accéder aux ressources et aux services du réseau. La distribution de la fonction d'authentification repose d'une part (i) sur le calcul par l'AS en intelligence avec les RSUs et à intervalles réguliers (appelés durées d'observation), du nombre seuil de requêtes qu'il aurait reçues pour une densité seuil d'OBUs donnée associée au déclenchement de la distribution de l'authentification, et du nombre de requêtes d'authentification qu'il a effectivement reçues et d'autre part (ii) sur la délégation au travers des paramètres des certificats volatiles, des privilèges de l'AS à l'OBU en cours d'authentification ou de réauthentification lorsqu'en particulier le nombre de requêtes d'authentification effectivement reçues par l'AS est supérieur au nombre seuil de requêtes de déclenchement de la distribution. A l'aune de l'analyse des performances de notre solution initiale dans le Chapitre 2.2, nous avons proposé une méthode concrète de détermination des densités seuil d'OBUs associées au déclenchement de la distribution de l'authentification. Tous ces éléments permettent à notre approche de

distribution de l'authentification de s'adapter automatiquement et continuellement aux changements des conditions de circulation dans le réseau tout en étant entièrement contrôlée par l'opérateur à travers le serveur d'authentification. La distribution se montre ainsi à la fois dynamique, flexible et adaptée au contexte des réseaux véhiculaires opérés. Les analyses de performance qui ont été conduites dans ce contexte confirment l'intérêt de cette distribution et notamment sa capacité à améliorer la robustesse et l'efficience du processus d'authentification mais aussi son efficacité par rapport à l'utilisation de la ressource radio lorsque la densité des OBUs dans le réseau augmente. Ces propriétés ont aussi été confirmées dans les scénarios DSRC où le service d'authentification est associé au même canal que d'autres services de même priorité, à condition bien entendu que le débit de ces services ne soit pas de nature à bloquer la mise en œuvre de la distribution de l'authentification. Finalement, en amplifiant les performances de notre solution initiale, notre approche de distribution de l'authentification ouvre la voie à l'accès ubiquitaire aux ressources et aux services du réseau véhiculaire dans des configurations parmi les plus attendues à savoir des configurations de forte densité d'OBUs, de déploiement restreint des RSUs, de complexité matérielle minimale des nœuds du réseau et même d'opération de services concurrents du service d'authentification.

Conclusion

Nous nous sommes intéressés dans cette thèse à la problématique de l'authentification dans les réseaux véhiculaires opérés. Avant les propositions de solutions, nous nous sommes livrés à un exercice de situation dans lequel le contexte et les contours de la thèse ont été définis. Nous nous proposons ici de revenir sur l'ensemble du déroulement de ces travaux pour en souligner les aspects les plus saillants.

1. Nos travaux

Arrivé au terme de cette thèse, il importe de revenir sur les principales étapes nous ayant conduit aux résultats que nous avons obtenus. On retiendra que nous avons tout d'abord introduit dans le Chapitre 1.1 les principales architectures de communication des réseaux véhiculaires. Au-delà des typologies architecturales qui ont été faites, nous avons introduit les principales contributions, aussi bien au niveau des projets industriels et des projets de standardisation que des travaux de recherche académiques. A la suite des présentations et analyses que nous avons faites, il a été possible de déduire les potentiels des différentes architectures notamment en termes d'applications et de possibilités de déploiements. Nous sommes arrivés en particulier à la conclusion que les architectures de réseaux ad-hoc hybrides sont celles offrant le potentiel le plus prometteur puisqu'elles permettent de tirer parti concomitamment des avantages applicatifs et des caractéristiques des réseaux à infrastructure et des réseaux ad-hoc mais aussi d'engranger des gains de performance (*e.g.* débit, délai, optimisation de l'exploitation des ressources radio, etc.) et des avantages de la rationalisation du déploiement des points d'accès.

