Architecture for Decentralized Mitigation of Local Congestion in VANETs

Robert K. Schmidt[§], Achim Brakemeier[¶], Tim Leinmüller[§], Bert Böddeker[§], and Günter Schäfer[‡]
[¶]Daimler Research and Technology, Ulm Germany, achim.brakemeier@daimler.com
[§]DENSO AUTOMOTIVE Deutschland GmbH, Germany, {r.schmidt|t.leinmueller}@denso-auto.de
[‡]Telematics/Computer Networks Research Group, Technische Universität Ilmenau, Germany, guenter.schaefer@tu-ilmenau.de

***Abstract*—The limited communication resources in VANETs have to be used efficiently to achieve reliable communication even in high load situations, where high packet loss is expected. Packet loss can occur on the channel or it occurs in the local queue due to a saturated channel. In this case, information becomes outdated and hence can be dropped. In this article, we propose multiple steps to solve this problem. We establish a model that determines the network capacity and the influence of hidden stations. The state of overloading the channel beyond the network capacity is named local congestion. Each vehicle has to evaluate the current channel load independently based on observations of the channel. With this consideration, we provide concepts for efficient use of available communication resources so that vehicles are able to receive as much information as possible from surrounding vehicles. To achieve that, we present a cross-layer framework for efficient channel usage motivated by the previous model. The framework comprises default mechanisms which efficiently avoid local congestion. We further show the integration of two advanced mechanisms and their interrelation. An evaluation of the combination provides strong indications that this framework allows to solve the identified problems and significantly improves communication reliability.**

***Index Terms*—Active safety applications, cross-layer-optimization, medium access control, reliability, vehicle-to-vehicle communication.**

I. Introduction

VANETs aim at reducing fatalities and injuries in road traffic by enabling vehicles to exchange information on their status. Active safety for driver and passengers shall be improved by reliable, low delay communication of highly accurate information.

Communication in VANETs is based on IEEE 802.11p [1], an amendment to IEEE 802.11 that defines mechanisms for medium access in vehicular environments. It is a well-known fact that shared medium access can often not be realized without taking collisions on the channel deliberately into account. Especially, in high load situations the communication performance suffers from hidden stations and exposed stations.

Two reasons for packet loss can be distinguished, loss on the channel and local loss. Loss on the channel is caused by hidden stations and channel access collisions. The major problem is that vehicles are not notified of this loss. We refer to this state as *unreliable*. Local loss occurs when a vehicle experiences a saturated communication channel and hence is not able to transmit its packets. These packets overload the local message queues. We refer to this state as *local congestion*. When reaching a certain delay, the content of the congested packets becomes outdated once there is an updated information provided by the application. Hence, the outdated information can be dropped already before accessing the channel.

In this article, we provide models for both states. For the state unreliable, we determine the reduction of the communication range, i.e. the reduction of the distance to the transmitter where communication with low packet loss is still possible, even with hidden stations. For the state of local congestion, we discuss the network capacity available in IEEE 802.11p. From these models, we identify means to avoid or mitigate unreliability of communication and local congestion. Based on local measurements of the channel load and the knowledge of what kind of information is to be transmitted, we discuss how to configure the whole communication system appropriately. We aim at maximizing the amount of received information by employing a cross-layer design.

We propose a flexible and adjustable framework for Decentralized Congestion Control (DCC) that is able to integrate existing approaches in harmonization with the currently proposed protocol architecture for intelligent transportation systems by ETSI/COMeSAFETY [2], [3]. The framework provides rules of interaction between different communication layers. With the integration of two approaches, we evaluate the flexibility of the framework and discuss the improvement of communication reliability by the combination of the two approaches.

The remainder of this article is structured as follows. Section II provides background information about congestion in VANETs, determines the network capacity and explains assumptions on the applications. In Section III, the DCC architecture and the cross-layer approach are presented as well as per-packet transmission parameter control. Section IV evaluates the proposed framework by discussing the installation of two specific approaches in the framework and by investigating improvement of communication reliability. The integration of related approaches into the proposed DCC architecture is shown in Section V, followed by the conclusions and outlook in Section VI.

II. Network Capacity Limits

In this section, models of certain VANET communication characteristics are introduced that will be used to derive basic parameters for the DCC framework in section III. Starting with a simple communication channel model, interference-based packet loss is discussed, the network capacity defined and the definition of *local congestion* is derived. We review a metric for channel load estimation based on measurements, i.e. the channel busy time.

