

# System Design for Information Dissemination in VANETs

Marc Torrent-Moreno\*, Andreas Festag†, and Hannes Hartenstein\*

\*Institute of Telematics, University of Karlsruhe, torrent@tm.uni-karlsruhe.de, hartenstein@rz.uni-karlsruhe.de

†NEC Deutschland GmbH, festag@netlab.nec.de

**Abstract**— In the architectural design of a communication technology the assignment of responsibilities to its different modules or layers is a key issue. The modularization and assignment of functions to modules has a strong impact on the system performance. In this paper, we address data forwarding as a key responsibility of a VANET's (Vehicular Ad hoc NETwork) communication device. More specifically, we discuss two different approaches, *packet-centric forwarding* (PCF) and *information-centric forwarding* (ICF), both aimed to disseminate information in a VANET environment. Basically, assuming a layered protocol design adapted to VANETs, it is argued where and how functions related to node connectivity and data transport could be implemented.

Discussing pros and cons of ICF and PCF, we define a modular information-based architecture with a hybrid approach for dissemination of safety information where: *i*) information forwarding responsibilities reside in the application protocol layer(s) and exploit the applications' capability of information modification, aggregation, and invalidation, *ii*) packet forwarding functionalities are implemented in the network protocol layer to rapidly disseminate information of very high priority (*safety-of-life*), and *iii*) low-cost nodes incapable of processing safety-related information, can be used to increase network connectivity.

## I. INTRODUCTION

Currently, several initiatives around the world [1], [2], [3], [4], [5] are developing vehicular safety applications by means of short-range wireless technologies. These projects, often sponsored by governments, join the efforts of different companies, universities and standardization bodies [6]. All of them envision a future where equipped vehicles are able to create spontaneous networks (VANETs) and, communicating among themselves, turn roads into a safer place.

This document addresses VANETs as communication networks in which safety applications represent the primary use and safety data is disseminated via wireless communication in the network. Every communicating vehicle, referred to as node, acts as a receiver and a potential forwarder of data. As a receiver, a node decides whether to notify the driver about the safety information. As a forwarder, a node determines whether to forward the information to other nodes.

M. Torrent-Moreno and A. Festag acknowledge the support of the German Ministry of Education and Research (BMB+F) for the project 'NoW – Network on Wheels' under contract number 01AK064F.

VANETs differ from conventional communication networks in many aspects. We make the following observations:

### Type of communication, end-to-end notion revisited.

Typically, applications in conventional networks use unicast communications, i.e., peer protocol entities are well-defined by a node or group identifier. Safety applications, as primary application type in VANETs, address mainly geographical areas in which data needs to be distributed.

**Packet vs. information.** In conventional packet-switched networks, application messages are broken into smaller segments, termed packets, and individually transmitted across the network. The data payload in a packet remains unchanged until reaching its destination. However, information about road safety is commonly regarded as timely and spatial temporal *state information* that is distributed (exchanged) among the nodes in the communication network; each node evaluates the received safety state, merges it with the local state, and then decides how to communicate the updated state information. This operation, that allows to aggregate, modify and invalidate the information to be forwarded, is commonly referred to as *in-network* processing. Further, it is a known concept in wireless networks, and also applied to VANETs non-safety applications in [7].

### Application requirements vs. medium conditions.

VANETs' communication protocols will have to cope with *i*) an unreliable radio channel, where wireless signals strongly fluctuate due to multi-path propagation, and *ii*) highly dense scenarios with many nodes sharing a limited wireless medium when fully deployed. Therefore, the design of smart (meaning robust and efficient) strategies is needed in order to achieve the high reliability required by VANETs' safety applications.

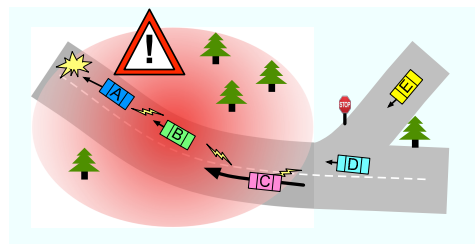


Fig. 1. Dissemination of safety information in a VANET. Vehicle A realizes an emergency situation and determines that it is relevant to all nodes inside the shadowed area.