Ayant situé nos travaux dans un contexte architectural ad-hoc hybride, et en particulier dans un contexte technologique de type WLAN, nous avons introduit dans le Chapitre 1.2, la sécurité des WLANs et en l'occurrence celle du standard WLAN le plus connu et le plus largement déployé actuellement, soit le standard IEEE 802.11. Nous avons à cette occasion relevé les insuffisances des mécanismes de sécurité mis en œuvre dans ces réseaux, notamment leur inadéquation dans des environnements dynamiques où les stations clientes ne sont pas toujours nécessairement sur le même lien ou à un saut du premier nœud fixe opéré, leur propension à laisser libre accès à nombre de services du réseau lorsqu'ils sont implémentés sur les couches hautes, etc. Au-delà des attaques, des mécanismes de sécurité en vigueur dans ce type de réseau et de leurs faiblesses, nous nous sommes plus spécifiquement intéressés à la sécurité des réseaux véhiculaires. Nous avons en particulier montré à travers le prisme de leurs caractéristiques spécifiques - notamment leurs caractéristiques applicatives - 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 s'intéressait aux services ITS ou aux services non-ITS. S'agissant des contributions dans le domaine de la sécurité des réseaux véhiculaires, nous avons de manière générale noté: (i) l'absence d'un modèle de sécurité global intégrant les caractéristiques et les contraintes spécifiques des réseaux véhiculaires et en particulier les problématiques de sécurité de l'ensemble des services pouvant y être opérés (*i.e.* services ITS et services ITS), (ii) l'absence un schéma architectural d'opérateur de réseau ou de service et par conséquent la non prise en compte des problématiques de sécurité associées à l'instar de celles relatives à l'authentification pour l'accès au réseau et aux services.

Après la Partie 1 où les motivations de nos travaux ont été fondées, nous nous sommes attachés dans la Partie 2 à répondre à la problématique de l'authentification et de sa mise en œuvre dans les réseaux véhiculaires et en particulier dans les réseaux véhiculaires opérés s'appuyant sur une technologie de type WLAN. Nous avons pour ce faire présenté et analysé dans le Chapitre 2.1, des architectures et des protocoles pour l'authentification dans les réseaux véhiculaires opérés. Ces architectures recoupent essentiellement une architecture réseau ad-hoc hybride autorisant des communications multi-sauts entre les véhicules et les points d'accès et une architecture de sécurité encore appelée infrastructure de confiance et de sécurité, régissant et implémentant les relations de confiance et de sécurité entre les principales entités que sont: l'autorité publique des transports, l'opérateur réseau et les véhicules. L'authentification dans ce contexte se fonde sur la différenciation entre les services dits ITS et les services de nature plus commerciale dits non-ITS. Cette authentification et les architectures associées implémentent divers mécanismes susceptibles d'assurer au-delà de l'authentification mutuelle et de l'autorisation, la sécurité des données d'authentification, l'intimité numérique des utilisateurs, l'interdiction d'accès aux protocoles et services de la couche 3 avant l'achèvement du processus d'authentification, le respect des contraintes temps réel et la disponibilité de l'authentification. La traduction concrète de ces implémentations est faite au travers d'une part, d'une extension de l'authentification TLS, appelée AUCRED, qui assure, sur la base des certificats à clé publique ECC, l'authentification mutuelle entre le serveur d'authentification et les véhicules, mais aussi la délivrance des certificats volatiles anonymes à ces derniers, et d'autre part, du protocole EGEMO qui assure, au niveau de la couche 2, l'acheminement géographique multi-sauts par la diffusion du protocole EAP, lui-même transporteur du protocole AUCRED.

Les propriétés spécifiques du protocole AUCRED (authentification mutuelle et délivrance des lettres de créance, négociation des suites cryptographiques et dérivation des clés, intégrité des messages, confidentialité de certains messages, protection contre le rejeu, protection contre les attaques par dictionnaire, réauthentification rapide, indépendance des sessions, protection contre des attaques de type DoS, etc.) et celles du protocole EGEMO (transport des paquets EAP, acheminement sans état, acheminement par diffusion, relayage opportuniste, acheminement multi-chemins, transport sécurisé, etc.) ayant été présentées et appréhendées, nous avons réalisé dans le Chapitre 2.2, par le biais du simulateur GrooveNet, une analyse comparative des performances entre notre solution d'authentification et l'approche classique d'authentification sur un saut par le protocole EAPoL. Cette analyse a permis de démontrer, de manière générale, la supériorité de

notre solution quant à son potentiel d'accroissement de la disponibilité, de la robustesse et de l'efficience de l'authentification. Plus en détails, notre solution s'est révélée particulièrement avantageuse pour certaines plages de densités de points d'accès et de véhicules dont quelques unes ont pu être traduites sous forme d'heuristiques mathématiques. En revanche des dégradations par rapport notamment à l'efficacité de l'utilisation de la ressource radio, bien que relatives, ont été relevées dans les scénarios de forte densité de véhicules.

