Protection de la vie privée, innocuité et immunité envers les cybermenaces dans les futurs réseaux de véhicules autonomes connectés

Gérard Le Lann

Protection de la vie privée, innocuité et immunité envers les cybermenaces dans les futurs réseaux de véhicules autonomes connectés

Gérard Le Lann

INRIA, Paris Rocquencourt, France
gerard.le_lann@inria.fr

Résumé. Ni les communications radio envisagées pour les véhicules autonomes connectés actuellement définies par des standards, ni le balisage périodique ne procurent de propriétés d'innocuité (quasi-élimination des accidents graves) meilleures que celles assurées par la robotique embarquée. Les protocoles supplémentaires fondés sur la pseudonymie à clés publiques sont imparfaits. Les atteintes à la vie privée, l'espionnage et les cyberattaques de véhicules sont possibles. Les analyses qui mettent en évidence les faiblesses de ces approches (ensemble baptisé WAVE 1.0) sont détaillées, suivies d'une présentation de solutions qui assurent à la fois l'innocuité maximale et l'immunité envers les cybermenaces (ensemble baptisé WAVE 2.0). On met en évidence le choix de société induit par le choix entre WAVE 1.0 et WAVE 2.0.[1]

1 Introduction

Comme ce fut le cas lors de précédentes innovations technologiques, les choix de solutions pour les réseaux de véhicules autonomes connectés (VAC) induisent ou reposent sur des choix de société, lesquels peuvent être difficilement discernables par les premiers concernés, à savoir tous les humains amenés à circuler dans ces véhicules, en tant que conducteurs (tant que cette fonction existera) ou passagers. S'agissant de technologies innovantes et de résultats de recherche appliquée ou théorique (on en verra quelques exemples), une identification correcte des enjeux posés par l'émergence des réseaux auto-organisés de VAC sur routes, autoroutes et en milieux urbains requiert des connaissances spécifiques. Le but principal de cette publication est d'en fournir un condensé, afin de permettre au lecteur de se forger sa propre vision des enjeux en question. Se pourrait-il que derrière des bienfaits abondamment documentés et médiatisés se cachent des risques involontairement ou volontairement passés sous silence ? L'innocuité (quasi-élimination des accidents graves) fut l'un des premiers objectifs visés avec les véhicules autonomes (fin des années 70). L'emploi de technologies radio, prises en considération vers la fin des années 80, conduisit à

[1] Publication C&ESAR 2017 avec quelques mises à jour.

définir un objectif supplémentaire, à savoir la sécurité des données d'ordre personnel et l'immunité envers les cybermenaces. Au chapitre 2, on présente brièvement les deux ensembles de solutions existant à ce jour, en concluant avec le choix de société auquel nous sommes confrontés. Les principales déficiences des solutions en passe d'être déployées ou standardisées sont analysées au chapitre 3. Le chapitre 4 est consacré à une présentation simplifiée de solutions émergentes qui garantissent l'innocuité. La protection de la vie privée est traitée au chapitre 5. Au chapitre 6, on montre que ces solutions garantissent également l'immunité envers les cybermenaces.

2 Véhicules autonomes connectés et enjeux de société

Les véhicules autonomes actuellement en circulation sont dotés d'un système bord et de capteurs diversifiés (radars, lidars, caméras, etc.) assurant des fonctions de navigation fondées sur la robotique embarquée et la géolocalisation GNSS (GPS, Glonass, Galileo, etc.). Une réduction significative—division par 10—des accidents graves (blessures sérieuses, invalidités permanentes, pertes de vies humaines) est l'un des buts principaux à l'origine des travaux visés par la conduite autonome ou automatisée. Ce but Φ d'innocuité *(safety)* ne semblant pouvoir être atteint dans les réseaux véhiculaires [1] en se limitant à de tels systèmes bord, la communauté ITS (Intelligent Transportation Systems) a entrepris des travaux ayant pour but de doter les véhicules d'émetteurs/récepteurs radio. Outre les échanges de messages V2V (*vehicle-to-vehicle*) entre véhicules, ces équipements permettent les échanges de messages V2I (*vehicle-to-infrastructure*) et I2V entre véhicules et nœuds terrestres (*road-side units* (RSU), nœuds de réseaux de télécommunications wifi/LTE/4G et 5G bientôt) afin d'offrir l'accès à des fournisseurs de services publics et privés. C'est dans ce but que fut défini le standard WAVE (*Wireless Access in Vehicular Environments*), qui comprend en particulier le standard IEEE 802.11p [2], variante particulière du wifi (son équivalent européen est le standard ETSI ITS-G5), et le standard IEEE 1609.4 [3]. À partir de 2020, décision à l'instigation du NHTSA (*National Highway Traffic Safety Administration*), tous les véhicules mis en circulation aux USA devront être dotés d'un système bord équipé de moyens de communications conformes au standard WAVE. Si rien n'entrave leur déploiement, cette obligation s'imposera en Europe et ailleurs. Cette perspective est inquiétante, à plus d'un titre.

Les solutions WAVE ne procurent pas d'amélioration significative en matière d'innocuité par rapport à celle obtenue avec la robotique embarquée—cf. §3.1. En conséquence, le balisage (*beaconing*) périodique fut ajouté aux solutions WAVE : tout véhicule doit émettre en mode diffusion (*broadcast*) entre 1 et 10 fois par seconde un message V2V (Cooperative Awareness Message (CAM) en terminologie ETSI (EN 302 637-2)), donnant sa géolocalisation (coordonnées spatiales GNSS), l'heure UTC d'émission, sa vitesse, etc. [4-5]. Cela est supposé permettre à tout véhicule d'entretenir une carte de situation environnementale, notée LDM (*Local Dynamic Map*), donnant les positions présumées exactes de ses voisins, à tout instant, dans une zone centrée sur lui-même. L'entretien de LDM est supposé permettre d'assurer l'innocuité, supposition erronée—cf. §3.2. Le champ « source » d'un message V2V

ne doit pas permettre de révéler l'identité du véhicule émetteur, ni de le pister, car cela serait contradictoire avec un autre but conditionnant l'avènement des VAC, à savoir la sécurité des données d'ordre personnel et l'immunité envers les cybermenaces (but Π). Parmi diverses possibilités, celles basées sur la pseudonymie (*pseudonymity*) sont les plus étudiées par la communauté ITS. On distingue quatre approches, en cours d'investigation [6]. Aucune d'entre elles n'est exempte de défauts. Elles sont toutes basées sur l'existence d'autorités de certification (AC) qui délivrent un certificat d'authentification unique pour chaque véhicule au moment de son enregistrement/immatriculation. Selon les standards actuellement en cours de définition (IEEE 1609.2-2013 [7] et ETSI 102941-v1.1.1 [8]), un message est considéré valide s'il est émis par un véhicule authentifié. Les identités des émetteurs sont « obscurcies » en recourant à des couples {pseudonyme, certificat} fournis par des infrastructures à clés publiques (*Public Key Infrastructures*), que nous noterons FPC pour fournisseurs de pseudonymes certifiés. Malheureusement, appliquées au balisage périodique, ces solutions entrainent un gaspillage de ressources (communications, puissance de calcul des systèmes bord) qui peut être énorme. De plus, elles sont imparfaites vis-à-vis de nombreuses cybermenaces. La faiblesse intrinsèque de la plupart des approches en cours d'investigation est qu'elles se cantonnent au cyberespace, en étant pratiquement complètement décorrélées des comportements accidentogènes dans l'espace physique. C'est l'un des grands défis auxquels est confrontée la communauté ITS : comment atteindre le but Π sans rendre inatteignable le but Φ (ou inversement) ? Nous verrons que ce défi peut être relevé avec d'autres solutions.

Nous noterons WAVE 1.0 l'ensemble comprenant les protocoles WAVE, le balisage périodique et les mécanismes de pseudonymie basés sur les FPC. Les solutions WAVE 1.0 sont fondées sur une conception très particulière des VAC, vus comme des ordiphones (*smartphones*) sur roues. Il est clair que les risques encourus avec les ordiphones, tablettes et équipements utilisant des communications sans fil, seront également encourus par les humains lors de leurs déplacements en VAC, ainsi que par les véhicules eux-mêmes, éventuellement inoccupés. La possibilité de prise de contrôle à distance a déjà été démontrée, y compris par des organismes étatiques—le FBI a pointé les risques potentiels (*lethal weapons*) encourus avec des VAC inoccupés.

Enfin, cette perspective est inquiétante du point de vue du modèle économique sous-jacent. Les déploiements de nœuds en densité suffisante pour garantir la connectivité sans faille entre VAC et réseaux terrestres nécessiteront des investissements importants. Lesquels seront rentabilisés via les coûts facturés pour utilisation (intensive) des RSU et des réseaux de télécommunications. Auxquels il faut ajouter les coûts des services FPC. Ces coûts sont-ils justifiés ?

