Bigger is Better - Combining Contention Window Adaptation with Geo-based Backoff Generation in DSRC Networks

Bernhard Kloiber*, Jérôme Härri†, Thomas Strang* and Stephan Sand*

*Institute of Communications and Navigation
German Aerospace Center (DLR), Wessling, Germany
Email: {bernhard.kloiber, thomas.strang, stephan.sand}@dlr.de

†Mobile Communications
EURECOM, Sophia Antipolis, France
Email: jerome.haerri@eurecom.fr

***Abstract*—The vision of safer transportation is strongly driven by the introduction of Vehicular Safety Communications (VSC) to enable new cooperative safety applications. In highly dense traffic scenarios, however, the current Dedicated Short Range Communications (DSRC) technology is expected to face serious performance problems due to simultaneous transmissions making packets to collide with each other.**

In this paper, we first analyze the sources of packet collisions. The analysis reveals a significant amount of simultaneous transmissions as vehicles have chosen the same backoff counter, especially in the close vicinity, which is the most critical area with respect to safety. Based on these observations, we then introduce a new concept for DSRC backoff generation called *geo-backoff*. It implements two countermeasures: First, we increase the Contention Window (CW) to reduce the probability of simultaneous transmissions in general. Second, we exploit geographical information for generating the current backoff counter to further reduce the probability of packet collisions at short (critical) ranges. We analyze our concept from a traditional TX-RX perspective (latency) as well as an RX-centric perspective (update delay). The simulation results indeed have shown that geo-backoff is able to improve the communication performance, but the improvement is mainly dominated by just increasing the CW.

I. INTRODUCTION

The year 2015 poses a decisive milestone for the vision of Intelligent Transport Systems (ITS) as car manufacturers will start to equip their vehicles with ITS communication technology [1]. Once rolled out, vehicles are able to exchange (safety-related) information between each other. Several message types have been defined in order to group this kind of information. One of the most relevant is the so called Cooperative Awareness Message (CAM) [2], which contains the vehicles current status, like position, speed and heading. CAMs are required to be periodically broadcasted by each vehicle. Thus they enable new cooperative safety applications like Cooperative Adaptive Cruise Control (CACC) [3]. Especially safety-related applications require a high up-to-dateness of the current status information about neighboring vehicles, which is of higher quality the more regular CAMs are received. Consequently, the reliability of such applications heavily depends on the reliability of the communication technology itself. ITS-G5 is used for Vehicular Safety Communications (VSC) in Europe [4]. It is based on the well-known Wireless Local Area Network (WLAN) standard IEEE 802.11 [5], operating in a dedicated frequency band located around 5.9 GHz.

IEEE 802.11 implements a Medium Access Control (MAC) scheme called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which coordinates the access on the shared communication medium among multiple vehicles in a decentralized manner. CSMA/CA is a contention-based and probabilistic access scheme. Specifically, this means that if the channel is currently occupied, the transmitter switches into contention mode, by generating a random backoff counter, chosen from the integer interval $[0; CW-1]$, with the Contention Window (CW) specifying the size of the interval. The backoff counter represents a random waiting time, which only elapses during an idle channel period. When elapsed, the transmitter is allowed to access the channel. Here, the random backoff procedure shall ensure that several contending transmissions do not result in simultaneous transmissions, which automatically would lead to packet collisions.

Obviously, the probability of simultaneous transmissions heavily depends on the CW size. To make sure that even with an increasing number of contenders the probability of simultaneous transmissions remains low, the Binary Exponential Backoff (BEB) mechanism has been introduced, which adapts the current CW size depending on the feedback (acknowledgement) from the destination (unicast mode) [5]. Since CAMs are transmitted in broadcast mode, BEB is useless for VSC. Without BEB the CW size for CAM transmissions only consists of 8 slots[1] and will not grow with increasing contention. Consequently, each vehicle may have collision-free contention with at most 7 of its neighbors. Considering highly dense traffic scenarios (e.g. multi-lane highways), each vehicle is expected to have more than 7 contending neighbors, which is a recipe for packet collisions.

The reason for keeping such a small CW is based on the traditional TX-RX perspective, i.e. aiming to keep the end-to-end delay (latency) as low as possible. The periodic dissemination of CAMs, however, is dedicated to provide regular information updates to the corresponding receivers. Hence, the performance of cooperative safety applications heavily depends on the delay between two consecutive successfully received CAM updates (update delay or inter-reception time), i.e. an RX-centric perspective. If too long, the VSC application is not able to detect a dangerous situation in time.