A l'aune des résultats précédents, nous avons introduit dans le Chapitre 2.3 une approche d'optimisation du transport de l'authentification visant à réduire le nombre de paquets générés dans le réseau lors du processus d'authentification, en particulier dans les scénarios de forte densité de véhicules. Cette approche d'optimisation consiste à reproduire virtuellement les densités de véhicules ayant présenté les résultats les plus favorables et pour lesquelles des heuristiques ont été déduites lors de notre évaluation initiale. Ces densités correspondent généralement à des densités suffisamment fortes pour assurer la connectivité entre les véhicules et suffisamment faibles pour éviter une trop grande contention pour l'accès au canal ou de trop nombreuses interférences et collisions. La reproduction virtuelle de ces densités est mise en œuvre au travers des décisions de relayage du protocole de transport EGEMO. Ce relayage se veut probabiliste et différé pour certaines de ses occurrences. L'évaluation des performances de notre approche d'optimisation a révélé, en particulier pour les fortes densités de véhicules, une amélioration notable de l'efficacité de l'authentification quant à l'utilisation de la ressource radio et une réduction tout aussi notable de la bande passante consommée. Tous ces gains ont par ailleurs été obtenus sans altération de la disponibilité de l'authentification par rapport aux cas où l'optimisation n'est pas mise en œuvre.

Compte tenu du rôle particulier de l'authentification, considérée comme un service précédant et conditionnant l'accès aux ressources et aux autres services du réseau opéré, et en réponse à la mise en concurrence de ce service avec d'autres services des réseaux DSRC, nous avons proposé dans le Chapitre 2.4 une méthode de priorisation du service d'authentification mettant à contribution la diversité des canaux radio DSRC. Ainsi, au lieu d'associer le service d'authentification à un seul canal comme ce serait le cas dans le modèle DSRC actuel, notre approche étend ce dernier en introduisant la possibilité d'associer un service et en particulier le service d'authentification à plus d'un canal. En se basant ensuite sur une technique d'évaluation locale de l'état des canaux radio, notre approche permet de transmettre les paquets d'authentification dans des conditions préférentielles par rapport aux paquets d'autres services DSRC. Quand bien même cette évaluation locale de l'état des canaux serait loin d'équivaloir à une évaluation optimale de l'état des canaux à l'échelle de tout le réseau, elle reste néanmoins moins onéreuse et plus adaptée au contexte des réseaux véhiculaires marqué par une très forte dynamique des nœuds. Il est toutefois à noter que les avantages attendus de notre approche de priorisation ne peuvent véritablement prendre toute leur mesure que dans des configurations multi-interfaces où le nombre de canaux de service associés au service d'authentification est inférieur ou égal au nombre d'interfaces sur chaque nœud du réseau. Les analyses de performance réalisées dans ce contexte révèlent la

capacité de notre approche de priorisation à rendre l'authentification des véhicules à la fois plus efficiente et plus robuste en présence notamment de services tiers très consommateurs de bande passante.

Afin de maintenir des niveaux élevés de performance de l'authentification dans les scénarios de forte densité des véhicules, et ce, sans accroître la complexité matérielle des nœuds du réseau (*e.g.* une seule interface radio par nœud) et même en présence de services tiers concurrents du service d'authentification, nous avons proposé dans le Chapitre 2.5, une approche de distribution de la fonction d'authentification ou du rôle de serveur d'authentification. Cette approche vise à amplifier la disponibilité et l'efficience de l'authentification et par conséquent celles de l'accès aux ressources et aux services, en déclenchant la relocalisation de l'authentification suivant la densité des véhicules dans le réseau. Des approches concrètes de calcul de la densité seuil de déclenchement de la relocalisation de l'authentification sont proposées. Ce processus de relocalisation est décidé par le serveur d'authentification qui distribue ou délègue la fonction d'authentification aux véhicules déjà authentifiés. La collecte des données nécessaires à cette prise de décision est faite en coopération avec les points d'accès qui exploitent les informations de mobilité véhiculées par le protocole EGEMO. Ainsi, l'authentification des véhicules peut se faire au plus près de ces derniers, ce qui limite la propagation du trafic d'authentification dans le réseau sans fil et évite une trop grande dégradation des performances du processus d'authentification lorsque la densité des véhicules est très forte. Les analyses de performance que nous avons conduites dans ce contexte confirment l'intérêt de la distribution et notamment sa capacité à amplifier la robustesse et l'efficience du processus d'authentification mais aussi son efficacité par rapport à l'utilisation de la ressource radio lorsque la densité des véhicules dans le réseau augmente. Ces propriétés ont aussi été confirmées dans les scénarios DSRC où le service d'authentification est associé au même canal que d'autres services de même priorité. Bien entendu cette confirmation ne peut tenir que dans la mesure où le débit de ces services n'est pas de nature à bloquer la mise en œuvre de la distribution de l'authentification. Finalement, en amplifiant les performances de notre solution initiale, notre approche de distribution de l'authentification ouvre la voie à l'accès ubiquitaire aux ressources et aux services du réseau véhiculaire dans des configurations parmi les plus attendues, à savoir, des configurations de forte densité de véhicules, de déploiement restreint des points d'accès, de complexité matérielle minimale des nœuds du réseau et même d'opération de services concurrents du service d'authentification.

