Some Open Safety Issues in Vehicular Networks

Gérard Le Lann

Some Open Safety Issues in Vehicular Networks

Gérard Le Lann, INRIA, RITS Team, 78153 Le Chesnay cedex, France
gerard.le_lann@inria.fr

I. INTRODUCTION

We consider autonomous and automated vehicles circulating on major roads and highways, forming vehicular networks ranging from strings (single-lane pre-planned platoons or ad hoc strings) to multi-lane ad hoc vehicular networks (VANETs) [1]. Efficiency (e.g., higher asphalt utilization ratio, shorter travelling times, no human time devoted to driving) and improved safety are major motivations for such vehicles and networks. In a nutshell, safety objectives are to reduce fatalities and accidents by a large factor (e.g., ratio of 10) compared to current statistics, for all driving scenarios, under demanding worst-case conditions which cannot be handled by humans (goal Ω). For example, reaction latencies shall be much smaller than 1 second, in the presence of very small inter-vehicular spacing (ranging from 1 meter to a few meters), at low/high velocities, respectively.

For proving safety, it is necessary (albeit not sufficient) to demonstrate that vehicular networks are endowed with two major properties: dependability and timeliness (time-bounded termination). Safety in vehicular networks rests on various disciplines such as, e.g., robotics, signal processing, kinematics, mobile wireless (radio, optical) communications, computer science, formal software engineering, artificial intelligence, cyber security, human/behavioral sciences, to name a few.

In this position paper, we briefly review some accepted beliefs which may hide open issues regarding dependability or timeliness in SC scenarios, and we give examples of shortcomings and challenges. Due to space constraints, we focus solely on protocol/algorithmic design issues, failures, limitations of on-board technologies, and radio channel access latencies in the presence of contention. Despite their importance, software issues (correct instantiations of protocols, algorithms, and applications) are not addressed here. We use the terminology defined by S. Shladover: Automation is autonomy augmented with wireless communication capabilities. For fulfilling goal Ω, should we shoot for autonomous driving or for automated driving? Should we trust human supervision (ultimately, if ever needed, some human is in charge) or full automation rather (absolutely no human intervention)?

II. ISSUES RELATED TO AUTONOMOUS DRIVING

Autonomous vehicles are equipped with on-board perception capabilities (e.g., lasers, radars, lidars, cameras), GNSS devices (e.g., GPS), emaps, and companion software (e.g., navigation, SLAM). On-board perception capabilities work exclusively in line-of-sight (LOS) conditions, and achieve reactive safety only, i.e. avoidance of visible static or moving obstacles.

A. *Issue 1: Human factors—Is safety improved with autonomous driving?*

With autonomy, supposedly most of the time, humans can do whatever they like while travelling. However, autonomy does not free humans from being vigilant. Whenever some hazardous condition develops (can they be enumerated?), a human is responsible for taking proper actions in case his/her vehicle appears not to be doing "the right thing at the right time". Such are the laws in many countries, and this is stipulated in contracts issued by car manufacturers and insurance companies. Problem is that a human may not react quickly enough and appropriately to an event occurring unexpectedly while he/she is playing some game on a smartphone (to give an example). And we know perfectly well that "authority sharing" (is it better to trust a human or some automaton in exceptional or unexpected situations?) is an area with numerous open problems. Likely, that could be the reason why a number of respected experts posit that "with autonomous vehicles, we might see more accidents than with ordinary human driving". It may well be that autonomy will not fulfill goal Ω.

B. *Issue 2: Unavailability and inaccuracies—Can we trust emaps and GNSS devices for achieving safety?*

Local situational awareness is a necessity (hazards may develop with proximate vehicles only). Despite impressive achievements, emaps do not provide what is expected. Emaps provide static data (topology, geography, infrastructures), previously recorded. They are not meant to reflect the occurrence of some hazardous condition (vehicles about to collide) in no more than about 100 ms. Furthermore, global views and absolute geo-localization are not needed. Accurate knowledge of local relative positioning of vehicles suffices, measured by LOS perception devices. Finally, space-time coordinates provided by GNSS devices may be inaccurate, due to adverse conditions (bad weather, physical obstructions). Since losses of satellite signals may last several seconds, worst-case global time (UTC) inaccuracy τ may be in the order of a few milliseconds and worst-case geo-positioning inaccuracy γ in the order of a few dozens of meters, enough for causing accidents. Solutions based on ignoring inaccuracies γ and τ cannot fulfill goal Ω.