Some of the VSC research community have proposed several approaches to dynamically adapt the CW size: Balon et al. [6] increased the reception probability of VSC broadcast transmissions by dynamically adapting the CW size based on analyzing the sequence number of packets. Rawat et al. [7] applied Balons CW adaptation strategy and combined it with a transmit power control strategy based on the vehicle density. Thus they improved the throughput and the average end-to-end delay. In [8], Stanica et al. also identified the problem of small CW sizes in current VSC and proposed to adapt the current CW as a function of the vehicle density to improve the beacon reception probability. All these approaches dynamically adapt the current CW size, which is indeed the right approach, but they lack an evaluation from an RX-centric perspective (update delay), which is more suitable to investigate the performance of CAM dissemination.

A first approach to analyze the effects of the CW size in beaconing vehicular networks from an RX-centric perspective is provided in [9] by measuring the inter-arrival time as well. In contrast to [6], [7], [8] the authors concluded that increasing the CW does not improve the beaconing performance in vehicular networks. A possible reason might be their simplified communication scenario (e.g. no path loss, closed network, low communication range).

In this paper we provide the following contributions: First, we analyze the impact of increasing CW, based on the current state of the art introduced above, according to an RX-centric metric (update delay) within a more realistic communication scenario. Second, we investigate a combination of an increasing CW and generating the DSRC backoff by exploiting geographical information.

Based on a detailed analysis of the different sources of packet collisions, we introduce a new concept called *geo-backoff*, which consist of two steps: First, we increase the CW in order to reduce the probability of simultaneous transmissions in general. Second, we aim to further reduce the probability of simultaneous transmissions in the close vicinity, which is the critical area regarding vehicular safety, by position-dependent generation of the current backoff counter. Our simulation results show, that the amount of simultaneous transmissions can be reduced significantly, which improves the update delay performance as well. However, the improvement is dominated by just increasing the CW size. Applying the *geo-backoff* function in addition only results in a slight reduction of simultaneous transmissions but shows no improvement of the update delay.

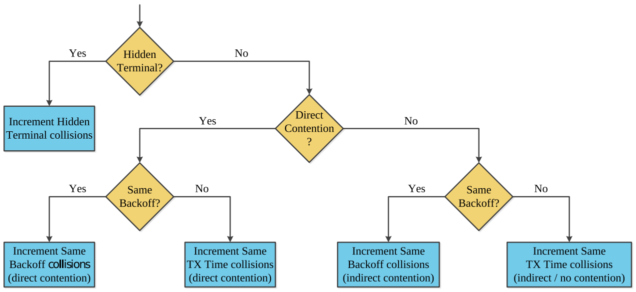


Fig. 1. Decision flow chart to classify different situations causing a collision.

II. SOURCES OF PACKET COLLISIONS

In order to address the problem of packet collisions properly, we are first interested in understanding the sources of collisions on the wireless channel. Therefore, we implemented a classification scheme for packet collisions, as illustrated in Fig. 1. Once a collision is detected, we identify the following reasons:

- *Hidden terminal collision:* Both transmitters have been hidden to each other.
- Direct contention: Each transmitter attempted to access the channel, but each sensed a busy channel, which was currently occupied by the same transmitter.
  - *Same backoff collision (direct contention):* Both transmitters have chosen the same backoff counter during direct contention phase.
  - *Same TX time collision (direct contention):* Although not having chosen the same backoff counter, both transmitted at the same time.
- Indirect contention: Either the channel was currently occupied by different transmitters during their transmission attempt, or there was no contention at all.
  - *Same backoff collision (indirect contention):* Both vehicles were blocked by different transmitters each, but have chosen the same backoff counter.
  - *Same TX time collision (indirect / no contention):* Both transmitters accidentally transmitted at the same time.

Fig. 2 shows the absolute number of collisions as a function of the distance between the two collision inducing transmitters for the default mechanism, i.e. uniform random backoff generation using a CW with 8 slots.

---

[1] Currently, CAMs are foreseen to be transmitted on the AC_VI queue representing the second access priority according to the Enhanced Distributed Channel Access (EDCA) in [5].

