On safety in ad hoc networks of autonomous and communicating vehicles: A rationale for time-bounded deterministic solutions

Gérard Le Lann

On safety in ad hoc networks of autonomous and communicating vehicles: A rationale for time-bounded deterministic solutions

Gérard Le Lann

RITS – INRIA Paris-Rocquencourt

Abstract

Ad hoc networks of autonomous vehicles endowed with inter-vehicular communication (IVC) capabilities are in our future. Avoidance of accidents in safety-critical (SC) scenarios is a major concern. We show that IVCs can "solve" safety-related problems that are not within the grasp of sensing/robotics. A rigorous definition of SC IVCs is given, based on the Bounded Move (BM) requirements. Longitudinal SC scenarios in ad hoc strings and lateral inter-string SC scenarios as they arise on highways are examined. Since current WAVE standards (IEEE 802.11p, ETSI ITS-G5) fail to meet the BM requirements by huge margins, novel solutions are sought. We present the cohort construct—a string with a specification, a deterministic MAC protocol that also achieves fast string-wide message dissemination, and two distributed agreement algorithms. Worst-case time bounds achieved by these solutions are given, showing that they meet the BM requirements. Anonymity issues are briefly addressed.

Keywords *: Vanets; Strings; Self-Driving Vehicles; Safety; MAC Protocols; Reliable Inter-Vehicular Communications; Time-Bounded Message Dissemination; Agreements; Anonymity.*

1 Introduction

Vehicular networks range from platoons with a lead vehicle piloted by a human driver to open ad-hoc vehicular networks, a.k.a. VANETs, comprising communicating autonomous vehicles. Safety issues appear to be the least studied in this area. The focus of our work is on safety-critical (SC) scenarios, where severe accidents (severe injuries and fatalities) inevitably occur when such scenarios are not handled correctly. In addition to on-board sensing/robotics, IVCs are considered for achieving safety properties. Since both technologies have known intrinsic limitations (in addition to experiencing temporary or permanent failures), using them redundantly is mandatory for meeting safety regulations. We show that IVCs can "solve" safety-related problems that are not within the grasp of sensing/robotics. We consider VANETs on highways, which are settings where velocities can be very high, thus exacerbating safety problems—acceptable delays in cyber space, and response times in the physical space, shall be very small. Human lives being at stake, delays in cyber space must have strict and proven upper bounds under worst-case conditions (*vehicular density*, *channel contention, concurrency and failures*). We are thus led to look for deterministic solutions, radically different from today's WAVE standards. Upper bound for MAC access delays (resp., message dissemination or agreement delays) is denoted λ (resp., Δ).

2 Safe automated driving on highways and today's WAVE standards

In the current ITS literature, the term "safety" is used without being given a precise definition. That must be corrected. In our case, a fundamental open question is: What is the exact meaning of "safety criticality"? We have devised unambiguous definitions, stated as the Bounded Move (BM) requirements—see Subsection 3.1. Via discussions with foreign colleagues active in the IEEE 802 Committee, we have comforted our early diagnosis regarding today's WAVE standards for V2X communications (IEEE 802.11p and ETSI ITS-G5): designed for providing "best effort" V2V and V2I communications (mobile access to Internet and cloud services (infotainment, weather data, traffic conditions, etc.)), they are inappropriate for the handling of SC IVCs. A major weakness lies with CSMA/CA (MAC-level protocol). Obviously, there cannot be such bounds as λ and Δ with CSMA/CA. Moreover, *stochastic average* delays in moderate/worst-case contention conditions are

