Anonymat, non-traçabilité et sécurité-innocuité dans les réseaux de véhicules autonomes connectés

Gerard Le Lann

▶ **To cite this version:**

Gerard Le Lann. Anonymat, non-traçabilité et sécurité-innocuité dans les réseaux de véhicules autonomes connectés. 8ème Atelier sur la Protection de la Vie Privée (APVP'17), Equipe Privatics du laboratoire CITI d'Inria / INSA-Lyon, Jun 2017, Autrans, France. hal-01556192v1

HAL Id: hal-01556192

https://hal.science/hal-01556192v1

Submitted on 4 Jul 2017 (v1), last revised 21 Jul 2017 (v2)

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.

Anonymat, non-traçabilité et sécurité-innocuité dans les réseaux de véhicules autonomes connectés

Gérard Le Lann, RITS, INRIA Paris-Rocquencourt

8ème Atelier sur la Protection de la Vie Privée (APVP'17) – Autrans, juin 2017
Version finale

Résumé

Les véhicules autonomes seront également « connectés », par adjonction aux systèmes bord de moyens de communication radio définis dans les standards IEEE 802.11p et ETSI ITS-G5, notés WAVE 1.0 dans ce document. Les communications inter-véhiculaires ont pour but de contribuer significativement à la réduction du taux d'accidents (propriété d'innocuité meilleure qu'avec la seule robotique embarquée). Une analyse rigoureuse des solutions sur lesquelles sont fondés ces standards permet d'établir que WAVE 1.0 ne procure pas d'amélioration significative en matière d'innocuité (en sus de la robotique embarquée) et que WAVE 1.0 rend possible des atteintes à la vie privée qui n'existent pas avec les véhicules à conduite humaine. Les risques passés en revue sont *la perte d'anonymat, l'usurpation d'identité, la traçabilité (espionnage des trajets suivis par les véhicules), les intrusions distantes des systèmes bord*. On développe un argumentaire en faveur de l'avènement d'un nouveau standard de communications radio et optiques inter-véhiculaires—noté WAVE 2.0, fondé sur des solutions existantes qui assurent à la fois l'innocuité maximale et la discrétion absolue (l'élimination des risques examinés).

1. Sécurité-innocuité, protection de la vie privée et véhicules autonomes connectés

Voici environ 30 ans, la communauté ITS (Intelligent Transportation Systems) a engagé des travaux sur les véhicules à conduite partiellement/totalement automatisée. Une première motivation liée au concept de « platoon » était (et est toujours) une réduction significative des distances entre véhicules, notamment à vitesses élevées (but Ω_1). Environ 90% des accidents résultant de fautes humaines, une autre motivation était (et est toujours) une augmentation de la « safety », c'est-à-dire une réduction significative du taux d'accidents—une réduction d'un facteur 10 est souvent citée pour quantifier l'innocuité maximale recherchée (but Ω_2). En français, la propriété de « safety » est traduite par « sécurité-innocuité », notée ici « innocuité » pour simplifier. Ces deux buts, a priori contradictoires, constituent le but Ω.

Les véhicules autonomes actuellement en circulation sont dotés d'un système bord assurant des fonctions de navigation fondées sur la robotique embarquée et la géolocalisation GNSS (GPS, Glonass, Galileo, etc.). Voici une douzaine d'années, constatant que le but Ω ne pouvait être atteint en se limitant à de tels systèmes bord, des travaux ont été engagés pour « augmenter » ces derniers avec des émetteurs/récepteurs radio. C'est dans ce but que fut défini le standard WAVE (Wireless Access in Vehicular Environments [1]), qui comprend en particulier le standard IEEE 802.11p, variante particulière du wifi (son équivalent européen est le standard ETSI ITS-G5). A partir de 2020, décision fédérale 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 à ce standard, que nous noterons WAVE 1.0. Cette obligation concerne tous les constructeurs automobiles opérant sur le marché nord-américain, donc l'industrie US et l'industrie automobile européenne et asiatique. Si rien n'entrave

le déploiement de WAVE 1.0, cette obligation s'imposera d'elle-même en Europe et ailleurs (Canada, Amérique Latine, Asie, Australasie, etc.). La logique à l'œuvre est donc la suivante :

- la robotique embarquée ne suffit pas pour assurer l'innocuité maximale (ce qui est exact),
- l'adjonction des solutions WAVE 1.0 le permettra.

