



# Safety in Vehicular Networks-On the Inevitability of Short-Range Directional Communications

Gérard Le Lann

## ► To cite this version:

Gérard Le Lann. Safety in Vehicular Networks-On the Inevitability of Short-Range Directional Communications. 14th International Conference ADHOC-NOW, 2015, Jun 2015, Athens, Greece. 14 p., 10.1007/978-3-319-19662-6\_24 . hal-01172595

**HAL Id: hal-01172595**

**<https://inria.hal.science/hal-01172595>**

Submitted on 10 Jul 2015

**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.

# Safety in Vehicular Networks—On the Inevitability of Short-Range Directional Communications

G rard Le Lann

INRIA, Paris Rocquencourt, France  
gerard.le\_lann@inria.fr

**Abstract.** Safety implies high dependability and strict timeliness under worst-case conditions. These requirements are not met with existing standards aimed at inter-vehicular communications (V2V) in vehicular networks. On-going research targets medium-range omnidirectional V2V communications and short-range directional communications, which we refer to as neighbor-to-neighbor (N2N) communications. Focusing on the latter, we investigate the time-bounded message dissemination (TBMD) problem as it arises in platoons and ad hoc vehicle strings, referred to as cohorts. Informal specifications of TBMD, of a solution, are given. We show how to guarantee cohort-wide dissemination of any N2N message generated by a cohort member, either spontaneously or upon receipt of a V2V message. Dissemination time bounds are given for worst-case conditions regarding N2N channel contention and N2N message losses. These results add to previously demonstrated merits of short-range directional communications as regards safety in vehicular networks.

**Keywords:** Safety; Vehicular Ad Hoc Networks; Platoons; VANETs; Automated Vehicles; Time-Bounded and Reliable Wireless Mobile Communications; Directional Antennas; String Control.

## 1 Introduction

Networks of automated (autonomous and communicating) vehicles, such as platoons and VANETs [1], are complex safety-critical cyber-physical systems-of-systems. As of now, numerous safety issues remain open. A few solutions are emerging. However, they fail to meet numerous requirements related to the handling of safety-critical (SC) scenarios. Autonomy essentially rests on perception solutions, namely robotics (radars, lidars, cameras, etc.), which work exclusively in line-of-sight (LOS) conditions, and achieve passive safety only. Active safety in non-LOS (NLOS) conditions is mandatory. With active safety solutions, a vehicle can “tell” other vehicles what it intends to do, rather than letting them guess via perception capabilities (which might be hazardous). Moreover, active safety serves to “enforce” specific behaviors on other vehicles, so that collective behaviors are risk-free. Active safety in NLOS conditions implies highly dependable and time-bounded communications. Existing standards, e.g., IEEE 1609, 802.11p or ETSI ES 202 663, specify omnidirectional radio communications [2]. In this paper, we consider vehicular networks on major roads and highways. Given that SC scenarios may develop far away from road-side units, only vehicle-to-vehicle (V2V) communications need be examined. In the sequel, “V2V communications” stands for medium-range ( $\approx 200$  m) omnidirectional communications.

Limitations of passive safety, of V2V communications, relative to dependability and time-bounded terminations, are reviewed in detail in Section 2. In Section 3, we concentrate on

string formations, either planned (platoons) or ad hoc, which happen to instantiate most frequent driving regimes, and we show how to circumvent weaknesses of V2V communications. The companion concepts of short-range ( $\approx 30$  m) directional neighbor-to-neighbor (N2N) communications and cohorts are presented. In Section 4, we introduce and specify the time-bounded message dissemination (TBMD) problem as well as  $\Pi$ , an algorithmic solution. An analytical expression of worst-case cohort-wide dissemination termination bounds is given and numerically illustrated. This paper is a contribution to a series of previous publications which demonstrate the merits of short-range, radio or optical, directional communications.

## 2 Limitations of Existing and Emerging Solutions

Behaviors of vehicles are under the control of on-board (OB) systems, which comprise perception and radio communications equipment, as well as space-time localization devices (GNSS receivers). Lane changes, on-ramp merging, emergency breaking/stopping, are examples of SC scenarios. For demonstrating safety, one must show that dependability and time-bounded termination requirements are met under worst-case conditions, namely high V2V message loss ratios, high channel contention, high traffic density, and inaccurate space-time data. It is known that GNSS devices may deliver inaccurate data, due to adverse conditions (bad weather, obstructions). Since losses of satellite signals may last several seconds, worst-case geo-positioning inaccuracy  $\gamma$  may be in the order of a few dozens of meters, and worst-case global time (UTC) inaccuracy  $\tau$  in the order of a few milliseconds.

