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

Gérard Le Lann

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 (mise à jour le 21 juillet 2017)

Résumé

Les véhicules autonomes seront également « connectés », par adjonction aux systèmes bord de moyens de communication radio définis dans les standards US WAVE (ETSI ITS G5 sont les standards européens équivalents). 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). Les versions initiales de WAVE permettent des atteintes à la vie privée qui n'existent pas avec les véhicules à conduite humaine. Des solutions complémentaires furent donc définies (standards IEEE 1609.2, ETSI 102941) afin d'éliminer ces risques. L'ensemble comprenant WAVE et ces solutions complémentaires est noté WAVE 1.0. Des analyses rigoureuses permettent 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 n'est pas satisfaisant en matière de protection de la vie privée. Les principaux risques encourus sont examinés. On développe un argumentaire en faveur de l'avènement de nouveaux standards de communications radio et optiques inter-véhiculaires—noté WAVE 2.0, fondés 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. 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, 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 le permettra.

Or, on peut facilement démontrer que :

- WAVE ne procure pas d'amélioration significative en matière d'innocuité (en sus de la robotique embarquée),
- WAVE 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 qu'il convient de connaître lorsque l'on se préoccupe des risques relatifs à la vie privée.

2. WAVE, smartphones sur roues et WAVE 1.0

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 qui nous concernent ici sont les suivantes :

- Portée radio wifi de 300 m environ, en omnidirectionnel (360° autour du véhicule émetteur)
- Protocole MAC de type CSMA/CA, ne garantissant pas de délai d'accès au canal radio
- 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.

A cela, il faut ajouter le balisage (« beaconing ») : tout véhicule diffuse périodiquement une balise (message V2V) donnant son nom « source », sa localisation, sa vitesse, l'heure d'émission, etc. Jugé indispensable pour assurer l'innocuité, chaque véhicule entretenant une carte environnementale, qui donne les positions de tous les véhicules présents dans une zone wifi centrée sur lui-même. Les balises sont les CAM (Cooperative Awareness Messages) définis dans ETSI 302637-20-v1.3.0 et les BSM (Basic Safety Messages) définis dans SAE J2945.1-2.2).

En simplifiant, les véhicules connectés conformes au standard WAVE 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. Par exemple :

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

Des solutions supplémentaires destinées à éliminer ces problèmes (standards IEEE 1609.2, ETSI 102941) sont fondées sur l'emploi de pseudonymes authentifiés délivrés par une autorité de certification—Public Key Infrastructure [3]. Dans ce document, nous notons WAVE 1.0 l'ensemble constitué de WAVE et de ces solutions supplémentaires.

Pour ce qui concerne l'innocuité, de nombreuses publications ont mis en évidence l'inadéquation de WAVE, principalement due aux choix de communications omnidirectionnelles de portée moyenne, de protocole MAC probabiliste, et d'hypothèses (implicites) irréalistes (notamment, coordonnées spatiales exactes, et communications fiables—les problèmes de fiabilité

posés par les pertes de messages sont quasiment ignorés). Une analyse succincte de WAVE fournie en Annexe explicite certaines des raisons pour lesquelles WAVE ne permet pas d'atteindre le but Ω.

Pour ce qui concerne la discrétion (« privacy ») absolue, c'est-à-dire l'élimination des risques (cf. ci-dessus), les solutions supplémentaires ne sont pas satisfaisantes [4-8]. L'utilisation de pseudonymes, qui remplacent les adresses IP/MAC de WAVE, impose de satisfaire des exigences antagonistes. Un pseudonyme inchangé pendant trop longtemps permet l'espionnage et le traçage des trajets. Les changements, rechargements et abandons de pseudonymes doivent donc être « suffisamment » fréquents. Ils ne peuvent s'effectuer que dans des zones particulières (« mix zones ») qui sont censées ne pas contenir d'attaquants. Outre la fragilité de cette hypothèse, cela n'est pas satisfaisant [8]. 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. Avec WAVE 1.0, l'attaquant ne risque rien, car ces attaques peuvent être conduites à distance.

