Fixing the performance issue of the IEEE 802.11p MAC layer CSMA based broadcast protocol

Maximilian Strauch

***Abstract*—The IEEE 802.11p standard specifies the physical and MAC layer operations for interchanging wireless broadcast messages in a vehicular environment and is part of the IEEE WAVE standard for vehicular safety applications. Nevertheless using the IEEE 802.11p MAC layer on scenarios with high node densities results in a congestion issue manifested by low packet reception ratios which might result in further problems for safety services in a vehicular context.**

This article motivates the issue through empirical evidence, gathered in an advanced simulation model. Furthermore two completely different solution approaches are presented: an asynchronous, improved ETSI DCC version along with a deterministic synchronous approach to perform time division multiplexing through an IEEE 802.11p MAC overlay layer by preserving full IEEE 802.11p compability.

This article summarizes the results presented in the paper *"Congestion Control for Vehicular Safety: Synchronous and Asynchronous MAC Algorithms"* by S. Subramanian *et al.* from the VANET conference 2012.

***Index Terms*—IEEE 802.11p, broadcast protocol, empirical performance analysis, DCC, TDM**

I. Introduction

A. The context of VANETs

Communication between vehicles (*V2V*) or between vehicles and the infrastructure (or *roadside*, *V2I*) have a growing importance. Thereby V2V denotes a direct communication link between cars inside a road enivironment to interchange messages for security reasons (e.g. accident warning) or other use cases [1]. The V2I is used as a communication link between the vehicle and intelligent roadside stations (*IRS*, e.g. traffic sign). The IRS nodes are gateway nodes which might provide a gateway into the internet for user convenience or provide security mechanisms to forward an emergency call or provide other services [2]. If vehicles communicate this way the network is called a Vehicular Ad Hoc Network (VANET).

The term Dedicated Short Range Communication (*DSRC*) is the technology associated to this concept of *V2V* or *V2I* communication. This technology differs between different countries (USA, Europe, Japan) but is assigned to the 5 GHz frequency band providing seven 10 MHz channels for communication. One channel is reserved for security related use and has a high availabilty and low latency providing an emergency communication link [2] [1]. The European Telecommunication Standards Institute (*ETSI*) provides its own standards but they correspond to the IEEE standards [3] [4] [5]. The concept of DSRC ranges from safety scenarios, to protect beings and prevent accidents, over traffic efficiency scenarios, to control traffic flow and prevent traffic jams, to infotainment tasks to provide internet connection via IRS or other roadside gateway mechanisms [2]. An example use case is shown in figure 1.

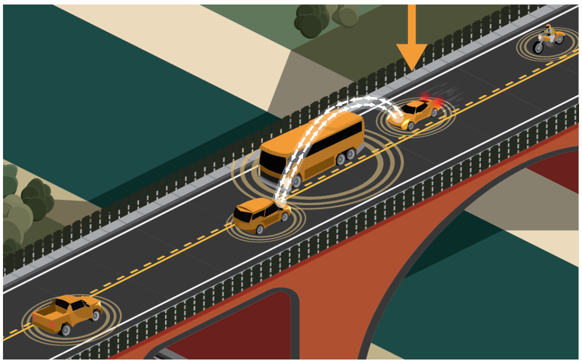


Fig. 1. An application of DSRC and V2V communication: *road safety*. A driver is warned if the passing lane is occupied and a slower-moving vehicle cannot be passed safely. Adapted from: [6], courtesy of U.S. DOT.

B. Technical implementation

The protocol stack used to provide this DSRC safety services is called IEEE WAVE *or* Wireless Access to Vehicular Environment. IEEE WAVE enables communication over a range of approximately 1000m between vehicles driving with up to 200km/h. Thereby a vehicle can be a car, a truck, a rail vehicle or a ship. The entire WAVE protocol stack is fairly complex utilizing many algorithms and structures to enable a richness of features as already described.

The physical (*PHY*) layer and MAC layer are of particular interest for this article since they currently have an issue where for high node densities the package reception ratio degrades and therefore congestion arises. Both layers are provided by the IEEE 802.11p standard [7]. IEEE 802.11p is based on the IEEE 802.11 WLAN standards (a/b/g/n) and tuned to fit the needs of embedded devices in the vehicular context [4]. The reason for using the existing WLAN technology is very simple: it is a well tested technology with highly available chipsets for a cheap price since WLAN devices are very common [4].