Due to VANETs' specific characteristics and requirements we proposed in [8] a communication system with a tailored architecture. Still though, a smart assignment of responsibilities to the different communication entities is required to ensure an optimal performance of safety applications in vehicular environments.

This document presents a system design with a reasoned assignment of responsibilities to the different entities of a VANET's communication system. More specifically, we make use of the fundamental functionality of *information dissemination* (Fig.1) to question the commonly accepted definition of multi-hop data forwarding as network protocol layer functionality. Afterwards, taking into account the most relevant aspects of VANETs' applications and environments we reason and depict a system design addressing the correspondent communication challenges of the different vehicular scenarios.

Based on two different strategies for information dissemination in VANETs, i.e., packet centric forwarding (PCF, network layer) and information centric forwarding (ICF, application layer), we develop a *hybrid* communication approach with the following key features:

- Forwarding of *safety* information executed by application (not managed by network layer).
- Capability of aggregation, modification, and invalidation of safety information during the dissemination process.
- Packet forwarding supported at the network layer for specific types of information, e.g., of *safety-of-life*.
- Capability of adaptation to channel state.
- Support of a heterogeneous network architecture with *smart* and *dumb* nodes.

The remaining sections of the document are organized as follows: Section II describes the relevant aspects (and assumptions) for dissemination of safety information in VANETs and presents the reasoning for our proposal of a hybrid approach. Section III presents a simple, modular, and robust system architecture that fulfills the requirements of our hybrid approach while offering sufficient flexibility for future applications and interaction between different types of nodes. Section IV discusses the most relevant functionality in a VANET's communication system, i.e., information dissemination, and its related work. Finally, Section V gives an outlook and concludes the document.

## II. ASPECTS OF VEHICULAR COMMUNICATIONS

In this section we first list the most relevant aspects or/and assumptions that have to be taken into account when designing a VANET's communication system. Then, we describe two approaches for information dissemination, and finally we justify the derived system.

### A. Characteristics/Assumptions

**Two different types of nodes:** In VANETs we distinguish between *smart* and *dumb* nodes. A smart node has relatively strong computational resources, typically access to

on-board sensors of cars, and executes a number of applications for traffic safety and driving comfort. In contrast, a dumb node is a cost-efficient device with limited computational capabilities, typically but not only, installed as cheap road-side unit. From a complete system perspective, a dumb node works as a simple forwarder required to improve network connectivity with low penetration rates or in situations with low traffic density. Dumb nodes, therefore, will not be able to process the information contained in the message payload.

**Layered architectural approach:** Though the considerable differences existing between VANETs and conventional networks, we regard protocol layering as a reasonable approach to manage the complexity of VANET technology (e.g., [8]). Therefore, in this document we will refer to the different – OSI – layers, specially to network and application layer, when assigning the different functionalities for different types of information dissemination.

**Diverse types of applications:** We can classify VANET's applications in three main groups with respect to the relevance of their information: *safety-of-life*, *safety* and *non-safety*. All three, as their names suggest, present very different requirements with respect to reliability and delay. Hence, not only a prioritization but also different strategies might be required to satisfy their specific demands in a shared communication medium.

**Hazard detection:** We consider two different ways of detecting a hazard that potentially compromises road safety:

- *Warning message.* A vehicle receives a warning message from another node that detected the hazard, e.g., car crash message or icy road message.
- *On-board sensors and/or state information.* A node's safety application detects a new hazard processing the different state information gathered from other nodes and/or the on-board sensor's state, e.g., hard deceleration of the vehicle or two vehicles driving in different roads approaching an intersection at high speed.

The main difference between both groups is the node originating the information, i.e., the one that detects the hazard directly, by its 'own means'.