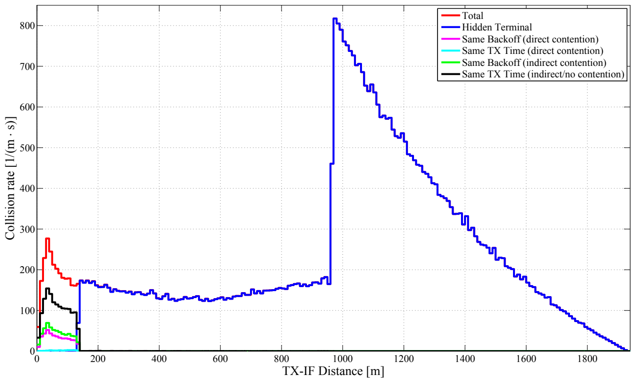


Fig. 2. Collision rate (normalized in time and space) for the various collision types dependent on the distance between the two colliding transmitters.

The plot reveals some interesting effects, we would like to clarify first. Considering the total amount of collisions (red curve), two peaks can be identified. The one at approx. 970 m is caused by an excessive increase of hidden terminal collisions, which occur if both transmitters are outside of each others communication range ($\approx$ 970 m). The peak at approx. 30 m is a side effect given by the highway scenario. Since the highway has a width of approx. 30 m, up to this range the number of collisions is growing in lateral as well as longitudinal direction. Beyond that range, only the longitudinal direction still contributes to the number of collisions.

Considering the hidden terminal collisions (black curve), we can see an excessive increase at the communication range ($\approx$ 970 m). But it also reveals a sudden increase at approx. 135 m. This effect is caused by the Clear Channel Assessment (CCA) threshold [5]. By default it is 20 dB above the RX sensitivity threshold (-85 dBm) and is used to declare the channel as busy only if the received signal strength is above -65 dBm. This is used in case the signal strength of an incoming packet is above the RX sensitivity threshold, but the terminal could not synchronize on the preamble and is not able to decode the rest of the packet. Although there is an ongoing packet transmission, thanks to the CCA threshold, the terminal is allowed to transmit its own packet if the current signal strength is below -65 dBm. Otherwise the channel would be declared as busy, which is the case for ranges up to approx. 135 m (w.r.t. our used radio propagation model). Long story short, the CCA mechanism allows to have hidden terminal collisions even within the communication range, but is limited to approx. 135 m.

A more detailed view according to the shares of the different collision types is presented in Fig. 3. It shows the different collision types normalized by the total number of collisions over the distance between the two collision inducing transmitters. Beyond the distance of approx. 135 m, the hidden terminal collisions clearly dominate all the other collision types with a relative amount of 99 % and more. A proposal of how to address hidden terminal collisions can be found in [10].

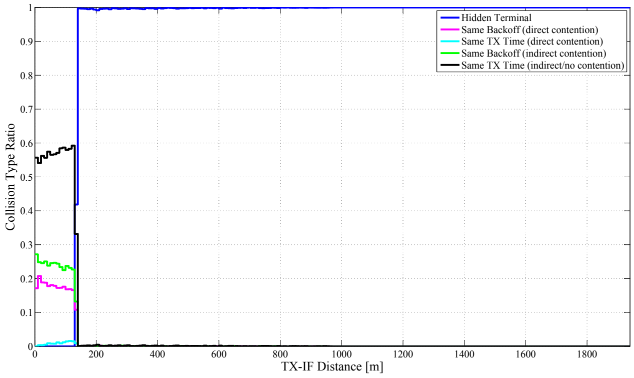


Fig. 3. Relative amount of collisions for the various collision types dependent on the distance between the two colliding transmitters.

As we are focusing on cooperative safety applications, we are more interested in reducing collisions at lower (critical) distances. Still significant with approx. 45 %, we will focus here on the *same backoff* collisions, as they can be clearly identified with a single trigger event, i.e. both transmitters have chosen the same backoff counter. This leads to a certain degree of synchronization between the transmitters causing a simultaneous transmission.

III. THE GEO-BACKOFF CONCEPT

We propose a new IEEE 802.11 MAC adaptation concept called *geo-backoff*, which is based on two steps: First, we reduce the probability of simultaneous transmissions in general by increasing the CW. Second, we aim to further reduce the probability of simultaneous transmissions in the immediate vicinity by exploiting the vehicles current position to generate the backoff counter.

A. Step 1: Contention Window Adaptation

The main objective in this work is to improve the communication performance in the context of vehicular safety, especially at close ranges, where reliable communication is safety critical and packet collisions are undesirable. Regarding the results from Sec. II, the intuitive approach to reduce the amount of collisions at close ranges is to reduce the probability of vehicles choosing the same backoff counter. Therefore, a reasonable starting point is to simply increase the CW size. That it makes sense to increase the CW, and by implication improve the communication performance, was already demonstrated in [6], [7], [8].