A. Path Loss Model

The log-distance path loss model [4] is widely used in order to model the attenuation of a transmitted signal over distance. According to this model, the received signal strength $P_r(d)$ at distance d is

$$P_r(d) = \frac{P_0}{d^\rho} \tag{1}$$

where P_0 is the received signal strength at unit distance of 1m and ρ is the path loss coefficient. P_0 can be either measured or obtained with the free space formula [5]. ρ depends on environmental conditions and represents the empirical part of the model[1]. For example, in free space environment ρ is equal to 2 whereas in urban scenarios where there are many shadowing objects and reflections, ρ can reach values up to 4 [4].

B. Detection Range

We denote the distance where receiving vehicles detect an ongoing transmission and hence sense a busy channel as Detection Range D. Vehicles beyond this distance are allowed to use the channel for a concurrent transmission, also known as spatial reuse of the communication channel. According to IEEE 802.11 [6], this distance depends on two signal strength thresholds, the minimum receiver sensitivity P_{Sens} and the carrier sense threshold P_{CS}. In the VANET context (for 10 MHz channels) they are defined as $P_{Sens} = -85$dBm and $P_{CS} = -65$dBm [1]. A transmitting vehicle is not allowed to send as long as there is an ongoing reception of a packet with minimum signal strength of $P_{Sens} = -85$dBm or total energy of signals above $P_{CS} = -65$dBm. Note that the standard leaves open what happens if a packet is received with an energy level below P_{CS}. Here, we assume that more sensitive receivers are allowed to abort the reception in favor of a pending transmission. Doing so, a transmitting vehicle must be aware that he causes interference and hence may cause packet loss.

Accordingly, D is the distance where the resulting signal strength equals P_{Sens} after subtracting the path loss. With Eq. 1, we calculate D for a given energy threshold $P_{Sens}$and path loss exponent ρ

$$D = \sqrt[\rho]{\frac{P_0}{P_{Sens}}} \tag{2}$$

For the moment, we assume the absence of interference and hence neglect P_{CS}, which determines the detection range under interference.

[1]"This (empirical approach) has the advantage of implicitly taking into account all propagation factors, both known and unknown, through actual field measurements." [4]

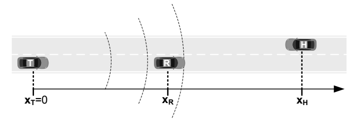

Fig. 1. Hidden station model: T's transmission is not detected at vehicle H

C. Communication Range under Interference

The commonly known hidden station problem can be denoted as a 3-tupel (T, R, H). A transmission of station T is interfered by a hidden station H if H cannot detect T's transmission (Fig. 1). This interference leads to packet loss at a receiver R located in-between, determined by the Signal-to-Inference Ratio (SIR) of T and H at the receiver location. In the following, we develop a simple one-dimensional model in order to analytically determine the severity of the hidden station and derive the reliable communication range.

x_R and x_H denote the distances of receiver and hidden station relative to the transmitter location $x_T = 0$. With the simple path loss model, we derive the SIR Γ at receiver R as

$$\Gamma(x_R, x_H) = \frac{P_T(x_R)}{P_H(x_R)} = \frac{P_{T,0}}{P_{H,0}} \frac{(x_H - x_R)^\rho}{x_R^\rho} = \left(\frac{x_H}{x_R} - 1\right)^\rho \tag{3}$$

where same power at unit distance is assumed, $P_{T,0} = P_{H,0}$. Hidden stations occur at a distance to the transmitter where the transmission cannot be detected, i.e. $x_H \geq D$. Assuming the worst case where the hidden station is located at D, we calculate the ratio of the remaining communication range C for transmitter T as

$$C = \frac{D}{\Gamma_C^{1/\rho} + 1} \tag{4}$$

where Γ_C is the minimum SIR needed for a successful reception. We can now express the reliable communication range as the distance to T where the received signal strength from T is stronger than the one received from H. Further, we assume an optimal receiver which is able to decode information from the signal slightly stronger than inference from H, i.e. $\Gamma_C \rightarrow 0$dB[2]. The path loss exponent does not influence the maximum communication range, hence

$$\lim_{\Gamma_C \rightarrow 1} C = \frac{D}{2} \tag{5}$$

Obviously, for H located at distance D to T, R is able to decode T's packet up to a distance $\frac{D}{2}$ to T at best, assuming T and H experience the same signal attenuation.

As stated before, this model assumes a constant detection range. However, under high load situations this detection range is not achieved since the accumulated interference makes it impossible to clearly detect an OFDM signal. In this case, the receiver sensitivity does not determine the detection range, but the carrier sense threshold P_{CS} as introduced in

[2]A ratio of 0dB is equal to 1 for the equation

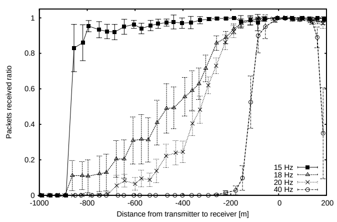

Fig. 2. Communication range reduction under high-load situations.