Since IEEE 802.11p is derived from the IEEE 802.11a technology it shares the MAC layer protocol which is based on CSMA [7]. IEEE 802.11p lacks the mechanism of ACKs since a V2V or V2I device sends a packet to all devices in the near range (broadcast) [4]. One major adaption is done at the contention window (*CW*) of CSMA for IEEE 802.11p: the back-off counter is selected from the static interval $[0, \mathrm{CW}]$ where CW is fixed [4]. For CSMA/CD, used in "regular" ethernet, the interval from which the back-off counter is selected is $[0, 2^i - 1]$ where i denots the number of failed transmission attempts [8, p. 29]. This value is therefore dynamic since i changes per node over time.

Many studies of the near past reported that IEEE 802.11p has serious issues with high node densities where the packet reception ratio drops as revealed by [9], [10], [11], [12]. The authors of these publications observed that packets get often destroyed for nodes which are close by although CSMA uses a back-off mechanism to wait a specific time before retransmitting based on randomly picking a delay which is based also on unsuccessful attempts of the node [4].

In this article the paper *"Congestion Control for Vehicular Safety: Synchronous and Asynchronous MAC Algorithms"* from *S. Subramanian et al.* [5] is presented along with some backing from [4] where an analytical approach to analyzing this issue is presented. The base paper [5] empirically *analyzes* the performance problem of IEEE 802.11p CSMA based broadcast messages and presents two different solutions.

The rest of this article is therefore organized as follows: first the issue is presented in more detail with some background information. Then two different soltuions to solve this problem from [5] are explained. This article finishes with a brief overview over related work and a conclusion of the results of [5]. The next subsections give some background information needed for the main content.

C. Simulation setup

The empirical results of [5] shown are generated through the simulation of a simple six lane road with a length of 2 km[1]. The vehicles are evenly and equidistant spaced on the lanes and different densities are created by controlling the number of vehicles placed on the lanes. The lanes wrap-around by their length creating an infinite long lane. The simulation software used by [5] is the ns2 [13] platform along with the `80211MacExt` to simulate the IEEE 802.11p functionalities [5]. Some important values of the simulation setup are:

- CW is fixed to $\mathrm{CW} = 15$ (static CW value).
- The broadcast safety packets are periodic and have a periodicity of 100ms.
- The broadcast packets have a length of 200byte and take around 0.55ms to be transmitted.

D. Back-off process of IEEE 802.11p

The back-off process of IEEE 802.11p is used to avoid packet collisions. Transmitting directly whenever a node wants to send will result in many collisions. So the back-off process coordinates the time when a node transmits a packet considering currently ongoing transmissions and therefore it tries to reduce the amount of collisions. Figure 2 shows the process of transmitting a typical packet according to IEEE 802.11p MAC layer.

Every slot consists of an inter-frame space (*IFS*), back-off slots and a packet transmission [4]. At the beginning a node, which is ready to send, selects its back-off counter from $b \in [0, \mathrm{CW}]$ [4], assuming $b = 6$ for the example from figure 2.

[1]Each lane has a width of 4m. Therefore the simulation field has a size of 0.048km^2 which is equal to around eight FIFA soccer fields or the wing area of 91 Boing 747 airplanes.

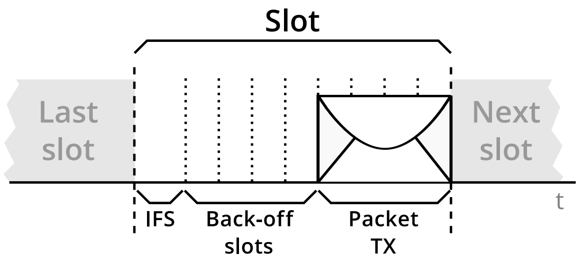


Fig. 2. IEEE 802.11p back-off process for a typical packet. A node decrements its back-off counter until it reaches zero and then transmits the packet. Adapted from: [4].