B. Step 2: Geo-based Backoff Generation

Regardless of whether the CW size is increased, the current DSRC backoff generation is based on a uniformly distributed random process and is not able to distinguish between close-by and far-away. In this step we further aim to generate different backoff counters for contending vehicles, which are located in the immediate vicinity, by using their current positions. Therefore, two approaches have been investigated and are described hereafter.

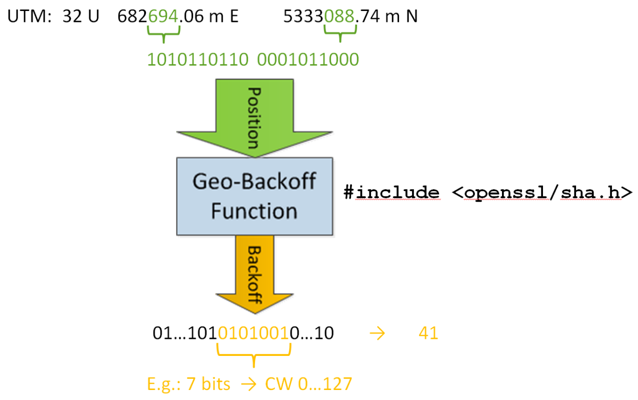


Fig. 4. Prototype implementation of our crypto-hash based geo-backoff function.

1) Crypto-hash Based Geo-Backoff: Our first attempt to further reduce close-by collisions is to make use of cryptographic hash functions. These special functions have a relevant property:

> *A slight change in the original message (e.g. a bit-flip) results in a significant change of the hash value.*

This property is known as the *avalanche effect*. The term was first introduced by Feistel in 1973 [11], but the concept is actually based on *diffusion*, already introduced by Shannon in 1949 [12].

For our crypto-hash based geo-backoff concept, we intend to transfer this property to VSC, i.e. we aim to have a geo-backoff function, which provides the following property:

> *A slight change in position (e.g. difference by just a few meters) results in a significant change of the generated backoff counter.*

Hence, our initial idea is to use a cryptographic hash function to calculate the backoff counter with the current position as input. As close-by vehicles only show a minor change in position, our crypto-hash based geo-backoff function is expected to generate a significant different hash value, from which the backoff counter is extracted.

Another interesting property of the crypto-hash based geo-backoff is that it is working on absolute positions only. There is no need to transmit the current position of other vehicles before, in order to determine the current distance. That means no additional overhead is introduced by using the crypto-hash based geo-backoff. In order to avoid that two close-by vehicles will generate the same crypto-hash value, a certain position precision is required, i.e. close-by vehicles must provide different position measures.

Our implementation approach for the crypto-hash based geo-backoff function is illustrated in Fig. 4. It takes the current position of the backoff generating vehicle as input. To get a high variety of the position inputs, we extract the relevant digits only. In our case we consider distances up to 999 m (in order to cover the communication range) with a resolution of 1 m. Note that the geo-backoff function is not only limited to Universal Transverse Mercator (UTM) coordinates. Other coordinate systems can be used as well.

Once the relevant digits have been extracted from the position coordinates, they are passed to the geo-backoff function. Here, the geo-backoff function is represented by the cryptographic hash function SHA-256. As a consequence, our SHA-256 geo-backoff function calculates a 256 bit hash value from the corresponding position input. Since the entire hash value is too long to represent an appropriate backoff counter, we extract a certain amount of bits from the hash value to generate the backoff counter (e.g. 8 bit for a backoff counter between 0 and 255). For well designed cryptographic hash functions it does not matter which bits are extracted, as each output bit depends on all input bits (completeness property [13]).

2) Grid based Geo-Backoff: The second geo-backoff approach investigated in this paper is based on a grid, which is mapped onto the road. Then the backoff counter is generated depending on which cell the vehicle is currently located in. The big advantage of the grid based geo-backoff concept is that dependent on the grid design/mapping it can be guaranteed, that vehicles in different cells will generate different backoff counters for sure.

In order to satisfy the latency requirements for safety-critical messages, the size of the contention window cannot be arbitrarily large. Hence, grid cells may recur at a certain distance, and therefore the backoff counter values as well. To avoid *same backoff* collisions within a certain grid section, equal backoff counter values should be mapped to cells, which are displaced as far as possible. Another layout criterion is the cell size. If designed too small, backoff counter values are recurring at shorter distances. If chosen too big, the probability that at least two vehicles are located within the same cell (they would choose the same backoff counter) is too high.