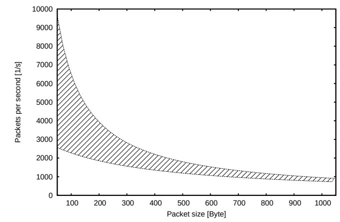

Fig. 3. Network capacity derived from parameters given in IEEE 802.11(p).

the previous section. We further developed our model with this consideration. Our simulation study in [7] validates that the communication range under interference can be severely reduced. An emergency vehicle approaching a traffic jam experiences high interference by hidden stations in the traffic jam. At the tail-end vehicles, this interference leads to significant packet loss. Only, when the emergency vehicle is very close to the tail-end vehicles, the SNR for the transmission of the emergency vehicle is always high enough to receive the packet successfully. In this case, the receiver is within the reliable communication range of the emergency vehicle. Fig. 2 displays the reduction of communication range down to $\frac{1}{10}$ of the original detection range.

D. Network Capacity Model

Local congestion in VANETs depends on the amount of data that can be transmitted over the wireless channel (excluding access layer overhead). We assume the same modulation scheme and respective data rate for all vehicles, for example QPSK-1/2 coding with 6MBit/s [8] data rate (Table I). This data rate applies to the frame body whereas the frame header always uses the lowest and most robust data rate. For determining the network capacity in bytes per second, we also have to consider the MAC layer. It introduces additional data-rate-independent overhead like backoff and interframe spaces. During these periods, the channel is reported idle but cannot be used for communication. The reason behind this is to avoid two stations accessing the idle channel at same time. In IEEE 802.11p, this is implemented by the AIFS (Arbitration Interframe Space) function which provides the following equations

$$T_{BO} = Rnd(0, CW) \times aSlotTime \tag{6}$$

$$aCWmin \leq CW \leq aCWmax \tag{7}$$

$$AIFS(i) \in (2, 3, 6, 9) \tag{8}$$

$$T_{AIFS(i)} = AIFS(i) \times aSlotTime \tag{9}$$

With Eq. 6, 7, 8, 9, Eq. 7 and $CW = aCWmin$ for broadcast mode, we calculate the total overhead including preamble and PLCP header

$$T_{Overhead} = T_{AIFS(i)} + T_{BO} + T_{aPreambleLength} + T_{aPLCPHeaderLength} \tag{10}$$

From the parameters given in IEEE 802.11-2007 [6] and IEEE 802.11pD9 [1], we calculate the minimum and maximum rate-independent per-frame overhead in microseconds given by highest and lowest access category (AC): 54μs for AC_VO (Voice) and 340μs for AC_BK (Background). The minimum overhead assumes immediate channel access where $Rnd(0, CW) = 0$, and for the maximum overhead $Rnd(0, CW) = CW$.

Taking into account the resulting effective transmission time for a given packet size and data rate (6MBit/s) the minimum and maximum network capacity is visualized in Fig. 3. This figure presents the maximum number of packets that can be sent per second in case of optimal distribution of the transmission, i.e. no MAC collisions.

Vehicles that receive such a high number of packets can be referred to as being in *local congestion*. The channel is saturated and does not allow any additional transmission, thus packets have to be locally dropped as the information becomes outdated quickly. The high likeliness of congestion can be derived from the above discussion on the network capacity. In high vehicle densities, the capacity can be easily reached. Even worse, from the hidden station model derived in the previous section, we see that packet loss on the channel is experienced at any load due to hidden stations and channel access collisions[3]. For the rest of the paper, we assume the lowest access class as default access class since it provides the largest contention window which reduces the channel access collisions.

We assume that the packet size is fixed from the application and cannot be split. From the discussion above, we derive that

- large packets are not efficient as the probability of hidden station collisions is increased [7],
- small contention window increases the channel access collision probability,
- large contention window reduces the network capacity.

E. Channel load metric

A common metric to estimate the load on the wireless channel is the Channel Busy Time (CBT) as standardized in IEEE 802.11k [10]. For a given period, it returns the ratio where the channel was reported busy from the access layer.

The CBT is mainly influenced by the receiver state. For the time when a packet is received with a signal strength above

[3] which can be reduced by a larger contention window [9] but at the expense of more MAC overhead.