Les diffusions de balises (« beacons ») anonymisées doivent être les plus fréquentes possibles (10 Hz) pour assurer (supposément) l'innocuité. Ainsi, tout véhicule peut recevoir plusieurs centaines de balises toutes les 100 ms, qu'il s'agit de décoder (pseudonymes et clés de chiffrement). Cela peut conduire à saturer les calculateurs des systèmes bord (qui ont d'autres tâches « safety-critical » à exécuter, par exemple un moteur d'IA pour la reconnaissance de l'environnement, les algorithmes de navigation, etc.). Cela peut également conduire à saturer le canal radio dédié (canal CCH), donc entraîner des délais d'accès au canal radio bien trop grands, ce qui rend inutilisables les cartes environnementales. Réduire les fréquences entraîne des risques de collisions (les cartes environnementales deviennent imprécises, car les changements de positions entre diffusions deviennent significatifs). D'autres questions restent ouvertes, notamment comment démontrer qu'un nœud terrestre sera toujours accessible pour recharger de nouveaux pseudonymes quand ce sera nécessaire, et comment éliminer les attaques rendues possibles lorsque l'on a recours aux communications V2I (typiquement, les « man-in-the-middle attacks »). Concernant le chiffrement des balises, les désaccords persistent au sein des communautés WAVE et ETSI G5. Certains prônent l'emploi de balises chiffrées, d'autres l'emploi de balises « en clair », car de nombreuses applications peuvent devoir lire les contenus des balises [6].

Nous pouvons donc conclure : WAVE 1.0 ne permet ni d'atteindre le but Ω (innocuité maximale) ni d'assurer la discrétion absolue. Le standard WAVE est un parfait exemple d'une non-solution d'un problème donné (Ω), et qui en crée de nouveaux, inexistants sans elle (perte de discrétion). Les faiblesses intrinsèques de WAVE 1.0 sont principalement dues à l'ignorance d'un principe fondamental, parfaitement connu et respecté dans tous les domaines qui posent des problèmes d'innocuité (par exemple, transport aérien, centrales nucléaires, spatial, sites industriels à risque), innocuité qui peut être mise à mal par les cyber-attaques : séparation totale entre les parties « non critiques » et les parties « critiques » des systèmes utilisés, chaque partie étant dotée de solutions spécifiques, les échanges ne s'opérant que via des passerelles « temps réel » et sécurisées. Les vies humaines étant en jeu, ce principe doit être respecté lors de la conception de solutions destinées aux réseaux de véhicules autonomes connectés. L'erreur majeure commise avec WAVE a été de croire qu'une seule et même solution pourrait permettre d'obtenir à la fois l'innocuité (« critique ») et l'accès aux réseaux de télécommunications et leurs services (« non critiques »). Toute adjonction de « solutions » (par exemple pour la discrétion) est inévitablement non satisfaisante : on ne rend pas correcte une mauvaise solution en la complexifiant (WAVE 1.0).

D'autre part, conçues voici environ une douzaine d'années, les solutions WAVE commencent à dater. Elles ne tirent pas partie des nouvelles technologies apparues depuis lors (par exemple, communications radio courte portée, communications optiques). La création du consortium 5GAA (V2X cellulaire) est, de facto, une menace pour l'avenir de WAVE. WAVE semble donc être en passe de devenir un exemple de « solution obsolète avant déploiement » [4]. Le remplacement de WAVE par des communications 5G ne change absolument rien aux analyses et conclusions données ci-dessus : l'innocuité maximale dans les réseaux de véhicules autonomes connectés ne peut être obtenue qu'à la condition de recourir (1) à des moyens radio distincts de ceux utilisés en télécommunications et (2) à des protocoles et algorithmes distribués spécifiques.

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

Contrairement à la croyance actuelle, il existe des solutions permettant d'obtenir l'innocuité maximale tout en assurant la discrétion absolue. Nous notons WAVE 2.0 l'ensemble de telles solutions qui pourraient, espérons-le, servir de bases à des futurs standards.

Le but Ω, parfaitement justifié, ne peut être atteint qu'avec des solutions permettant la « proactive safety », contrairement à la seule « reactive safety » obtenue avec la robotique embarquée [9] (concepts qui sortent de la thématique APVP'17). Des exemples de solutions sont référencés 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.

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).

Comme dans tout système chargé d'assurer l'innocuité, les systèmes bord seront scindés en deux parties, la partie WAVE 2.0 et la partie WAVE 1.0 étant physiquement séparées, ne communiquant que via une (ou plusieurs) passerelle(s) sécurisée(s).

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) ».

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 [10].