To obtain an efficient grid layout, we aim to distribute the grid cells in longitudinal direction along the road shape, so that each cell only covers parts of the road, i.e. the locations at which a vehicle is likely to appear. Therefore, we intend to make use of the current location information along a certain road, obtained for instance from map information. In lateral direction, we try to map the cells on one lane each. In principal, we use a hash function again, which takes the current position along the road and the current lane number as input and calculates the corresponding backoff counter. Assuming that map information, including road topology and more, is available, and assuming that GNSSs like Galileo in combination with additional sensors are able to provide lane level position precision, it should be feasible for vehicles to map themselves into the corresponding cells with sufficient reliability.

IV. EVALUATION BY SIMULATIONS

The geo-backoff concept presented above has been evaluated by means of simulations. The corresponding scenario and results are described hereafter.

A. Scenario

In DSRC-based vehicular networks the problem of packet collisions is the worse the higher the traffic/data load. Thus, a multi-lane highway has been implemented within the ns-3 network simulation framework [14], to represent a challenging communication scenario. The highway has a length of 10 km with 6 lanes in each direction. To avoid border effects, the evaluation has been limited to the core of the highway, i.e. between 2.5 km and 7.5 km. For each lane the vehicles have been generated following an Erlang distribution with a mean time-ahead distance of 2 seconds[2], plus an additional time gap of 0.25 seconds to account for the vehicles' length. As we are focusing on the communication issues in VSC, the mobility of the vehicles have been simplified, i.e. no lane change maneuvers and all vehicles are driving with constant speed, which is increased from the outer (20 m/s) to the inner lane (40 m/s) with an increment of 4 m/s.

In order to comply with the European Profile Standard ITS-G5 [4], the Wi-Fi implementation in ns-3 has been adapted accordingly. That means, CAMs are transmitted with a maximum power of 33 dBm on the 10 MHz control channel at 5.9 GHz with a default data rate of 6 Mbit/s. As we are focusing on MAC layer effects, a simple radio propagation model has been used. We have chosen the log-distance path loss model with exponent 2.35 in order to achieve a communication range of approx. 970 m ($\approx$ 1 km). That a maximum communication range of about 1 km is not unrealistic, has been demonstrated, for instance, by Gallagher *et al.* [15] as well as Schmidt *et al.* [16]. The error model in our simulation is Signal to Interference and Noise Ratio (SINR) based (see [14]).

To evaluate our results we make use of the following metrics:

- *Collision rate:* The number of packet collisions, normalized in time and space.
- *Collision type ratio:* The relative shares of the different packet collision types.
- *Latency:* The end-to-end delay between the transmitter and the corresponding receiver (traditional TX-RX metric).
- *Update delay (UD):* The elapsed time between two consecutive successfully received CAMs from the same transmitter (RX-centric metric).

Based on its definition, the update delay is a pure receiver-based metric and is perfectly suited to evaluate the up-to-dateness of current status information about the corresponding vehicle from a communications perspective. In other publications, e.g. [17], [18], [19], [9], the update delay is better known as '(Packet) Inter-Arrival Time' or 'Inter-Reception Time'. However, the main difference is that we use a special representation called *Complementary Cumulative Distribution Function (CCDF)*. The advantages are twofold: First, the distribution keeps all the measured information which is not the case by focusing on average values and/or confidence intervals. Second, as we are focusing on the reliability of VSC, we are interested in probability values very close to 1. Although using a log-scaled probability axis, the CDF does not provide the necessary resolution around 1. By using the CCDF = 1 − CDF, we can get (theoretically) an infinite resolution around the value we are interested in.

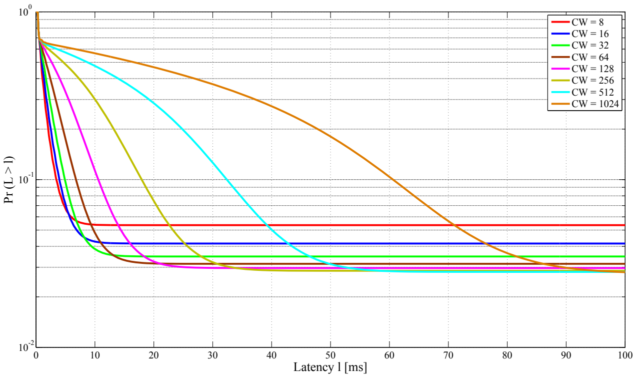


Fig. 5. Latency CCDF within the close vicinity (up to 100 m).

