EMERGENCY INFORMATION DISSEMINATION IN MOBILE NETWORKS FOR VEHICLES

Ioan Chisalita and Nahid Shahmehri
Department of Computer Science, Linköping University, SE-581 83, Linköping, Sweden

Keywords: Safety vehicular communication, reactive protocol, safety information, vehicular networks.

Abstract: Due to the unacceptably high number of accidents with severe consequences, in-vehicle safety systems that provide a better service to drivers are needed. One of the key technologies for supporting the development of efficient safety systems is vehicular communication. In this paper we propose a reactive protocol for disseminating emergency notifications to vehicles in traffic. The communication performance and the protocol usefulness for help avoiding accidents are investigated via computer simulations. The results of the evaluation indicate that timely and reliable communication can be provided by the proposed protocol.

1 INTRODUCTION

Every year, more than one million people die worldwide on the roads (Evans, 2004). In addition, the financial impact of traffic accidents is enormous: for example, in 2003 the total of accident-related losses reported in the U.S. was more than $230 billion (Biswas, Tatchikou & Dion, 2006). For improving traffic safety, extensive investigations into the causes of accidents and crash countermeasures have been conducted over the course of the last decade (Bishop, 2000). Many of these studies have identified driver error as the major cause of crashes (i.e. 90 %). Consequently, a great deal of effort has been directed towards helping drivers and reducing operator error. On-board safety systems are considered to have a great potential for reducing the number of accidents, e.g. reductions with up to 70 % were predicted for specific crashes (DOT, 2003).

Safety systems that make use of data wirelessly exchanged between vehicles are able to efficiently act towards avoiding collisions (Miller & Huang, 2002). These systems extend the perception of vehicles in comparison to safety systems based only on sensors such as radar. They are also capable to cope with complex traffic situations. However, the development of a communication system that provides support to in-vehicle safety systems pose difficulties due to the specifics of the environment in which the exchange of data takes place. In the traffic environment, the vehicles can constantly change their position, heading and velocity. They also join and exit the traffic in a relatively random manner, and can rapidly pass through zones with very different transmission patterns. In addition, the development of traffic safety applications requires communication systems that can assure low latency and high reliability (Biswas, Tatchikou & Dion, 2006).

Considering the above aspects, the dissemination of safety information was considered to benefit from the use of direct communication between vehicles that form an ad-hoc network (Chisalita & Shahmehri, 2006). This type of communication implies that no servers are involved in controlling the exchange of data, and the network is organized and maintained by vehicles alone. In this paper we consider the above approach, and propose a reactive protocol for effectively distribute notifications about dangerous situations that occur in traffic.

The rest of the paper is organized as follows. Section II presents related work. Section III provides an overview of the proposed protocol. Section IV presents details on the reactive operation of this protocol. Section V presents an evaluation of the protocol. Finally, section VI summarizes the paper and presents future directions.

2 RELATED WORK

Work in vehicular communication has been mostly focused on three aspects: network management, medium access, and communication protocols. The

Chisalita I. and Shahmehri N. (2006).
EMERGENCY INFORMATION DISSEMINATION IN MOBILE NETWORKS FOR VEHICLES.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 284-289

work presented in this paper relates to the last aspect, and we survey below related contributions.

Various routing protocols have been proposed for distributing data in mobile ad-hoc networks (Royer & Toh, 1999). However, since these protocols require the sender to know the identities of the receivers, their applicability to safety vehicular communication is limited (Biswas, Tatchikou & Dion, 2006). Also, the establishment of routes from sender to destination(s), and their maintenance, is time and bandwidth consuming. Consequently, most of the protocols proposed for routing in ad-hoc networks do not map well for safety vehicular communication.