Data rate	Modulation	Coding rate	Sensitivity
3	BPSK	1/2	-85 dBm
4.5	BPSK	3/4	-84 dBm
6	QPSK	1/2	-82 dBm
9	QPSK	3/4	-80 dBm
12	16-QAM	1/2	-77 dBm
18	16-QAM	3/4	-73 dBm
24	64-QAM	2/3	-69 dBm
27	64-QAM	3/4	-68 dBm

TABLE I
DATA RATES, MODULATIONS, RECEIVER SENSITIVITIES AS SPECIFIED BY IEEE 802.11 FOR 10 MHZ CHANNEL BANDWIDTH.

the minimum sensitivity P_{Sens}, the channel is reported busy. If no packet is currently received, but there is a high energy level on the channel, above the Carrier Sense Threshold P_{CS}, the channel is also reported busy.

The parameters for the CBT have to be standardized for VANETs in order to ensure that all vehicles have a common channel evaluation criterion and compute the CBT in the same way. These parameters include: Evaluation period T, Receiver sensitivity for CBT P^{CBT}_{Sens}, Carrier sense threshold for CBT P^{CBT}_{CS}.

Note that for receiving packets, the effective receiver sensitivity may be higher, depending on hardware capabilities. For the CBT these values must be determined according to standardized rules so that vehicles come to similar evaluations of the load. Otherwise, this would lead to unfairness in channel access.

F. Transmit traffic model

In order to structure the various safety applications, a rough classification of the load is made in this section. From IEEE 802.11p, four categories of messages are given, AC_VO (Voice), AC_VI (Video), AC_BE (Best Effort) and AC_BK (Background). As there are only minor parameter differences between AC_VO and AC_VI, we can map the categories to three categories: High, medium, low priority.

Currently, the standardization of VANET applications foresees mainly two types of messages, periodic Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) [11], [12], [2]. Additionally, control messages may announce services on other communication channels.

Summarizing, we have the following traffic classification:

- *Type:* Periodic message, event-driven message, control message
- *Access Category:* High, medium, low

Furthermore, the set of applications must be able to provide an estimation on how many messages can be generated per second even in emergency situations. A specific distribution of the traffic model is out of scope of this paper.

G. Summary

The channel load should be limited to a quite defensively chosen threshold in order to avoid local congestion and mitigate the impact of hidden stations. A channel load below 50% with respect to 6MBit/s may reduce the packet loss as it lowers the probability of channel access collisions as well as hidden stations. Therefore, an estimation of the current network load is needed. Unfortunately, determining the percentage of the current capacity usage, i.e. the channel load, is difficult as the spatial reuse makes the channel load calculation time- and space-variant. The spatial separation of the vehicles and the resulting value of signal attenuation determines if a transmission can be detected as a packet or if it is interpreted as noise. The presence of interference makes this consideration more complex. Hence, vehicles are not necessarily able to identify the global number of packets on the channel per second. Nevertheless, the commonly proposed metric Channel Busy Time may provide an acceptable estimation of the channel load.

As the channel load results from various parameters like transmit power, message rate, many possibilities for adjustments on different layers arise. The periodicity of messages is determined by the applications and influences the likeliness of hidden stations as well as channel access collisions. The transmit power may be roughly determined by the application in terms of desired spatial spread but it must be set at the access-layer. There, more aspects to determine the appropriate transmit power arise, e.g. the current interference level. The transmit power also strongly influences the detection range and hence the channel load at far distances. The access layer further offers the adjustable parameters transmit data rate and carrier-sense threshold. The lower the data rate modulation scheme, the lower the minimum SNR needed to decode the information. This robustness goes at the expense of transmission time and hence the duration of a busy channel. With the (adjustable) carrier-sense threshold, an evaluation of the channel state determines whether a vehicle is basically allowed to transmit.

All parameters have strong interdependencies across layers, from access layer up to application layer. As a consequence, a cross-layer approach is needed to adapt the most important parameters of communication dynamically according to the load and communication purpose. Neither the access layer nor the application layer nor any other layer is able to decide which setting is the best. We assume that only the combination of knowledge can adjust the communication parameters significantly better than any layer on its own. The access layer cannot simply drop arbitrary messages but the facilities layer must be informed to gracefully reduce the generation rate of periodic messages. Therefore, we propose a cross-layer framework for DCC as described in the next section.

III. DECENTRALIZED CONGESTION CONTROL

Following, we introduce requirements that have to be fulfilled by the cross-layer architecture for DCC. From these requirements, we then develop the framework layer-by-layer. Finally, we explain the behavior of DCC, i.e. the DCC function.