### 2.1 Limitations of Passive Safety

Existing autonomous (AU) vehicles can avoid hitting static or moving “obstacles”, surrounding vehicles in particular. An AU vehicle adapts its behavior according to its perception of how other vehicles move, and vice-versa. Consider AU vehicle  $V$  that wants to move to lane  $j$ .  $V$ ’s indicators may or may not be “obeyed” by others. Unless vehicles on lane  $j$  are “cooperative”, i.e. manage to create a convenient “slot” for  $V$ ’s insertion,  $V$ ’s lane change maneuver is unfeasible. Consider now three adjacent lanes  $j-1$ ,  $j$ , and  $j+1$ , AU vehicle  $X$  in lane  $j-1$ , AU vehicle  $Y$  in lane  $j+1$ , and truck  $H$  in lane  $j$ .  $X$  and  $Y$  want to overtake  $H$ . They do not “see” each other due to  $H$ . Simultaneously,  $X$  and  $Y$  start a lane change maneuver so as to occupy the same slot ahead of  $H$ . At high velocities, this hazardous situation may not be detected in time by perception devices, leading to an accident. In case this hazard is detected in time, both maneuvers are aborted. Tie-breaking (which vehicle goes first, if ever) is conditioned upon the perception of unpredictable and fortuitous motions. In both examples, either the dependability or the time-bounded termination requirement is not met. To computer scientists, this is the well-known “starvation” problem that arises with cyber processes that share resources in a mutually exclusive manner. In vehicular networks, rather than data or processes, asphalt slots are the resources shared by moving processes. It is well known that algorithmic solutions based on passive waiting (perception here) may never terminate. The only algorithmic solutions that achieve time-bounded termination are based on reliable inter-

process communications and agreements (“semaphores”, “locks”, etc.). Similar solutions are needed for achieving active safety in vehicular networks.

## **2.2 Limitations of V2V communications**

Mobile radio communications are inherently unreliable. Moreover, with the CSMA-CA MAC protocol at the core of existing standardized V2V communications, there are no worst-case upper bounds for channel access delays, thus no such bounds for message delivery delays.

### **Unreliability**

At times, V2V message loss ratios may be too high, even in LOS conditions [3]. With very few exceptions, solutions proposed for Xcast operations (Multicast, Broadcast, or Geocast) rest on a “no acknowledgment” policy, or on positive-acknowledgment-and-retransmission (PAR) protocols [4]. Without acknowledgments, 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. Moreover, these 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. The time budget for delivering V2V messages and acks successfully is in the order of 400 ms (a vehicle moving at 108 km/h would travel 12 m, enough for creating collisions). Given that omnidirectional radio links may be garbled longer than 400 ms, resending messages and/or acknowledgments is useless. Novel solutions specifically designed for achieving reliable time-bounded V2V message deliveries are needed.

### **No Timeliness**

The problem of how to guarantee bounded channel access delays (BCAD) with omnidirectional antennas remains unsolved, when considering realistic worst-case assumptions, i.e. hundreds of contenders, variable number of lanes, space-time inaccuracies  $\gamma$  and  $\tau$ . We mean strict, non-stochastic, time bounds. CSMA protocols only provide a “best effort” service, which is unsatisfactory. Moreover, unfairness may be experienced by contenders [5,6], 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 inference range of one of the senders; as a result, computations of backoff periods are incorrect, which leads to amplified unfairness. Reservation-based protocols, a.k.a. scheduling-based protocols, do not solve BCAD [7,8]. 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 [9,10] 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  $\gamma$  and  $\tau$  need be assumed arbitrarily small for STDMA to be correct (or simply efficient). Ditto for SDMA [11] and LCA [12]. An additional unpleasant feature of existing V2V MAC protocols is the high variability of access

delays, very small under modest traffic and contention, very large (close to unbounded) under high traffic and contention.

### Limited Scope and Relaying

V2V messaging is commonly used in SC scenarios. For example, vehicles involved in an accident do Xcast ( $M$ ), announcing “accident at location  $Z$ , immediate stop or change lane”. Given that the distance between senders of  $M$  and vehicle strings moving towards  $Z$  is much larger than 1-hop range in general, multi-hop relaying is resorted to. Most of the work conducted on geocasting focuses on minimizing the number of relaying vehicles as well as copies of  $M$ , ignoring message losses. What if vehicles in charge of relaying do not receive  $M$ ? Are copies of  $M$  delivered to all string members within stipulated time bounds? In cooperative adaptive cruise control (CACC) approaches, where string stability is a major issue [13], consequences of V2V message losses and time-unbounded message deliveries regarding safety are ignored, with few exceptions [14,15,16]. Furthermore, data collected in platooning experiments show that it is inappropriate to rely on V2V broadcast from the lead vehicle [17].

Given that existing V2V communications are not satisfactory, on-going research investigates novel “deterministic” MAC protocols aimed at V2V communications and transport protocols which “guarantee” message deliveries. Another stream of research focuses on solutions that depart from V2V communications, although based on mastered radio technology. Such an approach is presented in Section 3.