Several specific protocols have been proposed for dissemination of data between vehicles. These protocols can be classified as reactive or proactive. Reactive protocols employ the sending of notifications to warn oncoming vehicles. Proactive protocols provide traffic data in a regular manner. In this case, the vehicles have a constant and up-to-date view of the traffic. Using proactive protocols, safety systems can have early information and are able to predict well in advance the possibility for an accident to occur. Consequently, they can efficiently act towards eliminating it. In comparison, safety systems supported by reactive protocols can only limit the consequences of dangerous situations that have already occurred. However, there are situations in traffic that require the sending of notifications, or in which the vehicles can benefit by having explicit notifications about road hazards.

Several communication protocols for distributing notifications to vehicles have been previously proposed. Briesemeister (2001) introduced a protocol for implementing a warning system for traffic jams. This protocol employs a method of estimating the size of the traffic jam for controlling the distribution of messages. However, this solution cannot be generalized for supporting other traffic applications. Yang et al. (2004) proposed a protocol for distributing warning messages that use an analytic approach for adapting the transmission rate. Nevertheless, this proposal applies only for notifications about rear-end accidents. A broadcast protocol that performs relaying of notifications based on an estimation of the transmission area covered by nearby vehicles was proposed in (Sun at al., 2000). However, Briesemeister (2001) demonstrated that the technique can be unreliable.

We propose a protocol that is both proactive and reactive. The proactive operation allows an efficient organization of the vehicular network, and delivers data used by in-vehicle safety systems to identify hazards in traffic (Chisalita & Shahmehri, 2006). The reactive operation considers the specific organization of the network when distributing emergency data in traffic. We note that even when using reactive protocols, the vehicles usually still need to regularly exchange some identification data in order to be able to organize the network. We have extended the use of this data for realizing the proactive component of the protocol. In previous work we report on the network organization and the proactive operation (Chisalita, 2006). In this paper we focus on the reactive operation of the protocol.

Our work in the context of the DSRC standard (ASTM, 2003) is discussed below. DSRC (Dedicated Short Range Communication) was initially proposed for vehicle-to-road communication and recently extended for vehicle-to-vehicle communication. The standard specifies the MAC layer, the link layer and the radio layer for vehicular communication systems. However, DSRC do not address multihop communication and network organization. We propose techniques for managing the vehicular network, and for forwarding information. Our work is complementary to DSRC. The protocol we propose can also be implemented using DSRC radios and channels, and can be used for augmenting DSRC functionality when providing safety services.

3 SAFETY VEHICULAR COMMUNICATION OVERVIEW

In safety vehicular communication, traffic data needs to be transferred in a timely manner between vehicles that may not know about each other. Reactive protocols should also aim to deliver notifications to as many hosts as possible, which may require data transmission in large areas. However, the receiving hosts should be enabled with filtering capabilities as they may not be interested in all the received messages. Considering these requirements, we controlled the delivery of safety information by two methods.

First, we define a method for organizing the vehicles. Vehicular network organization is essential for obtaining scalable and reliable communication. Therefore, we propose the grouping of vehicles in manageable clusters that are defined based on the current interest in traffic of the vehicles. Each vehicle creates and maintains its virtual cluster, which is defined as a *local network* (Chisalita, 2006). An example is presented in Figure 1. The data needed for performing the network organization is provided via the proactive operation of a dedicated communication protocol (Chisalita & Shahmehri, 2006). Thus, if data provided by a vehicle is considered useful, the receiver registers this vehicle in its local network. Further on, if the information about the sender is not updated within a time interval, the sender is removed from the local network.

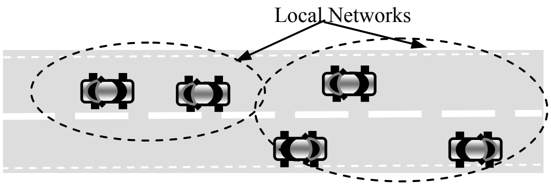

Figure 1: Example of local networks.