Les accidents ne peuvent se produire qu'entre véhicules proches les uns des autres. Il est donc évident que les transmissions radio omnidirectionnelles de 300 m de rayon sont inadaptées (en particulier, elles maximisent le nombre de véhicules tentant d'accéder en même temps à un canal radio). Il est préférable d'utiliser des communications directionnelles en ligne-de-vue (donc à courtes portées), optiques [11-12] ou/et radio [13-21], permettant les communications directes N2N (« neighbor-to-neighbor ») entre véhicules voisins :

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

***** Extraits de [20-21] 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 N2N 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 N2N optiques (LED, VLC, cameras)
- Pas de communications V2I
- Pas de balisage périodique
- Les messages N2N ne contiennent pas d'adresses MAC ou IP
- Tout message N2N 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 [9]; ces solutions sont accompagnées de preuves (cf. publications scientifiques du domaine),
- La discrétion absolue est possible.

La discrétion 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 N2N) est inoffensive, et même souhaitable (voir plus loin).

5. WAVE 2.0 et discrétion absolue

Les constructions, protocoles et algorithmes WAVE 2.0 sont des exemples de solutions assurant la discrétion-par-conception (« privacy-by-design »).

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, n fonction inverse de la vitesse [20-21]. Lorsqu'un véhicule isolé X (rang 1) est rejoint par un autre véhicule (isolé ou tête de cohorte), un protocole de « join » est exécuté, qui sert à authentifier le(s) rang(s) du/des véhicules qui va/vont suivre X dans la cohorte en formation, afin de contrecarrer toute tentative d'usurpation de rang (de la part de X ou d'un autre véhicule). Les véhicules d'une même cohorte (resp. de cohortes adjacentes) communiquent directement entre eux par messages N2N 2-hops (resp. 1-hop) dont les noms « source » et « destinataire » 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. Afin de contrecarrer les attaques de type « masquerading » ou de « sybil attacks », on doit s'assurer que l'émetteur d'un message N2N est bien celui qu'il prétend être. Le protocole MAC dénommé SWIFT qui, contrairement au CSMA/CA de WAVE, 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 [20] tolère les défaillances fortuites. Avec un paramétrage de SWIFT différent de celui donné en [20], 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. Tout 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 une scission de cohorte (« cohort split ») afin d'isoler physiquement le véhicule suspect. Cela permet de déjouer quasi-instantanément les « sybil attacks ».

On montre également qu'avec un paramétrage approprié de SWIFT, on garantit l'intégrité des contenus des messages N2N échangés dans une cohorte. Une falsification de contenu lors d'une dissémination ou de relayage de message N2N est immédiatement détectée. La cohorte concernée

a le choix : exécuter un algorithme d'accord distribué (qui donnera le contenu correct) ou bien déclencher une scission de cohorte.

Pour le cas des cohortes adjacentes, l'authentification des véhicules qui sont 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, sans intervention humaine. La validation des contenus des messages N2N 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.

2) Espionnage des trajets suivis par les véhicules

L'idée selon laquelle le balisage 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 la diffusion de message (« broadcast ») de WAVE est non acquittée, 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 (notamment lorsque tous les véhicules diffusent des balises à 10 Hz), les localisations reçues peuvent dater, et les dates d'émissions réussies être différentes les unes des autres. Voici une seconde raison pour laquelle, sous hypothèses réalistes, les cartes environnementales sont 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.

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 (la partie « non critique » WAVE 1.0 des systèmes bord). Avec ce choix, on dispose donc d'une seconde parade contre les « sybil attacks ». Les solutions WAVE 2.0 ne reposent pas non plus sur le balisage (ni sur l'existence de cartes environnementales). L'espionnage distant des trajets est donc impossible avec WAVE 2.0.

L'espionnage rapproché d'un véhicule particulier via ses messages N2N n'est pas d'une très grande utilité. 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 associations rangs/voies/véhicules changent de façon imprévisible. Ces associations peuvent de plus être modifiées à tout moment par les membres d'une cohorte. Par exemple, pour flouer un éventuel espion, ils décident via un accord distribué 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 cyber-attaques de type intrusions peuvent prendre diverses formes (contamination par virus, malware, piratage de données personnelles, jamming, etc.). Possibles avec WAVE 1.0 (via les communications de portées moyennes V2V et V2I), les intrusions *à distance* sont impossibles avec WAVE 2.0. Les faibles 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. Enfin, le jamming des canaux radio est toléré en WAVE 2.0 grâce aux communications N2N 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 N2N 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, le chiffrement serait néfaste. En effet, l'écoute par des voisins des messages N2N 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).