2. Bilan et perspectives

L'intérêt pour les réseaux véhiculaires est grandissant mais les travaux dans ce domaine et en particulier dans le champ de la sécurité restent encore relativement modestes. Les travaux réalisés dans cette thèse sont parmi les premiers ambitionnant de fonder une armature de sécurité globale pour ces réseaux. La problématique de l'authentification est en effet au cœur des architectures de sécurité dans la mesure où elle précède, conditionne et

détermine la mise en œuvre des autres objectifs de sécurité. Au-delà de l'appropriation d'une problématique encore marginalement traitée dans le contexte des réseaux véhiculaires, l'originalité de nos travaux tient: (i) des efforts réalisés pour intégrer - dans le schéma d'authentification - les caractéristiques et les contraintes spécifiques des réseaux véhiculaires, (ii) de l'intégration de ce schéma d'authentification dans une architecture opérateur et de la perspective qui est ainsi donnée à l'opérateur désireux d'adopter et de déployer ces réseaux et (iii) du positionnement avant-gardiste et pragmatique de ce schéma d'authentification qui s'inscrit d'emblée sur une technologie concrète dédiée aux communications véhiculaires (*i.e.* DSRC/IEEE 802.11p) et appelée à être largement ubiquitaire sur les routes et autoroutes de demain.

Bien que des avancées aient été réalisées au travers de cette thèse, des efforts importants doivent encore être consentis pour compléter et parfaire nos travaux. Des analyses supplémentaires de nos contributions peuvent par exemple être conduites pour étudier plus avant, le comportement de nos contributions suivant des topologies et des modèles de mobilité des véhicules plus complexes et des modèles de trafic - des services autres que l'authentification - plus contraignants. Des études de calibrage peuvent également être réalisées sur des paramètres comme le facteur de non-traçabilité introduit dans le Chapitre 2.1 ou encore la durée d'observation utilisée dans la distribution de l'authentification et introduite dans le Chapitre 2.5. On peut également envisager dans le cadre de la distribution de l'authentification que son déclenchement ne soit pas seulement fonction de la densité des véhicules mais aussi d'autres paramètres comme la probabilité de partitionnement du réseau ou la répartition courante des serveurs délégués (*i.e.* véhicules jouant le rôle de serveur d'authentification). Même si on peut légitimement s'attendre à ce que l'authentification AUCRED, présentée dans le Chapitre 2.1, hérite des mêmes propriétés que l'authentification TLS dont elle est une extension, il reste qu'une confirmation peut toujours être obtenue au travers d'une analyse formelle réalisée avec un outil d'analyse des protocoles de sécurité comme AVISPA [AVISPA]. Au-delà, nos contributions doivent être complétées par des travaux définissant des mécanismes de découverte des paramètres du réseau (*e.g.* identifiant et position des points d'accès, politique de sécurité, etc.) et des mécanismes de dérivation des associations de sécurité entre les véhicules et les points d'accès dans un contexte architectural ad-hoc hybride.