**Two opposite and challenging network situations:** In vehicular environments two scenarios can be identified that require two opposite communication strategies: sparse and dense networks. In dense networks, such as cities or major highways with a large portion of equipped vehicles, the data load on the channel should be controlled in order not to exceed the limited wireless bandwidth. In contrast, in sparse networks, such as in the introduction phase of such a technology, channel saturation is not an issue. Moreover, messages should be repeated since equipped vehicles are most likely out of wireless radio range of each other; vehicles inside the area of influence of a hazard, but not reachable at the time it is detected, should also be notified.

Note that in case of experiencing a dense network, the forwarding strategy is required to be very efficient in terms of overhead while ensuring high reliability to *priority* messages with the most important payload, i.e., *safety-of-life*.

**Safety information must be kept ‘alive’:** Safety hazards can be associated with a time duration and geographical area while/where they can potentially affect vehicles’ safety state. Therefore, and taking into consideration the existence of sparse network scenarios, we assume that the distribution of some state information will be repeated (e.g., periodically or at detection of a new neighboring vehicle) for a defined duration of time while being inside a specific geographical area. This time and area are commonly referred as *time of validity* and *area of validity*. The specific strategy to optimize this repetition process is out of the scope of this document. However, we discuss in Sec. III how the functionalities should be assigned in order to address the different VANETs’ requirements.

### B. Two Approaches for Information Dissemination

In this study, we identify two opposite approaches for information dissemination in VANETs: *packet-centric forwarding* and *information-centric forwarding*. Packet-centric forwarding refers to the conventional approach for packet-switched communication where the source breaks the information into data packets and address them to one or more network nodes. In VANETs, this group typically comprises nodes located inside a geographic area. With PCF the responsibility of information dissemination resides on the network layer, i.e., specific forwarding algorithms, located at the network layer in a stacked protocol architecture as in the OSI model, try to provide efficient and reliable delivery of these packets over potentially multiple wireless hops. In contrast, information-centric forwarding does not rely on an end-to-end semantic implemented in network layer: the safety information issued as single-hop broadcast by a source node is processed at every receiving node, and afterwards (modified or not) redistributed if required. With ICF, therefore, the responsibility of information dissemination resides on the application itself. Both, packet-centric and information-centric forwarding represent two extreme but valid approaches for dissemination of safety information. Making the simplifying assumption that a node (or communication system) is basically comprised of two main interconnected entities, a communication domain (radio modem, medium access, routing and transport protocols) and an application domain (see Sec. III), we describe both approaches in more detail: **Packet-centric forwarding (PCF):** With this approach, a vehicle realizing a hazardous situation by its ‘own means’ (i.e., not from a warning message) generates an information and creates a data packet containing the application payload (commonly, type of emergency and location and time it was noticed). To disseminate the packet geographically by the network layer<sup>1</sup> the application also determines, for the packet header, the *area of validity* and the *time of validity*. In order to keep an information ‘alive’ inside the *area of validity*, being capable to forward the message to nodes outside of radio range, nodes receiving a message store it at the network layer (during the *time of validity*).

<sup>1</sup>The specific packet dissemination strategy is out of the scope of this document. However, some aspects are discussed later in Sec. IV.

**Information-centric forwarding (ICF):** With this strategy, when a vehicle detects a hazard it ‘single-hop’ broadcasts a packet (containing the type of hazard, the point of time and the location when and where the hazard was noticed). A vehicle that receives this message will deliver the message directly to the correspondent application, without any further action required from the network layer. Then, the application in turn merges the new information with the (locally-stored) safety information and decides about further procedures with respect to the hazard, i.e., whether and when to issue a new single-hop broadcast to the wireless channel.

### C. Motivation for a Hybrid Approach

In the previous subsections we have presented relevant aspects with respect to VANETs and two valid approaches for information dissemination, ICF and PCF. In this subsection we will point different benefits and drawbacks of both strategies due to the different VANETs’ aspects and scenarios in order to assist the design process of the most appropriate communication system.