exceedingly high, due to medium-range omnidirectional communications, radio (resp., interference) range in the order of 250 m (resp., 400 m). Consider the following highway setting, not uncommon at pick hours in many countries: 3 lanes each direction and dense traffic (1 vehicle per 12.5 m). A simple calculation leads to the following result: any vehicle may experience (destructive) interferences from up to 384 vehicles. Even if one assumes some "reasonable" communications activity ratio, say 25%, one finds that up to 96 vehicles may be contending for channel access. Under such conditions, current WAVE standards fail to meet the BM requirements by huge margins. This is shown in [Y13] where MAC delays induced by the IEEE 802.11p protocol are evaluated via analytical modeling and NS-2 simulations. For various channel loads, assuming 1 vehicle every 12 m, highest stochastic delays range between 75.3 ms and 211.8 ms. Requirement BM_0 is not met with such values for λ (worst-case delays are theoretically unbounded). Lack of acknowledgements with multicast and broadcast communications is another major weakness. It is simply impossible to argue about safety (even less to *prove* safety) when a sender does not know whether a message carrying SC data has been correctly delivered to intended recipients or has been lost. Reliance on V2I communications via terrestrial infrastructures and nodes, such as road-side units (WAVE, WiFi, LTE or 5G relays), rather than direct V2V communications, can only lead to poorer results. Reachability is not guaranteed since SC conditions may develop anywhere anytime, far away from a terrestrial node. Mixing SC communications and ordinary communications within terrestrial nodes is a violation of the very fundamental segregation/isolation principle in SC applications. Security threats are safety threats since it is very easy to jam or to spy on a terrestrial node. Moreover, terrestrial nodes may be used for launching all sorts of attacks, man-in-the-middle attacks for example. Delays can only get worse than with direct V2V communications, since transiting via a node inevitably introduces additional latencies. The delivery of every SC message must be acknowledged, which exacerbates the latency problems. What happens when a terrestrial node fails? Trying to tweak existing WAVE standards is vain and unjustified. Since collisions can only involve vehicles that are very close to each other, short-range directional communications suffice. Novel solutions for SC IV communications and SC IV coordination are briefly presented in Subsections 3.2 and 3.3. Message passing with these solutions is anonymous—see Subsection 3.4. Future standards specifically aimed at SC IVCs may emerge from solutions similar to those presented herein.

3 Recent results

Solutions to safety related problems necessarily rest on worst-case analyses. They can only be conducted with constructs that have specifications, also necessary for reasoning about (and proving) properties. Cohorts—strings with a specification [LL15], appear to be an early example of cyber-physical constructs appropriate for ad hoc vehicular networks. The cohort concept, originally devised for minimizing the number of vehicles involved in a collective rear-end collision, has proven to be fruitful regarding safety-related problems in general. A cohort that moves at velocity v cannot comprise more than $n^*(v)$ members [LL15]. In [LL16], we have refined this concept as follows, so as to mirror real mobility patterns: $n^*(v)$ is an inverse function of v, i.e. the fastest the smallest (or vice versa). Which we write as follows: $v.n^*(v) \leq b$. Values of bound b may be part of future standards aimed at safety. (String and cohort are used interchangeably in the sequel.)

3.1 The Bounded Move (BM) requirements

Safety related problems would receive trivial solutions if one could assume that vehicles involved in a SC scenario do not move while messages are being exchanged. Since this is unrealistic, the best we can aim at is to quantify distances travelled in worst-case conditions. That is the purpose of the BM requirements, where σ stands for the smallest "car slot" (σ = smallest car size + smallest IV gap), i.e. 7 m approximately:

- BM_0: a MAC protocol is acceptable only if the *distance travelled in λ time units* by any vehicle is *significantly smaller than σ.*
- BM_1: a string-wide acknowledged message dissemination algorithm is acceptable only if the *distance travelled in Δ_d time units* by any vehicle is *smaller than σ*.
- BM_2: a string-wide or an inter-string agreement algorithm is acceptable only if the *distance travelled in Δ_a time units* by any vehicle is *smaller than 2σ*.

Solutions to safety related problems that come with no *worst-case time bounds* simply cannot be trusted, since it is impossible to tell whether they meet such requirements or any others equally constraining and unambiguous. Bounds λ and Δ are established by resorting to analytical calculus. Simulations are irrelevant. Our solutions can be compared against other protocols/algorithms only if their worst-case time bounds are given (not our duty), be they obtained by analytical calculus, asymptotic analyses, or (max,+) algebra—to name a few possibilities.

3.2 SWIFT: A deterministic MAC protocol and an efficient algorithm for string-wide dissemination of acknowledged messages