En sus des axes d'étude et de recherche précédents, on peut aussi compléter nos travaux en s'intéressant à d'autres problématiques dans le vaste champ de la sécurité des réseaux véhiculaires. Ainsi par exemple, des mécanismes de supervision coordonnés par l'infrastructure fixe et visant à détecter les intrusions et les comportements non coopératifs ou non conformes - au travers des systèmes de réputation, des schémas de vérification de données, pour ne citer que ceux là, - pourront être investigués et intégrés à nos contributions.

Références

[ADYA04] A. Adya, P. Bahl, J. Padhye, A. Wolman and L. Zhou, "A Multi-Radio Unification Protocol for IEEE 802.11Wireless Networks", IEEE BROADNETS, 2004

[ALT99] Althouse, Extending the Littoral Battlespace (ELB). Advanced Concept Technology Demonstration (ACTD), NATO Information Systems Technology Panel Symposium on Tactical Mobile Communications, June 1999

[ANAN01] Ananthapadmanabha R., B. S. Manoj and C. Siva Ram Murthy, "Multi-hop Cellular Networks: The Architecture and Routing Protocols", 12th IEEE International Symposium, 2001

[AODV] IETF, "Ad Hoc On Demand Distance Vector (AODV) Routing", RFC 3561, July 2003

[ARBA02] William A. Arbaugh, Narendar Shankar, Y. C. Justin and Kan Zhang, "Your 802.11 Wireless Network Has No Clothes", IEEE Wireless Communications, December 2002

[AUE05] Auerbach Publications, "Wireless Security Handbook", 2005

[AUTOCONF] Ad hoc Network AutoConfiguration (AutoConf), http://www.ietf.org/html.charters/autoconf-charter.html

[AVISPA] Automated Validation of Internet Security Protocols and Applications (AVISPA) project, http://avispa-project.org/

[BECK99] M. Becker, A.-L. Beylot, G. Damm and W.-Y. Thang, "Automatic run-time choice for simulation length in MIMESIS", RAIRO vol. 33 no1 pp. 93-115, 1999

[BICKET05] John Bicket, Daniel Aguayo, Sanjit Biswas and Robert Morris, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network", proceedings of ACM MobiCom, September 2005

[BLUM04] Jeremy Blum, Azim Eskandarian, "The Threat of Intelligent Collisions", IEEE Computer Society, 2004

[CALM] Communications, Air-interface, Long and Medium range (CALM) ISO project, http://www.isotc204wg16.org/

[CARB04] Bogdan Carbunar, Ioanis Ioannidis and Cristina NitaRotaru, "JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", proceedings of ACM WiSe, 2004

[CARTALK] CARTALK project, "Safe and Comfortable Driving based upon inter-vehicle communication", http://www.cartalk2000.net

[CHEI06] O. Cheikhrouhou, M. Laurent-Maknavicius and H. Chaouchi, "Security Architecture in a Multi-hop Mesh Network", 5th Conference on SAR, June 2006

[CISC02] Cisco White Paper, "Wireless LAN Security", http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/, 2002

[COMESAFE] Communications for eSafety (COMeSafety) project, http://www.comesafety.org

[COOPERS] CO-OPerative SystEms for Intelligent Road Safety (COOPERS), http://www.coopers-ip.eu/

[CSI02] Csilla Endrődi, Zoltán Hornák, "Efficiency Analysis and Comparison of Public Key Algorithms", CSCS2002, Szeged, July 4, 2002.

[CVIS] Cooperative Vehicle-Infrastructure Systems (CVIS) project, http://www.cvisproject.org

[C2C-CC] CAR 2 CAR Communication Consortium (C2C-CC), http://www.car-to-car.org/

[C2C-CC07] CAR 2 CAR Communication Consortium, "CAR 2 CAR Communication Consortium Manifesto", August 2007

[DRIVE] DRIVE project, http://www.ist-drive.org/

[DSRC] 5.9 GHz DSRC, http://grouper.ieee.org/groups/scc32/dsrc/index.html

[DTLS] IETF, "Datagram Transport Layer Security", RFC 4347, April 2006

[DUDA06] A. Dutta et al., "Problem Statement for Heterogeneous Handover", Internet-Draft<draft-ohba-pobopts-heterogeneous-requirement-01.txt>, MOBOPTS Research Group, 2006

[EAP] IETF, "Extensible Authentication Protocol (EAP)", RFC 3748, 2004

[EAP-KER] IETF, "The Kerberos Network Authentication Service (Version 5)", RFC 1510, September 1993

[EAP-PSK] IETF, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method", RFC 4764, 2007

[EAP-SRP] IETF, "The SRP Authentication and Key Exchange System", RFC 2945, 2000

[EAP-TLS] IETF, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008

[ECC87] N. Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag, 1987

Communication Simulation Systems Based on Properties of Urban Areas", International Journal of Computer Science and Network Security (IJCSNS), VOL.6 No.10, 2006

[FESTAG04] A. Festag, H. Fußler, H. Hartenstein, A. Sarma, and R. Schmitz, "FleetNet: Bringing Car-to-Car Communication into the Real World", ITS World Congress, 2004.