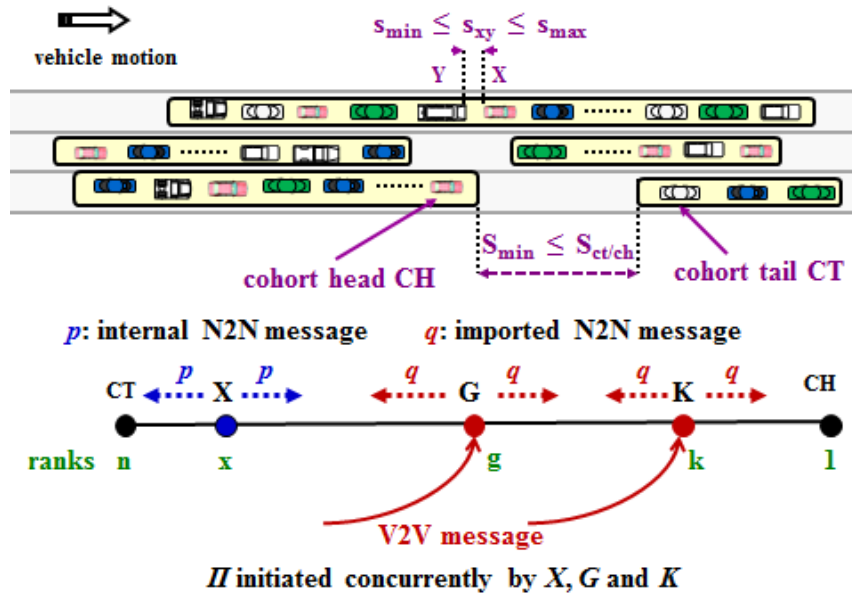
## 3 Cohorts and N2N Communications

### 3.1 Principles

A cohort is a string of fully automated vehicles circulating in the same lane, bound to meet rigorously defined specifications [18,19]—see Fig. 1. Cohorts may be pre-planned (platoons, with or without a human driver in a lead vehicle) or ad hoc open linear VANETs, possibly short-lived, vehicles joining in or leaving anytime. To the exception of head  $CH$  and tail  $CT$ , every cohort member has two neighbors. Cohort members share some common knowledge, such as  $n$  and  $n^*$ , the current number of members and the highest possible number of members, respectively, velocity dependent safe spacing intervals, denoted  $s_{xy}$ , highest deceleration rate ( $dc$ ) and highest acceleration rate ( $ac$ ). Values for bounds  $n^*$ ,  $dc$  and  $ac$  will be set by standardization bodies. Variable  $n$  is updated via the TBMD algorithm (see Section 4). Below  $dc$  or  $ac$ , cohort membership does not change. Membership changes occur in case vehicles want to leave or to join, maneuvers that rest on inter-vehicular agreements. Members are assigned consecutive ranks, 1 for  $CH$ , and  $n \leq n^*$  for  $CT$ . Safe inter-cohort spacing intervals (which depend on velocities), denoted  $S_{ct/ch}$ , are also specified. Due to these intervals, cohorts do not “interfere” with each other as long as  $dc$  and  $ac$  rates are not exceeded. In the opposite case, e.g., occurrence of a “brick wall” phenomenon within some cohort, other cohorts are immune to rear-end collisions.

A member which violates  $dc$  or  $ac$  Xcasts a V2V message, signaling the instantiation of emergency conditions, possibly leading to a cohort split (see further). Cohort-wide coordination can be accomplished via algorithms resting on N2N directional communications.

There is no need to “pollute” the ether with 360° antennas over, e.g., 200 m, for coordinating consecutive members of a given cohort. Very short-range (e.g., 30 m), small beamwidth (e.g., 30°) front-looking and rear-looking directional radio antennas suffice [20], possibly steerable and power controlled. Observe that they would complement radars and lidars regarding spacing control, as well as V2V communications, thereby instantiating diversified redundancy (V2V and N2N communications are allocated different radio spectra), which is essential regarding safety. Most notably, communications among cohort members are not disrupted when V2V channels experience physical jamming [21]. Neighbors exchange N2N messages and beacons, upstream and downstream.



**Fig. 1.** Cohorts and principles of algorithm II illustrated

Hop-by-hop N2N message passing also serves to perform a cohort-wide dissemination of any given V2V message, which may not be received by all targeted members. This is one of the motivations for exploring the TBMD problem. Due to the linear structure of cohorts and directional N2N communications, radio interferences may occur only among a limited set of vehicles proximate to each other, which permits to solve BCAD. Thus, the highest delay incurred with transmitting a N2N message or a beacon between two neighbors, in the absence of failures, is known (see further).