**Existence of dumb nodes:** *Dumb nodes* are an extremely important requirement for a successful initial deployment of a VANET, when only a small portion of equipped vehicles exist. Dumb nodes can act as simple data forwarder being able to temporary cache information and adapt its forwarding behavior to changing conditions in their vicinity. The limitation of dumb nodes is the fact that applications are not available as in smart nodes. The required compatibility with nodes that are not able to process or understand the information in a message payload makes a solution inappropriate where solely ICF is implemented. Consequently, the required existence of dumb nodes favors the use of the PCF approach, specially in the first years of a potential deployment of such as system.

**Scalability:** ICF presents a clear benefit with respect to *scalability*. We assume that the available wireless bandwidth is limited and also that, in dense networks, vehicles in the vicinity might detect same or related safety events. Since with ICF the application would process the payload of a data packet, ICF facilitates the aggregation, modification, and invalidation of information. These procedures can considerably reduce the overhead created by redundantly transmitted information. Consequently, some portion of wireless bandwidth can be ‘saved’ with respect to a same hazard being noticed by different sources, specially when keeping a (variable over time) information ‘alive’.

**Safety-of-life messages in dense network situations:** In case an emergency is detected in a dense network a strategy capable to disseminate the information in an extremely reliable, efficient and rapid manner is required. In this situation, where there is a *safety-of-life* message, ICF capabilities (aggregation, modification, and invalidation) are not so important. PCF offers the benefit of easily track the messages to avoid redundant –harmful– message duplicates in a simple and rapid way at network layer, i.e., safety critical packets should not be modified nor processed by the

application before being forwarded. Therefore, this strategy can be implemented as a service of the (common to all applications and types of nodes) communication domain.

The conclusion of this argumentation points to a hybrid approach. A strategy combining both PCF and ICF would enable receivers of a safety message to include both remote and local knowledge before forwarding the safety information. At the same time, geo-addressing capabilities are offered from the network layer, e.g., for dissemination of *safety-of-life* data, and the compatibility of *smart* and *dumb* nodes is ensured. In the following section we present a proposal of an appropriate system design for information dissemination that fulfills all requirements presented above while trying to keep a clean and modular architecture.

### III. HYBRID APPROACH FOR SYSTEM ARCHITECTURE

In the previous section we have argued for:

- assignment of the responsibility of message forwarding at the different applications,
- implementation of a reliable and efficient geocast strategy at the network layer, and
- compatibility between smart and dumb nodes.

Based on these fundamental decisions we introduce a software architecture that allows a clear system design and an unambiguous assignment of functions. The software architecture structures the function set of a VANET node in the two different architectural domains mentioned above, an *application domain* and a *communication domain*.

We regard the *application domain* as a component that comprises all safety applications. These applications gather all safety information available to inform the driver of unsafe situations and assist other nodes forwarding relevant safety data.

The *communication domain* is composed of all mechanisms and protocols needed to deliver the relevant information to the correspondent destinations with the reliability required by the different applications (when possible).

Note that a strong coupling between the *application* and the *communication domain* is implied. Applications must assist the *communication domain* in their task of delivering information respecting its relevance. At the same time, applications can benefit from the knowledge of the capacity limitations and actual status of the wireless channel.

Fig. 2 depicts a high level structure of the proposed system. The figure basically shows the two main building blocks of a VANET node, the *application domain* and the *communication domain*, with the most relevant functions for dissemination of safety information. *Application domain* and *communication domain* interact via interfaces for exchange of safety data to be sent to, or received from, other nodes and state information. While the detailed specification of both domains and the correspondent interfaces is beyond the scope of this document, this section describes *i)* how the required functions in a VANET node are assigned to appropriate domains and structured into functional blocks (Fig. 3), *ii)* the proposed data dissemination strategies for both types of safety messages, and *iii)* how the compatibility with dumb nodes can be achieved.

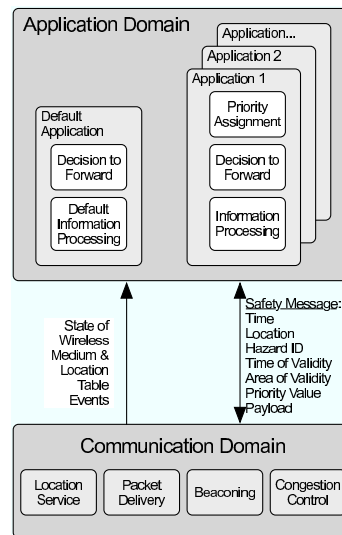


Fig. 2. High level view of the proposed architecture for VANET nodes.