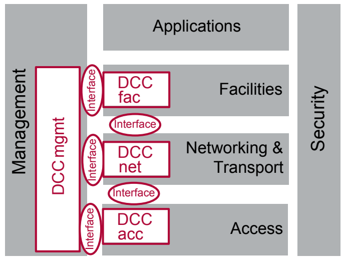

Fig. 4. Overview of the DCC architecture integrated in the ETSI/COMeSAFETY architecture for ITS [3].

A. Requirements for DCC cross-layer approach

From the results of the previous section and with the knowledge that there are already several independent mechanisms that can contribute to DCC, the following requirements can be derived. The DCC has to provide means to

- *Avoid local congestion:* Messages should not be dropped as any information issued is assumed to be safety-critical. DCC shall ensure that this information is transmitted.
- *Mitigate unreliability:* Hidden stations cannot be avoided. Hence, DCC shall engage means to improve the reliability of communication in a fair manner. This may include a strict reduction of communication as a tribute to lower the channel load. The control of transmit power, modulation scheme selection, transmit interval, and sensitivity has to be possible from all layers in order to support various approaches for DCC.
- *Extend functionality by flexible integration of additional mechanisms:* Beyond a basic configuration, extensions should be easily feasible in order to leverage existing approaches for DCC.
- *Distribute status information across layers:* In case, DCC has to restrict the transmission, all layers must be informed of that action. Concerned layers shall know, how DCC adapted the communication system for a particular transmission.
- *Graceful degradate:* All layers should contribute proactively to the reduction of transmitted data in high load situations to avoid that the access layer has to delay and drop packets as a last resort to maintain communication reliability.

B. DCC framework and architecture integration

This subsection describes the components of the DCC framework and shows the integration into the ETSI/COMeSAFETY protocol architecture for ITS [2], [3]. Fig. 4 depicts this integration and shows the interfaces between the different DCC components.

1) DCC_mgmt: Using the specified interfaces, all layers can request the state of the DCC given by state values, parameters and models described in the background section. In a database, all relevant parameters and options are stored, e.g.

- Network design limits (Ranges of parameters and model parameters, e.g. channel model, transmit and receive model,
- Regulatory limits and device-dependent parameters,
- Reference parameters.

For the rest of the article, all parameters stored in the database will be referred to with the prefix ”DCC_” and the type of value, i.e. ”min”, ”max”, ”def”, ”ref”. The first two parameters define the range of value adaptation, ”def” describes the default value and ”ref” the currently adapted value.

2) DCC_app: Closest to the application is the Facilities layer. The context of the application message is known and can be used to adapt the communication system according to the purpose of the CAMs. For received messages, this component supports the decision to forward the message. It can calculate the benefit of this decision. Approaches like relevance-based forwarding, e.g. [13] may implement this DCC component.

3) DCC_net: This layer realizes all mechanisms that need access to the neighbor information like the neighbor table or do need interaction with other vehicles to adjust the transmission parameters. This includes approaches like multi-hop beaconing, transmit power control algorithms with feedback, etc.

4) DCC_core: This layer implements the concepts that adjust the reference parameters based on the channel load. Once a high channel load is detected and mechanisms in the higher layers did not properly avoid this situation, the transmission parameters are adjusted until the channel load is reduced. It therefore observes the channel busy time and the locally offered load. Based on that, the reference parameters are adapted by the following four schemes:

Transmit Data Rate Control (TDC) is in charge of selecting the modulation scheme for the transmission of the packet. The lower the rate, the more robust the transmission against interference. *Transmit Power Control (TPC)* defines the transmit power and the knowledge of the effective radiated power at the antenna which is given by regulation, e.g. $DCC_staTxPower = 33$dBm. *Transmit Rate Control (TRC)* limits the maximum number of transmitted packets. The vehicle should not overload the channel with too many transmissions. TRC delays packets that exceed the defined maximum rate. It observes the arrival time between two subsequent packets to be sent. Note that the minimum minimum packet interval can also be set to 0 in order to have an option for flooding of very high priority messages. For the maximum minimum packet interval, a value should be chosen that is not too high as the information is useless in case it is delayed too much. *DCC Sensitivity Control (DSC)* adjusts the receiver sensitivity and carrier sense-threshold, which determines if a vehicle is allowed to transmit depending on signal strength. Changing this threshold to a higher value may lead to an abort of the transmission with a low receive signal level in case a high priority message arrives from an application.

ACR	Category	Priority	Example
0	Intrinsic	High	N/A
1	Event	High	First DENM
2	Recurrent	High	CAM high priority
3	Event	Medium	DENM Repetition
4	Recurrent	Medium	CAM standard
5	Event	Low	DENM Multi-Hop
6	Recurrent	Low	CAM near-field
7	Intrinsic	Low	Repetitions

TABLE II
SAMPLE MAPPING OF ACCESS PARAMETERS TO A GIVEN NUMBER OF ACCESS RANK (ACR).