A la question « que signifie *connecté* ? », la réponse habituelle est « connecté aux réseaux de télécommunications et à Internet ». D'où les nombreux articles sur « l'Internet des Véhicules ». Or, l'innocuité n'a jamais fait partie des objectifs visés ni par ces réseaux ni par Internet. Les ordiphones sur roues peuvent tuer. Les VAC et les futurs réseaux de VAC sont donc des instances de systèmes-de-systèmes critiques, et leur conception doit être conforme aux principes établis au cours des 40 dernières années dans ce domaine (transport aérien, métro, centrales nucléaires, sites à risque,

etc.). Dans aucun de ces systèmes les concepteurs ne font reposer l'évitement d'évènement redouté (accident dans notre cas) sur l'accès à un réseau externe partagé. Au contraire : tout ce qui est critique est distinct de ce qui est non-critique (séparation physique et/ou logicielle). Par exemple, bien qu'étant dotés de moyens de télécommunications avec le sol, les avions de ligne « se débrouillent tout seuls » pour éviter les collisions dans les couloirs aériens (détection de situation accidentogène via les équipements TACAS). L'approche WAVE 1.0 viole donc l'un des principes fondamentaux du domaine des systèmes critiques.

Les VAC sont des véhicules *communicants*. Pour assurer l'innocuité, ils échangent des *safety critical messages* (*sc-messages*) en étant *déconnectés* de tout réseau autre que celui/ceux qu'ils forment spontanément. Pour d'autres raisons, les VAC peuvent de plus être *télé-communicants* (ce qui est sous-entendu par « connecté ») et échanger des *télé-messages* à contenus non critiques comme informations de trafic, météo, loisirs, travail, infotainment, places de parking libres, etc. Outre les risques d'espionnage et d'intrusions, les réseaux de télécommunications sont sujets à défaillances. Ils ne peuvent donc en aucune manière garantir les propriétés désirées d'innocuité. Les technologies, les canaux radio et les protocoles utilisés pour les sc-messages sont donc nécessairement différents de ceux constitutifs de WAVE 1.0. Outre la radio, les communications optiques sont appelées à jouer un rôle significatif dans les réseaux auto-organisés de VAC. Les potentialités de l'optique ne sont pas exploitées dans le standard WAVE, qui commence à dater. On trouve dans la littérature scientifique des solutions qui permettent d'atteindre à la fois le but Φ et le but Π. Nous les noterons WAVE 2.0. Elles reposent sur la prise en compte explicite de la nature cyberphysique [9] des réseaux de VAC. Les choix de solutions ne sont pas innocents. Nous sommes dès à présent confrontés au choix de société suivant :

- ou bien rien n'entrave le déploiement des standards WAVE (vieillissants) ou de leurs futures versions 5G et des solutions associées (WAVE 1.0), et alors nous pourrons être surveillés et sujets aux cyberattaques lors de nos déplacements motorisés, sans avoir d'autre choix que de payer pour être surveillés et attaqués, et sans bénéficier de garantie d'innocuité meilleure que celle assurée par la robotique embarquée,

- ou bien, sous les actions combinées des mondes académique, juridique, sociologique et éthique, ainsi que du monde industriel [par exemple, systèmes temps réel embarqués, outils de validation/vérification, communications radio courte portée, technologies optiques passives, équipementiers qui ont opté pour ces technologies, circuits intégrés pour le chiffrement, horloges à dérive infinitésimale, ingénierie des protocoles, des algorithmes distribués, des systèmes à très haute disponibilité], une nouvelle génération de standards émergera (WAVE 2.0), et notre mobilité sur roues ne pourra faire l'objet de surveillance ou de cyberattaques. Ces solutions, à coûts d'utilisation nuls comparés à ceux de WAVE 1.0, garantiront également l'innocuité maximale, ce qui intéressera le monde des assurances, les autorités de santé publique, ainsi que les autorités chargées de la sécurité au sens large.

3 Déficiences des solutions WAVE 1.0

Pour atteindre le but Φ, les VAC impliqués dans une manœuvre à risque doivent au préalable se coordonner en des délais très courts. Comme exemples de telles manœuvres, on peut citer changement de voie, freinage brutal, libération de voie pour véhicule prioritaire, entrées sur autoroute de façon entrelacée (*zipper merging*), traversée de carrefour et de rond-point sans feux de signalisation. La coordination consiste à influencer les comportements de véhicules proches, avec leur accord explicite, à l'instar des écritures distantes (*remote writes*) en informatique qui permettent de modifier l'état d'une ressource partagée dans un système distribué. Par exemple, une insertion entre deux véhicules doit être précédée par l'envoi d'une demande, des réponses positives (négatives) retournées par les véhicules qui acceptent (qui n'acceptent pas) de créer un espace suffisant pour l'insertion, puis la confirmation par le véhicule demandeur. La robotique seule, par nature fondée sur l'observation passive (*reactive safety*), ne permet pas d'influencer les comportements de véhicules voisins *(proactive safety*), ce qui est indispensable pour atteindre Φ [10]. L'adjonction de moteurs d'intelligence artificielle (IA) et le recours à l'apprentissage automatisé (*machine/deep learning*) ne changent rien à ce constat. Les décisions sont meilleures que celles prises sans IA et sans apprentissage, mais si elles restent inexprimées, on n'assure que la *reactive safety* : les véhicules voisins de *X* doivent deviner, par observation du déplacement physique de *X*, les intentions de *X*. Les accords inter-véhiculaires explicites sont plus que nécessaires. Cela étant posé, une question essentielle est de savoir si une solution proposée pour les communications inter-VAC satisfait des contraintes strictes de temps de réponse permettant de démontrer l'innocuité.

3.1 Déficiences des solutions WAVE pour l'innocuité

Les caractéristiques de WAVE qu'il suffit de connaître ici sont les suivantes : antennes omnidirectionnelles de portées radio de 300 m environ, rayons d'interférence radio (IR) de l'ordre de 450 m, 7 canaux radio, dont 1 canal de contrôle (CCH) attribué aux sc-messages et aux balises, et 6 canaux de service SCH attribués aux télémessages, chacun de 6 Mbits/s avec le codage retenu actuellement. Le protocole MAC est probabiliste (CSMA-CA), donc pas de bornes supérieures sur les délais d'accès aux canaux radio. Les sc-messages sont des messages événementiels (Decentralized Environmental Notification Message (DENM) en terminologie ETSI (EN 302 637-3)). Les messages émis en diffusion (les balises, notamment) ne sont pas acquittés. Un émetteur ne peut donc savoir s'il doit répéter un message diffusé éventuellement perdu, d'où absence de bornes supérieures sur les délais de livraisons réussies des messages diffusés. WAVE en mode V2V ne peut assurer l'innocuité. Cela est démontré dans de nombreuses publications ([10-14] par exemple). Les bornes supérieures du délai d'accès au canal CCH doivent être de l'ordre de 20 ms en pires cas de contention (plus grand nombre possible de véhicules dans un disque de rayon IR). Dans [11], il est montré que pour diverses charges du canal CCH correspondant à une densité de 1 véhicule tous les 12 m, les délais obtenus avec WAVE, établis par calcul analytique et simulations (NS-2), sont compris dans l'intervalle [75,3 ms – 211,8 ms].

Noter que ces délais sont des moyennes (pas des bornes pires cas). Les délais d'accès sont infinis (« rien ne passe ») lorsque le canal CCH est saturé, ce qui peut survenir avec les diffusions de balises à fréquence élevée. Avec WAVE en mode V2I, les délais sont obligatoirement plus élevés qu'en mode V2V. Contrairement à ce qui est affirmé sans preuves, l'arrivée des communications 5G ne changera rien de fondamental au constat établi plus haut. Le relayage intermédiaire via des nœuds 5G introduira lui aussi des retards additionnels. Les délais *moyens* seront plus petits qu'avec WAVE version 802.11p. Cela n'est d'aucun intérêt pour l'innocuité. Seules comptent les *bornes supérieures pires cas* des délais. Les nombres pires cas de véhicules en compétition d'accès au canal radio sont les facteurs déterminants. La largeur de la bande passante a une influence minime, surtout avec des protocoles MAC non déterministes—le cas de la technologie cellulaire 5G. D'autres technologies radio et d'autres protocoles MAC sont nécessaires.

3.2 Inutilité du balisage périodique pour l'innocuité

L'un des écueils évidents auxquels est confronté le balisage périodique, notamment à 10 Hz, est la saturation du canal CCH. Ce sera le cas sur autoroutes multivoies aux heures de pointe et en milieu urbain. A titre d'exemple, considérons le rond-point de la Place de l'Etoile à Paris et un disque D de diamètre IR ≈ 450 m centré sur l'Arc de Triomphe, donc incluant le rond-point, les 12 rues/avenues radiales, l'avenue circulaire et les carrefours avoisinants. Tout véhicule présent dans D peut subir des interférences radio (qui le rendent « muet » et « sourd ») de la part de tout autre véhicule présent dans D mais aussi de tout véhicule non inclus dans D à moins de ≈ 450 m. Donc, ce sont tous les véhicules situés à moins de ≈ 670 m du centre du rond-point qu'il faut comptabiliser pour estimer le nombre pire cas de tentatives ratées d'accès au canal CCH. Ce qui n'a jamais été fait, car les conclusions sont connues d'avance.