#### A. Communication Domain

The *communication domain* is common to smart and dumb nodes, and provides the following main functions:

**Addressing:** The *communication domain* is capable of different address types. A unicast address identifies a single node and it is used for point-to-point communication. A broadcast address refers to all nodes within one wireless hop. A geocast address identifies all nodes that are located inside of a geographical area.

**Packet delivery:** Corresponding to the addressing type, the *communication domain* provides to applications different modes of packet delivery for unicast, broadcast, and geocast. The geocast mechanism must provide reliability and efficiency (i.e., to avoid redundant messages) in order to fulfill the requirements exposed in Section II-C and can make use of the *Location Table* (LT, where positions of other nodes are maintained as soft state). Broadcast messages, on the other hand, are considered as a one time (unreliable) transmission addressed to nodes in range only.

Note that although *non-safety* applications have not been taken into account in the previous sections, we have to address them shortly at this point in order to develop a common *communication domain* for all types of applications in VANETs. For this reason, we consider few instances of geocast packet delivery strategies (Fig. 3). The latter decision responds to the different reliability requirements of the possible future applications and the existing trade-off with overhead efficiency, e.g., higher reliability could be achieved for *safety-of-life* at the cost of higher, but controlled, redundancy.

**Congestion control:** The *communication domain* has the goal of ensuring a perfect stability of the network at all times: it avoids network congestion by monitoring the network utilization and controlling the packets transmission. Applications assist the congestion control in order to ensure that the safety importance of the different communications is respected. For this reason, we propose the use of a simple priority value; the application determines the

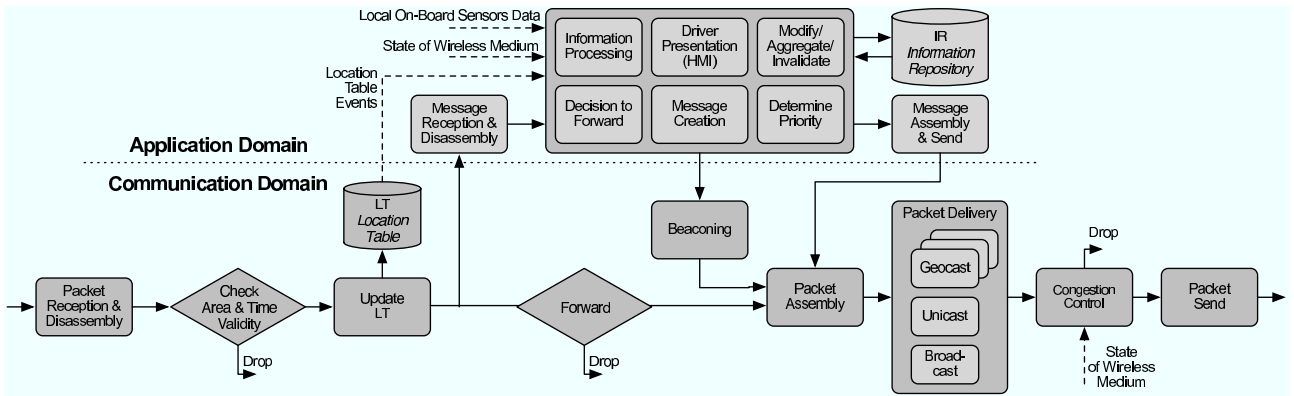


Fig. 3. VANET's node information flow with a generic smart application.

priority based on the relevance of the information and assigns the value to each message. This value is used by the *communication domain* to take adequate decisions when controlling the load on the channel. Basically, we consider that congestion control strategies combines a set of mechanisms including deferring packet transmission, smart discard of low-priority packets, and dynamic setting of transmission parameters on a per packet basis (e.g., power control [9]).