### 3.2 Dependability Within and Across Cohorts

By definition, like any safety-critical cyber-physical system, cohorts are timed systems. Being open systems, some notion of global time (UTC) is needed. Depending on the problem under consideration, “good” clocks/timers may suffice, or “highly accurate” clocks/timers are needed. Failure of an OB process shall result in a specific state transition or maneuver in the physical space (e.g., reaching an emergency lane as soon as possible). Since V2V communications are prone to frequent transient failures, it is quite difficult to specify worst-

case conditions not leading to impossibility results. Fortunately, given the peculiarities of cohort constructs, it is possible to devise simple solutions to dependability problems arising in cohorts. Let  $\eta$  stand for some finite time interval. Every  $\eta$ , a failure detection algorithm is run by a vehicle OB system, in charge of checking V2V/N2N antennas as well as every other equipment (processors, robotics devices, etc.). Every cohort member must “prove” it is operational via the periodic transmission of a N2N beacon to its neighbor(s). A member or a N2N link is declared “failed” by member  $V$  in case no beacon or message has been received by  $V$  on this link for  $\eta$  time units. Picking up any value for  $\eta$  smaller than 500 ms would be safe, since behaviors of vehicles are also under the control of robotics (at 90 km/h, vehicles would travel less than 12.5 m).

A vehicle that experiences an OB system failure must leave its cohort, reduce its velocity (possibly reverting to manual driving) or stop (reaching an emergency lane), and a cohort split is undertaken (see below). A failed N2N link disrupts the cohort-wide communication chain. (Safety is not necessarily sacrificed, since local inter-neighbor coordination may be achieved via robotics, assuming “reasonable” velocities.) Therefore, we must address the network partitioning issue. Many impossibility results have been established regarding agreement or consensus in the presence of partitioning in cyber models of wired static networks [22]. Such results do not hold necessarily in cyber-physical systems in general, in cohort-structured vehicular networks in particular. Cyber-physics complicates matters, but also favors solutions that cannot be considered in cyber systems. Cohorts are a case in point: Communication network partitioning leads to physical network partitioning. In order to preserve cohort-wide integrity, it suffices to trigger a cohort split maneuver whenever a N2N link is declared “failed”. Consider cohort  $C$  and two neighbors  $X$  and  $Y$ ,  $Y$  following  $X$ . If  $X$  (resp.,  $Y$ ) declares “failed” the  $X/Y$  link, then  $X$  (resp.,  $Y$ ) does Xcast (“cohort split”), which V2V message may be received by all or some members of  $C$  and other cohorts, and sends a “cohort split” N2N message to  $Y$  (resp.,  $X$ ) and to its other neighbor (if any), prior to starting the physical split maneuver.  $X$ , tail of truncated cohort  $C$ , and  $Y$ , head of a new cohort, activate a dissemination algorithm within the new cohorts being created.  $Y$  decelerates until safe spacing  $S_{ct/ch}$  is instantiated between  $X$  and  $Y$ . Conditions permitting,  $X$  would accelerate so as to expedite the split maneuver.

The need for N2N communications has been illustrated in [18], where a solution is given to the problem of safe inter-vehicular spacing in the presence of failures of robotics equipment. N2N communications serve to achieve dependability within strings, as well as across strings by disseminating received V2V messages. In [19], we show how to back up V2V communications in lane change scenarios with N2N communications among a limited subset of cohort members. In Section 4, with the TBMD problem, we address issues of concern to all members of a cohort.

## 4 Time-Bounded Message Dissemination in Cohorts

The need for investigating distributed dependable coordination problems (agreement, dissemination) is stressed in [23]. Agreement amounts to deciding on a unique choice among multiple differing proposals, whereas dissemination amounts to delivering a message to every intended vehicle, both in the presence of failures. An informal specification of the TBMD

problem is given in Table 1, of a solution (algorithm  $\Pi$ ) in Fig. 2. Solving TBMD is interesting from theoretical and practical viewpoints. For example, instabilities/shock waves in CACC regimes are eliminated by resorting to algorithm  $\Pi$  (dissemination of a N2N message that tells “new velocity is ...”).

#### 4.1 The Cohort-Wide Time-Bounded Message Dissemination Problem

Processes that instantiate  $\Pi$  are run by OB systems (in the sequel, “member” or “vehicle” are used interchangeably). Consider a cohort  $\Gamma$  and an unknown constantly changing set  $W$  of vehicles within  $\Gamma$ ’s radio range. Imported (*imp*) and internal (*int*) are two types of N2N messages subject to dissemination throughout  $\Gamma$ . At unknown times,  $W$ ’s members Xcast V2V messages. When received by a cohort member, V2V message  $M$  is wrapped in a N2N message typed *imp* used for disseminating  $M$ . Due to losses, not all cohort members may receive  $M$ . Our goal is to show that whenever a V2V message is heard of by at least 1 member, that message is delivered to all members, in the absence of cohort split. A V2V message carries a unique identity ID, which serves to uniquely identify its copies as an imported N2N message. At unknown times, cohort members may create internal N2N messages spontaneously, which messages are exchanged among neighbors in order to be disseminated. Every internal N2N message is assigned a unique identity by its creator. Some V2V messages ought to be acked/nacked, which entails repetitions. Thus, multiple copies of a given V2V message may be generated and received at different times by various cohort members. Achieving best performance figures implies detecting and suppressing such copies. (As for type *int* N2N messages, see Subsection 4.2.)