C. *Issue 3: Limited knowledge—Are LOS capabilities sufficient for achieving safety?*

There are obvious limitations with LOS capabilities and reactive safety. Consider lane changes. So far, the insertion of a vehicle in a string has been mostly looked at on a "local scale", implicitly assuming that no more than 1 insertion operation would be performed at any given time, which is

unrealistic. Indeed, multiple concurrent insertions at different "slots" within a string are routinely attempted. Most often, whenever necessary, human drivers are able to decide that it is better to defer an intended lane change that would result into unfeasible or/and abrupt decelerations for some string members, which is especially useful when vehicles move at medium/high velocities. Consider now some autonomous vehicle *W* that starts moving to lane *L*, for being inserted behind vehicle *V*. Inevitably, an accident occurs if, simultaneously, *V* brakes abruptly (due to insertions "granted" by vehicles further ahead in the string), and *W* enters lane *L*. Since causal conditions develop beyond LOS, *W* cannot "know" that this maneuver shall not be attempted. Non-LOS (NLOS) capabilities—that do not come with autonomy—are mandatory for fulfilling goal Ω.

D. Issue 4: Does safety hold in the presence of failing LOS perception capabilities?

Safety may not be guaranteed in case a short-range radar would fail. Consider *Y* following *X* closely, and a SC scenario where, at the same time, *X* brakes abruptly and *Y*'s radar fails (permanently or temporarily). Inevitably, *Y* collides with *X*. Duplicated radars might not be safer (the same cause would bring them down). This observation holds for every LOS capability, e.g. lidar scanners that do not work when it rains (reflectance of rain drops). Diversified redundancy is a well-known principle applied in every mature safety-critical domain. Some NLOS capabilities radically different from LOS capabilities are needed for fulfilling goal Ω. This issue is raised here (and echoed further) for the reason that, so far, too little work has been directed at the problem of how to achieve safety in the presence of failures in vehicular networks.

E. Issue 5: Does autonomy entail time-bounded actions/reactions?

Since perception capabilities achieve reactive safety only, an autonomous vehicle can only "adapt" its behavior according to other vehicles' motions, unable to "influence" these motions, a severe limitation. Consider autonomous car *V* on highway 101 that wants to move to rightmost lane and exit 101. *V*'s indicators may or may not be "obeyed" by vehicles (human driven or not) in this lane. Unless they are "cooperative", i.e. they manage to create a convenient "slot" for *V*'s insertion, that lane change maneuver is impossible. There is no difference with human driving. With autonomy, one faces the following dilemma:

- either reactive safety is achieved, but intended maneuvers may not be performed as desired, i.e. no timeliness (*V* cannot exit highway 101 where desired),
- or the opposite.

Proactive capabilities (that do not come with autonomy) are mandatory for fulfilling goal Ω.

III. ISSUES RELATED TO AUTOMATED DRIVING

Let us now consider automated vehicles, i.e. autonomous vehicles equipped with wireless communication capabilities. Let us focus exclusively on radio communications (due to space limitations, optical communications are not examined). So-called "connected vehicles" are vehicles enabling WiFi communications for infotainment purposes. They are not within our scope of consideration. Starting 2020, vehicles built in the USA will have to be equipped with radios conformant to the IEEE 802.11p and 1609 standards (very similar to ETSI G5 standard), enabling V2X medium-range (≈ 250 m) omnidirectional communications based on CSMA-CA. On roads and highways, SC scenarios may develop far away from road-side units. Thus, safety shall be proved assuming V2V (vehicle-to-vehicle) communications only. Over the past decade, numerous publications have been devoted to "demonstrating" that automated vehicles can achieve proactive safety in LOS and NLOS conditions, by resorting to published MAC protocols and companion V2V communications protocols. Let us review some open issues.