**Beaconing:** Beacons are periodic messages broadcasted by the *communication domain* to support both, the ad hoc routing/forwarding protocol and the applications. Apart from the position of a vehicle, beacons also contain state information common to relevant applications, e.g., speed and direction. On reception of a beacon, a vehicle is aware of their surrounding conditions and can, eventually, detect unsafe situations. Note that due to the different requirements between safety applications and routing/forwarding protocols, applications could motivate the increase of the message generation period, e.g., at high speeds or in the vicinity of an intersection. We also consider the possibility of sending more than the own state information, i.e., sending other's nodes learned state can increase the vicinity awareness further than one hop distance.

**Location Service:** The *communication domain* has to provide to the application a distributed algorithm that resolves the location of other nodes in the network. This module is also responsible of maintaining the Location Table to assist both routing/forwarding protocols and applications.

### B. Application Domain

The *application domain* is where all applications reside. Apart from the *default application* (addressed in Sec. III-D), all safety related applications include the following key functionalities:

**Information repository (IR):** In order to detect certain unsafe situations and be able to take the optimal decision in case an emergency occurs, each application contains a repository where the current surrounding status relevant to this specific application is kept. Local mechanisms and processes enable aggregation, modification, or invalidation of cached information when the IR is updated. Note that a

higher benefit can be accomplished when a central IR common to all applications exists. Possible benefits could be: memory efficiency, improved aggregation capabilities and interoperability between applications.

**Information processing:** When receiving state (safety) information, either from local sensors or through the *communication domain*, applications process the information and update the safety state of the IR.

**Driver presentation:** When detecting an unsafe situation the application assists the driver in preventing a potential accident. The presentation methods can differ between car companies and implementations.

**Forwarding state/safety information:** An application that detects or is aware of a certain hazard can decide to forward it either immediately (*safety-of-life*) or to trigger a forwarding process to periodically issue the information in application-specific intervals (*safety*). Also, it could motivate a higher frequency of *communication domain's* beacons if necessary. In the next subsection, the different types of addressing strategies suggested for the different types of safety messages is discussed.

**Priority determination:** Once the decision to issue some safety information to other vehicles is taken, applications determine a safety value based on a priority function. This function takes into account the type of hazard, duration of time that has passed since the hazard occurred, distance between the local position and the position where the hazard occurred, and the local state of the wireless medium (network congestion). The result of the function is a single priority value that is assigned to the message and passed to the communication system. The priority value will be used by the *communication domain*, within its congestion control module, in order to handle the message from a safety perspective.

Finally, another capability common to all applications should be considered. In order to save some bandwidth and channel access time, a module able to join different applications payloads into a single message should be implemented (*Message Assembly* in Fig. 3). The same capability could be implemented in the *communication domain's* module *Packet Assembly* in order to also combine beaconing information.

### C. Dissemination Strategies of Safety Information

After having introduced the main functionalities of both, application and communication domains, we describe how the different types of safety messages are managed by the proposed system:

**Safety-of-life messages** are non-periodic event-driven messages that are geocasted as a result of the detection of an imminent situation that endangers the life of drivers and passengers in vehicles by a system's own means. When node's application receives a *safety-of-life* message, the node recalls that the *communication domain* handles the immediate dissemination, i.e., PCF. Since the application does not need to re-forward the information, it just processes the information, stores it in the IR, and warns the driver if required. *Safety-of-life* messages contain the *priority* (highest value), the *time* and the *location* the event occurred, and the type of event (*Hazard ID*). The existence of dumb nodes, though, require two additional fields (see Sec. III-D), *time of validity* and *area of validity* where the message should be forwarded. For distribution in a geographic area, the *network domain* provides a reliable and efficient geocast delivery mechanism.

Note that the selection of this strategy for *safety-of-life* is also justified by the rapid changing state of this information, e.g., emergency break, intersection collision warning. The *efficient and reliable* geocast mechanism, i.e., the instance of geocast (Fig. 3) used by *safety-of-life* applications, should ensure the one-time dissemination to all reachable nodes inside the *area of validity*. An application can still re-issue the information after certain time as *safety-of-life*, or even *safety*, if considered appropriate.