**Table 1.** The cohort-wide TBMD problem

| Assumptions   |
|---|
| <ul style="list-style-type: none"> <li>- Timed system model.</li> <li>- Set <math>\Gamma</math> of <math>n</math> vehicles, forming a cohort. Cohort members create N2N messages at will, which messages are relayed throughout <math>\Gamma</math>.</li> <li>- Unknown set <math>W</math> of vehicles within <math>\Gamma</math>’s radio range. These vehicles create and Xcast V2V messages at will. Every Xcast is heard of by at least 1 cohort member.</li> <li>- A V2V message received by a cohort member is relayed throughout <math>\Gamma</math> as a N2N message.</li> <li>- OB system failures.</li> <li>- Unreliable V2V communications: some V2V messages may be acked/nacked and repeated.</li> <li>- Unreliable N2N communications: up to <math>f \geq 0</math> losses, not leading to a cohort split.</li> </ul> |
| Properties  |
| <ul style="list-style-type: none"> <li>- Validity: Every N2N message is successfully delivered to every member.</li> <li>- Time-bounded Termination: Cohort-wide dissemination triggered by member <math>X</math> terminates in at most <math>\Delta_x(f)</math> time units.</li> <li>- Termination Awareness: For every N2N message <math>m</math>, every member <math>X</math> is knowledgeable of a dissemination termination time <math>T_x(m)</math>.</li> </ul>   |



For any fault-tolerant distributed algorithm that rests on message-passing, one must specify integer  $f$ ,  $f > 0$ , the highest number of losses (messages or acks/nacks) that may be experienced in the course of execution. Worst-case  $f$  might be specified in future safety standards for every safety-critical algorithm. Any reasonable valuation of  $f$  may be violated. Consequently, it is also mandatory to specify which actions ought to be performed whenever the “up to  $f$ ” assumption happens to be violated. Failures of N2N links that would violate the “up to  $f$ ” assumption lead to a cohort split (see above). If algorithm  $\Pi$  is running,  $\Pi$  is aborted, and restarted within newly formed cohorts. Therefore, neither OB system failures nor N2N link failures need be taken into account in the design of  $\Pi$ . Conversely,  $\Pi$  shall withstand N2N link failure patterns that do not violate the “up to  $f$ ” assumption. In the sequel,  $m$  stands for a message meant to be disseminated throughout cohort  $\Gamma$ , regardless of its type (*imp* or *int*). The activation of primitive  $send(m)$  results in the sending of  $m$  to a 1-hop neighbor. For a member ranked  $r^{th}$ , the set of neighbors  $N$  comprises members of ranks  $r-1$  and  $r+1$  in the general case. For *CH* (resp., *CT*),  $N$  comprises member ranked  $2^{nd}$  (resp., ranked  $(n-1)^{th}$ ).

The dissemination of message  $m$  terminates successfully if and when  $m$  has been delivered to every cohort member (Validity). An analytical expression of  $\Delta_x(f)$  must be given (Time-bounded Termination). Knowing that dissemination terminates does not suffice. Some cyber-physical action  $\Psi(m)$  is stated in  $m$ , such as, e.g., “merge with left lane”, “reduce velocity to 50 km/h”. Cohort members need to know when to perform an action, thus the Termination Awareness property. Not an integral part of TBMD, the Synchronicity property (the termination time is the same for all members) is commonly stated in many distributed agreement problems arising in timed systems. As shown further, Synchronicity can always be achieved in the case of internal N2N messages, under certain conditions in the case of imported N2N messages.

## 4.2 Solving TBMD: Algorithm $\Pi$

Algorithm  $\Pi$  may be event-triggered, or time-triggered, e.g., periodically, by any member. Disseminations may overlap and the dissemination of any given message usually entails bi-directional relaying. Solving TBMD implies solving two problems altogether (often addressed separately). One is the MAC-level BCAD problem, the other one is the link-level dissemination problem per se. Thus, one is led to contemplate a cross-layer solution. Timeliness figures depend on how efficient cross-layering is. In the presence of failures, time-bounded dissemination does not boil down to mere hop-by-hop relaying. Vehicles keep moving while a message is disseminated. Consequently, the challenge is to achieve termination times  $\Delta_x(f)$  that are tight and that do not depend on whether dissemination proceeds upstream or downstream.

### Intra-Cohort Hop-by-Hop Message Passing

N2N message passing is performed via a point-to-point PAR protocol. Observations made in Subsection 2.2 do not apply here, since receivers and senders know each other (they are neighbors). Moreover, fading, interferences and collisions which contribute to garbling V2V communications are less of a problem with short-range directional communications.