The determination of the level of interest is performed using a set of traffic-related rules. The criteria used for defining these rules were:

- *Vehicle position.* This data is needed by in-vehicle safety systems for identifying dangerous situations, e.g. (Sun et al., 2000).
- *Service area extent.* Research in traffic safety has indicated that vehicles in proximity usually have important data (e.g. vehicles situated within 300-500 m), e.g. (Yang et al., 2004).
- *Local network composition.* Traffic analyses have indicated that the number of vehicles that can provide useful data is limited (e.g. 15-20) (Asher & Galler, 1996).
- *Parameters of the driving situation*, e.g. relative distance between vehicles, relative heading, road status, vehicle status, road type. Accident reports indicated that these parameters are strongly related to crashes (DOT, 2003).

The size of a local network was denoted as Service Area Threshold (SAT) and was initially set to 300 m. The maximum number of hosts in a local network was denoted as MNH, and was set to 20. The suitability of these values (i.e. for SAT and MNH) was then validated via simulations (Chisalita, 2006).

Further on, we propose an anonymous context-based protocol for delivering safety data among vehicles. This protocol is a scoped broadcast where the identities of the destinations are not known by default. Therefore, the vehicles are required to analyze the received messages in order to determine if they are the intended destination. The data used in proactive operations is encapsulated in Basic Safety Messages (BSMs) that are regularly sent at short intervals. These messages contain data needed by on-board safety systems for assessing hazards in traffic. Examples are position, velocity, heading and status of vehicles, and data about the road type and status. Data included in BSMs is also used for determining the level of interest for senders, and for organizing the vehicular network. Filtering and forwarding of BSMs are performed using a set of traffic-related rules that make use of contextual information (Chisalita & Shahmehri, 2006).

Data about hazards that occur in traffic is encapsulated in Warning Messages (WAMs). These messages are issued when an in-vehicle safety system detects a hazard in traffic and considers that other vehicles should be announced about it. The safety system should also specify the transmission and digest of WAMs, e.g. sending frequency and time validity. In our work we have mostly focused on supporting the efficient distribution of notifications rather than providing specific techniques for disseminating WAMs in particular traffic situations. Thus, we propose a general mechanism for issuing notifications that can be further specified for diverse safety applications. Warning messages can be disseminated in an area specified by a local network, or in larger areas. These messages are by default accepted by vehicles. However, we also provide means for defining the conditions that need to be fulfilled for warning messages to be accepted.

4 WARNING MESSAGES DISTRIBUTION

We introduce in the followings the techniques that we have proposed for generating and forwarding warning messages.

4.1 WAMs Generation and Content

Warning messages are generated when dangerous events occur in traffic. A WAM is generated when a safety system detects a hazard that can pose dangers to other vehicles. The message can then be issued a number of times in order to increase the probability of being received by other vehicles. If the danger persists, other WAMs can be generated.

As previously mentioned, a received warning message is usually accepted by a vehicle. However, the protocol can be configured so that the receivers perform filtering of WAMs. For this, two options were included within WAMs. The first addresses the acceptance of notifications issued by hosts from the same local network. Thus, it is possible to issue WAMs that should be received only if the sender is part of the receiver's local network. For implementing this option, we provided a field *default acceptance* in WAMs. The second option refers to the emergency degree of the traffic situation that required the WAM to be sent. Thus, WAMs contain indications of the *criticality* of the situation. We use this term to indicate how dangerous a traffic situation is at a certain moment in time. Two parameters are used to describe dangerous traffic situations: *criticality type* and *criticality level*. The criticality type provides a high-level description of the situation. The criticality level is a parameter that provides the possibility to set a numeric value for indicating the level of emergency associated with a dangerous situation. The criticality level and type can be used for deciding if a WAM should be accepted or not.

The WAMs structure is presented in Table 1. Each warning message contains the sender identity and the moment when the message was sent. These two fields uniquely identify the transmitted message. WAMs also contain the position of the dangerous situation or event, and a short description of it. Other types of information included in WAMs are the criticality type and level, a retransmission counter, and the default acceptance indication. Additional information concerning dangerous situations can be also provided using the reserved field *Other data*.