Or, on peut facilement démontrer que :

- WAVE 1.0 ne procure pas d'amélioration significative en matière d'innocuité (en sus de la robotique embarquée),
- WAVE 1.0 rend possible des atteintes à la vie privée, atteintes qui n'existent pas avec les véhicules à conduite humaine.

Nous détaillons ci-après les caractéristiques techniques de WAVE 1.0 qu'il convient de connaître lorsque l'on se préoccupe des risques relatifs à la vie privée.

2. WAVE 1.0 et smartphones sur roues

Les véhicules autonomes *et connectés* formeront des réseaux ad hoc spontanés sur routes, en ville et sur autoroutes [2]. Ils pourront communiquer entre eux directement (communications V2V, où V = véhicule) et avec leur environnement (communications V2I, où I = infrastructures). Les caractéristiques techniques de WAVE 1.0 qui nous concernent ici sont les suivantes :

- Portée radio de 300 m environ, en omnidirectionnel (360° autour du véhicule émetteur)
- Le V2I permet à un véhicule de communiquer avec des nœuds terrestres (road-side units, relais wifi, 5G bientôt), afin d'accéder à Internet, au Web, à des « clouds »
- Pour pouvoir être acheminés, les messages V2V ou V2I contiennent un nom « source » (qui émet) et un nom « destinataire » (qui est censé recevoir), qui sont des adresses MAC ou IP
- Le beaconing : tout véhicule diffuse périodiquement un message donnant son nom « source », sa localisation, sa vitesse, l'heure d'émission, etc. Jugé indispensable pour assurer l'innocuité (par connaissance des véhicules circulant dans une même « zone » wifi).

En simplifiant, les véhicules connectés conformes au standard WAVE 1.0 peuvent être vus comme des *smartphones sur roues*. Ainsi, les problèmes d'atteinte à la vie privée qui sont bien connus avec les smartphones, tablettes et équipements utilisant des communications sans fil, se posent également avec les véhicules autonomes connectés WAVE 1.0. Dans ce document de travail, nous mettons en exergue les risques suivants encourus avec les solutions WAVE 1.0 :

- *perte d'anonymat des émetteurs,*
- *usurpation d'identité (« masquerading »),*
- *espionnage des trajets suivis par les véhicules,*
- *intrusion à distance des systèmes bord.*

Le dilemme actuel est donc le suivant :

Les bénéfices escomptés pour la société résultant du remplacement de la conduite humaine par la conduite partiellement ou totalement automatisée sont énormes [3], notamment en matière d'innocuité.

A la question « comment obtenir une innocuité maximale, meilleure que celle assurée par la robotique embarquée », la réponse actuelle est « utiliser les communications WAVE 1.0 ».

Malheureusement :

- les solutions WAVE 1.0 ne garantissent pas de propriétés d'innocuité significativement meilleures que celles assurées par la robotique embarquée,
- les solutions WAVE 1.0 reposent sur des choix techniques ouvrant la voie à des menaces en matière de vie privée inexistantes avec la conduite humaine [4], [5], [6].

Le standard WAVE 1.0 est un parfait exemple d'une non-solution d'un problème donné, et qui en crée de nouveaux (inexistants sans elle). Conçues voici environ une douzaine d'années, les solutions WAVE 1.0 commencent à dater. Elles ne tirent pas partie des nouvelles technologies apparues depuis lors. WAVE 1.0 est un exemple de « solution obsolète avant déploiement » [3].

Une analyse succincte de WAVE 1.0 fournie en Annexe explicite les raisons principales pour lesquelles WAVE 1.0 ne permet pas d'atteindre le but Ω, et est antagoniste avec les exigences de discrétion.

3. Buts de WAVE 2.0 : innocuité maximale et discrétion absolue

Contrairement à la croyance actuelle, il existe des solutions permettant d'atteindre le but Ω (innocuité maximale) tout en assurant la discrétion absolue (élimination des risques, cf. supra). Nous notons WAVE 2.0 le futur standard qui, espérons-le, sera fondé sur ces solutions.

Le but Ω, parfaitement justifié, ne peut être atteint qu'avec des solutions assurant la « proactive safety », contrairement à la seule « reactive safety » obtenue avec la robotique embarquée [7] (concepts qui sortent de la thématique APVP'17). Des exemples de solutions sont brièvement présentés en section 4. En section 5, nous donnons les raisons pour lesquelles la discrétion absolue est possible avec les solutions WAVE 2.0.