Therefore, repeating N2N messages or acknowledgments (acks/nacks) is founded. It follows that a N2N message may have multiple copies, which copies must be eliminated in order to avoid wasting communication bandwidth. Let  $\lambda$  stand for the highest N2N hop delay, in the absence of losses. Delay  $\lambda$  includes (1) the delay incurred with transmitting a N2N message, (2) a receiver's OB processing time (e.g., CRC checking). Delay  $\lambda$  is derived from the N2N link bandwidth and the highest length of a N2N message (acks/nacks are shorter). Operation  $send(m)$  may fail. Let  $Send(m)$  stand for the primitive that serves to perform a successful transmission of  $m$  on a 1-hop N2N link ( $m$  possibly repeated). A cohort member knows about success when an ack is received. Whenever  $f \neq 0$ ,  $Send(m)$  involves a number of sends and acks/nacks, which contribute to augmenting N2N channel contention. Let  $\Lambda$  stand for the duration of  $Send(m)$  for a no-loss transmission, and  $\Lambda'$  stand for the duration of  $Send(m)$  in the presence of 1 loss ( $m$  or ack/nack).

### Algorithm II

Solution II rests on “sufficiently good” timers and clocks. UTC is provided to OB processes by space-time localization devices (e.g., GNSS) and OB clocks updated often enough. With GNSS outages lasting in the order of 20 s, cheap clocks of intrinsic drift in the order of  $0.5 \cdot 10^{-4}$  would achieve inaccuracy  $\tau$  of UTC readings in the order of 1 ms, i.e. a discrepancy in the order of 2 ms for any two vehicles, which suffices for “synchronizing” the physical maneuvers of vehicles. Consider member  $X$ , of rank  $k$ . Upon arrival at (resp., creation by)  $X$ , an imported (resp., internal) N2N message  $m$  is tagged with dissemination termination time  $T_x(m)$ . Let  $t_x(m)$  stand for  $m$ 's arrival/creation time read on  $X$ 's local clock. Thanks to the cohort construct,  $X$  can compute dissemination duration  $\Delta_x(f) = h\Lambda + f\Lambda'$ , where  $h$  stands for the highest number of N2N hops that separate  $X$  from  $CT$  or  $CH$ . Trivially,  $h = \max \{k-1, n-k\}$ , and  $T_x(m) = t_x(m) + \Delta_x(f)$ .

Message identities that are still current are stored in a list in local OB memory, list denoted  $L_x$  for member  $X$ . A table denoted  $A_x(m)$  is created at  $X$  for message  $m$ . Identity  $id(m)$  in  $L_x$  points at  $A_x(m)$ .  $A_x(m)$  and  $id(m)$  are saved for  $\Delta_x(f)$  time units, discarded afterwards (erased or moved to a data recorder).

**Notations and variables** ( $X$  stands for a cohort member,  $n > 1$ ):

-  $N(X)$ : set of  $X$ 's neighbors

- N2N message types: *imp*, *int*

-  $t_x(m)$ :  $m$ 's creation time at  $X$

-  $timer_x(m)$ : timer for  $m$  at  $X$

-  $T_x(m)$ :  $m$ 's dissemination termination time for  $X$

Table  $A_x(m)$  contains  $id(m)$ , message  $m$ ,  $t_x(m)$ ,  $timer_x(m)$ , and  $T_x(m)$

-  $\Delta_x(f) = h\Lambda + f\Lambda'$ : duration of cohort-wide dissemination of  $m$  in the presence of up to  $f$  faulty N2N transmissions

-  $c\_int(m)$ : event that triggers the creation of internal N2N message  $m$

-  $c\_imp(m)$ : event that triggers the creation of imported N2N message  $m$  (arrival of V2V message  $M$ , identity  $ID$ )

-  $r(m)$ : receipt of  $m$  (from a neighbor)

-  $aw_x(m)$ : awakening of  $timer_x(m)$

```

case c_int(m):
begin create m; compute unique identity id(m); call P; record [type(m) = int, tx(m), Tx(m)] in m; Send (m) to neighbor(s) listed in N(X) end

case c_imp(m):
begin if ID found as id(m) in Lx then discard M else
begin create m copy of M; id(m) := ID; call P; record [type(m) = imp, tx(m), Tx(m)] in m; Send (m) to neighbor(s) listed in N(X) end end

case r(m):
% from neighbor Y %
begin read m if id(m) in Lx then
begin read Ax(m) if [type(m) = imp and Ty(m) < Tx(m)] then
begin timerx(m) := current timerx(m) - (Tx(m) - Ty(m)); Tx(m) := Ty(m); % note 1 %
update Ax(m) end
discard m
end else % note 2 %
begin
% first receipt of m %
store id(m) in Lx; copy m; timerx(m) := Tx(m) - (current time - tx(m)); create Ax(m);
Send (m) to opposite neighbor (if any)
end
end

case awx(m):
begin suppress id(m) in Lx; suppress Ax(m) end

Procedure P
begin store id(m) in Lx; tx(m) := local time value; compute  $\Delta_x(f)$ ;
timerx(m) :=  $\Delta_x(f)$ ; Tx(m) := tx(m) +  $\Delta_x(f)$ ; create Ax(m) end