In cohorts, members assign themselves consecutive integers, called ranks, starting from 1 for an isolated vehicle. See [LL15-LL17] for how ranks are computed whenever cohort membership is modified. SWIFT, a collision-free MAC protocol, is based on member ranking and small beamwidth directional RF antennas that are power controlled [BJ12]. They can be built out of WAVE conformant omnidirectional antennas. The level of power used by a vehicle that transmits a 1-hop LOS neighbor-to-neighbor (N2N) message to its predecessor or its successor is a function of the gap (approx. a 2-15 m range) with the targeted neighbor. Short range power control does not eliminate interferences with vehicles beyond a targeted neighbor. Via a worst-case analysis, one finds h, the highest number of contiguous members that are within the interference range of a transmitter. Integer h is a measurement of spatial reuse. Lobes of small beamwidth antennas may encompass adjacent lanes. This is taken into account in the design of SWIFT, which rests on a slotted channel, aligned to UTC, thanks to GPS receivers, backed by on-board clocks. Cheap clocks suffice, since drifts need not be small. Channel slot allocation is conducted according to ranks. Every member owns 2 slots per frame ($2h$ slots in each frame), h slots serviced downstream, followed by h slots serviced upstream. Members which own the same rank modulo h can transmit in the same time slot, in the same direction, without interfering with each other. Since h is a small integer, spatial reuse is good. Fast *symmetrical* string-wide dissemination of *acknowledged* N2N messages mandates that the ordering of channel accesses must match the ranking and the counter-ranking of members, which is not feasible with CSMA/CA or TDMA protocols—SWIFT is not equivalent to conventional TDMA [H15]. Acknowledgements of N2N messages sent in one direction are piggybacked on N2N messages flowing in the opposite direction, entailing a negligible overhead. String-wide message dissemination serves to build common knowledge, which is essential for achieving SC IV coordination. We have established the following bounds:

- Worst-case channel access delay: $\lambda = 2h\theta$, θ standing for the largest message transmission duration.
- Worst-case string-wide acknowledged message dissemination delay in the presence of f faulty N2N links, for a string comprising n members and moving at velocity v: $\Delta_d(n,f) = 2h\theta\ \{f+1+\lceil (n-1)/h \rceil\}$, $n \leq n^*(v)$.

Considering conservative numerical figures (h = 4, θ = 1 ms), one finds λ = 8 ms, i.e. 0.56 m for v = 250 km/h (highest velocity referred to in WAVE standards). Requirement BM_0 is met.

Valuation of bound b is not arbitrary. With v in km/h, and $n^*(250) = 4$ (highest number of rear-end collisions in "brick wall" conditions), we have $b \leq 1{,}000$. Let us check Δ_d for two extreme cases: v = 180 (n^* = 5) and v = 10 (n^* = 100). Assuming up to 1 loss (message or acknowledgement) per N2N link, not leading to a string split, we have $f < n^*$. One finds (*dist* standing for distance travelled):

$\Delta_d(5,4)$ = 48 ms, and *dist* ≤ 2.4 m; $\Delta_d(100,99)$ = 1 s, and *dist* ≤ 2.78 m.

Requirement BM_1 is met, despite the fact that every N2N message must be sent twice. Assuming no losses, we find: $\Delta_d(5,0)$ = 16 ms, and *dist* ≤ 0.8 m; $\Delta_d(100,0)$ = 208 ms, and *dist* ≤ 0.58 m.

Note the significant reductions in distances travelled. This shows that results regarding safe or/and "cooperative driving" with IVCs (e.g., CACC) based on ignoring message losses are of limited practical relevance.

3.3 Time-bounded distributed agreements

Eligo and LHandshake [LL17] are distributed agreement algorithms aimed at achieving safe IV coordination in the presence of concurrent conflicting events and/or inputs to agreement, referred to as "proposals". Time-bounded agreement (TBA) problems arise whenever p members, $1 < p \leq n$, issue conflicting proposals concurrently, entailing unfeasible maneuvers (e.g., acceleration request(s) and string split request, or deceleration request(s) and string insertion request(s)). (Concurrency issues are almost totally ignored in the literature devoted to IV coordination.) All string members shall reach the same decision D in bounded time, at UTC times comprised within an interval of size ε. Stipulated properties are as follows:

- *Validity*: Decision value $D = \Psi\{\text{proposed values}\}$.
- *Agreement:* No two members decide differently.
- *Time-Bounded Termination*: Every member decides in at most Δ_a time units.
- *Synchronicity*: ε shall be such that the difference between distances travelled by the member earliest to post D and the latest to do so is an order of magnitude smaller than σ.

Ψ stands for any appropriate function in cyber-physics. Eligo (I choose in Latin), which builds on SWIFT, solves the TBA problem in strings, achieving bound Δ_a denoted Δ_{swa}. LHandshake, which builds on Eligo, solves the TBA problem as it arises in sets of strings circulating in adjacent lanes, achieving bound Δ_a denoted Δ_{isa}. Extending the results given in [LL17], we have $\Delta_{swa}(n,f,p) = 2h\theta\ \{1+p+2[f+\lceil (n-1)/h \rceil\}$.