Les enjeux sont multiples de par leurs dimensions juridique et sociétale. Dans les réseaux de véhicules autonomes connectés, le vol de méta-données peut entraîner le « vol » de vies humaines. Qui d'une autorité de réglementation, d'un constructeur automobile, d'un loueur de véhicules, d'un équipementier (capteurs, actionneurs), d'un industriel du numérique (firmware, OS, intergiciels, applicatifs), sera tenu pour responsable d'atteintes à la vie privée à conséquences indiscutablement sérieuses ou graves ? Les évolutions souhaitables des réglementations en vigueur qui autorisent le déploiement de WAVE 1.0 vont se heurter aux intérêts de l'industrie automobile et de ses écosystèmes—retours sur investissements aussi rapides que possible dans un marché hautement compétitif. Les véritables risques seront pris par les utilisateurs, à leur insu. Le taux d'accidents ne diminuera pas de manière significative, notamment lorsque seront déployés des réseaux hétérogènes de véhicules (de degrés d'automatisation SAE allant de 0 à 5), c'est-à-dire au cours des 10-15 prochaines années. Les inerties au changement reposeront sur toutes sortes de mauvais arguments. S'il en est un qui peut être rejeté sans discussion possible, c'est « on ne connaît pas d'autres solutions (que WAVE 1.0) ».

L'avènement de WAVE 2.0 permettra aux acteurs de l'industrie automobile (constructeurs traditionnels et nouveaux acteurs issus de l'industrie numérique) d'offrir aux futurs passagers de véhicules à conduite partiellement ou totalement automatisée les choix suivants :

► Activer explicitement l'option WAVE 1.0, par exemple pour accéder à Internet, sachant que 1) cela entraîne des risques en matière de vie privée et de vol de données personnelles, 2) cela ne procure pas l'innocuité maximale

► Activer seulement l'option WAVE 2.0 (sans activer WAVE 1.0), pour bénéficier de l'innocuité maximale et de discrétion absolue, au prix de ne pas accéder à Internet, Web, etc. via le système bord (possible via le(s) smartphones du/des passagers)

► Activer les deux options WAVE 1.0 et WAVE 2.0.

Probablement, à terme, l'option WAVE 2.0 sera systématiquement activée sur les véhicules à conduite très fortement automatisée (niveaux SAE 4 et 5).

4. Principes et solutions pour WAVE 2.0

Les réseaux de véhicules autonomes connectés sont des systèmes-de-systèmes cyber-physiques critiques. En conséquence, les solutions correctes des problèmes posés reposent nécessairement sur une ou des construction(s) cyber-physique(s). Les cohortes (formations linéaires ad hoc de véhicules, dotées de spécifications, généralisation du concept de « platoon ») sont sans doute le premier exemple de telles constructions [8].

Au lieu de transmissions radio omnidirectionnelles de 300 m de rayon environ, il est possible d'utiliser les communications optiques—par définition directionnelles et en ligne-de-vue [9-10], ou radio, elles aussi directionnelles et de faibles portées, permettant les communications directes entre véhicules voisins [11] :

- longitudinalement, dans une cohorte
- latéralement, entre cohortes.

***** Extraits de [12-13] pour les communications radio directionnelles longitudinales *****

Every vehicle is equipped with a backward looking and a forward looking directional antenna, small beamwidth (e.g., 25°), short-range (e.g., up to 20 m), possibly steerable in order to accommodate lane curvatures. SC messages are exchanged as neighbor-to-neighbor (N2N) messages. They may carry all types of safety data, such as, e.g., "lane blocking ahead,", "new velocity set to 60 km/h", "move to left lane asap". A cohort head or an isolated vehicle assigns itself rank 1. Insertion of vehicle *Y* behind some member ranked *r* leads to re-ranking: *Y* assigns itself rank *r*+1, and new *Y*'s followers, if any, increment their previous ranks. Re-ranking (-1) is also performed in case some member leaves a cohort. Re-ranking rests on N2N messaging.