Table 1: Warning Message.

Message type	Hazard position
Host identity	Retransmission counter
Sending moment	Hazard description
Criticality type	Criticality level
Other data	Default acceptance

4.2 WAMs Forwarding

As WAMs contain indications about dangerous situations in traffic, they are subject to retransmissions. Delivering a warning message to as many hosts as possible in a short time was the desideratum, and we took advantage of the redundancy provided by a flooding-alike technique. Thus, the retransmission of WAMs is controlled by counters. Each WAM includes a retransmission counter that indicates how many times it was retransmitted. When a host retransmits a warning message, the retransmission counter is decreased and the new value is included in the (re)transmitted message. A host that received and considered a warning message, it retransmits it if the message was not previously retransmitted and if the retransmission counter is higher than zero. The retransmission counter is set to a higher value if the (original) issuer of a WAM decides that it is of importance to disseminate the message in a larger geographical area. We defined the retransmission counter on the basis of the maximum number of hosts (i.e. MNH) that can coexist in a local network. Thus, the retransmission counter was specified as β*MNH, with $\beta = 1$ for large area notifications, and $\beta = 0.5$ for notifications within a local network.

A problem related to WAMs retransmission is that the same message can be forwarded at the same moment by a number of hosts close to each other. This lead to a peak-load on the channel, which can in turn reduce the communication quality. Even more, it can lead to information loss. For alleviating the consequences of this behavior, we enforce the deferring of retransmitted WAMs. Thus, each host waits a short time interval before retransmitting a WAM. One possibility is to randomize this interval. We implemented this approach by randomly selecting a deferring interval between 0 and 0.1 s. Another possibility is to calculate a deferring interval that is inversely proportional to the distance to sender. This approach allows distant vehicles to relay messages faster, leading to a more rapid propagation of data in an extended area. We implemented this approach by specify the interval for deferring the WAM retransmission as:

$$Tdefer = \left\{ \begin{matrix} \left\{ \begin{matrix} Tdr * k * \dfrac{SAT}{D}, Tdefer < T\max \\ T\max \end{matrix} \right\}, D < k * SAT \\ Tdr \end{matrix} \right\}$$

In the above formula, *D* is the distance to sender, *SAT* is the size of the communication service area, *k* is a system parameter, *Tmax* is a maximum value for the deferring interval, and *Tdr* is a regular value for deferring the WAMs retransmission.

5 EVALUATION

An evaluation environment was developed by integrating the proposed communication protocol within a well-known network simulator, i.e. GloMoSim. Traffic simulators have been developed for generating movement patterns close to those of real vehicles. For evaluating the performance of the reactive component of the protocol, we used the *delivery delay for WAMs*, and the *WAM dissemination success*, i.e. the number of vehicles that should receive a WAM reported to the number of vehicles that received it. These metrics were evaluated when WAMs were transmitted in the presence of dissemination of BSMs.

The free parameters that we have used were:

- Load density, 6 - 20 [vehicles/km/lane].
- Vehicles mobility, maximum speed: 10 - 40 [m/s].
- Service area threshold (SAT), 50 - 600 [m].

Beside the communication performance, the system usefulness for help avoiding accidents was investigated. We examined if specific crashes can be avoided by using a collaborative safety system based on reactive vehicular communication. We first simulated the accidents and the safety system operations in order to derive requirements on communication (e.g. latency) (Chisalita, 2006). We then investigated if WAMs sent by specific vehicles can fulfill these requirements.

When investigating the communication performance, we used a general traffic scenario modeling a two-lane bi-directional road. The movement of the vehicles was specified using a car-following model given in the literature (Chisalita, 2006). For investigating the system usefulness to accident avoidance, we used realistic accidents modeled using their descriptions given in crash research (DOT, 2003).