**Safety messages** are 'periodic' event-driven messages that are the result of the awareness of an unsafe situation, not *safety-of-life*, during a certain time. All safety applications will be repeatedly broadcasting (single hop) safety information (not beacons) during its time of validity<sup>2</sup> in order to improve reliability and connectivity (sparse networks). Note that the information sent can be different each time that it is transmitted since it can be updated (aggregated) in short time, i.e., ICF. In particular, we stress the need of mechanisms able to improve the scalability of the network and avoid redundant repetitions, e.g., discard the transmission of a specific information if any neighbor in the close surrounding just did it or restrict the repetitions just in case a new neighbor/s appear. *Safety messages* contain the same header fields as *safety-of-life* messages and additionally application specific data if required in the payload, e.g., size of icy road surface. Note that the dissemination in a geographic area is implicitly performed by the *application domain* when deciding whether the information is worth to be forwarded to its neighbors.

### D. Compatibility with Dumb Nodes, Default Application

The *application domain* of a dumb node is much simpler than of a smart node since many functions are not available, such as complex application logic, presentation to the

<sup>2</sup>With ICF a new *time of validity* can be determined by each 'receiving' application depending also on local state.

driver, etc. We propose that a dumb node provides a common *default application* that, at least, is able to interpret time and area of validity (*Default Information*, Fig.3). In particular, a dumb node is not required to process and interpret the message payload. The default application is able to temporarily cache and to re-broadcast cached messages.

In contrast to a smart node's *application domain*, a dumb node caches a safety message in a *Message Repository (MR)*. This message is re-broadcasted periodically while its time and area of validity are still valid. The re-send interval is either fixed with a default *period* or dynamic depending on the priority value. Note that *safety-of-life* messages will not be stored in the *MR*.

We recall that the described default application is also part of the *application domain* of smart nodes. This way, the compatibility among nodes having different implementations or versions of future safety applications would be ensured.

## IV. INFORMATION DISSEMINATION STRATEGIES

As stated in previous sections, the most prominent forwarding/disseminating strategy in vehicular environments is *geocast*, a mechanism capable to efficiently distribute a message to all nodes inside a geographical area. Furthermore, as commented above, one of the geocast instances should take into account the high reliability requirement of *safety-of-life* applications, i.e., the key tradeoff existing between efficiency and reliability must be appropriately balanced and optimized.

It is well known (e.g., [10]) that simple flooding in a geographic region, which is the most obvious algorithm, results in redundant re-broadcasts, contention and collisions in wireless medium access. Enhanced forwarding strategies that can reduce the overhead and improve efficiency have been proposed.

In the literature for mobile ad hoc networks exist several studies on improving efficiency of data dissemination, including *probabilistic* [10], *area-based* [10], [11], and *neighbor-knowledge schemes* [12], [13]. These, however, do not consider the key aspects of vehicular communication (see Sec. II), specially the high requirements of *safety-of-life* applications.

Moreover, the basic principle of VANET's forwarding/disseminating strategies, i.e., select forwarding nodes that offer the maximum 'forwarding benefit', should also take into account vehicular topologies restricted to street-bound scenarios. Following these guidelines in the context of data forwarding in VANETs, exemplary strategies are represented by: [14] where nodes closer to the destination are selected to forward a message in order to offer a maximum progress in a multi-hop communication; [15] where a node at a road's intersection decides that its location makes itself the optimal forwarder; or [16], that although it does not use road scenarios, it addresses sparse vehicular networks with a temporary caching of messages and their 'physical transport' of messages towards the destination.

Although all mentioned strategies already present solutions to several challenges, due to the particularly high requirements of *safety-of-life* applications the optimal strategy for an ‘efficient and reliable geocast’ is still an open issue.