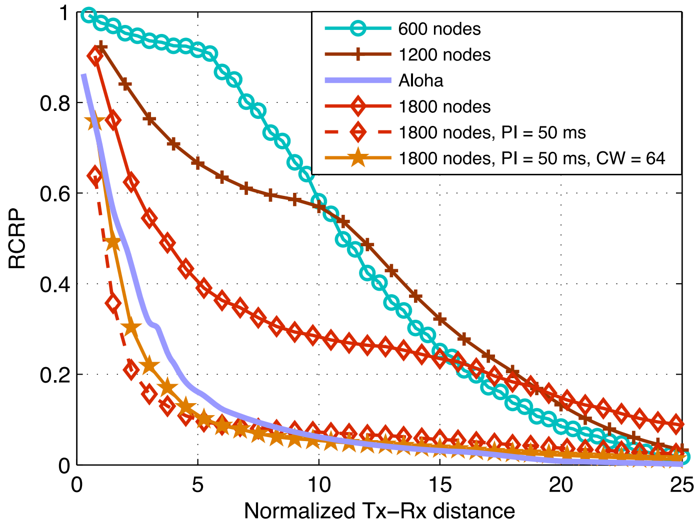


Fig. 3. IEEE 802.11p transmission performance. Normalized TX-RX distance on the x-axis against the RCRP on the y-axis for multiple device densities. The higher the device density grows the faster the RCRP drops. PI $= 50$ ms indicates a scenario where only 50ms out of 100ms broadcast messages can be sent. Adapted from: [5].

After the IFS - where no transmission is allowed - is passed the first back-off slot begins. Since $b > 0$ the node decrements b to $b = 5$ at the beginning of the first back-off slot. At the beginning of the fifth back-off slot, b is decremented to $b = 1$ but the node senses a busy channel so it freezes b and goes idle until the next slot begins and the next IFS is passed. At the second back-off slot of the next slot it will begin transmitting regardless of the channel state since $b = 0$ and possibly create a collision [4].

This also shows the problem why the congestion issue exists: when a node has decremented its counter to zero it will send ignoring the state of the channel [4]. And if there is a node which also counted down to zero both packets will collide. Since the CW value is relatively small (e.g. commonly 15 [5], [4]) and high node densities have many nodes which want to communicate at the same time it is very likely that many nodes selected initially the same CW value and end at zero the same time creating a collision.

II. Problem Presentation

The congestion issue comes from the fact that many devices count their back-off counters synchronously down and start transmitting at the same time destroying packets of other transmitting nodes [5]. Since the packets are small compared to the periodicity most of them are transmitted directly [5]: the standard 200byte message takes around 0.55ms and is repeated every 100ms. Hence packet collisions are of special interest compared to the delay of a packet transmission caused by the back-off waiting time [5].

Figure 3 shows the result for the simulated lane environment for different node densities. The normalized TX-RX distance is simply calculated by dividing the distance between transmitter and receiver by the inter-node-spacing which is equidistant. The ratio of correctly received packages (*RCRP*) can be interpreted as the probability of a successful transmission [5]. In general it can be seen that for fixed periodicity, fixed packet size and a growing node density the distance over which nodes can safely communicate (*carrier sense range, CSR*) drops. In an ideal scenario the number of discovered nodes should remain constant for any node [5]. Furthermore figure 3 shows that for growing node densities the rate of successful transmitted packets drops significantly. By reducing the allowed transmission time from 100ms to the half and plotting also results for an ALOHA MAC layer instead of IEEE 802.11p it can be observed that the functions have similar behaviour. This leads to the observation that with growing node densities the performance of IEEE 802.11p degrades to an ALOHA-behaviour [5] [4].

The ALOHA protocol was developed in 1970 to connect the islands of Hawaii. The MAC layer is responsible for creating an organized access of all attendees to a channel [14]. Every attendee, who wants to send, sends at any time. If two attendees send at the same time a collison will occur and both must send their packet again. Before that both wait a random amount of time. Another premise is that all packages have the same length. The collision is detected by the sender through a missing ACK of the recipient [14]. The ALOHA protocol can be analyzed for its throughput using a random distribution model (Poisson distribution). A channel managed by ALOHA is utilized by $\approx$ 18%. This value is low since there is no organization and every attendee sends at a random time [14].

The *slotted* ALOHA MAC layer is an upgrade which behaves the same except for the fact that the time is slotted and an attendee can only start sending at the beginning of a slot. The throughput is therefore higher at $\approx$ 36.8% [14].