La croyance selon laquelle le balisage périodique est nécessaire pour atteindre le but Φ est erronée. La question fondamentale est la suivante : que peut-on faire avec une LDM ? Une LDM est une structure de données sujette à des lectures (par un VAC) entrelacées avec des écritures (contenus des balises reçues par ce VAC, au fur et à mesure de leurs réceptions) exécutées des dizaines ou des centaines de fois par seconde, selon le nombre d'émetteurs de balises en portée radio. Se posent donc tous les problèmes étudiés au cours des 30 dernières années par la communauté Informatique Distribuée (*global states*, *snapshots*, *consistent data replication despite concurrency and failures*, etc.). Étonnamment, ces problèmes sont complètement ignorés dans la littérature dédiée au balisage périodique, qui se focalise uniquement sur des « réglages » et compromis possibles entre fréquences de diffusion, exactitude des localisations, débits souhaitables du canal CCH. Le but de ces « réglages » est d'éviter la saturation du canal CCH qui résulterait de trop nombreuses collisions. Une fois trouvé un « bon réglage » (par simulation), le problème est considéré résolu. À tort. L'erreur est de supposer que les collisions d'accès au canal radio sont les seules causes de pertes de balises, ce qui revient à *postuler* la diffusion fiable ou/et atomique, problème redoutable dans les réseaux/systèmes distribués. Ce postulat impli-

cite invalide sérieusement les résultats publiés, car un message transmis sans collision sur le canal CCH peut très bien ne pas être reçu/livré partout : certains véhicules peuvent ne pas recevoir des balises reçues par d'autres, bien qu'étant éventuellement très proches les uns des autres. On peut supposer que ces pertes en réception ne sont pas problématiques, grâce aux rafraichissements périodiques des LDM. Cette hypothèse est infondée. La non-réception d'une balise b_i émise par X n'est pas « compensée » par la réception de la balise suivante b_{i+1} émise par X. Le comportement de X perçu par 2 VAC quelconques P et Q est le modèle Byzantin [15] : les dernières positions de X écrites dans leurs LDM respectives sont différentes. Supposons que X se déplace à 90 km/h et un balisage à 1 Hz. L'écart entre la position de X enregistrée dans LDM(P) et celle enregistrée dans LDM(Q) peut donc être de l'ordre de 25 m. Les accidents sont inévitables avec de telles imprécisions.

Des algorithmes (*terminating atomic broadcast*, *consensus*, etc.) permettent de rendre cohérents (en l'occurrence, identiques) les états des diverses LDM sous certaines conditions qui, malheureusement, ne sont pas réunies dans les réseaux de VAC. On connaît depuis longtemps de nombreux résultats d'impossibilité. En modèle asynchrone (délais sans bornes supérieures connues—le cas avec WAVE), le consensus est impossible en présence de diffusion non atomique [16]. Dans ces réseaux, il est impossible de fixer un seuil pour le nombre de pertes de messages, donc de balises. En modèle synchrone (bornes supérieures des délais connues), ni l'unanimité ni la majorité absolue ne peuvent être obtenues lorsque le nombre de pertes excède des valeurs modestes [17-18]. Outre les mauvaises réceptions de balises, les délais d'accès au canal CCH étant nécessairement différents pour différents véhicules, l'union de vues locales « prises » à des instants différents (les géolocalisations GNSS contenues dans les balises) ne peut être une vue globale qui a existé, comparable à une prise de vue globale instantanée. Les écarts temporels dus au protocole MAC induisent des erreurs de localisations spatiales. On sait aussi que les coordonnées spatiales fournies par un équipement GNSS ne sont pas toujours exactes, et que les signaux satellites ne sont pas toujours reçus correctement. De plus, quels que soient les progrès à venir en matière de précision des localisations GNSS, il est assez facile de falsifier/rejouer (*spoofing*) les signaux satellitaires et de tromper les récepteurs de plusieurs dizaines de mètres [19]. Enfin, les comportements postérieurs à l'instant t ne peuvent être déduits avec certitude des positions ou trajectoires passées lues dans les LDM à l'instant t, quelles que soient les analyses prédictives considérées. D'une part, ces mouvements sont interdépendants, éventuellement dictés par des événements inattendus (information absente des LDM). D'autre part, même si l'on postule l'invraisemblable, à savoir des LDM parfaitement identiques, les accidents sont possibles si les systèmes bord utilisent des analyses prédictives différentes. Il est très peu probable qu'existe un jour un standard international imposant une méthode prédictive unique. Toutes ces raisons font qu'il est dangereux de croire que les LDM permettent de « faire mieux » que la robotique embarquée vis-à-vis de l'innocuité.

Cette conclusion n'est pas surprenante. Le balisage périodique est (lui aussi) de type observation passive. Il ne peut donc assurer la *proactive safety*. Au mieux, un balisage pseudopériodique peut servir à fournir des informations de trafic de nature

statistique—comme le font déjà certaines applications disponibles sur ordiphones. Mais à quels coûts ? Quel est l'intérêt pour un véhicule *X* de devoir traiter des (dizaines ?, centaines ?) d'arrivées de balises par seconde émises par des véhicules dont *X* ne croisera jamais la route ? Avec des balises pseudonymisées, le gaspillage de ressources est injustifiable, et les fréquences φ supérieures à 1 Hz infaisables dans la plupart des cas réalistes. Selon diverses sources, avec les technologies abordables, pour un algorithme de signature ECDSA-256, il en coûte ≈ 1 ms pour signer et ≈ 4 ms pour vérifier. Ignorons le temps pris pour l'inspection de CRL (cf. ci-dessous). Si *k* est le nombre de véhicules en portée radio omnidirectionnelle, et en estimant à environ 20% la proportion de temps pris par la gestion des interruptions et des processus, on a $\varphi = 2$ Hz $\rightarrow k < 100$, et $\varphi = 10$ Hz $\rightarrow k < 20$. Les valeurs moyennes réalistes de *k* sont bien plus grandes. Quant aux valeurs pires cas... Avec des circuits spécialisés (coûteux), il est possible de signer et de vérifier plus rapidement. C'est inutile. L'erreur à l'origine des difficultés brièvement passées en revue est de croire qu'il faut connaitre des positions absolues (GNSS), alors que les accidents peuvent être évités en connaissant seulement les distances relatives entre véhicules voisins.

3.3 Limitations des solutions fondées sur les FPC

On distingue les métadonnées (identifiants) des données (contenus des messages). Pour les balises, le chiffrement des données semble abandonné, car chiffrer et déchiffrer les positions GNSS induit des délais (en émission, en réception) qui peuvent être rédhibitoires. Au point que sont étudiées des variantes où même les métadonnées ne seraient pas pseudonymisées.

Principes des solutions en cours de standardisation

L'approche choisie est la pseudonymie à clés publiques (asymétriques), dont les principes (très simplifiés) sont les suivants. Tout véhicule doit être enregistré et authentifié avant d'être mis en circulation. Pour un véhicule *V* d'identité administrative ID, une AC délivre un certificat d'enregistrement (CE_{id}) et enregistre de façon chiffrée dans ses bases de données l'information ID ↔ CE_{id}. Le certificat CE_{id} est inscrit dans la boite noire infalsifiable de *V*. À l'instar des *Event Data Recorders*, une boite noire, notée TPD (*tamper-proof device*), équipe désormais tous les véhicules. *V* peut immédiatement entrer en contact avec *Z*, un fournisseur de pseudonymes certifiés (FPC). *V* fournit CE_{id} à *Z*, qui envoie à *V* un certain nombre de couples {pseudonyme ps, certificat de pseudonyme ce_{ps}} associés à CE_{id}. Enregistrés dans le TPD de *V*, ils permettront à *V* d'émettre ses premiers messages avant d'entrer à nouveau en contact avec un FPC pour obtenir de nouveaux pseudonymes certifiés. Dans la littérature, ce nombre oscille entre des dizaines de milliers et des centaines de milliers. L'information CE_{id} ↔ {ps, ce_{ps}} est également fournie par *Z* à une AC de niveau hiérarchique supérieur, notée HAC. Un pseudonyme certifié a une durée de validité limitée et, idéalement, doit être à usage limité (unique ou un « petit » nombre de fois). Tout message émis est signé avec la clé privée du pseudonyme ps utilisé, accompagné du certificat ce_{ps} correspondant. Un véhicule récepteur vérifie la signature à l'aide du certificat ce_{ps}. Si la signature est invalide, *m* est ignoré. Pour ce qui concerne les *révo-*

cations en cas de comportements « malhonnêtes » (*malicious*), deux approches principales sont examinées, fondées sur des *listes de révocation de certificats* CRL (*certificate revocation list*) distribuées aux FPC, selon que les CRL contiennent les pseudonymes certifiés révoqués ou les certificats CE_{id} révoqués. Une *éviction* de véhicule (son ID est invalidée) est prononcée par une autorité chargée du respect des lois. Un véhicule doit pouvoir être ré-identifié (révélation de son ID), d'où l'emploi de pseudonymes réversibles (contrairement à l'anonymisation des métadonnées, volontairement irréversible—cf. §4.3), notamment pour assurer l'imputabilité (*non-repudiation, auditability, liability*). Une ré-identification ne doit s'effectuer que par échange sécurisé et accord explicite entre AC et HAC qui, vraisemblablement, reposeront sur un consensus authentifié. Si les AC « se font confiance », même étant situées dans différents pays, elles pourront disposer des mêmes CRL. Avec WAVE 1.0, le même TPD sert pour les sc-messages, les balises, et les télé-messages, en contradiction avec le principe de ségrégation—cf. §4.1.