Via cohort-wide dissemination of N2N messages, vehicles build common knowledge about the current state of their cohort, as well as the current state of their proximate environment, thus enabling distributed consistent (safe) collective decisions and behaviors. **********

Succinctement, les caractéristiques techniques des solutions connues pour WAVE 2.0 sont les suivantes :

- Communications V2V par antennes radio directionnelles, à contrôle de puissance/portée :
  - En longitudinal, faisceau radio de l'émetteur de l'ordre de 20°, portées jusqu'à 30 m
  - En latéral, faisceau radio de l'émetteur de l'ordre de 90°, portées jusqu'à 20 m
- Communications V2V optiques (LED, VLC, cameras)
- Pas de communications V2I
- Pas de « beaconing » périodique
- Les messages V2V ne contiennent pas d'adresses MAC ou IP
- Tout message V2V est acquitté.

Avec de telles caractéristiques, on montre que :

- Les problèmes d'innocuité maximale ont des solutions : protocoles et algorithmes d'accord distribué à temps de réponse bornés en présence de défaillances, qui assurent les coordinations indispensables entre véhicules, cf. les Bounded Move Requirements ; ces solutions sont accompagnées de preuves (cf. publications scientifiques du domaine),
- La discrétion absolue est possible.

La discrétion (« privacy ») n'implique pas nécessairement la confidentialité (« secrecy »). C'est le cas ici. L'espionnage de méta-données est à combattre. Par contre, l'écoute volontaire ou

involontaire par autrui de données échangées (les contenus des messages V2V) est inoffensive, et même souhaitable (voir plus loin).

5. WAVE 2.0 et discrétion absolue

1) Anonymat des émetteurs et usurpation d'identité

En ville, sur routes ou sur autoroutes, les véhicules qui se suivent forment spontanément des cohortes circulant dans des voies parallèles, hormis dans les carrefours et ronds-points. Dans une cohorte de n membres, chaque véhicule calcule son rang, de 1 à n (fonction de la vitesse v), avec $n(v) \leq n^*(v)$ [8]. Les véhicules d'une même cohorte ou de cohortes adjacentes communiquent directement entre eux par messages 1-hop dont les noms « source » (qui émet) et « destinataire » (qui est censé recevoir) sont des couples d'entiers $\{r, j\}$, où r est un rang et j un numéro de voie. Dans un groupe de cohortes adjacentes, on a la propriété d'unicité : un couple $\{r, j\}$ ne peut correspondre qu'à un seul véhicule. Comme il n'existe aucune relation possible entre un couple d'entiers valide pendant un certain temps pour un véhicule donné et les identifiants intrinsèques de ce dernier (adresse MAC/IP de son système bord, numéro de plaque minéralogique, de plaque numérique, etc.), l'anonymat est assuré.

L'anonymat pose le problème de l'authentification : en présence d'attaques de type « masquerading » ou de « sybil attacks », on doit s'assurer que l'émetteur d'une information V2V « critique » est bien celui qu'il prétend être. Les solutions WAVE 1.0 sont basées sur l'utilisation de pseudonymes certifiés par une autorité de confiance distante, accessible dans un « cloud », les pseudonymes devant être changés « assez souvent » [14]. Outre l'obligation de recourir à des communications V2I—sujettes à attaques diverses, ces solutions souffrent de limitations [15]. Par ailleurs, rien n'interdit à un véhicule/émetteur authentifié d'émettre des messages (chiffrés ou pas) aux contenus mensongers (« bogus data »), afin d'en tirer un avantage (déclarer un embouteillage imaginaire pour libérer un parcours bien précis) ou pour créer des conditions chaotiques accidentogènes, l'attaquant ne risquant rien (avec WAVE 1.0, ces attaques peuvent être conduites à distance).

En WAVE 2.0, le protocole MAC dénommé SWIFT qui, contrairement au CSMA/CA de WAVE 1.0, garantit des délais d'accès canal bornés en pire cas, permet également la détection immédiate d'usurpation d'identité dans une cohorte. La version donnée en [12] tolère les défaillances fortuites. Avec un paramétrage de SWIFT différent de celui donné en [12], on montre que dans une cohorte, lorsqu'un véhicule échange des messages avec son prédécesseur ou son successeur, il ne peut ni mentir sur son rang ni émettre à des instants autres que ceux qui lui sont attribués, sous peine d'être démasqué. Un véhicule suspect est immédiatement « déconnecté » de la cohorte dans laquelle il se trouve : ses liens de communication avec son prédécesseur et son successeur sont coupés par ces derniers, qui exécutent alors un « cohort split » afin d'isoler physiquement le véhicule suspect.