Assume $p = \lceil (n/10 \rceil$. Let us check that Eligo meets BM_2 in both cases.

v = 180 km/h: $\Delta_{swa}(5,0,1)$ = 32 ms, and $dist \leq 1.6$; $\Delta_{swa}(5,4,1)$ = 96 ms, and $dist \leq 4.8$.
v = 10 km/h: $\Delta_{swa}(100,0,10)$ = 488 ms, and $dist \leq 1.36$; $\Delta_{swa}(100,99,10)$ = 2.072 s, and $dist \leq 5.76$.

● Worst-case lateral inter-String agreement delays. Let g stand for the number of consecutive members that must reach agreement, e.g., that receive an insertion request from an adjacent vehicle ($g < 5$ in realistic cases). We have shown that LHandshake achieves $\Delta_{isa}(g,f,p) = 2\sigma_{max}+\Delta_{swa}(g,f,p)$, where σ_{max} stands for the worst-case delay involved with transmitting and delivering a V2V message (a join request, a response), MAC access delay included. Whether LHandshake meets the BM_2 requirement depends fully on σ_{max}, which may take unbounded values with WAVE standards. Novel protocols for lateral V2V communications are sought (on-going work).

The broadcasting of medium-range omnidirectional V2V messages is believed to suffice for coping with non-LOS SC scenarios, e.g., accidents. Alas, the reliable broadcast problem has no time-bounded solutions—the case with VANETs (see Section 2). Something else is needed for coordinating the behaviors of vehicles heading toward crashed vehicles (brutal braking and random lane changes lead to more accidents) or crossing an intersection with no traffic lights safely and efficiently. For the latter case, circumventing impossibility results appears feasible with cyber-physical solutions (the cohort construct and hybrid radio/optical communications).

3.4 Naming and anonymity

IP/MAC addresses appear in WAVE conformant V2V messages. Periodic beaconing (1-10 Hz) is based on assuming that beacons are delivered reliably, and in time (to be useful), a flawed assumption. The building of inaccurate "maps" of proximate vehicles contributes to overloading communication channels and on-board computers. There are better ways for building situational awareness. Finally, doing this amounts to breaching anonymity voluntarily. Every vehicle reveals its existence and time-dependent geolocations to unknown recipients within a disc of radius in the order of 250 m, making tracking, spying and hacking much easier. Solutions based on pseudonyms issued by a trustable third party (a cloud-based authentication body) cannot be considered either: they rest on V2I communications, and they suffer from known limitations [W10]. Names that appear in N2N messages are integers (member ranks). There is no possible linkage between such names and identifiers proper to a vehicle (IP/MAC addresses, plate number). Moreover, rank/vehicle mappings change arbitrarily often in ad hoc vehicular strings. Consequently, tracking, spying or hacking are hardly feasible, only by an adjacent vehicle within the directional lobe of the targeted "victim". Which eavesdropper would be interested in learning that an adjacent string decides to set its velocity to 55 km/h? Authentication issues do not arise within a string (no masquerading is feasible with ranks). Across strings, there are simple solutions based on hybrid radio/optical communications. None of these properties hold with today's WAVE standards.

References

[BJ12] Bazan O. and Jaseemuddin M., "A survey on MAC protocols for wireless ad hoc networks with beamforming antennas", IEEE Communications Surveys & Tutorials, vol. 14(2), 2012, 216-239.

[H15] Hadded M. et al., "TDMA-Based MAC protocols for vehicular ad hoc networks: A survey, qualitative analysis, and open research issues", IEEE Communications Surveys & Tutorials, vol. 17(4), 2015, 2461-2492.

[LL15] Le Lann G., "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, 347-360. http://link.springer.com/chapter/10.1007%2F978-3-319-19662-6_24 & https://hal.inria.fr/hal-01172595

[LL16] Le Lann G., "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

[LL17] Le Lann G., "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

[W10] Wiedersheim B. et al., "Privacy in inter-vehicular networks: why simple pseudonym change is not enough", 7th IEEE/IFIP Intl. Conference on Wireless On-demand Network Systems and Services, (WONS), 2010, 176-183.

[Y13] Yao Y. et al., "Delay analysis and study of IEEE 802.11p based DSRC safety communication in a highway environment", Proc. IEEE INFOCOM 2013, 1591-1599.