The evaluation was performed for a BSMs frequency of 10 BSMs/second. The tests were performed using the standard radio layer of GloMoSim (i.e. based on IEEE 802.11), and CSMA as the MAC scheme. The propagation model was two-ray and the nodes had a transmission range of 320 m. For investigating the success of disseminating WAMs, we define a *zone of interest* that contained the vehicles that should receive specific WAMs. For particular accident scenarios, this zone contained all the vehicles in the simulation. For the general traffic scenario, the zone was the extent of a local network when WAMs were generated only within local networks. When WAMs were generated in larger areas, the zone contained vehicles in behind on the same lane, and vehicles in front on the opposite lane, situated at less than 500 meters from the vehicle that issued the WAM (when the WAM was generated).

For evaluating the communication performance we randomly selected hosts that generated WAMs. The moments when these messages were issued were also randomly selected. When not varied, the SAT was 300 m, the maximum achievable velocity was 25 m/s, and the network load was 6 veh/km/lane. The initial settings for the deferring approach based on the distance to sender were Tmax = 0.2 s, Tdr = 0.05 s, and k = 3.

We exemplify in Figure 2 the delay for WAMs dissemination in a large area as a function of network load. The graph shows the metric variations for both deferring approaches, and present average and maximum delay values. For low and high network loads, the delay had larger values. For low network loads, a small number of vehicles could retransmit the issued WAMs. Consequently, more retransmissions were needed for WAMs to reach distant vehicles, which induced longer delays. For high network loads, the contention for accessing the medium was accentuated, and the vehicles waited a longer time before being able to send WAMs. Consequently, the delay increased. In these tests, the random deferring technique assured smaller delays that the technique based on the distance to sender.

The results of the evaluation indicated that large area dissemination of WAMs (e.g. till 3.5 km) with relatively low delays (e.g. 0.8 seconds) is possible with the proposed protocol. We note that delay values less than 1 second were considered appropriate for delivering emergency notifications in large areas (Briesemeister, 2001).

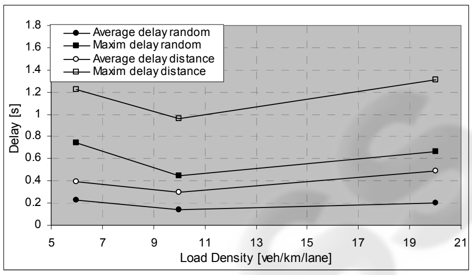

Figure 2: Delay – load density.

The information dissemination success was 100 % when the random deferring technique was used. However, for the technique based on the distance to sender the metric has decreased to 86 %, which indicated that this approach was less reliable.

We also investigated the dissemination of WAMs only within a local network. In this case we employed the random approach for deferring the WAMs retransmission. The results revealed patterns similar to the previous tests, but with considerably lower values for the delay. For instance, the highest value of the maximum delay was 4 times lower for WAMs dissemination within local networks. The information dissemination success was again 100%.

As previously mentioned, we have also investigated the usefulness of the proposed protocol in avoiding collisions. These tests involved a significant number of relevant traffic accidents (Chisalita, 2006). We exemplify in here these analyses with an intersection scenario that is introduced in Figure 3. Two vehicles, V1 and V2, are involved in a crash as follows. V2 is initially stopped and then tries to pass the intersection. The driver in V2 fails to notice the approaching vehicle V1. When the driver in V1 realizes that V2 indeed wants to pass the intersection, she/he tries to brake, but is too late and V1 crashes into V2.

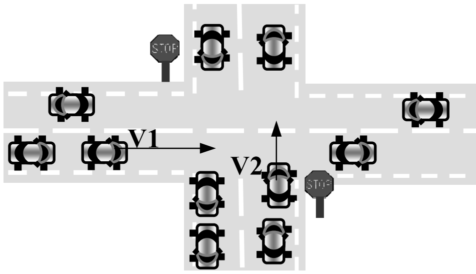

Figure 3: Intersection accident scenario.