B. Results

The common justification for keeping a small CW (currently 8 slots) is based on the traditional TX-RX perspective, i.e. to strictly limit the end-to-end delay (latency) of CAMs to 100 ms maximum, as postulated in [3]. Sure, increasing the CW will increase the latency as well. But the question is: *do we violate the latency requirements if increasing the CW?*

Hence, we start by first analyzing the latency behavior after applying step 1 (i.e. increasing the CW size only). Fig. 5 shows the latency distribution within the close vicinity (i.e. up to 100 m) for various CW sizes (powers of 2). Even for the latency we use the CCDF representation, due to the advantages mentioned above. It simply provides the probability (y-axis) of exceeding a given latency value (x-axis).

As expected, the figure clearly shows the increasing latency with increased CW size. It also shows that the different curves are converging towards a certain probability value. This is the probability of not receiving a CAM at all (infinite latency), i.e. 1 - reception probability. Obviously, increasing the CW also increases the reception probability. However, the improvement of the reception probability is getting less significant with increasing the CW size. For CWs of 256 and more the reception probabilities have converged to approx. the same value. Although the latency by using a CW size of 1024 is still below the requirement of 100 ms (see [3]), this could be an indication for selecting an "optimal" CW size regarding latency and reception probability. Assuming the CW size is only increased within certain limits, then, the answer to the previous question is: *increasing the CW is fully in line with the latency requirements for CAM based safety applications!*

As we are focusing on the CAM dissemination performance, the delay between two consecutive successfully received CAM updates from the same transmitter (update delay) is of much more interest (RX-centric perspective). First, we compare the update delay performance of the default backoff approach with

---

[2] Recommended time-ahead distance in Germnay

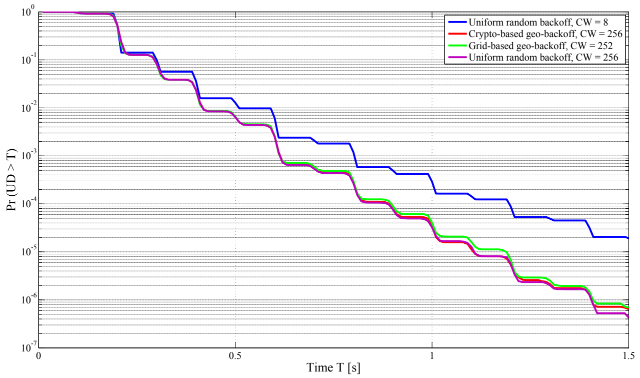


Fig. 6. Comparison of the Update Delay performance within the close vicinity only (up to 100 m).

our geo-backoff implementations within the entire communication range. In that case, the results show no significant improvement. Hence, we do not show them here.

Next, we will focus on the close vicinity, which is much more critical for vehicular safety than large ranges. Fig. 6 compares the update delay performance of the default uniform random backoff mechanism (CW = 8) with our geo-backoff implementations within a range of 100 m. In order to differentiate the improvements coming from the CW increase (step 1) and the improvements coming from the geo-based backoff generation (step 2), we also show the default backoff mechanism with similar CW size (CW = 256), as used for the geo-backoff approaches. Similar to the latency plot, the various update delay CCDF curves provide the probability (y-axis) of exceeding a given time delay value (x-axis). To provide a better understanding of how to use the update delay CCDF figures, lets assume a cooperative safety application, which requires to receive the next CAM update from other vehicles within the critical range after 1 second latest with a probability of 0.9999. That means the probability of exceeding an update delay of 1 s should be less than 10^{-4}. This can be easily checked by evaluating the update delay CCDF curves. Considering Fig. 6, we can observe that all approaches with increased CW size are able to fulfill this example requirement, except the default mechanism. But even more interesting is the fact that the default mechanism with increased CW performs just as well as the geo-backoff approaches.