Figure 3 also shows that increasing the CW value by *approx.* four times does not affect the RCRP significantly [5]. Since 802.11p degrades to an ALOHA-like behaviour for high node densities there are no guard zones[2] around a transmission provided which one could expect due to the carrier sense mechanism [5]. Figure 4 shows the empirical probability mass function (*PMF*) for the distance to the closest concurrent transmitter [5]. It can be observed that for growing node densities the distance to the nearest concurrent transmitter drops. For a density of 1800 nodes the probability is at around 21.5% that the nearest transmitting node is only around 20m away and statistical majority is at distances under 75m. Therefore it can be seen that there are no guard zones provided by the protocol where in a fixed perimeter around a node no other node transmits. But these guard zones should by theory exist due to the *carrier sense* mechanism [5]. This also emphasizes the drift to an ALOHA like behaviour.

[2]A "guard zone" is an area around a node in which this node can sense ongoing transmissions also known as *carrier sense range* (*CSR*).

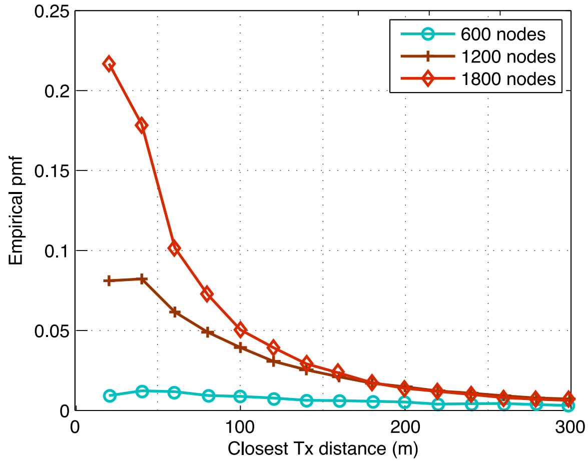


Fig. 4. No guard zones are provided by 802.11p. The x-axis shows the distance from a node to the nearest node which transmits concurrent. The y-axis shows the frequency of this distance in the empirical simulation of [5]. The CSR is 297m [5]. Adapted from: [5].

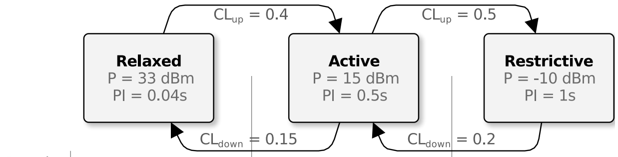
It can be concluded that the congestion problem of IEEE 802.11p arises from the fact that the probability of two devices staying in the same carrier sense range and counting their back-off counter both down to zero increases significantly [5]. The solution proposed by [5] tries to solve this issue by reusing and refining an existing solution from ETSI on the one hand and making the IEEE 802.11p synchronously by slotting the time and setting up a contention mechanism between nodes for these time slots on the other hand [5].

III. Asynchronous solution

A. Introduction of plain DCC

Regarding the shown congestion issue the ETSI developed a solution called Decentralized Congestion Control (*DCC*) to solve congestion at high node densities [3]. This approach consists of a state machine which sets transmission parameters according to the current state and tries to get the issue under control using these means [3, p. 20].

Figure 5 shows a simplified version of the state machine of DCC. Beneath other parameters a state includes the transmit power (*P*) and the packet transmission interval (*PI*) [3]. In contrast to the plain IEEE 802.11p protocol where P, PI and the other parameters are fixed this approach adapts the values to the environment and the channel load. Therefore the transitions are core elements to control the behaviour. They are coupled to the channel load (*CL*) which is the fraction of time when the received power is greater than the carrier sense threshold (*CST*) which is basically a fixed power threshold value [5].



Density			
600	1%	91%	8%
1200	1%	90%	9%
1800	1%	90%	9%

Fig. 5. DCC state machine with parameters power (*P*) and packet transmission interval (*PI*). Underneath the state distribution gathered from the simulation is shown for every state and the different node densities [5]. Adapted from: [5], [3].

- The transitions to a more restrictive state occur when the channel load for the last second was larger than CL_{up} [5].
- The transitions to a more relaxed state occur when the channel load for the last five seconds was lower than CL_{down} [5].

To evaluate the improvement of DCC over plain IEEE 802.11p one can take a look at Figure 6 (a) from the simulation [5]. For distances up to 300m the RCRP is significantly better in comparison to plain 802.11p [5]. This performance boost comes from a reduction of traffic through DCC, meaning that less packets are sent per time compared to IEEE 802.11p. This way DCC was able to improve the RCRP. Figure 6 (b) shows this pitfall: using plain 802.11p the total number of received packets is significantly better than DCC although DCC might improve the RCRP per packet [5].