```

**Fig. 2.** Informal specification of *II* for member *X*

## Discussion

Algorithm *II* is relatively simple (correctness proofs are not presented due to lack of space). By definition, being created by a unique member, an internal N2N message carries a unique termination time, which UTC time is copied unchanged by every member. Therefore, *II* achieves Synchronicity for such messages. Inaccuracy  $\tau$  can be made negligible (see above). Distance discrepancies are in the order of 5 cm for any two vehicles moving at 90 km/h with  $\tau$  in the order of 1 ms. On the contrary, an imported N2N message may be created by more than one member. Consider any two members *P* and *Q* that receive the same V2V message, which is assigned a unique pair  $\{m, id(m)\}$ . They compute the same arrival times  $t_p(m)$  and  $t_q(m)$  in case they receive the same copy of that message. Conversely, they compute  $t_p(m) \neq t_q(m)$  if they receive different copies. Whatever the case, they are assigned different ranks. It follows that  $T_p(m) \neq T_q(m)$ . Thus, should the case arise (see note 1),  $timer_x(m)$  and  $T_x(m)$  are updated to smaller values, in order to maximize the number of members that compute termination times closer to smallest termination time. Nevertheless, *II* as given in Fig. 2 does not achieve

Synchronicity in general, in the case of imported N2N messages. The discrepancies between computed termination times mostly depend on the wait-for-ack/nack delays and which policy is used to Xcast V2V messages. If Synchronicity is mandatory, one must invoke an agreement algorithm, or a variation of  $\Pi$  (not presented here due to space limitations) whereby copies of an imported N2N message keep being propagated, rather than discarded (see note 2). Synchronicity would then be traded against higher message load, i.e. higher termination times for all members.

Algorithm  $\Pi$  does not impose any particular rule regarding when a member ought to instantiate cyber-physical action  $\Psi(m)$  stated in  $m$ . Options are (1) upon receipt of  $m$ , (2) upon reaching termination time, i.e. when local timer awakes, (3) some combination of (1) and (2). Similarly, the assignment of a numerical value to  $f$  known to all members is “orthogonal” to  $\Pi$ . This mandatory global knowledge may derive from some future standards (static assignment) or may be dynamically updated (while vehicles move) by resorting to a distributed agreement algorithm. The latter approach shall be more trustable given that, very likely,  $f$  is an increasing function in  $n$ , as well as time and location dependent. Let us observe in passing that this essential question of how to assign “good” values to variables appearing in safety-related performance figures, such as termination bounds, is almost totally ignored in publications devoted to safety issues in vehicular networks. In case a “good” value for  $f$  would be exceeded and detected by some member, that member undertakes a cohort split and  $\Pi$  is aborted, to be restarted in cohorts resulting from the split. (Due to space limitations, how to detect a violation of postulated  $f$  is not detailed here.)

### 4.3 Time-Bounded Termination

N2N channel contention occurs between members of the same cohort, as well as with members of cohorts circulating in adjacent lanes. Indeed, due to road/highway curvatures, communications triggered by vehicles in adjacent lanes may interfere with each other, despite the small beamwidth and short range of N2N antennas. Thus the need for a MAC protocol which solves the BCAD problem as it arises with cohorts. Previous work on directional MAC protocols is mostly aimed at ad hoc sensor networks (mobility is not considered), with few exceptions [24,25,26]. Most often, these MAC protocols rest on the RTS/CTS scheme proper to V2V communication standards, which makes them unsuitable.

A MAC protocol designed recently (details are out of the scope of this paper) achieves bounds  $\Delta_x(f)$  smaller than bounds given below (tight bound formulae are more involved). Delays  $A$  and  $A'$  depend on the MAC protocol, as well as on the number of N2N radio channels available (7 channels with IEEE 802.11p). Let us assume single frequency band N2N radio devices. For creator  $X$  of rank  $k$ , we have:

$$\Delta_x(f) < 4\lambda [h + 3(f+2)] \quad \text{where } h = \max \{k-1, n-k\}.$$

Trivially, when creator  $X$  is  $CT$  or  $CH$ :  $\Delta(f) < 4\lambda [n-1 + 3(f+2)]$

These worst-case bounds are close to actual bounds for internal N2N messages. Most often, they are pessimistic for imported messages (imagine that a V2V message is received by 1 every 2 members, which trigger  $\Pi$  quasi-simultaneously).