Limitations

Elles sont bien documentées—cf. [20-23] par exemple. Dans [20], il est montré que les changements fréquents de pseudonymes ne suffisent pas pour éviter le retraçage, lequel est possible avec un balisage à 1 Hz et des changements de pseudonymes toutes les 10 s. Voici une liste incomplète d'ambiguïtés et de problèmes ouverts :

- utilisations illicites par les AC et les FPC des informations concernant les VAC, et piratages dont ils peuvent faire l'objet [24],
- les changements de pseudonymes doivent s'effectuer en « zones mixtes » (zones de densité élevée de VAC), tous les VAC effectuant ces changements en même temps ; comment sont obtenus les accords sur « nous sommes assez nombreux » et « nous faisons les changements maintenant » ?
- susceptibilité aux interceptions (suppressions, falsifications) via les relais terrestres lors des demandes d'attribution de nouveaux pseudonymes,
- qu'est-ce qu'un comportement « malhonnête » ?
- comment (et par qui) est remontée vers une AC ou un FPC une détection de comportement malhonnête qui entraine une révocation/éviction ?
- combien de temps s'écoule entre le début de comportement malhonnête de la part d'un véhicule et une révocation/éviction ; que peut faire le véhicule incriminé entre temps ?
- lourdeur de la gestion des CRL,
- qu'est-ce qui interdit à un véhicule d'émettre des messages pseudonymisés qui contiennent des données trompeuses (attaque « injection de leurre ») ?
- à quoi servent les pseudonymes face aux attaques « suppression » (messages légitimes non émis ou non relayés) ?
- conséquences dans l'espace physique de falsifications concernant la vérification des pseudonymes (un véhicule malhonnête qui reçoit un message légitime correctement signé prétend qu'il s'agit d'un message incorrectement signé) ; et le contraire ?
- manque de pseudonymes dû à l'inaccessibilité ou/et aux défaillances des réseaux de télécommunications, attaques déni-de-service, ou à la non-émergence de « zones mixtes » (l'attribution de pseudonymes « en excédent » assortis de

grandes durées de validité pour éviter la « panne » de pseudonymes favorise les attaques Sybil).

Il est supposé que les échanges entre un TPD et les équipements d'entrées/sorties (ES) radio d'un système bord sont parfaits. Notamment, un TPD est capable de surveiller ces échanges et d'agir en conséquence. Dans [25], on lit (une AC a décidé de révoquer toutes les clés d'un véhicule) : « *after the message (from the CA) is received and decrypted by the TPD, the TPD erases all the keys* ». Ce point mérite attention, car il soulève la question des attaques par intrusion, qui peuvent transformer un véhicule honnête en attaquant irrationnel, par installation d'un logiciel malfaisant. Dans cette publication, nous n'examinons que l'attaque MitM (*malware-in-the-middle*), inspirée de l'attaque classique *man-in-the-middle*, où un logiciel espionne et falsifie les échanges (signatures par exemple) entre un TPD et les équipements ES. Les messages sont donc rejetés par les destinataires. Les conséquences sont sérieuses, notamment dans le cas des balises, car les pertes en réception ne sont donc pas uniquement dues aux parasitages radio (cf. §3.2). Nous reviendrons sur ces points au chapitre 6.

L'orientation initiale des travaux du domaine remonte au début/milieu des années 2000 [25]. Certaines faiblesses furent identifiées peu de temps après [26]. En fait, à quelques exceptions près, l'immunité envers les cybermenaces dans les réseaux de VAC est traitée comme elle l'est dans les réseaux informatiques, c'est-à-dire en cyberespace, sans tenir compte des problèmes d'innocuité posés par des émetteurs de messages pouvant se déplacer à des vitesses éventuellement très élevées. Le flou le plus complet règne sur la définition de « comportement malhonnête » ainsi que sur les moyens (qui seraient eux-mêmes insensibles aux cyberattaques) de détection de « malhonnêteté ». Quant à l'exclusion/arrêt physique de véhicules malhonnêtes, on ne trouve quasiment rien. Une révocation/éviction n'a aucune influence sur les comportements (accidentogènes) d'un véhicule. La question centrale est : pendant combien de temps un véhicule peut-il « nuire » (créer des accidents par exemple) avant que d'être physiquement arrêté ? S'il est impossible d'exprimer une borne supérieure très proche de 0, alors les solutions considérées sont inadéquates.

3.4 Conclusion

Le lecteur aura sans doute anticipé deux évidences. Premièrement, les collisions ne peuvent survenir qu'entre véhicules suffisamment proches les uns des autres. Donc, pour l'innocuité, les communications V2V de courte portée sont suffisantes (pas de V2I). Deuxièmement, si l'on rétablit la différenciation évidente entre communications pour l'innocuité et les autres communications (les *safety data* ne sont pas des *personal data*), alors, on peut atteindre Φ et Π. À condition de ne pas utiliser le balisage périodique et en recourant à la pseudonymie sans accès en-ligne aux FPC. Tout en reconnaissant l'existence de sérieuses difficultés, la communauté WAVE 1.0 tente de s'en dédouaner en affirmant que l'on ne peut avoir à la fois innocuité et immunité envers les cybermenaces. C'est certainement vrai avec WAVE 1.0, mais cette assertion est fausse si l'on considère d'autres solutions proposées par un nombre croissant de scientifiques et d'ingénieurs. Tout ensemble de « solutions » fondées sur WAVE est

irrémédiablement insatisfaisant, car WAVE ne peut être « bon pour tout ». De plus, WAVE commence à dater. Le recours à d'autres solutions fondées sur des technologies apparues plus récemment est pleinement justifié. Elles pourraient constituer le socle des futurs standards destinés aux réseaux de VAC, solutions et standards que, par commodité, nous noterons WAVE 2.0.

Les solutions WAVE 2.0 reposent sur un petit nombre de principes, notamment la ségrégation critique/non critique. L'un des enjeux est de démontrer qu'avec ces solutions, *l'innocuité ne peut pas être compromise par les cyberattaques*.

4 Brève introduction aux solutions WAVE 2.0

4.1 Ségrégation critique/non-critique et imputabilité

Un exemple d'architecture d'un système bord est donné figure 1. Les sous-systèmes SC (chargés des fonctions *safety-critical*) sont isolés du sous-système non-SC chargé des autres fonctions. Les sous-systèmes SCR pour la robotique et SCC pour les communications sont dotés de processeurs/mémoires distincts de ceux d'un sous-système non-SC, et de leur propre alimentation. Les logiciels des sous-systèmes SC sont de niveau d'intégrité SIL-3 ou ASIL-D au moins (standards IEC 61508, ISO 26262), exécutés sous le contrôle d'un système d'exploitation destiné aux systèmes embarqués et/ou temps réel. Un sous-système non-SC est doté d'un système d'exploitation « grand public ». Les sous-systèmes non-SC assurent la *sécurité des données personnelles* échangées dans les télé-messages, qui peuvent être chiffrées. La diffusion des télé-messages d'alerte (par exemple, « embouteillage à 1,2 km », « accident à 900 m sur voie de gauche ») est assurée par un sous-système non-SC. Un télé-message d'alerte est vu (à tort) comme un sc-message en WAVE 1.0, où l'on confond *prévention des accidents* (but Φ et les sc-messages) et *aveu d'un échec* (un accident a eu lieu) via un télé-message émis a posteriori. Les VAC étant équipés de radars longue portée et de caméras (d'où détection à temps d'un obstacle ou de véhicules « qui freinent » pour éviter un obstacle), on peut douter de l'utilité de tels télé-messages vis-à-vis de Φ. Ils doivent plutôt être vus comme des moyens de diffusion d'information utile pour assurer la fluidité du trafic et l'optimisation des trajets.

Les sous-systèmes SC et le sous-système non-SC sont équipés d'un TPD, doté de son propre processeur, de sa mémoire et de sa propre alimentation. Les sous-systèmes SC partagent le même TPD (noté sc-TPD), distinct du nsc-TPD (sous-système non-SC). Un sc-TPD est inaccessible depuis un sous-système non-SC, donc a fortiori inaccessible via des télé-messages, contrairement aux nsc-TPD utilisés par les solutions WAVE 1.0. Le sc-TPD de *V* d'identifiant ID contient le certificat CE_{id} et les pseudonymes certifiés générés par une AC et un FPC lors de l'enregistrement de *V*. Contrairement à WAVE 1.0, le nombre de pseudonymes nécessaires est faible, de l'ordre de quelques centaines à quelques milliers, et ils peuvent être réutilisés, théoriquement ad infinitum.

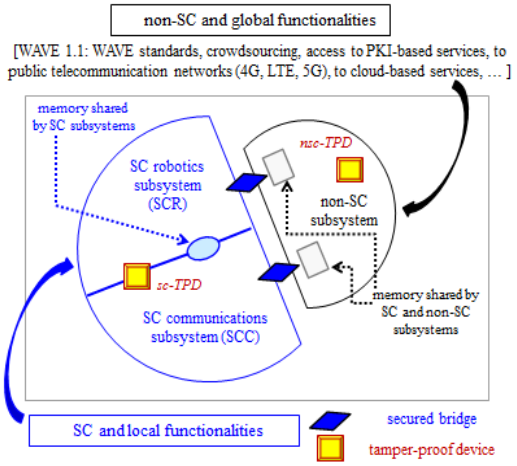

Figure 1. Exemple d'architecture d'un système bord

Une fois mis en circulation, les véhicules n'ont plus besoin d'accéder aux FPC. Un sc-TPD contient des prédicats, enregistre toute violation de prédicat et déclenche l'action appropriée. Pour les télé-messages d'alerte, on utilise les pseudonymes certifiés disponibles dans le nsc-TPD. Nous noterons WAVE 1.1 l'ensemble WAVE 1.0 sans le balisage périodique.