On montre également qu'avec un paramétrage approprié de SWIFT, on garantit l'authenticité des contenus des messages V2V échangés dans une cohorte. Une falsification de contenu lors d'une dissémination ou de relayage de message V2V est immédiatement détectée. La cohorte concernée a le choix : exécuter un algorithme d'accord distribué (qui donnera le contenu correct) ou bien déclencher un « cohort split ».

Pour le cas des cohortes adjacentes, l'authentification des véhicules qui vont être impliqués dans une manœuvre « safety-critical » est obtenue par communications optiques (LED et caméras), qui assurent l'équivalent de WYSIWYG ou de Seeing-is-Believing. L'authentification des contenus repose sur la codification des manœuvres possibles ainsi que sur la nécessité d'obtenir un accord (consensus) explicite de la part tous les véhicules concernés (voir aussi § 3).

2) Espionnage des trajets suivis par les véhicules

Le beaconing de WAVE 1.0 oblige tout véhicule à diffuser entre 1 fois et 10 fois par seconde sa position géographique (coordonnées spatiales GNSS) ainsi que d'autres variables (heure, vitesse, etc.), en V2V et en V2I, afin de permettre à tout véhicule d'entretenir une carte de situation environnementale dans une zone donnée.

L'idée selon laquelle le beaconing est indispensable pour assurer l'innocuité est triplement erronée. Premièrement, les cartes de situation environnementale entretenues par 2 véhicules très proches l'un de l'autre peuvent différer, car le « broadcast » WAVE 1.0 est non acquitté, donc non fiable. Les décisions comportementales prises par 2 véhicules sur la foi de ces cartes peuvent donc entraîner des accidents. Deuxièmement, les temps d'accès au canal radio étant non bornés avec WAVE 1.0 (notamment lorsque tous les véhicules diffusent à 10 Hz), les localisations reçues peuvent dater, donc être inexactes, donc inutilisables pour assurer l'innocuité. Troisièmement, une carte de situation environnementale mise à jour à l'heure UTC t ne permet absolument pas de prédire ce que feront les véhicules cartographiés après l'heure t. Les décisions des véhicules (changements de trajectoires, de vitesses, etc.) sont par définition interdépendantes, concurrentes, et potentiellement conflictuelles. Cette connaissance est cruciale pour l'innocuité. Elle est absente des cartes de situation environnementale.

Inutile pour l'innocuité, le beaconing est sans doute le meilleur moyen de favoriser l'espionnage des trajets, puisque les messages diffusés contiennent les adresses MAC/IP des émetteurs. Grâce aux relais terrestres, on peut donc trivialement tracer et enregistrer les trajets suivis par un véhicule donné (et connaître l'heure de passage sur un point d'un trajet).

Les solutions WAVE 2.0 ne reposent pas sur des coordonnées spatiales GNSS. Les coordonnées spatiales fournies par des récepteurs GNSS ne sont utilisées que de façon passive/locale, pour des services sans lien avec l'innocuité. Ce choix permet d'ailleurs d'éliminer les possibilités de « sybil attacks ». Seules les coordonnées temporelles (temps UTC) sont utilisées (canal radio slotté pour SWIFT). En outre, les solutions WAVE 2.0 ne reposent ni sur le beaconing, ni sur le relayage des beacons par relais terrestres. L'espionnage des trajets est donc impossible avec WAVE 2.0.

L'espionnage d'un véhicule particulier via ses messages V2V n'est pas d'une très grande utilité (voir aussi § 4). Quel est l'intérêt de pister le trajet suivi par un véhicule repéré par un couple $\{r, j\}$, lorsque ce couple ne révèle rien des identifiants intrinsèques à ce véhicule ? De plus, tout véhicule peut à tout moment s'insérer dans une cohorte ou quitter sa cohorte (ce que font les véhicules à conduite humaine). Ainsi, les mappings rangs/voies/véhicules changent de façon imprévisible. Ces mappings peuvent de plus être modifiés à tout moment par les membres d'une cohorte. Par exemple, pour flouer un éventuel espion, via un accord distribué, ils décident de faire + 25 sur leurs rangs courants, rendant impossible le pistage prolongé d'un véhicule particulier.

3) Intrusion à distance des systèmes bord

La prise de contrôle à distance d'un véhicule par voie radio a été démontrée de nombreuses fois (la CIA elle-même s'est illustrée dans ce domaine). Les intrusions peuvent prendre diverses formes (contamination par virus, malware, piratage de données personnelles, jamming, etc.). Elles sont possibles avec WAVE 1.0 (via les communications de portées moyennes V2V et V2I).