C. DCC Function

The previous subsections introduced the structure and components needed for DCC. In this subsection, the behavior of DCC over time is described. DCC adapts the reference values stored in the database located in DCC_mgmt. All three components of DCC are able to execute this adaptation. DCC_app and DCC_net may optionally adapt the reference parameters whereas the adaptation by DCC_core is mandatory, displayed in Fig. 5.

The mapping of reference transmission parameters on each packet is implemented by the Transmit Access Control (TAC). Each packet is assigned an Access Rank (ACR) which is determined by the classification described in Section II-F. This translates to a sample collection of eight different ranks.

The mechanisms in DCC_core adjust the reference parameters within the defined ranges according to the Channel Busy Time. Before transmitting a packet to the communication channel, the transmission parameters are set.

TAC computes the vehicle's current channel use per Access Rank. If the channel use is above the defined threshold per ACR, it increases the ACR. Then, TAC checks the load again for the next ACR. This is repeated until the transmit model is fulfilled. Packets that do not fit are assigned to the lowest ACR. Finally, the TAC is the last instance to intervene in the transmission by the following two steps

1) Check if packet exceeds the number of packets transmitted for this ACR
2) Map the reference values to packet according to the mapping given by the ACR.

Table II shows that the combination of parameters from the transmit traffic model can be mapped to an ACR. Examples for these mappings are also in the table. By default, each ACR translates to a particular default setting of transmission parameters. Over time, the reference values are adapted by the DCC components in case the channel load or transmit traffic increases. These values are then finally mapped to every transmission by the mapping function map. For a given packet pkt with ACR a and reference parameter $DCC\_ref\,\langle type\rangle$, the resulting transmission parameter tx_{param} is:

$$tx_{param}(pkt) = map(r, a) \tag{11}$$

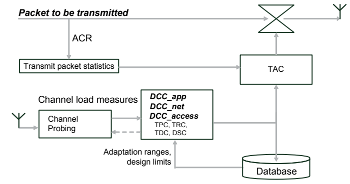

Fig. 5. Functional view of the access layer part, DCC_core.

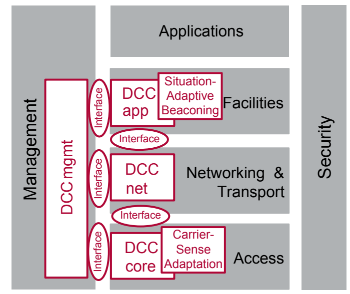

Fig. 6. DCC architecture with integration of Situation-Adaptive Beaconing.

More specifically, the reference parameters are $DCC\_refDataRate, DCC\_refTxPower, DCC\_refPacketInterval, DCC\_refSensitivity$. For the actual transmission, the values for tx_{param} are finally applied using the (per-packet) interfaces defined in the access layer. The generic description of the mapping function leaves room for different concepts. A specific mapping function is out of scope of this article.

IV. EVALUATION

In this section, we evaluate the proposed framework by discussing the integration of situation-adaptive beaconing on top of the DCC_core. We define two basic policies according to two kinds of the Cooperative Awareness Messages (CAMs) and a congestion policy that shall mitigate local congestion.

1) *CAM for basic awareness:* Optimized for highest reliability
2) *CAM for situation-adaptive awareness:* Optimized for high-rate near-field communication

For the less frequent CAMs sent with policy 1, we define all parameters to be set to maximum reliability, i.e. highest transmit power, lowest data rate, lowest sensitivity, lowest packet interval. In the first subsection, we investigate the reliability optimization based on the carrier-sense threshold adaptation by simulation (Parameter DCC_refSensitivity). The generation rate of messages for policy 2 by situation-adaptive beaconing is discussed in the second subsection. In the last subsection, we discuss the interrelation of the two policies with the remaining access-layer concepts TDC and TPC as well as TAC and the possibility for a congestion policy 3.