By reducing the number of packets per time another problem arises: in WAVE safety messages are exchanged very often and the quality of service relies on the fact of frequent updates (e.g. GPS position update) [5]. Therefore the behaviour of DCC – reducing to number of packets per time and increasing the quality this way – might be not reasonable and leads to the fact that DCC is not usable in safety applications where the packet throughput is important [5]. The origin of this issue with DCC can be seen in figure 5 where the state distribution from the simulation is shown: most of the time nodes stay independent of the density in the ACTIVE state with conservative parameters and a low PI [5]. This results in the low packet throughput shown before.

B. Improvement of DCC

The main issue with DCC is that the state machine does not differentiate fine enough between the different levels of congestion [5]. The authors of [5] developed an approach using only transmit power control (*TPC*) to gain more performance and preserve the other parameters from IEEE 802.11p.

Figure 8 shows a refined version of the DCC state machine incorporating more states. The first issue with plain DCC is that the CL is defined too low (figure 5) [5] and state transitions happen too fast. The challenge is to find a good

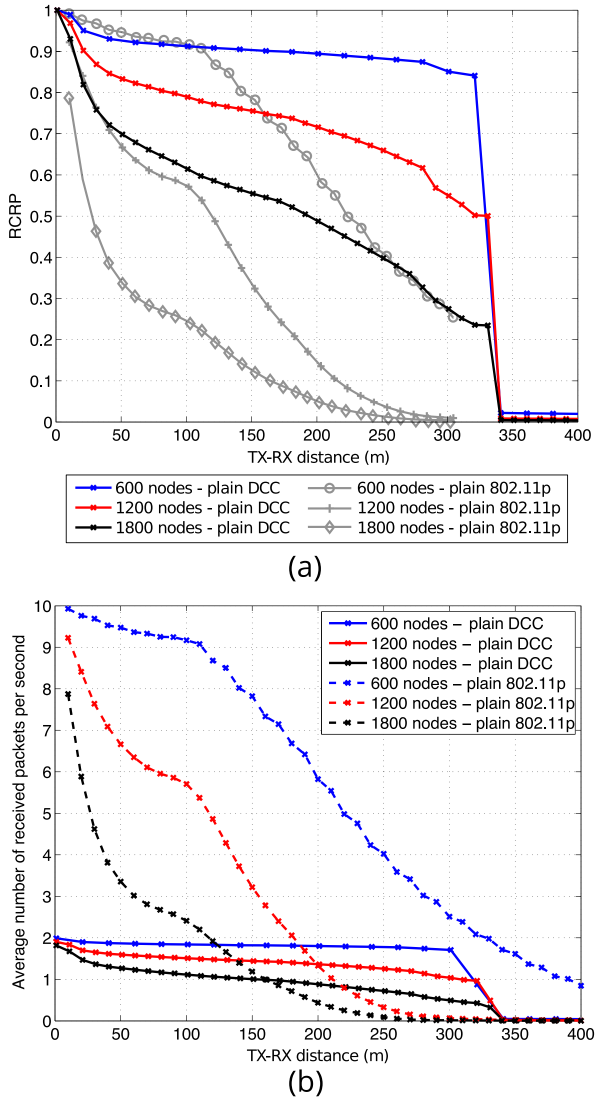


Fig. 6. DCC performance and pitfall. Diagram (a) shows DCC compared to plain IEEE 802.11p with the TX-RX distance on the x-axis and the RCRP on the y-acis. Diagram (b) shows the average received packets on the y-axis and the TX-RX distance on the x-axis. Adapted from: [5].

tradeoff for the CL so that it is large enough to maximize the utilization and that it keeps the packet collision rate low [5].

Another outcome of the empirical data from the simulations is that for all densities the total number of recieved packets increases along with increasing the CL up to 0.65 within $\pm 5\%$ [5]. When the CL exceeds 0.8 the number of received packets decreases [5]. By selecting 55% and 65% as CL thresholds the performance will be increased in comparison to plain DCC since they are gathered from empirical data.