Avec WAVE 2.0, les intrusions *à distance* sont impossibles. Les distances (longitudinale, latérale) séparant un attaquant d'un véhicule ciblé sont telles qu'un attaquant ne peut opérer de façon indétectable, en étant éloigné de sa cible. En effet, les communications étant directionnelles, un attaquant visant un véhicule X doit se maintenir assez longtemps dans le lobe

d'une des antennes de X, ce qui le rend détectable. En cas de doute, X supprime une éventuelle menace en changeant de voie. Les risques d'intrusions ayant pour but de prendre le contrôle d'un véhicule en vue de créer des accidents sont considérablement réduits par rapport à WAVE 1.0, car l'attaquant se met lui-même en danger. Néanmoins, on ne peut supposer l'impossibilité d'attaques irrationnelles, soit par intrusions cyber de systèmes bord, soit physiques (par exemple, suicides ou envois de véhicules « d'attaque » sans passager). Les accidents causés par ce genre d'attaques contribuent au taux résiduel non nul (but Ω_2).

Le piratage de données personnelles entretenues dans un système bord est impossible avec WAVE 2.0. La partie WAVE 2.0 d'un système bord est physiquement séparée de la partie WAVE 1.0, celle qui contient les données personnelles (voir § 6).

Enfin, le jamming des canaux radio est toléré en WAVE 2.0 grâce aux communications V2V optiques. Les véhicules attaqués peuvent rester coordonnés (manœuvres évasives déterminées selon l'angle de l'attaquant, vitesses réduites, arrêts sur voie d'urgence).

4) Pas de confidentialité (« secrecy ») ?

Un message V2V WAVE 2.0 contient le code de la manœuvre « critique » envisagée ou en cours. Ces codes sont standardisés, donc publics. Par exemple, 5 sur voie 2 « parle » à ses voisins de cohorte 4 et 6 (eux aussi sur voie 2) pour signifier « nouvelle vitesse fixée à 55 km/h ». Ou bien 18 sur voie 2 « parle » à 11 sur voie 3, pour indiquer une intention de changement de file. Il ne s'agit jamais d'informations personnelles, mais uniquement d'informations destinées à garantir l'innocuité. La confidentialité (par chiffrement des contenus) est inutile. Au contraire, elle serait néfaste. En effet, l'écoute par des voisins des messages V2V échangés par des véhicules engagés dans une manœuvre « critique » est bénéfique vis-à-vis de l'innocuité (c'est ainsi que l'on peut, par exemple, régler les problèmes de manœuvres simultanées conflictuelles). La « privacy » concerne uniquement les méta-données.

5) Pas de communications V2V en mode diffusion, de portées moyennes ?

La diffusion (« broadcast ») de messages par communications omnidirectionnelles de portées moyennes (≈ 300 m) est très utilisée dans les solutions basées sur WAVE 1.0. Malheureusement, les communications radio-mobiles étant non fiables, le « broadcast » de WAVE 1.0 est non fiable : l'un au moins des véhicules concernés ne reçoit pas, quel que soit le nombre de tentatives/répétitions (ce qui remet en cause l'approche « Cooperative Adaptive Cruise Control » prônée par la communauté WAVE 1.0). Pire, le « broadcast » ne permet pas d'accords entre véhicules lorsque les pertes de messages dépassent des taux de l'ordre de 1/3—voir les nombreux résultats d'impossibilité.

Cette difficulté est contournée avec les solutions WAVE 2.0 : le « broadcast » d'un message V2V est obtenu par relayage 1-hop en latéral et en longitudinal du dit message, avec acquittement à chaque relayage. WAVE 2.0 résout donc en même temps le problème de la diffusion fiable et de l'authentification dans tout groupe de cohortes « connexes » (adjacentes).

L'innocuité (absence d'accidents entre cohortes qui se suivent) est assurée sans recourir à un « broadcast » de portée moyenne—cf. plus loin. Subsiste donc le problème de pouvoir communiquer entre cohortes « dispersées », aux fins de coordination, typiquement le cas des traversées de carrefours et ronds-points sans signalisation. Les résultats d'impossibilité sont contournés en recourant à un « broadcast » de portée courte (les diamètres des carrefours ou ronds-points) de codage particulier.