L'idée centrale pour assurer une protection contre les cybermenaces débarrassée des limitations listées au §3.3 est la suivante. S'il existe une *organisation spontanée de VAC* au sein de laquelle les véhicules peuvent se faire confiance, alors il est inutile d'imposer la pseudonymisation de chaque sc-message. Il suffit (1) d'authentifier tout véhicule qui souhaite devenir membre d'une telle organisation, (2) d'anonymiser les métadonnées des messages émis ensuite par ces membres, sans devoir accéder à des FPC, (3) d'exclure sans délai tout véhicule au comportement malhonnête. Une telle organisation existe. Elle a été conçue pour l'innocuité. Il se trouve qu'elle est appropriée pour l'immunité envers les cybermenaces. Il s'agit des cohortes (cf. figure 2).

4.2 Cohortes

Le lecteur intéressé pourra consulter [27-30]. Les cohortes (formations linéaires ad hoc de véhicules) sont une généralisation des concepts de *platoon* et de *string*. Dotées de spécifications, elles sont sans doute le premier exemple de construction cyberphysique destinée aux réseaux de VAC. Dans une cohorte de n membres, chaque véhicule calcule son rang, de 1 à n. Un véhicule isolé s'attribue le rang 1. L'insertion d'un véhicule Y derrière un membre de rang r entraine une mise à jour des rangs : Y prend le rang r+1, et les successeurs de Y incrémentent leurs rangs respectifs. L'opération inverse s'applique en cas de départ d'un membre. Les messages échangés entre véhicules voisins sont notés N2N (*neighbor-to-neighbor*), longitudinalement dans une cohorte et latéralement entre cohortes adjacentes. Les messages N2N peuvent être des

sc-messages (manœuvres) ou des messages de gestion interne d'une cohorte (par exemple, dissémination de la nouvelle valeur de *n*). Les données des messages N2N sont des codes connus de tous, comme « nouvelle vitesse = *v* km/h », « changement de voie » (demande, réponse, confirmation), « entrée sur autoroute », « entrée dans carrefour ». Un message N2N est estampillé de l'heure UTC de sa création.

Un réseau de VAC est un ensemble ouvert constitué de groupes connexes de cohortes alignées sur plusieurs voies, un groupe connexe étant un ensemble de cohortes adjacentes dont les membres peuvent communiquer entre eux de façon transitive. On pose $v.n < b$: la vitesse maximale *v* d'une cohorte est une fonction inverse du nombre de ses membres. Une valeur réaliste de *b* (*v* en km/h) pour autoroutes est de l'ordre de 1200 (par exemple, 60 membres à 20 km/h, 6 membres à 185 km/h). La disponibilité d'un lien N2N entre 2 membres voisins ainsi que la non-défaillance de chacun d'eux sont vérifiées par émissions périodiques de « *heartbeat* » "je suis vivant", lorsqu'il n'y a pas de sc-message à transmettre. Lorsqu'un lien N2N (entre *X* et *Y* qui suit *X*) est silencieux trop longtemps, une scission de cohorte (*cohort split*) est déclenchée : *Y* décélère, jusqu'à créer avec *X* un espace inter-cohorte $S_{min}(v)$ suffisant tel que le véhicule de tête d'une cohorte qui en suit une autre ne peut entrer en collision avec le véhicule de queue de cette dernière, même en cas de freinage brutal. Pour toute artère bidirectionnelle (large rue, avenue, route, autoroute), on distingue les deux axes de directions opposées. Pour un axe donné, les voies (*lanes*) sont numérotées à partir de 1 pour la voie la plus à droite (à gauche pour certains pays). Les axes et les numéros de voie, notés *j*, sont enregistrés dans les cartes numériques. Dans un VAC, la connaissance de *j* est assurée par le sous-système SCR, par exemple via des mesures hybrides [31] ou des algorithmes de type SLAM visuel [32], qui permettent de ne pas dépendre de la qualité ou de la permanence des réceptions GNSS.

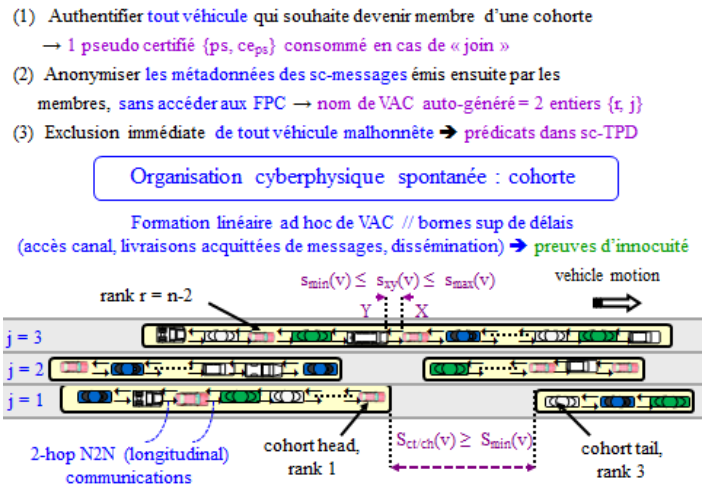

Figure 2. Cohortes, utilisation des pseudonymes certifiés, anonymisation

4.3 Anonymat

Un nom de VAC est donc un couple d'entiers {*r, j*}, où *r* est un rang et *j* un numéro de voie. Dans un groupe connexe de cohortes, on a la propriété d'unicité : à tout moment, un nom {*r, j*} ne peut correspondre qu'à un seul véhicule. De facto, ces noms sont des pseudonymes auto-générés (*pseudonym self-issuance*) non réversibles assurant l'anonymisation souhaitée—cf. fin de §4.1. Très compacts, de temps de traitement quasi-nuls, ils constituent un deuxième « écran » de masquage d'identité, en sus du pseudonyme certifié exigé pour admission dans une cohorte—cf. LgJoin, §6.1. Les solutions de pseudonymie proposées par les auteurs de [26] reposent sur les concepts de « *convoy, convoy members and vehicle sequence numbers* ». Il se trouve que cohorte, membres d'une cohorte, et rangs dans les cohortes, formalisent ces concepts.

4.4 Communications inter-véhiculaires et innocuité

Un sous-système SCC utilise des antennes à contrôle de puissance de faibles portées (au plus 30 m environ), omnidirectionnelles ou directionnelles (préférablement, pour une meilleure réutilisation spatiale [33-36]). Un petit nombre *c* de canaux radio sont alloués aux communications longitudinales, canal $i = (j\text{-}1) \bmod c$ utilisé par les véhicules sur voie *j*. Les autres canaux sont « coupés ». Il est donc impossible de « mentir » sur *i*. Un seul canal est alloué aux communications latérales. Un mode *busy tone* (signal d'occupation) est disponible pour les cas particuliers (arrêt/exclusion par exemple, cf. §6.2). Les communications optiques (VLC ou passives) sont assurées par des LED et des caméras [37-38]. Elles permettent en outre de préserver l'innocuité en cas de brouillage radio (*jamming*), la seule attaque distante possible. Les protocoles MAC de type TDMA sont de bons candidats pour les réseaux de VAC [39], notamment les protocoles TDMA *sans collision*. C'est le cas de SWIFT, le protocole MAC longitudinal présenté dans [29]. Leur intérêt réside dans la connaissance des instants auxquels un membre peut émettre, instants et rangs étant corrélés. Ainsi, un véhicule malhonnête ne peut « mentir » sur son nom ou/et sur l'instant auquel il émet, sous peine d'être démasqué. Un cycle SWIFT contient un nombre connu de trames, et démarre à une heure UTC connue, notée *T* (début d'une nouvelle heure UTC, d'une nouvelle minute UTC). Un membre de rang *r* transmet dans la trame de numéro *k* aux instants de début de tranche canal notés $dt_r(k)$ (phase descendante, rangs servis par valeurs croissantes) et $ut_r(k)$ (phase montante, rangs servis par valeurs décroissantes) :

$$dt_r(k) = T + [(r\text{-}1) \bmod h + 2h(k\text{-}1)]\,\theta, \quad r \neq n \text{ (queue de cohorte)} \qquad \textit{Eq. 1}$$

$$ut_r(k) = T + [2hk - 1 - (r\text{-}1) \bmod h]\,\theta, \; r \neq 1 \text{ (tête de cohorte)} \qquad \textit{Eq. 2}$$