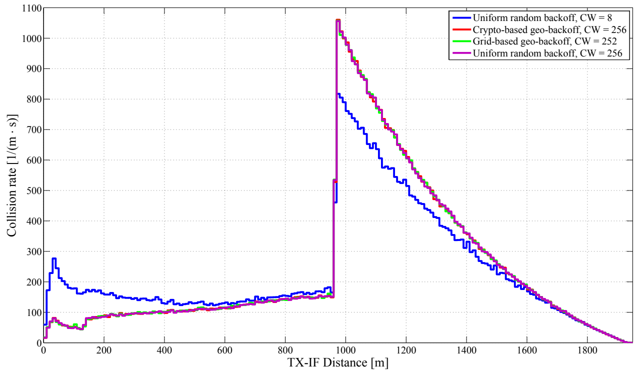
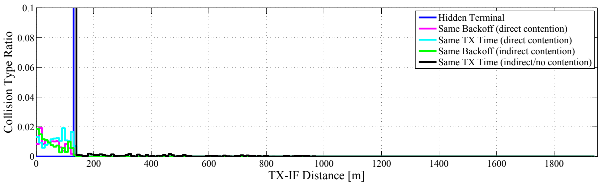
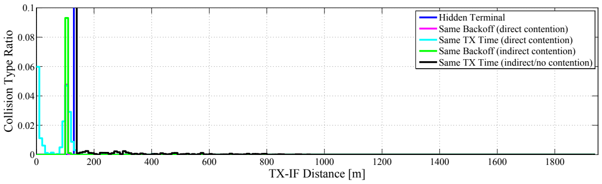


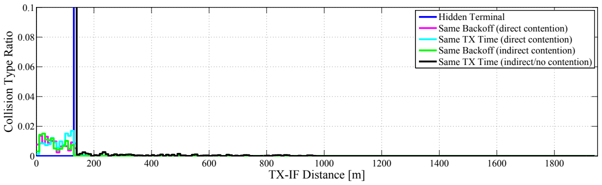
Fig. 7. Total collision rate over the distance between the two colliding transmitters for all considered approaches (distance resolution = 10 m).



(a) Crypto-based geo-backoff with a CW size of 256.



(b) Grid-based geo-backoff with a CW size of 252.



(c) Default backoff mechanism with an increased CW size of 256.

Fig. 8. Collision type ratio as a function of the distance between the two collision inducing transmitters.

This observation suggests that the improvement is not a result of the geo-backoff concept but of the increased CW. A closer look on the collisions again may provide a better understanding. Fig. 7 compares the total collision rates as a function of the distance between the two collision inducing transmitters for the different approaches with each other. The first observation from that figure is that compared to the default mechanism all approaches with increased CW show a significant reduction of the number of collisions within the communication range. Especially at very close distance (≈ 40 m), the collision rate has been reduced by approx. 71 %. This may explain the improved update delay performance within close vicinity (cf. Fig. 6). The second observation is that within the main hidden terminal area the behavior is the other way around. Thus, the approaches with increased CW now show slightly higher number of collisions than the default one. This behavior corresponds to our desired behavior introduced above, i.e. shifting collisions from close-by to far-away. But the most interesting observation again is that the crypto- and the grid-based geo-backoff approaches do not show any improvement compared to the default backoff mechanism with similar CW size.

A more detailed view is given by Fig. 8, showing the collision type ratio as a function of the distance between the two collision inducing transmitters for the crypto based geo-backoff, the grid based geo-backoff and the default mechanism with increased CW, respectively. Whereas the crypto based geo-backoff mechanism was able to reduce the *same backoff* collisions in the close vicinity from approx. 45 % to approx. 3-4 %, the grid based geo-backoff approach was able to reduce them completely up to a certain range. The peak after demonstrates the recurrence behavior of grid cells, due to a limited CW size. Then, vehicles at a certain distance (in our case approx. 100 m) will choose the same backoff counter for sure, if both are in contention with each other. Considering the default random mechanism with increased CW size, however, we can observe that it is able to reduce the *same backoff* collisions just as well as the crypto based geo-backoff approach. Apparently the crypto based geo-backoff function provides a similar backoff counter distribution as the default mechanism (uniformly distributed). This observation explains the similar behavior with respect to update delay performance and collision rate. Taking also the grid based geo-backoff approach into account, obviously a further reduction of the remaining *same backoff* collisions is not significant enough to show up in an additional improvement of the communication performance (cf. Fig. 6).

V. CONCLUSION

Small contention windows in DSRC-based VSC provide a high probability of contending vehicles choosing the same backoff counter. This leads inevitably to simultaneous transmissions causing packet collisions, especially at close ranges. In this paper we have introduced a new concept for the DSRC backoff procedure called *geo-backoff*: In a first step, we increase the CW to reduce the probability of choosing the same backoff counter in general. In the second step, we aim to further reduce the probability of simultaneous transmissions in the close vicinity by selecting the backoff counter as a function of the vehicle's current position. The simulation results have shown that the update delay performance (RX-centric) could be improved by using geo-backoff. However, further investigations have shown that this improvement is dominated by the first step only, i.e. increasing the CW. The conclusion we draw from these observations is not necessarily disappointing. Simply increasing the CW might be the most attractive solution here: first, it is simple and fully compliant with the current DSRC technology (no HW/SW modifications necessary). And second, increasing the CW size properly does not imply any latency issues referring to the requirements claimed in [3].