Les courtes portées des émetteurs/récepteurs radios WAVE 2.0 pourraient être considérées inadaptées dans certains scénarios, comme annoncer un accident ou la formation d'un

embouteillage, ce que l'on peut faire, sans garantie de succès, avec WAVE 1.0. Il faut tout d'abord noter que ces scénarios ne sont pas ceux pour lesquels sont conçues les solutions WAVE 2.0. Il s'agit d'annonces d'« échec » (on informe, a posteriori, qu'un accident a eu lieu) ou bien d'annonces ayant pour but la planification ou la gestion optimale des trajets (ce qui n'a rien à voir avec l'innocuité).

Prenons l'exemple de l'annonce d'un accident. Les véhicules accidentés préviennent les éventuels véhicules en approche du lieu de l'accident par envoi de messages d'alerte (code spécifique standardisé, connu de tous, « il y a accident »), en diffusion omnidirectionnelle de portée moyenne (≈ 300 m) qui donnent la position GNSS du lieu de l'accident. Avec WAVE 1.0, ces messages contiennent aussi les adresses MAC/IP. Ces informations sont donc connues de tous les véhicules avoisinants, alors qu'elles n'intéressent que la police, les secours, et les compagnies d'assurances. En WAVE 2.0, on exploite l'existence d'un espace inter-cohorte toujours suffisant pour éviter la percussion d'une queue de cohorte par la tête de la cohorte qui suit, espace calculé pour le pire cas connu sous le nom de « brick wall » [8], [12], [13]. Cet espace est maintenu grâce aux capteurs embarqués (radars, lasers, cameras). Un accident—une instanciation de « brick wall »—est donc détecté à temps par les capteurs de la/des tête(s) de cohorte(s) circulant dans la/les voie(s) bloquée(s) par l'accident. La diffusion de messages d'alerte à la WAVE 1.0 par les systèmes bord est donc inutile. Par ailleurs, il est possible de recourir à des solutions qui n'impliquent pas les systèmes bord.

6) Conclusion

La raison fondamentale pour laquelle les pertes de « privacy » sont possibles avec les véhicules autonomes connectés WAVE 1.0 est relativement évidente : non-respect du principe fondamental de ségrégation/isolation qui fait loi (1) dans le domaine des systèmes cyber-physiques critiques (complexes chimiques, centrales nucléaires, transport aérien, etc.), (2) dans le domaine des systèmes d'informations confidentielles/sécuritaires critiques, à savoir séparation totale entre les applications/services critiques et les applications/services non critiques.

Les vies humaines étant en jeu, et les atteintes à la vie privée pouvant avoir de graves conséquences, les (réseaux de) véhicules partiellement ou totalement automatisés appartiennent à ces deux domaines.

Les solutions WAVE 1.0 conviennent au « non-critique ». Prendre ces solutions comme point de départ pour élaborer des solutions de problèmes qui relèvent du « critique » est bien évidemment voué à l'échec. Il se trouve que les solutions WAVE 2.0, spécifiquement destinées au « critique » initialement (et découplées du non-critique), permettent de surcroît d'assurer la discrétion absolue (« privacy-by-design »).

6. Recommandations

Une quantité croissante d'experts émettent des avis critiques à l'encontre du standard WAVE 1.0. Les exigences combinées d'innocuité maximale et de discrétion absolue sont fondées, et des solutions existent. L'avènement d'un standard WAVE 2.0 est à la fois nécessaire et possible. Des juristes (les nouveaux Ralph Nader) ont commencé à œuvrer dans ce sens aux USA, accompagnés par des scientifiques, majoritairement nord-américains.

Il est souhaitable que les Européens se joignent sans attendre au mouvement, notamment en France.

Références

[1] 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

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

[3] B. Walker Smith, "Automated driving and product liability", Michigan State Law Review, vol. 1, 2017, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2923240

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

[5] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking", IEEE Xplore, DOI 10.1109/MSP.2014.2, 2014, http://www.ccs-labs.org/bib/eckhoff2014driving/eckhoff2014driving.pdf

[6] J. Petit et al., "Connected vehicles: Surveillance threat and mitigation », 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

[7] G. Le Lann, "Safe Automated Driving on Highways—Beyond Today's Connected Autonomous Vehicles", to appear in 8th CSDM Conference on "Towards smarter and more autonomous systems", Springer pub., 12-13 Dec. 2017, Paris.

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

[9] IEEE Spectrum, "LEDs Bring New Light to Car-to-Car Communication", Aug. 20, 2014, http://spectrum.ieee.org/transportation/advanced-cars/leds-bring-new-light-to-car-to-car-communication

[10] P. H. Pathak, "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

[11] R. Ramanathan, 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.