L'entier *h* est le nombre pire cas de membres consécutifs compris dans IR (rayon d'interférence radio) et θ la durée d'une tranche canal. La borne pire cas du temps d'accès canal est $2h\theta$. Exemples de valeurs réalistes : $h = 6$, $\theta = 1$ ms. Les coordinations inter-véhiculaires permettant d'éviter les collisions reposent sur les dissémination longitudinales et latérales de sc-messages. On montre dans [29-30] que les véhicules parcourent moins de 7 m en pires cas pendant que sont échangés les sc-messages servant à sceller les accords inter-véhiculaires dans les scénarios SC. La

primitive LgSend(*r*,*j*,*d*) permet à un membre *R* de rang *r* sur voie *j* de transmettre un message N2N de contenu *d* à 2 voisins immédiats, rangs *r*+1 et *r*+2 ou *r*-1 et *r*-2. La règle de filtrage suivante s'applique : en phase descendante, *R* ne traite en réception que les messages émis par ses 2 voisins (de rangs *r*-2 et *r*-1) dans les 2 tranches précédant la sienne ; tout autre message est ignoré ; idem en phase ascendante, en remplaçant les rangs *r*-2 et *r*-1 par *r*+2 et *r*+1. Règle de relayage : un message reçu à l'identique depuis 2 voisins contigus doit être relayé, et uniquement à cette condition. Règle de légitimité : pour qu'un contenu *d* de message N2N soit légitimé au sein d'une cohorte, *d* doit apparaitre dans au moins 2 messages créés par 2 membres non contigus. Les communications latérales entre cohortes adjacentes sont effectuées via la primitive LtSend(*r*,*j*,*d*), qui permet à un membre de rang *r* dans une cohorte sur voie *j* de transmettre *d* à des voisins latéraux sur voie *j*+1 ou *j*-1 (*j* > 0). Avec ces primitives, on instancie un multicast acquitté à délais bornés à travers un groupe connexe de cohortes (à comparer à la diffusion non acquittée à délais non bornés de WAVE).

5 Protection de la vie privée (cybermenaces distantes)

Les cybermenaces distantes ne sont à craindre qu'avec les télécommunications (données d'ordre personnel, professionnel, éducationnel, informationnel, etc.), gérées par les sous-systèmes non-SC. Le balisage n'étant pas utilisé, les cadences d'utilisation (non périodique) des pseudonymes certifiés sont uniquement déterminées par les cadences d'émission des télé-messages et, exceptionnellement, par l'émission de télé-messages d'alerte. De nombreux problèmes listés au chapitre 3 disparaissent. Un VAC peut être pisté lorsque les fonctionnalités WAVE 1.1 activées requièrent la géolocalisation GNSS. Récepteur GNSS coupé, le pistage est néanmoins possible par triangulation (nœuds RSU/réseaux de télécommunications). Cependant, dans les deux cas, l'identité du VAC pisté n'est pas révélée, sauf si le retraçage est possible. Il peut donc être prudent de couper WAVE 1.1 de temps en temps (cela peut être automatisé), notamment lors des départs de domicile et des retours. Rien n'oblige un utilisateur de VAC à activer les fonctionnalités WAVE 1.1. Les risques encourus (par exemple le piratage de données personnelles) seront donc pris en connaissance de cause. Le point positif est que les ordiphones-sur-roues de génération WAVE 2.0 ne seront pas dangereux (l'innocuité est « prise en charge » par les sous-systèmes SC). Bien sûr, si un ordiphone est utilisé à bord, alors le risque de traçabilité existe même si les fonctionnalités WAVE 1.1 ne sont pas activées.

Le problème des coalitions (attaques coordonnées) est ouvert. Les parades habituelles reposent sur l'hypothèse fondée qu'il existe une majorité de véhicules honnêtes. Parmi les difficultés auxquelles sont confrontées les solutions WAVE 1.1, on trouve (1) la définition de « groupe majoritaire » dans un réseau de VAC, (2) en opérationnel, comment identifier de tels groupes, (3) comment 2 VAC savent-ils qu'ils sont membres du même groupe. Avec les cohortes, ce « flou » est éliminé. Très précisément, nous posons comme hypothèse (*maj2/3*) qu'il n'existe pas plus de 1 membre malhonnête dans tout ensemble de 3 voisins (membres de rangs consécutifs).

6 Immunité envers les cybermenaces rapprochées

Par manque de place, il est impossible de détailler ici tous les scénarios. Nous présentons uniquement les mécanismes les plus essentiels. On distingue les cybermenaces passives (espionnage) des cybermenaces actives (attaques). Les données des sc-messages ne sont pas chiffrées. Avec des communications inter-VAC de courte portée et la règle de filtrage (cf. §4.4), un véhicule malhonnête est obligatoirement proche du véhicule attaqué. Il en découle qu'il s'expose lui-même à des risques physiques. On verra que les cybermenaces rapprochées sont déjouées, et sans intérêt. Donc, sauf attaque de type MitM subie par un véhicule honnête, seuls des attaquants irrationnels sont à craindre (états second, tentatives de suicide, etc.).

6.1 Authentification et admission dans une cohorte

Les pseudonymes certifiés {ps/ce_{ps}} disponibles dans un sc-TPD sont utilisés au moment des insertions dans les cohortes. Une insertion longitudinale s'effectue par activation d'une primitive LgJoin, décrite ici de façon simplifiée. Soit *R*, nom {1, *j*}, un véhicule (isolé ou tête de cohorte) qui se rapproche d'une cohorte Γ sur la voie *j* (*R* est plus rapide que Γ ou Γ décélère). Soit *Q* le véhicule de queue de Γ, et soit *P* son prédécesseur, de rangs $q > 1$ et $p = q\text{-}1$, respectivement. Supposons *P*, *Q* et *R* honnêtes et absence de défaillances. La première phase d'un LgJoin est une invitation. À peu près en même temps, les capteurs de *R* détectent *Q* et ceux de *Q* détectent *R*. À peu près en même temps, ou séquentiellement, *R* active LgSend(*demande d'insertion*) vers *Q* et *Q* active LgSend(*invitation*) vers *R*. Quand *P* reçoit la demande d'insertion de *R*, *P* active LgSend(*invitation*) vers *R*. *R* signe sa demande d'insertion avec la clé privée du pseudonyme choisi ps, accompagnée du ce_{ps} correspondant. Les réponses de *Q* et *P* sont positives (par hypothèse, *R* est honnête). On ignore ici les conditions d'admissibilité relatives à d'autres paramètres. *R* s'attribue alors le nom {q+1, *j*} et devient le nouveau véhicule de queue de Γ. Une fois qu'il a acquis le statut « membre de cohorte », un véhicule n'a plus l'obligation de pseudonymiser les métadonnées des messages N2N qu'il envoie à ses voisins. Il en est de même pour les messages N2N échangés latéralement.

Le mutisme de *Q* (pas de message d'invitation) se traduit par son exclusion/arrêt (violation du prédicat Ψ_1). Sous l'hypothèse *maj2/3*, une réponse peut être négative dans deux cas : *R* est malhonnête (signature de la demande d'insertion invalide), et *P* ou *Q* est malhonnête. *R* n'a aucun intérêt à être malhonnête. S'il l'est, c'est qu'il est victime d'une attaque MitM. *P* ou *Q* peut « mentir » en prétendant que la demande de *R* (honnête) est incorrectement signée. Intérêt : ne pas prendre le risque d'être ralenti (cf. §4.2, la contrainte $v.n < b$). Sur réception de réponse négative, *R* a le choix (stratégie « no/join ») : rester sur la voie *j*, à distance $S_{min}(v)$ de *Q*, ou bien dépasser Γ, ce qui peut l'obliger à s'insérer dans une cohorte adjacente, donc procéder à une opération LtJoin. L'insertion latérale est légèrement différente de LgJoin (quels VAC vont-ils jouer les rôles de *P* et de *Q* ?). La désignation de ces derniers repose sur des communications optiques directes qui assurent l'équivalent de WYSIWYG ou de Seeing-

is-Believing [40] sans intervention humaine. Les autres comportements malhonnêtes de *P* ou *Q* sont examinés au §6.4. La sanction en cas de mensonge est l'exclusion/arrêt. Si *P* est exclu, la réponse (positive) attendue par *R* est envoyée par le prédécesseur de *P*, qui est honnête (hypothèse *maj2/3*). Idem si *Q* est exclu. L'analyse est la même si *Q* est un véhicule isolé. Dans ce cas, *Q* est tenu de fournir à *R* un pseudonyme certifié (exigé par *R* si *Q* donne son rang correct). Dans tous les cas, l'innocuité est préservée : en cas de doute, *R* applique la stratégie no/join.

6.2 Imputabilité et exclusion/arrêt

L'exclusion/arrêt d'un véhicule sur détection de comportement malhonnête doit être possible *sans faire intervenir une entité distante*, tout en assurant l'imputabilité. AC et HAC sont informées a posteriori. Comme pour WAVE 1.1, les TPD jouent un rôle essentiel. Avec WAVE 2.0, les sc-TPD contiennent des prédicats. Par exemple :

- Ψ_1: nouveau voisin détecté par les capteurs et message d'invitation envoyé,
- Ψ_2: le nom $\{r,j\}$ dans un message N2N émis est le nom correct,
- Ψ_3: 2 transmissions consécutives dans la même direction sont séparées de $2h\theta$ au moins,
- Ψ_4 : la règle de relayage est respectée.