Figure 7 compares the performance of the optimized DCC variant against plain IEEE 802.11p. At high device densities the optimized DCC protocol provides a much higher reception rate [5]. For a density of 1800 devices at a distance of 50m the optimized DCC variant has a reception rate which is almost twice as high as the rate for plain IEEE 802.11p MAC (optimized 60% whereas plain IEEE 802.11p leads to

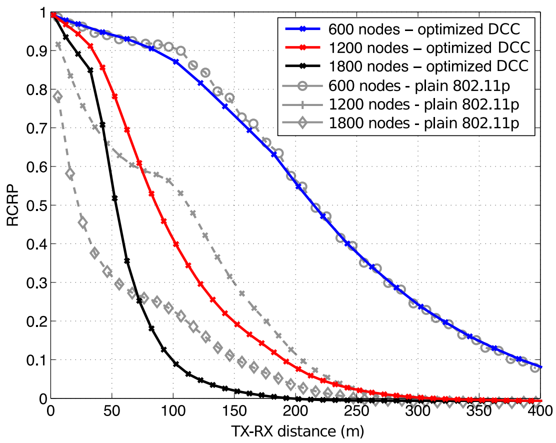


Fig. 7. The optimized DCC variant is much more performant than plain IEEE 802.11p. Adapted from: [5].

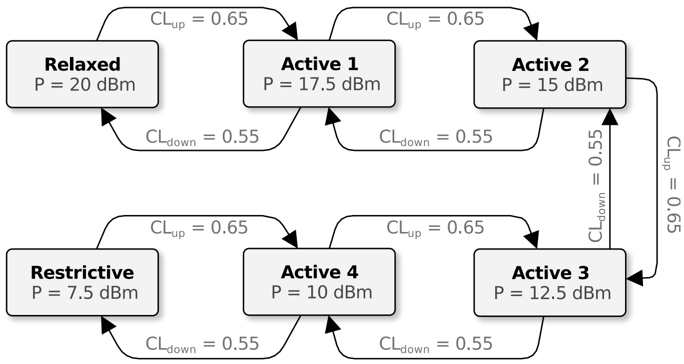


Fig. 8. By [5] optimized DCC state machine only using power control. Level transitions (CL_{up}, CL_{down}) work as for plain DCC. Adapted from: [5].

35% [5]). Since the optimized DCC state machine preserves all values from plain IEEE 802.11p and especially does not change the PI it does not change the number of transmitted packets per second in contrast to the plain DCC approach [5]. So the gain of RCRP does not come with a huge downside like plain DCC where less packets are transmitted [5]. To the contrary the optimized DCC has no degradation in the number of sent packets. The undesired ALOHA behaviour is also removed [5]. This asynchronous optimized DCC approach inside the DCC framework is fully compatible with IEEE 802.11p [5].

IV. Synchronous Solution and Improvement

Since DCC is asynchronous it behaves non-deterministic. The advantages of a synchronous MAC design are two-fold:

1) The resource allocation per node does not change from interval to interval unless the topology or density changes [5].
2) The transmission attempts of each node are periodic resulting in deterministic delays and small variations [5].

Using a time division multiplex (*TDM*) scheme these synchronous improvements can be used. With TDM the time is divided into equal time slots and nodes can contend for a slot to send their data. To ensure a full compability to the

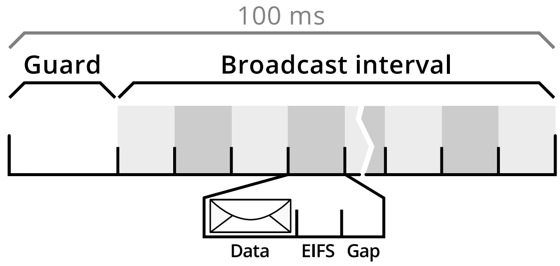


Fig. 9. Scheme of the SYNC layer behaviour based on TDM. A 100ms broadcast interval is divided into a short guard time (1ms) and 180 slots of length 0.55ms. A time slot consists of a typical broadcast safty messages with length 200 bytes an (E)IFS and a gap [5]. The numbers can be adjusted to custom values without violating the scheme [5]. Adapted from: [5].

asynchronous IEEE 802.11p MAC protocol this synchronous scheme is introduced as a seperate SYNC layer which is layed on top of the MAC layer [5]. The IEEE 802.11p MAC layer remains the original asynchronous layer and a custom SYNC layer containing the logic of this approach is then placed on top of the MAC layer and injects the packets in the original asynchronous layer in a manner that they are transmitted deterministic and synchronously [5]. Therefore the SYNC layer must overcome the fact that the injection time and packet transmission time does not coincide due to the back-off process [5]. Furthermore an accurate timing ($< 2\mu s$) over all nodes is needed to ensure that the clocks of the nodes are equal [5].