A. Issue 6: Are bounded MAC level access delays achievable with existing protocols?

Current MAC protocols designed for omnidirectional radios (standards, scientific publications) fail to solve the BCAD (bounded channel access delays) problem, under realistic worst-case assumptions, i.e. hundreds of contenders, variable number of lanes, space-time inaccuracies γ and τ. We mean strict, non-stochastic, time bounds. CSMA protocols and their variants only provide a "best effort" service, which is unsatisfactory. Unfairness may be experienced by contenders [2,3], due to numerous causes. For example, since propagation of omnidirectional signals (messages and collisions) is anisotropic, a collision may not be detected by all silent processes within interference range of one of the senders; as a result, computations of backoff periods are incorrect, which leads to augmented unfairness. Reservation-based protocols, a.k.a. scheduling-based protocols, do not solve BCAD [4,5,6]. First, access to reservation slots is not collision-free. Second, due to unreliable radio links, not all intended recipients are made aware of reservations heard by others, which results in contention and message collisions. Published variations of TDMA (time-division-multi-access) protocols do not solve BCAD either. Crux of the problem is how to assign a unique slot to every contender without resorting to collision-prone communications, under realistic assumptions. STDMA [7,8] which is based on observing that no two contenders may reside at the same space coordinates at the same time, cannot be considered either since inaccuracies γ or τ need be assumed arbitrarily small for STDMA to be correct (or simply efficient). Ditto for SDMA [9] and LCA [10]. To the best of our knowledge, none of the published MAC protocols devised for directional antennas solves BCAD either, under realistic worst-case assumptions.

B. Issue 7: Are time-bounded deliveries of V2V messages achievable with traditional PAR protocols?

Mobile radio communications are prone to failures, and V2V message losses may exceed acceptable figures, even in LOS conditions [11]. Solutions proposed for Xcast operations (Multicast, Broadcast, or Geocast) rest on a "no acknowledgment" policy, or on positive-acknowledgment-and-retransmission (PAR) protocols [12]. Without

acknowledgments (acks), failed message deliveries go unnoticed, which is not acceptable. PAR protocols cannot be used when a sender does not know a priori which vehicles shall receive its message and return acknowledgments (Geocast). Moreover, PAR protocols are inadequate for the handling of most SC scenarios. Consider the set of V2V messages and acks exchanged for coordinating a safe lane change or for broadcasting and relaying a V2V emergency message reliably. The time budget for delivering V2V messages and acks successfully is in the order of 300 ms (a vehicle moving at 108 km/h would travel 9 m, enough for creating collisions). Given that omnidirectional radio links may be garbled longer than 300 ms, resending messages and/or acknowledgments is useless. Novel approaches and protocols specifically designed for achieving reliable time-bounded V2V message deliveries are needed.

C. *Issue 8: Longitudinal safety—String-wide time-bounded message dissemination and distributed agreement*

Adaptive Cruise Control (ACC) has been extensively studied in control theory and by the robotics community [13,14] in the particular case of platoons. A lead vehicle, driven by a human, makes unilateral decisions such as changing velocity, which is sensed by its follower, and so on—platoon members instantiate a velocity change one after the other. Step-by-step perception takes time, thus cannot fully eliminate instability, i.e. sequences of successive amplifying accelerations or decelerations, while keeping safe, possibly optimal, inter-vehicular spacing. In Cooperative ACC (CACC) solutions, V2V communications are "added" to ACC. Typically, a velocity change triggered by a lead vehicle is carried in a V2V message multicast to platoon members. As expected, doing this leads to better performance figures and higher stability [15-17]. However, in analyses of CACC, channel contention delays are ignored, and message losses are not considered, with some notable exceptions [18-21]. In addition to lack of time bounds, there are two major weaknesses with CACC:

- What if a V2V message multicast by a platoon leader conflicts with a SC V2V message broadcast by a vehicle not member of that string?

- What if a V2V emergency message (e.g., "accident, break or change lane") multicast by a vehicle circulating ahead of a platoon leader is not received by that leader?

There is a need for (1) allowing any platoon member to multicast a SC V2V message (say *M*) to other members, (2) disseminating the contents of *M* downstream *and* upstream, despite failures of on-board systems and radio "links", deliveries completed in some worst-case bounded time (analytical expression given). This is foreign to the CACC concept. Moreover, some unique UTC time must be known to every member, time at which the action stipulated in *M* shall be performed (e.g., "new velocity is 45 km/h"). Note that doing this would achieve perfect string stability, unfeasible with CACC.

Whenever string members issue proposals (contents of various SC V2V messages) concurrently, some unique decision shall be made in (computable) bounded time by every member. Despite resemblance with Approximate Agreement or Consensus, these problems are not correctly solved with traditional algorithms, since physics matter with vehicular networks (see below).