A. Carrier-Sensing Threshold Adaptation

As we have shown in Section II-B, the detection range is determined by the two energy thresholds. This threshold determines which interference level is tolerated when starting a transmission. It is obvious that with a lower threshold,

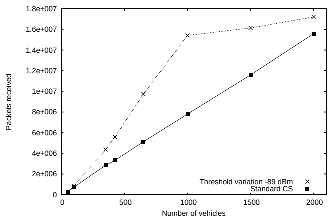

Fig. 7. Carrier sensing threshold adaptation.

far distant transmissions are less disturbed since the receiver is more sensible to ongoing transmissions. Especially when transmitting with high power, the threshold should be lower as the potentially caused interference would be higher. In a simulation study in [14], we have analyzed the impact of a globally lowered carrier sense threshold. As a result (Fig. 7) the total number of received packets was increased especially in high vehicle density scenarios. However, the adaptation of this threshold may lead to a transition from unreliable state to local congestion. Therefore, only packets with relaxed delay constraints should be assigned with a lower threshold as they will experience a higher channel access delay. On the other hand, packets with tight delay constraints which concern for example only near-by vehicles may have a higher carrier sense threshold at the expense of packet loss at far distances. The combination with transmit power adjustment will be discussed later.

B. Situation-Adaptive Beaconing

In [15], we have discussed the influence of the adaptation of the CAM rate on the position accuracy. Basically, the error of the last reported position from a vehicle depends on the age of the information and the velocity of the vehicle. Situation-adaptive beaconing aims at keeping position errors as low as demanded by the situation. For example, the beacon rate is increased once a critical traffic situation between two vehicles is imminent and therefore a high accuracy is needed.

In the DCC architecture the situation-adaptive beaconing is applied to Facilities layer as it knows the application context. We restrict the rate adaptation to the situation-adaptive CAMs which provide additional accuracy to the basic awareness CAMs. Using the interface DCC_app ↔ DCC_mgmt, the parameters for rate adaptation ranges are retrieved. With these values, the concepts described in [15] can appropriately adapt rate for a given situation.

As the rate adaptation by situation-adaptive beaconing is bounded by the DCC minimum and maximum parameters, the access-layer rate control will not delay any CAMs as long as we assume that there is no other significant additional amount of packets. This implementation shows how to graceful degrade in order to avoid delaying or dropping messages on the access-layer mechanisms. Nevertheless, they will engage if the higher layer mechanisms fail.

This discussion also shows the need for a facilities-layer based rate adaptation in addition to the access layer. It is not acceptable for proper active safety communication to simply delay or even drop arbitrary messages. The facility layer has to dynamically decide how much information a vehicle has to broadcast so that surrounding vehicles can properly evaluate if any dangerous situation arises.

ACR	Tx Power	Data Rate	Sensitivity
2	DCC_maxTxPower	DCC_minDataRate	DCC_minSensitivity
4	DCC_minTxPower	DCC_refDataRate	DCC_refSensitivity
6	DCC_minTxPower	DCC_maxDataRate	DCC_maxSensitivity

TABLE III
DCC MAPPINGS FOR CAMs.

C. Transmit Parameter Mapping

With the integration of the two approaches in the framework, the basic configuration for CAMs can be developed using the described policies mapped to ACRs. Table III shows the parameter mappings for ACR 2, 4, and 6. ACR 2 is the configuration with a high level of reliability, demanded by the basic awareness CAMs. ACR 4 allows to transmit a high number of packets which suits to the situation-adaptive awareness CAMs. As a fall back solution, in case the transmit traffic model is violated, the remaining packets are assigned with parameters according to ACR 6. This is supposed to avoid local congestion in parallel with low interference to other vehicles due to low transmit power.

V. Related Work

As there are various approaches that aim at improving communication reliability in VANETs, we discuss the integration of them in the DCC architecture. Basically, the integration location in the architecture is defined by the needed knowledge and focus of the approach. Torrent-Moreno et al. proposed in [16] an algorithm for fair transmit power adjustment in order to control the channel load caused by periodic messages. As it needs basic feedback from other vehicles and knowledge of the neighborhood, it can be integrated into the DCC_net component. In [13], Kosch et al. introduce a concept to determine the relevance of a message. With the quantification in terms of information benefit, messages can be assigned to a particular category according to IEEE 802.11e. Interestingly, the "nodes do not primarily aim at maximizing their own benefit, but head for transmitting information such that their neighbors are provided with the data they are most interested in." This setting makes the concept a potential implementation for assigning messages to an access rank. Hence, this is a functionality for DCC_app. Another mechanism for TRC in DCC_core is the adaptation of the contention window size by Mertens et al. in [9]. The adaptation relies on the packet error rate. In order to integrate it in the DCC framework, the adaptation would have to be based on the channel busy time. Otherwise, this channel load metric has to be added to DCC_mgmt. Candidate implementation for TRC and TPC are proposed in [17]. Based on the channel busy time, the algorithms adjust transmit power and transmit rate in order to maintain reliable communication in parallel with a smooth adaptation.