Assuming a N2N channel bandwidth in the order of 15 Mbits/s, typical values for  $\lambda$  would range between 0.3 ms and 1.2 ms. Let us choose  $\lambda = 1$  ms. Consider  $n = 20$ , and  $k = 14$ . One finds (bounds (in ms)):

$$\Delta_x(4) < 124 \quad \Delta_x(0) < 76 \quad \Delta(5) < 160 \quad \Delta(0) < 100$$

Under the Synchronicity option and for internal N2N messages, distances travelled at 90 km/h until cyber-physical actions  $\Psi(m)$  start being instantiated would range within bounds smaller than 4 m ( $\Delta(5)$ ) or 1.9 m ( $\Delta_x(0)$ ). Observe that bound  $\Delta(0)$  is smaller than the 100 ms figure frequently quoted for delivering a “critical” V2V message, which is a goal set to designers, not a proven bound. In fact, it is easy to demonstrate that the 100 ms requirement cannot be met with CSMA-CA channels, under realistic (between average and worst case) load conditions. A cohort-wide N2N dissemination algorithm such as  $\Pi$  outperforms any CSMA-CA V2V scheme with acks and repetitions whenever  $f > 0$ . Note that assuming the same  $f$  for V2V and N2N communications favors CSMA-CA V2V schemes, since medium-range omnidirectional communications are less reliable than short-range directional communications.

## 5 Conclusions

We provide novel results regarding the merits of short-range neighbor-to-neighbor (N2N) directional communications as regards safety in networks of automated vehicles. Notably, we show how N2N communications can be used for solving problems that have no solutions with medium-range omnidirectional communications. These results add to the existing literature on short-range directional radio and/or optical communications. It may be that time is right for standardizing N2N radio communications. They are based on mastered technologies, similar to standardized V2V radios, thus potentially low-cost. Given the very high level of safety achievable with a combined reliance on cohorts, N2N communications, and dissemination algorithms—in addition to robotics, it may be conjectured that safety authorities and insurance companies could be motivated for supporting the adoption of solutions akin to those presented in this paper.

## 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. M.L. Sichitiu and M. Kihl, “Inter-vehicle communication systems: A survey”, IEEE Comm. Surveys & Tutorials, vol. 10, 2, 2008, pp. 88-105.
3. K. Karlsson et al., “Field measurements of IEEE 802.11p communication in NLOS environments for a platooning application”, IEEE VTC Fall-2012, 5 p.
4. F.J. Ros et al., “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.
5. 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.

6. 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.
7. 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.
8. L. Bao and J. Garcia-Luna-Aceves, "A new approach to channel access scheduling for ad hoc networks", 7<sup>th</sup> ACM Int'l. Conference on Mobile Computing and Networking, 2001, pp. 210-221.
9. J. Grönkvist, "Assignment methods for spatial reuse TDMA", First IEEE Workshop on Mobile and Ad Hoc Networking and Computing, 2000, pp.119-124.
10. 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.
11. S.V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks", 4<sup>th</sup> IEEE Int'l. Conference on ITS, 2001, pp. 962-967.
12. S. Katragadda et al., "A decentralized location-based channel access protocol for inter-vehicle communication", *IEEE VTC Spring-2003*, pp. 1831-1835.
13. D. Swaroop and J.K. Hedrick, "String stability of interconnected systems", *IEEE Trans. Automatic Control*, vol. 41, 3, March 1996, pp. 349-357.
14. C. Lei et al., "Impact of packet loss on CACC string stability performance", 11th Intl. Conference on ITS Telecommunications (ITST 2011), Aug. 2011, pp. 381-386.
15. M. Sepulcre et al., "Cooperative vehicle-to-vehicle active safety testing under challenging conditions", *Transportation Research, Part C-26*, Elsevier, 2013, pp. 233-255.
16. 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.
17. C. Bergenheim 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.
18. G. Le Lann, "Cohorts and groups for safe and efficient autonomous driving on highways", *IEEE Vehicular Networking Conference (VNC)*, Amsterdam (NL), Nov. 2011, pp. 1-8.
19. G. Le Lann, "On the power of cohorts - Multipoint protocols for fast and reliable safety-critical communications in intelligent vehicular networks", *ACM/IEEE/IFAC/TRB ICCVE-2012, Beijing, Dec. 2012*, pp. 35-42.
20. 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, pp. 496-506.
21. N. Lyamin et al., "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks", *IEEE Communications Letters*, vol. 18, 1, Jan. 2014, 110-113.
22. N.A. Lynch, *Distributed Algorithms*. Morgan Kaufmann. ISBN 1-55860-348-4 (1996), 872 p.
23. S F. Dressler et al., "Inter-vehicle communication: Quo vadis", *IEEE Communications Magazine*, June 2014, pp. 170-177.
24. R.M. Yadumurthy et al., "Reliable MAC broadcast protocol in directional and omnidirectional transmissions for vehicular ad hoc networks", *ACM VANET'05*, Sept. 2005, pp. 10-19.
25. O. Bazan and M. Jaseemuddin, "A survey of MAC protocols for wireless ad hoc networks with beamforming antennas", *IEEE Communications Surveys & Tutorials*, vol. 14, 2, 2<sup>nd</sup> quarter 2012, pp. 216-239.
26. T.D.C. Little et al., « Directional communication system for short-range vehicular communications », *IEEE Vehicular Networking Conference (VNC)*, New Jersey, Nov. 2010, pp. 231-238.