D. *Issue 9: Lateral safety—Needs beyond communications*

With SC multi-lane scenarios (e.g., lane changes, merging lanes, overtaking, on-ramp merging), where one or multiple ad hoc short-lived groups of vehicles must coordinate their behaviors, we face problems similar to those investigated since the 80's in distributed cyber systems. Vehicles replace processes, and asphalt slots are the resources to be shared. Indeed, regarding distributed coordination for proactive safety in multi-lane scenarios, there is a need for solving such problems as Reliable Multicast, Non-Blocking Mutual Exclusion, Terminating Reliable Commit, Consensus (to name a few) in the presence of failures and concurrency [22].

Let us give an example of a scenario where the classical specification of Consensus is invalid (picking up *any* proposal as the unique decision may make no sense at all). Consider a set of vehicles circulating in lane 1, small inter-vehicular spacing and within radio range of each other, approaching a highway entrance. They must decide which vehicle *V* shall decelerate in order to let an incoming vehicle (on ramp) enter lane 1 ahead of *V*. Classical consensus algorithms (devised for cyber systems) may elect a vehicle that is too far away from the highway entrance location. (There are publications of that sort.)

Let us give another example. A long truck *T* circulates in lane *j*; one vehicle circulating in the lane left of *j* and another vehicle circulating in the lane right of *j* undertake concurrent conflicting lane changes, moving to the same "slot" ahead of *T*; with cameras or/and radars obstructed by *T*, either a crash occurs (vehicles do not see each other "in time") or none of the intended lane changes is performed. This is the well-known starvation-free mutual exclusion problem. Which kind of communication-based algorithms would break ties, within very small latencies, under realistic assumptions?

In the presence of concurrent requests for joining a string issued by proximate vehicles, corresponding agreements shall be instantiated and terminated sequentially, despite being run concurrently. (Recall that there are physical actions undertaken when agreement is reached; totally ordered terminations are mandatory.) Besides solving scheduling problems (agreement requests may be assigned different priorities or termination deadlines), we are invited to show how strings can be endowed with the (short-lived, physical) isolation and atomicity properties. Indeed, in the absence of aborts (emergency conditions), all string members must have completed an agreed action (e.g., "reduce velocity to …") prior to performing a new one (e.g., "accept new members"). Which kinds of distributed algorithms (lock-based, timestamp-based, etc.) should we be looking for? Running a distributed agreement algorithm (or any kind of communication-based algorithm) takes time, especially under worst-case contention and failure conditions (goal Ω). This may turn out to be problematic in complex and demanding, albeit common, SC scenarios. This echoes the following challenging question.

E. *Issue 10: Is fully automated driving achievable?*

There are SC scenarios where not enough time is left for inter-vehicular negotiations. Consider on-ramp merging with highway lane 1 under dense traffic conditions—small inter-vehicular spacing (e.g., 2 m)—and significant velocities (e.g., 60 km/h), at rush hour. Every vehicle has very little time for deciding "who goes first". Humans are reasonably good at handling such scenarios, performing alternated intertwining of vehicles in lane 1. Question: Can this be fully automated, and what would it take for meeting that challenge? (We have a response.)

Can it be that the handling of every possible SC scenario on major roads and highways be fully automated, scenarios not well mastered by humans included? In other words, can it be that fully automated driving may surpass human driving on roads/highways, despite failures and limitations of on-board technologies? If the answer is no, then we know that we have to address the highly complex issues related to human factors and "authority sharing", possibly making goal Ω elusive. Research is underway to solve those numerous open problems that arise with fully automated driving on roads and highways, exploiting every appropriate technology (e.g., ultra-high frequency sensing, vision, radio-based and visible light communications), so as to fulfill goal Ω. It might be that the full potential of some cheap existing technologies has yet to be tapped.

IV. SUMMARY

The need for solving those problems quickly reviewed in this position paper has been stressed recently [23]. We, among others, have been working on such problems. Issue 4 is addressed in [24,25]. Issues 7 and 9 are addressed in [26]. Issues 8 and 9 are addressed in [27].

REFERENCES

[1] G. Karagiannis 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.

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

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

[4] F. Borgonovo et al., "ADHOC MAC: New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services", Wireless Networks, vol. 10, 4, 2004, pp.359-366.

[5] H.A. Cozzetti and R. Scopigno, "RR-Aloha+: A slotted and distributed MAC protocol for vehicular communications", IEEE Vehicular Networking Conference, Oct. 2009, pp. 1-8.