ACKNOWLEDGMENT

The results presented in this paper have been achieved thanks to the activities carried out within the European FP7 GLOVE (joint GaliLeo Optimization and VANET Enhancement) project - Grant Agreement n. 287175. The objective of the GLOVE is to explore the potential technical, scientific and application benefits coming from the coupling between Vehicular Ad Hoc Networks and Galileo on-board receivers.

EURECOM acknowledges the support of its industrial members, namely, BMW Group Research and Technology, IABG, Monaco Telecom, Orange, SAP, ST Microelectronics, and Symantec.

REFERENCES

[1] T. Biehle, "WG Roadmap - Whats needed for Deployment 2015?" November 2012, Presentation at Car2Car Forum 2012.

[2] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI Std. EN 302 637-2, Rev. 1.3.0, August 2013.

[3] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," ETSI TC ITS, Technical Report 102 638, june 2009, version 1.1.1.

[4] ——, "Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band," ETSI TC ITS, European Standard 202 663, november 2009, version 1.1.0.

[5] *802.11-2012 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE IEEE Standard 802.11-2012, 2012.

[6] N. Balon and J. Guo, "Increasing broadcast reliability in vehicular ad hoc networks," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, ser. VANET '06. New York, NY, USA: ACM, 2006, pp. 104–105. [Online]. Available: http://doi.acm.org/10.1145/1161064.1161088

[7] D. Rawat, D. Popescu, G. Yan, and S. Olariu, "Enhancing VANET Performance by Joint Adaptation of Transmission Power and Contention Window Size," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, no. 9, pp. 1528–1535, Sept. 2011.

[8] R. Stanica, E. Chaput, and A.-L. Beylot, "Local density estimation for contention window adaptation in vehicular networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, Sept 2011, pp. 730–734.

[9] R. Reinders, M. van Eenennaam, G. Karagiannis, and G. Heijenk, "Contention window analysis for beaconing in VANETs," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, July 2011, pp. 1481–1487.

[10] B. Kloiber, J. Härri, F. de Ponte Müller, and S. Sand, "Random Transmit Jitter Against Correlated Packet Collisions in Vehicular Safety Communications," in *WiVEC 2014*, 2014.

[11] H. Feistel, "Cryptography and Computer Privacy," *Scientific American*, vol. 228, no. 5, 1973.

[12] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[13] J. Kam and G. I. Davida, "Structured Design of Substitution-Permutation Encryption Networks," *Computers, IEEE Transactions on*, vol. C-28, no. 10, pp. 747–753, 1979.

[14] Network simulator ns-3, http://www.nsnam.org. [Online]. Available: http://www.nsnam.org

[15] B. Gallagher, H. Akatsuka, and H. Suzuki, "Wireless communications for vehicle safety: Radio link performance and wireless connectivity methods," *Vehicular Technology Magazine, IEEE*, vol. 1, no. 4, pp. 4–24, Dec 2006.

[16] R. K. Schmidt, B. Kloiber, F. Schüttler, and T. Strang, "Degradation of Communication Range in VANETs Caused by Interference 2.0 - Real-world Experiment," in *Proceedings of the Third International Conference on Communication Technologies for Vehicles*, ser. Nets4Cars/Nets4Trains'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 176–188. [Online]. Available: http://dl.acm.org/citation.cfm?id=1987310.1987329

[17] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, ser. VANET '06. New York, NY, USA: ACM, 2006, pp. 1–9.

[18] Y. Fallah, C.-L. Huang, R. Sengupta, and H. Krishnan, "Analysis of Information Dissemination in Vehicular Ad-Hoc Networks With Application to Cooperative Vehicle Safety Systems," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 1, pp. 233 –247, jan. 2011.

[19] T. Tielert, D. Jiang, Q. Chen, L. Delgrossi, and H. Hartenstein, "Design methodology and evaluation of rate adaptation based congestion control for Vehicle Safety Communications," in *Vehicular Networking Conference (VNC), 2011 IEEE*, nov. 2011, pp. 116 –123.