[FLEETNET] FleetNet project, "Internet on the road", http://www.et2.tu-harburg.de/fleetnet

[FREE01] James A. Freebersyser, Barry Leiner, "A DoD perspective on mobile ad hoc networks", Ad Hoc Networking, Addison Wesley, pp. 29-51, 2001

[FUB02] H. Fußler, M. Mauve, H. Hartenstein, M. K¨asemann, and D. Vollmer, "Location-Based Routing for Vehicular Ad-Hoc Networks", ACM MobiCom, 2002

[FUNK08] Paul Funk and Simon Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 0", IETF Internet Draft, 2008

[GEONET] GeoNet project, "Geographic addressing and routing for vehicular communications", http://www.geonet-project.eu/

[GERL07] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker and C. Harsch, "Security Architecture for Vehicular Communication", International Workshop on Intelligent Transportation (WIT), 2007

[GOL04] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs", ACM International Workshop on Vehicular Ad Hoc Networks (VANET), 2004

[GUP00] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks", IEEE Transactions On Information Theory, Vol. 46, N°2, March 2000

[GROOVENET] GrooveNet: Vehicular Network Virtualization Platform, http://www.seas.upenn.edu/~rahulm/Research/GrooveNet/

[GST] GST project, http://www.gstforum.org/

[HAR08] C. Harsch, A. Festag and P. Papadimitratos, "Secure Position-Based Routing for VANETs", IEEE VTC-Fall, 2008

[HE04] Changhua He and John C. Mitchell, "Analysis of the 802.11i 4-Way Handshake", ACM WiSe, 2004

[HUB04] Jean-Pierre Hubeaux, Srdjan, Capkun and Jun Luo, "The Security and Privacy of Smart Vehicles", IEEE Computer Society, 2004

[IAW03] Information Assurance Workshop, "Wireless security threat taxonomy", IEEE Systems Man and Cybernetics Society, June 2003

[IEEE-P1609.2] IEEE P1609.2, "Standard for Wireless Access in Vehicular Environments: Security Services for Applications and Management Messages", 2006

[IEEE-802.1X] IEEE Std 802.1X, "IEEE 802.1x-2001 IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control", 1999

[IEEE-802.11] IEEE Std 802.11, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2007

[IEEE-802.11i] IEEE Std 802.11i, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements", 2004 (Now integrated in [IEEE-802.11])

[IEEE-802.11p] Status of Project IEEE 802.11p, IEEE Task Group TGp, http://grouper.ieee.org/groups/802/11/Reports/tgp_update.htm

[IEEE-802.11s] Status of Project IEEE 802.11s, IEEE Task Group TGs, http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm

[IEEE-802.11u] Status of Project IEEE 802.11u, IEEE Task Group TGu, http://grouper.ieee.org/groups/802/11/Reports/tgu_update.htm

[IEEE-802.16] IEEE Std 802.16, "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", 2004

[IEEE-802.3] IEEE Std 802.3, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part

3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", 2005

[IPSEC] IETF, "Security Architecture for the Internet Protocol", RFC 4301, December 2005

[ITS] ITS (Intelligent Transport Systems) ETSI project, http://www.etsi.org/WebSite/Technologies/IntelligentTransportSystems.aspx

[JANS04] Nicholas Jansma and Brandon Arrendondo, "Performance Comparison of Elliptic Curve and RSA Digital Signatures", University of Michigan, April 2004

[JAIN03] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu. Impact of Interference on Multi-hop Wireless Network Performance. In MobiCom, San Diego, CA, Sept. 2003

[JAYA07] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Framework", IETF Internet Draft, Work in progress, 2007

[KAR03] R. Karrer, A. Sabharwal, E. Knightly, "Enabling Large-scale Wireless Broadband: The Case for TAPs", proceedings of HotNets, 2003