[6] L. Bao and J. Garcia-Luna-Aceves, "A new approach to channel access scheduling for ad hoc networks", 7th ACM Int'l. Conference on Mobile Computing and Networking, 2001, pp. 210-221.

[7] J. Grönkvist, "Assignment methods for spatial reuse TDMA", First IEEE Workshop on Mobile and Ad Hoc Networking and Computing, 2000, pp.119-124.

[8] K. Amouris, "Space-time division multiple access (STDMA) and coordinated, power-aware MACA for mobile ad hoc networks", Proc. Global Telecommunications Conf., vol. 5, Nov. 2001, pp. 2890-2895.

[9] S.V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks", 4th IEEE Int'l. Conference on ITS, 2001, pp. 962-967.

[10] S. Katragadda et al., "A decentralized location-based channel access protocol for inter-vehicle communication", IEEE VTC Spring-2003, pp. 1831-1835.

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

[12] F.J. Ros, P.M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks", IEEE Trans. on Mobile Computing, vol. 11, 1, Jan. 2012, pp. 33-46.

[13] S. Shladover, "Longitudinal control of automated guideway transit vehicles within platoons," ASME Journal of Dynamic Systems, Measurement and Control, vol. 100, 4, 1978, pp. 291–297.

[14] D. Swaroop and J.K. Hedrick, "String stability of interconnected systems", IEEE Trans. Automatic Control, vol. 41, 3, March 1996, pp. 349-357.

[15] L. Xiangheng et al., "Effects of communication delay on string stability in vehicle platoons", Proc. IEEE Intelligent Transportation Systems Conference, 2001, pp. 625-630.

[16] G.J.L. Naus et al., "String-stable CACC design and experimental validation: A frequency-domain approach", IEEE Trans. Vehicular Technology, vol. 59, 9, Nov. 2010, pp. 4268-4279.

[17] R. Rajmani and C. Zhu, "Semiautonomous adaptive cruise control systems", IEEE Trans. Vehicular Technology, vol. 51, 5, Sept. 2002, pp. 1186-1192.

[18] C. Lei, and al., "Impact of packet loss on CACC string stability performance", 11th Intl. Conference on ITS Telecommunications (ITST 2011), Aug. 2011, pp. 381-386.

[19] M. Sepulcre, J. Gozalvez, and J. Hernandez, "Cooperative vehicle-to-vehicle active safety testing under challenging conditions", Transportation Research, Part C-26, Elsevier, 2013, pp. 233-255.

[20] C. Bergenhem et al., "V2V communication quality: Measurements in a cooperative automotive platooning application", SAE Intl. J. Passeng. Cars – Electron. Elec. Syst., vol. 7, 2, Aug. 2014, 9 p.

[21] S. Öncü et al., "Cooperative adaptive cruise control: Network-aware analysis of string stability", IEEE Trans. Intelligent Transportation Systems, vol. 15, 4, Aug. 2014, pp. 1527-1537.

[22] N.A. Lynch, Distributed Algorithms. Morgan Kaufmann. ISBN 1-55860-348-4 (1996), 872 p.

[23] F. Dressler et al., "Inter-vehicle communication: Quo vadis", IEEE Communications Magazine, June 2014, pp. 170-177.

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

[25] G. Le Lann, "Integrated safety and efficiency in intelligent vehicular networks: Issues and novel constructs", Proc. TRA 2012 - Transport Research Arena Europe, Athens, Greece, ScienceDirect, Elsevier, 2012, vol. 48, p. 951-961 - https://hal.inria.fr/hal-00735798

[26] G. Le Lann, "On the power of cohorts - Multipoint protocols for fast and reliable safety-critical communications in intelligent vehicular networks", Proc. ACM/IEEE/IFAC/TRB ICCVE-2012 Conference, Beijing, Dec. 2012, pp. 35-42 - https://hal.inria.fr/hal-00769133

[27] G. Le Lann, "Safety in vehicular networks—On the inevitability of short-range directional communications", Proc. 14th Intl. Conference on Ad Hoc, Mobile, and Wireless Networks (AdHoc-Now 2015), Athens, June-July 2015, Springer LNCS 9143, pp. 347-360. http://link.springer.com/chapter/10.1007%2F978-3-319-19662-6_24 & https://hal.inria.fr/hal-01172595