Voir §6.4 pour le prédicat Ψ_2. Le prédicat Ψ_3 découle des instants donnés par *Eq. 1* et *Eq. 2*. Voir §6.5 pour le prédicat Ψ_4. Comme observé au §3.3, la surveillance des échanges avec les ES bord et les modifications d'état relatives à Φ et Π sont assurées par un TPD. Un booléen *H* (halte) est présent dans un sc-TPD, partagé par les deux sous-systèmes SC, mis à « faux » initialement (enregistrement/authentification). Lorsqu'un prédicat est violé, le véhicule fautif (*X*) est exclu du réseau et arrêté. Pour ce faire, le sous-système SCC active la signalisation périodique *busy tone* (signal radio servant à alerter les voisins de *X*), fait *H* := vrai, et poste deux interruptions, l'une pour le sous-système SCR et l'autre pour le sous-système non-SC. La robotique embarquée prend le contrôle de *X* : ses feux de détresse sont activés, sa vitesse est réduite, jusqu'à atteindre une place de parking ou une voie d'arrêt d'urgence (position GNSS de *X* immobilisé fournie dans les derniers télé-messages). En parallèle, sur demande du sous-système SCC, un télé-message « halte » (forçage d'arrêt) est émis périodiquement par le sous-système non-SC. Ce télé-message est signé avec un pseudonyme certifié à usage unique disponible dans le nsc-TPD (une exclusion/arrêt est unique, avant remise en circulation). Les destinataires sont les organismes publics et privés chargés de gérer infractions et dépannages. Selon les législations à venir, il sera également possible ou obligatoire de diffuser avec le télé-message « halte » le contenu (chiffré) du sc-TPD qui contient l'historique des événements (mouvements, transitions d'état, violation(s) de prédicat(s)) ayant entrainé l'exclusion/arrêt. L'innocuité n'étant pas compromise en cas de violation de prédicat, on peut déclencher une exclusion/arrêt seulement lorsque le nombre de violations dépasse un seuil jugé acceptable.

6.3 Discrétion

Espionnage et pistage rapprochés sont trivialement faisables avec des caméras embarquées (lecture des plaques minéralogiques, prises de photos) et des lecteurs optiques. À part détecter un véhicule proche qui éveillerait des soupçons d'espionnage, et lui échapper en changeant de trajectoire autant que nécessaire (ce qui peut être automatisé), il n'existe guère de solutions pour contrer ce genre d'attaque silencieuse, irrationnelle sauf motifs particuliers. Le cyber-espionnage rapproché ne crée aucun risque supplémentaire. En effet, tout membre de nom $\{r, j\}$ « sait » qu'il a pour voisins des véhicules dont les noms sont $\{x, j\}$, $x \neq r$, $1 \leq x \leq n$. Idem pour les voisins latéraux lors d'échanges de messages N2N. Il n'existe aucune relation entre un nom $\{x, j\}$ et les identifiants du VAC qui utilise ce nom. Les messages N2N ne contiennent pas de coordonnées GNSS. A tout moment, un véhicule peut changer de voie, quitter ou s'insérer dans une cohorte, en s'assignant chaque fois des noms différents. Anonymat et intraçabilité sont assurés. Le cyber-espionnage rapproché n'a aucun intérêt.

6.4 Attaques sur les métadonnées

Admission dans une cohorte—Attaques sur pseudonymes certifiés

Si *R* est victime d'une attaque MitM, son message de demande (LgJoin) incorrectement signé sera rejeté par *P* et *Q*, et *R* appliquera la stratégie no/join. L'issue sera la même si *P* ou *Q* est malhonnête. L'innocuité est préservée. On voit donc la différence entre WAVE 2.0 (une admission légitime dans une cohorte est injustement déniée, sans perte d'innocuité) et WAVE 1.1 (rejets de sc-messages ou de balises en cas de signatures incorrectes ou correctes mais falsifiées, ce qui peut compromettre gravement l'innocuité).

Membre de cohorte—Attaques sur noms {*r, j*}

Il s'agit des *usurpations de nom* (*masquerading, impersonation*) et des attaques *Sybil* [41]. Irrationnelles ou pas, elles sont facilement déjouées. Considérons *R*, nom $\{r, j\}$, et les attaques déclenchées par ses deux voisins R'' et R', de noms respectifs $\{r'', j\}$ et $\{r', j\}$, où $r'' = r\text{-}2$ et $r' = r\text{-}1$ (l'analyse est la même pour les deux autres voisins de rangs r+2 et r+1). Si t est l'instant $dt_r(k)$ (voir *Eq. 1*) auquel *R* peut émettre un message en phase descendante, alors un message « signé » r'' est nécessairement émis à $t'' = t\text{-}2\theta$, émis à $t' = t\text{-}\theta$ s'il est « signé » r' (analyse identique avec $t = ut_r(k)$, voir *Eq. 2*). Toute attaque *usurpation de nom* (R'' tente de se faire passer pour R' ou inversement) est vouée à l'échec. Si R'' et R' émettent dans la même tranche canal, leurs attaques s'annihilent naturellement (collision canal). Sinon, l'occurrence de l'événement $[r'', t']$ ou de $[r', t'']$ est révélatrice d'une telle attaque, détectée sur violation du prédicat Ψ_2. De plus, sauf à émettre dans 2 tranches consécutives, le message N2N injecté ou relayé par R'' ou R' ne sera pas reçu 2 fois par *R*. Il sera donc ignoré (cf. règle de relayage, §4.4). Voir §6.5 pour l'attaque *suppression de message légitime*. Une attaque *Sybil* est possible en l'absence de collision (R'' ou R' réussit à émettre dans 2 tranches consécutives). Cette attaque est détectée (violation du prédicat Ψ_3), mais elle peut rendre possible une *injection de message illégitime*—cf. §6.5,

attaque pernicieuse : l'attaquant, nécessairement irrationnel puisqu'il sera exclu/arrêté, ne prend aucun risque physique. Les rôles *R″*, *R′* et *R* sont conservés à l'identique ci-dessous.

6.5 Attaques sur les données

Rappelons que la confidentialité (*secrecy*) n'est pas requise, au contraire. Les données *d* contenues dans les messages N2N sont cruciales pour l'innocuité. L'écoute fortuite (*overhearing*) n'a que des avantages, en particulier dans les cas de manœuvres à risque simultanées et conflictuelles (par exemple, changements de voies en sens opposés). La dissémination (volontaire) de ces données *d* est parfois exigée. Leur chiffrement serait désastreux.

Suppression ou falsification de message légitime

R′ malhonnête ne relaie pas (vers *R*) le message *m* qu'il a reçu de *R″* et du prédécesseur de *R″*. *R* qui reçoit *m* uniquement de la part de *R″* ne relaie donc pas *m* (règle de relayage). Ou bien *R′* malhonnête relaie *m* falsifié. *R* qui reçoit 2 messages différents de la part de *R″* et de *R′* ne relaie pas. Dans les deux cas, *R′* est exclu (violation du prédicat Ψ_4). *R* et *R″* ont le choix : soit exécuter une scission de leur cohorte Γ, *R″* devenant queue de Γ et *R′* tête d'une nouvelle cohorte Γ', soit *R* prend le rang *r′* = *r*-1 dans Γ. Dans les deux cas, *m* a été relayé complètement dans Γ (et non vu dans Γ' si Γ' est créée).

Injection de message illégitime (leurre)

Un sous-système SCC crée un message N2N légitime sur occurrence d'un événement dû à une condition particulière, événement posté soit par le sous-système SCR (par exemple, les capteurs détectent du verglas, d'où demande de décélération), soit par le sous-système non-SC (postage d'un télé-message). Dans une cohorte, l'occurrence d'un tel événement est nécessairement observée par plus de 1 membre. Un message illégitime créé ex nihilo par un membre malhonnête pour être disséminé dans une cohorte ne peut être légitimé, même en cas d'attaque *Sybil* : *R* est « trompé » par *R′*, et relaie un message illégitime qui semble avoir été relayé par *R″* (créé par *R′* en fait) au préalable. La règle de légitimité (cf. §4.4) permet de déjouer cette attaque. Un contenu *d* est considéré légitime s'il apparait dans au moins 2 messages créés par des membres de rangs non consécutifs. Il existe d'autres moyens de valider le contenu d'un message N2N disséminé dans une cohorte. Par exemple, avec la règle *maj2/3*, *d* est considéré légitime si *d* apparait dans au moins 2 messages créés par des membres de rangs consécutifs. Lorsque *d* stipule une action physique irréversible, il est conseillé de recourir à un accord distribué, permettant ainsi à chacun des *n* membres de « voter » (oui ou non). Si le oui l'emporte, l'action physique impliquée par le contenu d'un message créé à l'heure UTC *u* peut être exécutée à l'heure $t = u+\Delta(n,f)$, où $\Delta(n,f)$ est le délai pire cas de dissémination d'un message dans une cohorte de *n* membres en présence de *f* pertes/répétitions [30].

A toute cyberattaque correspond une violation de prédicat. Systématiquement ou au choix, une violation de prédicat entraîne un arrêt/exclusion, suivi si nécessaire d'une scission de cohorte. C'est ainsi que l'innocuité est garantie en présence de cyberattaques. Des protocoles MAC de type TDMA autres que SWIFT peuvent assurer les propriétés d'immunité désirées.