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

[13] G. Le Lann, "Fast distributed agreements and safety-critical scenarios in VANETs", Proc. IEEE Intl. Conf. on Computing, Networking and Communications (ICNC 2017), Santa Clara, CA, USA, Jan. 26-29, 2017, 7p., https://hal.inria.fr/hal-01402159

[14] M. Raya and J.P. Hubaux, "The security of vehicular ad hoc networks", 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Nov. 2005, 11-21.

[15] B. Wiedersheim 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.

Annexe – Une brève analyse de WAVE 1.0 (extraits de publications récentes)

WAVE standards for V2X communications, such as IEEE 802.11p and ETSI ITS-G5 are based on WiFi technology. They serve to provide so-called "connected vehicles" with access to Internet and cloud services (infotainment, weather data, traffic conditions, etc.), in addition to enabling *best-effort* IV communications.

Essential choices are reliance on CSMA/CA as the MAC-level protocol and omnidirectional communications, radio range in the order of 300 m, and interference range in the order of 500 m. There cannot be such bounds as λ with WAVE standards. On a crowded highway (3 lanes each direction, 1 vehicle every 12 m), the number of transmissions that may interfere with any given transmitter may be as high as 500 (6,000/12). Stochastic channel access delays are exceedingly high in moderate or worst-case contention conditions. This is shown in [W] where average values of MAC delays achieved by the IEEE 802.11p protocol range between 75.3 ms and 211.8 ms, for various channel loads, assuming 1 vehicle every 12 m. At 108 km/h, vehicles travel 6.35 m at least (the 211.8 ms figure is not a strict bound), which is much higher than stated in BM_0.

Mobile radio communications are unreliable. Lack of acknowledgements (acks) in multicast or broadcast modes under current V2X standards is another major weakness. Use of acks leads to the broadcast storm problem [X], no time-bounded solution published so far.

Since SC message dissemination and IV agreements must be achieved in bounded time despite losses of messages or acks, there cannot be such bounds as Δ_d and Δ_a. None of the BM requirements is met by current V2X standards. And ditto for solutions to IV coordination problems built out of these standards, such as CACC (Cooperative Adaptive Cruise Control), where V2V broadcast is implicitly assumed to be free from contention and fully reliable (corresponding results are meaningless for real-world conditions).

Vehicle centric beaconing considered harmful

In V2X messages, source and destination names are (statically or dynamically assigned) IP or MAC addresses. Knowledge of addresses is obtained by the multicasting or broadcasting of "existential" messages. Every vehicle publicizes its name and current geolocation (read from GNSS receivers), upon request (replying to a Geocast) or spontaneously.

Beaconing at frequencies in the 1 to 10 Hz range are recommended, which has severe drawbacks. In addition to overloading communication channels and OB processors, beaconing—as currently envisioned—amounts to breaching privacy voluntarily. Why should vehicles reveal their IP/MAC addresses and time dependent geolocations to unknown recipients within ranges in the order of 300 m, making tracking, spying and hacking much easier?

Periodic beaconing is aimed at building "situational awareness" in order to avoid accidents—very accurate time-dependent geolocations are required. This is an unfounded objective. By definition, accidents can only involve vehicles very close to each other. Therefore, short-range situational awareness suffices, which can be achieved with anonymous short-range IV

communications. It has been suggested that anonymity could be ensured by using pseudonyms provided by some cloud-based trusted authority [Y]. Unfortunately, this is unsatisfactory as regards privacy [Z]. Moreover, due to reliance on V2I communications, that is also antagonistic with safety.

V2I communications considered harmful

Reliance on V2I communications (V2V communications relayed via terrestrial nodes, such as road-side units or WiFi relays) can only lead to poorer results in terms of delays. Also, terrestrial nodes may fail, may be "attacked", and can be used for launching all sorts of attacks against vehicles, man-in-the-middle attacks in particular (e.g., masquerading, DDoS). V2I communications favor security threats. Security threats will exist also with upcoming 5G communications resting on terrestrial nodes.

Given that "smartphones on wheels" may infringe on privacy and put human life at risk, we can conclude:

Vehicular networks must be provided with specific radio channels and communication protocols distinct from those used in current WAVE standards, in existing and upcoming public telecommunication networks (Internet, 3G/4G/5G, etc.).