Finally, it is worth noting that while all strategies above reside directly at the *communication domain*, they could also be taken as guidelines when implementing retransmission policies at the application (ICF). For example, the approach of information-centric forwarding has been investigated for applications with map-based data abstraction in [7], and in the context of mobile peer-to-peer communication in [17], though both for non-safety applications.

## V. CONCLUSIONS

For dissemination of safety information in a VANET we identify packet-centric forwarding and information-centric forwarding as two basic approaches for information dissemination, and derive the necessity to support a heterogeneous network architecture. We propose a system architecture for VANETs that is hybrid in a twofold meaning: it supports packet-centric forwarding for *safety-of-life* applications, and information-centric forwarding for *safety* applications with relaxed requirements for real-time and reliability, but high aggregation potential. The architecture supports a common communication system for both smart and dumb nodes, whereas the latter represent cost-efficient devices with limited processing capabilities as (but not only) road-side units. We present a model of a VANET node with a simple modular structure, identify relevant functions for information dissemination, and assign functions to the modules. As a result, we achieve a simple and robust system model with low complexity as a basis for implementation.

## REFERENCES

- [1] NoW – Network on Wheels. <http://www.network-on-wheels.de>.
- [2] The PREVENT Project. <http://www.prevent-ip.org>.
- [3] Car 2 Car Communication Consortium. <http://www.car2car.org>.
- [4] Vehicle Infrastructure Integration (VII). <http://www.its.dot.gov/vii/>.
- [5] Internet ITS Consortium. <http://www.internetits.org>.
- [6] Dedicated Short Range Communications working group. <http://grouper.ieee.org/groups/scc32/dsrc/index.html>.
- [7] L. Wischof, A. Ebner, and H. Rohling. Information Dissemination in Self-Organizing Intervehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, 6(1):99–101, March 2005.
- [8] H. Fülller, M. Torrent-Moreno, A. Transier, M. Festag, and H. Hartenstein. Thoughts on a Protocol Architecture for Vehicular Ad-Hoc Networks. In *Proc. of WIT 2005*, pages 41–45, Hamburg, Germany, March 2005.
- [9] M. Torrent-Moreno, P. Santi, and H. Hartenstein. Fair Sharing of Bandwidth in VANETs. In *Proc. of VANET 2005*, pages 49–58, Cologne, Germany, Sept. 2005.
- [10] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The Broadcast Storm Problem in a Mobile Ad Hoc Network. In *Proc. of MobiCom*, pages 151–162, Seattle, WA, USA, Aug. 1999.
- [11] A. Durresi, V.K. Paruchuri, S.S. Ivengar, and R. Kannan. Optimized Broadcast Protocol for Sensor Networks. *IEEE Transactions on Computers*, 54(8):1013–1024, Aug. 2005.
- [12] W. Peng and X. Lu. AHBP: An Efficient Broadcast Protocol for Mobile Ad Hoc Networks. *Journal of Science and Technology*, 16(2):114–125, 2001.
- [13] J. Sucec and I. Marsic. An Efficient Distributed Network-Wide Broadcast Algorithm for Mobile Ad Hoc Networks. CAIP Technical Report 248, Rutgers University, Nov. 2000.
- [14] M. Torrent-Moreno, F. Schmidt-Eisenlohr, H. Fülller, and H. Hartenstein. Effects of a Realistic Channel Model On Packet Forwarding in Vehicular Ad Hoc Networks. In *Proc. of WCNC 2006, To Appear*, Las Vegas, NV, USA, April 2006.
- [15] C. Lochert, M. Mauve, H. Fülller, and H. Hartenstein. Geographic Routing in City Scenarios. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 9(1):69–72, Jan. 2005.
- [16] C. Maihöfer, T. Leinmüller, and E. Schoch. Abiding Geocast: Time-Stable Geocast for Ad Hoc Networks. In *Proc. of VANET*, pages 20 – 29, Cologne, Germany, Sept. 2005.
- [17] O. Wolfson, B. Xu, and H. Yin. Dissemination of Spatial-Temporal Information in Mobile Networks with Hotspots. In *Proc. of DBISP2P*, pages 185–199, Toronto, Canada, Aug. 2004.