The accident avoidance can be achieved by providing the driver in V1 with early information about V2's maneuver. Thus, we assumed that V2 sends a WAM when it starts to pass the intersection because it comes from a non-priority road. We then investigated if this WAM can be successfully received in time by V1 and by other vehicles in the simulation. The analysis indicated a delay of 0.64 ms for V2's WAM. This value was considerably lower than the latency required for avoiding the initial accident, i.e. 0.5 s. In addition, all the other vehicles received the WAM with similar delays.

To summarize, the proposed protocol allows for WAMs distribution with small delays in large areas and very low latencies in small areas. The delay values also fulfill the requirements of safety applications, and are similar to, or lower than, results obtained by pure reactive protocols (e.g. Yang et al., 2004). The high values of the dissemination success show that the emergency notifications were received by the hosts in need. In addition, investigations of accidents avoidance indicate the proposed solution to effectively support in-vehicle safety systems.

In previous work we have obtained good communication performance for the proactive operation of the protocol (Chisalita & Shahmehri, 2006). In this work we also investigated the communication performance when both the proactive and the reactive modes were active. The results indicated that the reactive operation did not pose significant overload on the communication.

6 CONCLUDING REMARKS

This paper focuses on the distribution of emergency notifications to vehicles in traffic. We propose a technique for disseminating warning messages that can fulfill requirements of safety applications. Simulation results indicate that the communication performs well in various conditions.

Future work includes investigations of alternative techniques that can provide even lower delivery latency while maintaining high dissemination success. Further specification of the content and digest of warning messages for implementation of specific safety applications is also of interest.

REFERENCES

Evans, L., 2004. *Traffic safety*, Bloomfields Hills, MI, Science Serving Society.

Chisalita, I., 2006. *Communication and networking techniques for traffic safety systems*, PhD Thesis, ISBN 91-85523-77-X, Linköping University, Sweden.

Zador, P., Krawchuk, S. & Voas, R., 2000. *Final report - Automotive Collision Avoidance System (ACAS) program*, Delphi-Delco Electronic Systems, U.S.A.

Bishop, R., 2000. Intelligent vehicle applications world-wide. *IEEE Intelligent Systems*, vol. 15, pp. 78-83.

Biswas, S., Tatchikou, R., & Dion F., 2006. Vehicle-to-vehicle wireless communication protocol for enhancing traffic safety. *IEEE Communications Magazine*, pp. 74-82.

DOT, 2003. *Intelligent Transportation Systems*, U.S. Department of Transportation, http://www.its.dot.gov/.

Miller, R., & Huang, Q., 2002. An adaptive peer-to-peer collision warning system. *IEEE Vehicular Technology Conference*, Birmingham, USA, pp. 317-321.

Royer, E.M., & Toh, C.K., 1999. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications,* Vol. 6, Issue 2, pp. 46-55.

Briesemeister, L., 2001. *Group membership and communication in highly mobile ad hoc networks*, PhD thesis, Technical University of Berlin.

Yang, X., Liu, J., Zhao, F., & Vaidya, N.H., 2004. A vehicle-to-vehicle communication protocol for cooperative collision warning. *Conference on Mobile and Ubiquitous Systems: Networking and Services*, pp. 114-123, Boston, USA.

Sun, M.-T., Feng, W.-C., Lai, T.-H., Yamada, K., Okada, H., & Fujimura K., 2000. GPS-based message broadcast for adaptive inter-vehicle communications. *IEEE Vehicular Technology Conference*, pp. 2685 – 2692, Boston, USA.

ASTM, 2003. *Standard specification for telecommunications and information exchange between roadside and vehicles systems – 5 GHz band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY),* ATM 2213-03.

Asher, H.J., Galler, B.A., 1996. Collision warning using neighboring vehicle information. *Intelligent Transportation: Realizing the Benefits*, Houston, Texas, USA.

Chisalita, I., Shahmehri, N., 2006. Adaptive dissemination of safety data among moving vehicles. *IEEE Personal, Indoor and Mobile Radio Communication Symposium*, Helsinki, Finland, in press.