[KOSCH05] T. Kosch, "Ad-hoc Connected Vehicles", MiNeMa Summer School, Klagenfurt, July 2005

[KUMAR02] K. Jayanth Kumar, B.S. Manoj and C. Siva Ram Murthy, "MuPAC: Multi-Power Architecture for Cellular Networks", proceedings of IEEE PIMRC, 2002

[LEIN96] B. Leiner, R. Ruth, A.R. Sastry, "Goals and challenges of the DARPA GloMo program",
IEEE Personal Communications 3 (6), pp 34-43, 1996

[LENS01] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes", Journal of Cryptology, 2001

[LI04] Tonghong Li, Chan Kwang Mien, Joshua Liew Seng Arn and Winston Seah, "Mobile Internet Access in BAS", proceedings of the 24th IEEE ICDCSW, 2004

[LUO03] Haiyun Luo, Ramachandran Ramjeey, Prasun Sinhaz, Li (Erran) Liya and Songwu Lu, "UCAN: A Unified Cellular and AdHoc Network Architecture", proceedings of ACM MobiCom, 2003

[MAHFO08] Mansoor Mahfoud, Nizar Al-Holou and Rami Baroody, "Next Generation Vehicle Network: Web Enabled", ICTTA, 2008

[MANET] IETF, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance
Issues and Evaluation Considerations", RFC 2501, January 1999

[MAN06] Rahul Mangharam, Daniel Weller, Raj Rajkumar, Priyantha Mudalige and Fan Bai, "GrooveNet: A Hybrid Simulator for Vehicle-to-Vehicle Networks", V2VCOM, 2006

[MISH02] Arunesh Mishra and William A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard", Technical report UMIACS-TR-2002-10, University of Maryland, 2002

[MOBIVIP] MobiVip project, http://www-sop.inria.fr/visa/mobivip/

[MOBOPTS] IP Mobility Optimizations (MobOpts), http://www.irtf.org/charter?gtype=rg&group=mobopts

[MOU05] H. Moustafa, G. Bourdon and Y. Gourhant, "AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture", proceedings of ACM VANET workshop in conjunction with MobiCom, September 2005

[MOU06] H. Moustafa, G. Bourdon and Y. Gourhant, "Providing authentication and access control in vehicular network environment", IFIP/SEC, May 2006

[NTRU] NTRU Communications and Content Security, http://www.ntru.com

[NOW] Network-on-Wheels (NOW) project, www.network-on-wheels.de

[OISHI06] Junya OISHI, Koichi ASAKURA and Toyohide WATANABE, "A Communication Model for Inter-vehicle 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

[OLSR] IETF, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003

[PALE04] Ashwin Palekar, Dan Simon, Glen Zorn, Joe Salowey, Hao Zhou and S. Josefsson. "Protected EAP Protocol (PEAP) Version 2" IETF Internet Draft, 2004

[PKIX] IETF, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008

[POTT00] G.J. Pottie and W.J. Kaiser, 'Wireless Integrated network sensors'. Communications of the ACM 43(5) : pp 51-58, 2000

[RAYA05] M. Raya and J. Hubaux, "The Security of Vehicular Ad Hoc Networks", ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), 2005

[RAYA07] Maxim Raya and Jean-Pierre Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security (JCS) - special issue on Security on Ad Hoc and Sensor Networks, January 2007

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 1978

[SAFESPOT] SAFESPOT project, "Cooperative vehicles and road infrastructure for road safety", http://www.safespot-eu.org

[SEVECOM] SEcure VEhicular COMmunication (SEVECOM) project, http://www.sevecom.org/

[SHAE05] Yasser Shaer, Ayman Kayssi, Ali Chehab, "SERAX: SEcure RAnge eXtensions in IEEE 802.11i", proceedings of IIT, 2005

[TLS] IETF, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006

[TLS-EXT] IETF, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006

[VINAY07] Vinayak S. Kumbar, Sneha Bharadwaj, Nagalaxmi B.V and Abhijeet Prem Jetly, "Cellular Based Remote Vehicle Data Access", IET Automotive Electronics, June 2007

[VII] Vehicle Infrastructure Integration (VII) project, http://www.vehicle-infrastructure.org

[WEST84] J. Westcott and G. Lauer, "Hierarchical routing for very large networks", Proc. IEEE MIL-COM '84, pp. 214-218, 21-24 October 1984