7 Conclusions

Les buts Φ et Π peuvent être atteints avec les solutions WAVE 2.0, fondées sur des communications radio courte portée et optiques, sur une construction cyberphysique (cohorte) émergeant spontanément dans les réseaux de VAC et sur l'emploi combiné de mécanismes de pseudonymisation et d'anonymisation. D'ores et déjà, de nombreux travaux viennent en support de l'approche WAVE 2.0 ([31-40] par exemple). La plupart des technologies nécessaires pour le déploiement des solutions WAVE 2.0 existent déjà, maitrisées par des acteurs industriels aux noms connus. Avec les ordiphones et autres appareils utilisant les communications sans fils, les avantages (services) justifient sans doute la prise de cyber-risques. Il n'en est pas de même avec les VAC. Les risques pris (invalidités irréversibles et pertes de vies humaines) sont trop graves. De plus, le modèle économique sous-jacent (investissements de la part des « fournisseurs », coûts d'utilisation pour les « clients ») est difficilement défendable. Il est possible de déployer des ordiphones-sur-roues inoffensifs, à coûts d'utilisation extrêmement bas. Les solutions WAVE 1.0 ne sont pas encore déployées. Il est donc temps de suivre les avis des scientifiques et des juristes qui ont « vu » quelques-unes des nombreuses déficiences mises en évidence dans cette publication, et de « geler » les déploiements prématurés de solutions inappropriées.

References

[1] Karagiannis G et al. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Comm. Surveys & Tutorials, vol. 13 (4), 4th quarter 2011, 584-616.

[2] IEEE Standard 802.11p. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 6: wireless access in vehicular environments. July 2010, http://www.ietf.org/mail-archive/web/its/current/pdfqf992dHy9x.pdf.

[3] IEEE 1609.4-2016 - Standard for wireless access in vehicular environments: Multi-channel operation https://standards.ieee.org/findstds/standard/1609.4-2016.html.

[4] Sommer C et al. Adaptive beaconing for delay-sensitive and congestion-aware traffic information systems. 2nd IEEE Vehicular Networking Conference (VNC), Dec. 2010, 1-8.

[5] Schoch E, Kargl F. On the efficiency of secure beaconing in Vanets. 3rd ACM Conference on Wireless Network Security (WiSec '10), March 2010, 111-116.

[6] Petit J, et al. Pseudonym schemes in vehicular networks: a survey. IEEE Comm. Surveys and Tutorials, vol. 17 (1) 1st quarter 2015, 228-255.

[7] IEEE 1609.2-2013 - Standard for wireless access in vehicular environments: Security Services for Applications and Management Messages.
http://ieeexplore.ieee.org/document/7426684.

[8] ETSI TS 102 941-v1.1.1 (2012-06) - Intelligent Transport Systems; Security; Trust and Privacy Management.

http://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf

[9] Rajkumar R et al. Cyber-physical systems: the next computing revolution. 47th Design Automation Conference, 2010, 731-736.

[10] Le Lann G. Safe automated driving on highways—beyond today's connected autonomous vehicles. 8th CSDM Conference on "Towards smarter and more autonomous systems", Springer pub., Dec. 2017, Paris, 13 p. https://hal.archives-ouvertes.fr/hal-01610957

[11] Yao Y et al. Delay analysis and study of IEEE 802.11p based DSRC safety communication in a highway environment. IEEE Infocom 2013, 1591-1599.

[12] Kyasanur P and N. Vaidya N. Selfish MAC layer misbehavior in wireless networks. IEEE Int'l Conference on Dependable Systems and Networks (DSN'03), 2003, 173-182.

[13] Karlsson K, Bergenhem C, and Hedin E. Field measurements of IEEE 802.11p communication in NLOS environments for a platooning application. IEEE VTC Fall-2012, 1-5.

[14] Tang J, Y. Cheng Y, and Zhuang W. Real-time misbehavior detection in IEEE 802.11-based wireless networks: An analytical approach. IEEE Trans. Mobile Computing, vol. 13(1), Jan. 2014, 146-158.

[15] Lamport L, Shostak R, and Pease M. The Byzantine Generals problem. ACM Transactions on Programming Languages and Systems, July 1982, 382-401.

[16] Fischer M.J, Lynch N.A, and Paterson M.S. Impossibility of distributed consensus with one faulty process. Journal of the ACM, vol. 32, n°2, April 1985, 374-382.

[17] Santoro N and Widmayer P. Agreement in synchronous networks with ubiquitous faults. Theoretical Computer Science 384, Elsevier Science Direct, 2007, 232-249.

[18] Schmid U, Weiss B, and Keidar I. Impossibility results and lower bounds for consensus under link failures. SIAM Journal of Computing, vol. 38, 5, Jan. 2009, 1912-1951.

[19] Zeng Kexiong (Curtis) et al. A practical GPS location spoofing attack in road navigation scenario. ACM HotMobile '17, Feb. 2017, 6 p.

[20] Wiedersheim B et al. Privacy in inter-vehicular networks: why simple pseudonym change is not enough. 7th IEEE/IFIP Intl. Conference on Wireless On-demand Network Systems and Services, (WONS), 2010, 176-183.

[21] Eckhoff D and Sommer C. Driving for big data? Privacy concerns in vehicular networking. IEEE Security & Privacy, vol. 12, n° 1, Jan.-Feb. 2014, 77-79.
http://www.ccs-labs.org/bib/eckhoff2014driving/eckhoff2014driving.pdf

[22] Petit J et al. Connected vehicles: Surveillance threat and mitigation. Black Hat Europe, 2015, 12 p. https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp2.pdf

[23] Collingwood L. Privacy implications and liability issues of autonomous vehicles. Journal Information & Communications Technology Law, vol. 26 (1), 2017, 32-45
http://dx.doi.org/10.1080/13600834.2017.1269871

[24] Matsumoto S and Reischuk R.M. IKP: turning a PKI around with decentralized automated incentives. 38th IEEE Symposium on Security and Privacy, May 2017, 410-426.

[25] Raya M and Hubaux J.P. The security of vehicular ad hoc networks. 3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN '05), 2005, 11-21.

[26] Studer A, Luk M, and Perrig A. Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs. 3rd Intl. Conference on Security and Privacy in Communications Networks (SecureComm), Sept. 2007, 422-432.

[27] Le Lann G. Cohorts and groups for safe and efficient autonomous driving on highways. 3rd IEEE Vehicular Networking Conference (VNC), Nov. 2011, 1-8.
https://hal.inria.fr/hal-00667366

[28] Le Lann G. Safety in vehicular networks—On the inevitability of short-range directional communications. 14th Intl. Conference on Ad Hoc, Mobile, and Wireless Networks (AdHoc-Now 2015), 2015, Springer LNCS 9143, 347-360. https://hal.inria.fr/hal-01172595/document

[29] Le Lann G. A collision-free MAC protocol for fast message dissemination in vehicular strings. IEEE Conference on Standards for Communications and Networking (CSCN'16), Oct.-Nov. 2016, 7 p., https://hal.inria.fr/hal-01402119

[30] Le Lann G. Fast distributed agreements and safety-critical scenarios in VANETs. IEEE Intl. Conference on Computing, Networking and Communications (ICNC 2017), Jan. 2017, 7p., https://hal.inria.fr/hal-01402159

[31] Toledo-Moreo R, Bétaille D, and Peyret F. Lane-level integrity provision for navigation and map matching with GNSS, dead reckoning, and enhanced maps. IEEE Trans. Intelligent Transport. Systems, vol. 11, 1, March 2010, 100-112.

[32] Lategahn H, Geiger A, and Kitt B. Visual SLAM for autonomous ground vehicles. IEEE Intl. Conference on Robotics and Automation (ICRA), May 2011, 1732-1737.

[33] Takai M, Zhou J, and Bagrodia R. Adaptive range control using directional antennas in mobile ad hoc networks. ACM MSWiM Conference, 2003, 92-99.

[34] Torrent-Morino M et al. Distributed fair transit power adjustment for vehicular ad hoc network sensors. IEEE SECON Conference, Sept. 2006, 479-488.

[35] Little T.D.C. et al. Directional communication system for short-range vehicular communications. 2nd IEEE VNC Conference, Nov. 2010, 231-238.

[36] Ramanathan R et al. Ad hoc networking with directional antennas: a complete system solution. IEEE Journal Selected Areas in Communications, vol. 23(3), March 2005, 496-506.

[37] IEEE Spectrum. LEDs bring new light to car-to-car communication. Aug. 2014. http://spectrum.ieee.org/transportation/advanced-cars/leds-bring-new-light-to-car-to-car-communication

[38] Pathak P. H. Visible light communication, networking, and sensing: a survey, potential and challenges. IEEE Communications Surveys & Tutorials, vol. 17 (4), 4th quarter 2015, 2047-2077, http://www.phpathak.com/files/vlc-comsoccst.pdf

[39] Hadded M et al. TDMA-based MAC protocols for vehicular ad hoc networks: a survey, qualitative analysis, and open research issues. IEEE Com. Surveys & Tutorials, vol. 17(4), 2015, 2461-2492.

[40] McCune J.M and Perrig A. Seeing-is-believing: using camera phones for human-verifiable authentication. Intl. Journal Security and Networks, vol. 4 (1/2), 2009, 43-56.

[41] Douceur J.R. The Sybil attack. 1st Intl. Workshop on Peer-to-Peer Systems (IPTPS '02), 2002, 251-260.