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

La diffusion de messages V2V par communications omnidirectionnelles de portées moyennes est très utilisée dans les solutions basées sur WAVE. Malheureusement, les communications radio-mobiles étant non fiables, la diffusion définie dans WAVE qui est non acquittée est elle-même non fiable : l'un au moins des véhicules concernés par un message V2V en diffusion peut ne pas prendre connaissance de ce message (perte en émission et/ou en réception), quel que soit le nombre de tentatives/répétitions. Cela remet en cause l'intérêt du balisage périodique (cf. section 2). Il y a pire. D'une part, il est irréaliste de postuler des bornes supérieures pour le nombre de pertes en émission et en réception. D'autre part, il a été démontré qu'il est impossible d'établir des accords (unanimité ou même une majorité relative) lorsque les pertes de messages dépassent des taux de l'ordre de 1/3—voir les nombreux résultats d'impossibilité [22], étonnamment ignorés par la communauté WAVE. Or, l'innocuité repose sur des accords distribués entre véhicules. En conséquence, plongées dans la réalité opérationnelle des réseaux de véhicules connectés, les solutions fondées sur la diffusion WAVE sont toutes sujettes à caution. C'est le cas notamment de l'approche « Cooperative Adaptive Cruise Control » fondée sur des diffusions de message V2V par un véhicule leader d'un platoon.

Cette difficulté et ces résultats d'impossibilité sont contournés avec les solutions WAVE 2.0 : la diffusion d'un message N2N 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).

Malgré sa non fiabilité, la diffusion de messages V2V par communications omnidirectionnelles de portées moyennes (à la WAVE) est présentée comme « la » solution dans certains scénarios, comme annoncer un accident ou la formation d'un embouteillage. 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 diffusion de messages d'alerte (code spécifique standardisé, connu de tous, « il y a accident »), qui donnent la position GNSS du lieu de l'accident. Avec WAVE, ces messages contiennent 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. Avec WAVE 1.0, on encourt les risques discutés en section 2.

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 » [10], [20], [21]. 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 par les systèmes bord est donc inutile. Par ailleurs, il est possible de recourir à des solutions qui n'impliquent pas les systèmes bord.

Pour les scénarios où il est nécessaire de disposer de l'équivalent d'une diffusion fiable entre cohortes non « connexes » (traversées de carrefours et de ronds-points sans signalisation, par exemple), les résultats d'impossibilité sont contournés en recourant à une diffusion sur canal spécifique de codage particulier.

6) <u>Conclusion</u>

Les vies humaines étant en jeu, et les atteintes à la vie privée pouvant avoir de graves conséquences, les propriétés d'innocuité maximale et de discrétion absolue dans les réseaux de véhicules connectés partiellement ou totalement automatisés sont fondamentales. 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, destinées au « critique » initialement, permettent de surcroît d'assurer les deux propriétés à la fois.

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] 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.

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

[5] 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

[6] 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

[7] 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

[8] 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.

[9] 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.

[10] 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

[11] 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

[12] 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

[13] 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.

[14] E. Shihab, L. Cai, and J. Pan, "A distributed asynchronous directional-to-directional MAC protocol for wireless ad hoc networks", IEEE Trans. on Vehicular Technology, vol. 58(9), Nov. 2009, 5124-5134.

[15] T. Korakis, G. Jakllari, and L. Tassiulas, “A MAC protocol for full exploitation of directional antennas in ad hoc wireless networks”, ACM Mobihoc Conference, 2003, 98-107.

[16] R.R. Choudhury, et al., “On designing MAC protocols for wireless networks using directional antennas”, IEEE Transactions on Mobile Computing, vol. 5(5), May 2006, 477-491.

[17] O. Bazan and M. Jaseemuddin, “A survey on MAC protocols for wireless adhoc networks with beamforming antennas”, IEEE Communications Surveys & Tutorials, vol. 14(2), 2nd quarter 2012.

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

[19] K. Chen and F. Jiang, “A range-adaptive directional MAC protocol for wireless ad hoc networks with smart antennas”, Int’l Journal of Electronics and Communications, Elsevier ScienceDirect, vol. 61, 2007, 645-656.

[20] 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

[21] 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

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

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

WAVE standards for V2X communications 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).

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, as well as those in use in existing and upcoming telecommunication networks (Internet, 3G/LTE/4G/5G).