VI. Conclusions & Outlook

With efficient usage of the limited communication resources, information exchange in VANETs may be improved significantly. In this article, we discussed the limitation of communication resources. Hidden stations are known to degrade the communication performance in terms of communication range. We specifically showed how they influence the communication range. From IEEE 802.11p we derived the network capacity and discussed the efficiency of different packet sizes.

In order to cope with the identified limitations, we elaborated on a cross-layer framework which is capable of adapting the communication system appropriately to the current load. Based on the widely used channel load metric Channel Busy Time and the load offered by the safety applications, various parameters can be adapted on a per-packet basis.

We discussed a possible implementation of the framework and showed the integration of an existing approach on situation-based rate adaptation. Further, we briefly discussed the integration of other approaches like decentralized transmit power control. The efficient combination of these approaches allows to profit from the strengths of each approach. Hence, the framework provides strong indications that the overall reliability of communication and accuracy of vehicle awareness can be significantly improved.

Our future work will comprise a deeper analysis of the interrelation of various concepts for DCC. We will investigate different policies in consideration with different transmit traffic models. Currently ongoing field trials may also provide further input to the DCC architecture.

VII. Acknowledgment

The authors kindly acknowledge the intensive and fruitful discussions in the Car2Car Communication Consortium, working group Communication.

References

[1] Institute of Electrical and Electronics Engineers, "IEEE P802.11p/D9.0 - Wireless Access in Vehicular Environments," November 2009, draft 9.0.

[2] PRE-DRIVE C2X, "Deliverable D1.2 - Refined Architecture," ETSI, Tech. Rep., 2009.

[3] R. Bossom, R. Brignolo, T. Ernst, K. Evensen, A. Frötscher, W. Höfs, J. Jääskeläinen, Z. Jeftic, P. Kompfner, T. Kosch, I. Kulp, A. Kung, A.-K. Mokaddem, A. Schalk, E. Uhlemann, and C. Wewetzer, "European ITS communication architecture — Overall framework — Proof of concept implementation," EC FP7 Deliverable, EC Information Society Technologies Programme, Tech. Rep., March 2009.

[4] T. S. Rappaport, *Wireless Communications: Principles and Practice (2nd Edition)*. Prentice Hall PTR, December 2001.

[5] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[6] Institute of Electrical and Electronics Engineers, "IEEE Std 802.11-2007," June 2007.

[7] R. K. Schmidt, T. Köllmer, T. Leinmüller, B. Böddeker, and G. Schäfer, "Degradation of Transmission Range in VANETS caused by Interference," *PIK - Praxis der Informationsverarbeitung und Kommunikation (Special Issue on Mobile Ad-hoc Networks)*, vol. 32, pp. 224–234, 2009.

[8] D. Jiang, Q. Chen, and L. Delgrossi, "Optimal data rate selection for vehicle safety communications," in *VANET '08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. New York, NY, USA: ACM, 2008, pp. 30–38.

[9] Y. Mertens, M. Wellens, and P. Mähönen, "Simulation-Based Performance Evaluation of Enhanced Broadcast Schemes for IEEE 802.11-Based Vehicular Networks," in *VTC Spring*, 2008, pp. 3042–3046.

[10] Institute of Electrical and Electronics Engineers, "IEEE Std 802.11k-2008 - Radio Resource Measurement of Wireless LANs," June 2008.

[11] ETSI, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions (ETSI TR 102 638 V1.1.1)*, European Telecommunications Standards Institute, June 2009.

[12] ——, *Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications (ETSI TR 102 698)*, European Telecommunications Standards Institute, June 2009.

[13] T. Kosch, M. Strassberger, S. Eichler, C. Schroth, and C. Adler, "The Scalability Problem of Vehicular Ad Hoc Networks and How to Solve it," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 22–28, 2006.

[14] R. K. Schmidt, T. Leinmüller, and G. Schäfer, "Adapting the Wireless Carrier Sensing for VANETs," in *6th International Workshop on Intelligent Transportation (WIT)*, Hamburg, Germany, March 2010.

[15] R. K. Schmidt, T. Leinmüller, E. Schoch, F. Kargl, and G. Schäfer, "Exploration of Adaptive Beaconing for Efficient Intervehicle Safety Communication," *IEEE Network Magazine, Special Issue on Advances in Vehicular Communications Networks*, vol. 24, pp. 14 – 19, 2010.

[16] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3684–3703, 2009.

[17] C. Khorakhun, H. Busche, and H. Rohling, "Congestion Control for VANETs based on Power or Rate Adaptation," in *5th International Workshop on Intelligent Transportation (WIT)*, Hamburg, Germany, March 2008.