[WU01] Hongyi Wu, Chunming Qiao, Swades De and Ozan Tonguz, "Integrated Cellular and Ad Hoc Relaying Systems: iCAR", IEEE Journal on Selected Areas in Communications, 2001

[YAN04]X. Yang, J. Liu, F. Zhao and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning" International Conference on Mobile and Ubiquitous Systems (MobiQuitous), 2004

[YUN05] Yunpeng Zang, Lothar Stibor Georgios Orfanos, Shumin Guo and Hans-Juergen Reumerman, "An Error Model for Inter-Vehicle Communications in Highway Scenarios at 5.9GHz", ACM PE-WASUN, 2005

[ZADEH02] Ali N. Zadeh, Bijan Jabbari, Raymond Pickholtz and Branimir Vojcic, "Self-Organizing Packet Radio Ad Hoc Networks with Overlay (SOPRANO)", IEEE Communications Magazine, 2002

[ZAR02] Magda El Zarki, Sharad Mehrotra, Gene Tsudik and Nalini Venkatasubramanian, "Security Issues in a Future Vehicular Network", EuropeanWireless, 2002

[ZHAN02] Junbiao Zhang, Jun Li, Stephen Weinstein and Nan Tu, "Virtual Operator based AAA in Wireless LAN Hot Spots with Ad-hoc Networking Support", ACM Mobile Computing and Communications Review, 2002

[ZOIC05] Roxana Zoican and Dan Galatchi, "Mobility in Hybrid Networks Architectures", proceedings of IEEE TELSIKS, 2005

Valorisation

1. Publications

[TCH06-C1] Christian Tchepnda, Hassnaa Moustafa and Houda Labiod, "Hybrid Wireless Networks: Applications, Architectures and New Perspectives", proceedings of IEEE IWWAN, New York, NY, USA, 2006

[TCH06-C2] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "Securing Vehicular Communications: An Architectural Solution Providing a Trust Infrastructure, Authentication, Access Control and Secure Data Transfer", proceedings of IEEE AutoNet/Globecom 2006, San Francisco, CA, USA, 2006

[TCH07-C1] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "Vehicular Communications Security Challenges", proceedings of JDIR, Marne-la-vallée, France, 2007

[TCH08-C1] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "A panorama on Vehicular Networks Security", proceedings of International Workshop on Interoperable Vehicles (IOV) – Internet Of Things (IOT), 2008

[TCH08-C2] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "A Layer-2 Multi-hop Authentication and Credential Delivery Scheme for Vehicular Networks", proceedings of IEEE Globecom 2008, New Orleans, USA, 2008

[TCH08-C3] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "Performance Analysis of a Layer-2 Multi-hop Authentication and Credential Delivery Scheme for Vehicular Networks", proceedings of IEEE VTC 2008 Spring, Marina Bay, Singapore, 2008

[TCH08-C4] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "Prioritizing and Enhancing Vehicular Networks Authentication Process Using DSRC Channels Diversity", proceedings of IEEE WiMob 2008, Avignon, France, 2008

[TCH08-J1] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "On Analyzing the Potential of a Layer-2 Multi-hop Authentication and Credential Delivery Scheme for Vehicular Communications ", Special Issue (SI) of Wireless Personal Communications (WIRE) – Springer Journal, 2008

[TCH08-J2] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, "Vehicular Networks Security: Attacks, Requirements, Challenges and Current Contributions", IGI Global - IJACI (International Journal of Ambient Computing and Intelligence), 2008

[TCH08-B1] Christian Tchepnda, Hassnaa Moustafa, Houda Labiod and Gilles Bourdon, Chapter "Security in Vehicular Networks", Book title "Vehicular Networks: Techniques, Standards and Applications ", Auerbach Publications – CRC Press (Taylor & Francis Group), 2008

2. Brevets

INPI # 07 55945 "Procédé de communication entre un nœud source et un nœud destinataire" - Christian Tchepnda & Hassnaa Moustafa

INPI # 08 52617 "Gestion de service dans un réseau multi-canaux et multi-sauts" - Christian Tchepnda & Hassnaa Moustafa

INPI # 08 56508 "Distribution d'une fonction d'authentification dans un réseau mobile" - Christian Tchepnda & Hassnaa Moustafa