Figure 9 shows the basic TDM scheme used to create a synchronous communication. Each node selects a slot in the broadcast interval and the SYNC layer will push a packet to the 802.11p MAC layer at the beginning of a slot to start contention [5]. The problem here could be that the pushed packet in the MAC layer is delayed due to the back-off counter and ongoing transmissions [5]. This problem does not occur due to the clever structure of the TDM scheme: a node can transmit directly (which we want to achieve for the SYNC layer) when (a) the channel is free for at least the time EIFS[3] and (b) its back-off counter is zero [5]. Since a slot consists of EIFS and a small gap at the end (see figure 9) the channel is sensed free at the beginning of every slot and condition (a) is satisfied. For condition (b) the back-off counter must be lowered to 0 by the 802.11p MAC layer [5]. Since the broadcast interval has much more silence periods (not all of the 180 slots might be used by a transmission) than the CW value (e.g. $CW = 15$) so that the back-off counter is zero when a new packet from SYNC arrives [5]. Then the packet can be transmitted directly [5].

Accurate and equal clocks between the different nodes are provided through the Global Positioning System (*GPS*) [5]. It is most likely that vehicular systems have a GPS receiver on-board for obtaining location information and this receiver can provide time information to enable a sub-microsecond level

[3]*Abbr. for* Extended IFS which is used in CSMA after a collision occurred to prevent the node from directly retransmitting the packet. Here it is used as a waiting time.

accuracy which matches the $< 2\mu s$ time requirement [5].

By now we are able to bypass the IEEE 802.11p MAC layer scheme to enforce a synchronous scheme. The next step is to find an algorithm to decide whether a node can occupy a slot or not (contention mechanism) [5]. The core idea is to occupy resources which are far apart as possible [5]. This is done by a greedy algorithm that chooses low energy slots (where not much communication is happening) and updates this selection every L broadcast intervals [5]. In particular the algorithm goes through these steps [5]:

1) Every node observes the average energy for every slot for the last K broadcast intervals and orders these N slots in an increasing order [5].
2) The node picks randomly a slot x out of the first M slots where $M \ll N$ [5]. The first M slots are considered as the slots with the lowest energy [5].
3) In one of L broadcast intervals the node transmits a smaller packet in its slot to listen to other other devices in the remaining time and recalculates the list from 1). If the current slot is not any longer part of the first M slots the node continues with step 2 [5].

Figure 10 shows the results from the empirical simulation of this approch in comparison to the other presented approaches. First of all it can be seen in figure 10 (a) that the proposed scheme overcomes the plain IEEE 802.11p performance for all device densities for close distances [5]. It is very close to 100% for the near range but plain IEEE 802.11p is better at longer distances [5]. Moreover the SYNC MAC does not change significantly with different densities as compared to plain 802.11p [5]. Figure 10 (b) compares the proposed scheme to the previously presented optimized DCC variant. Just like at plain 802.11p the SYNC MAC performs better at close ranges than the optimized DCC and achieves a significantly higher RCRP for near distances which is close to 100% [5]. Furthermore the SYNC MAC was stress-tested with a random association of all contributing nodes to one of the 180 slots at the beginning. It turned out that almost all devices converged in approximately 15 broadcast intervals ($\approx$ 1.5s) to a orderly re-selected slot usage even under fading and mobility [5].

Another point are the existence and size of guard zones. For plain IEEE 802.11p the distance that 90% of the contained nodes are discovered is 13m whereas for SYNC MAC this number grows to 55m at a density of 1200 nodes [5]. For a density of 1800 nodes plain 802.11p cannot provide any guard zone between the current node and its nearest neighbour whereas SYNC MAC provides a guard zone of 35m [5].

V. Conclusion and Related Work

A. Related work

The presented congestion issue for IEEE 802.11p MAC layer and VANETs in general, having a low packet reception rate at high node densities, is well studied. To name but a few especially [9] and [10], [11] and [12] disovered the performance breakdown of the CSMA mechanism at high densities.

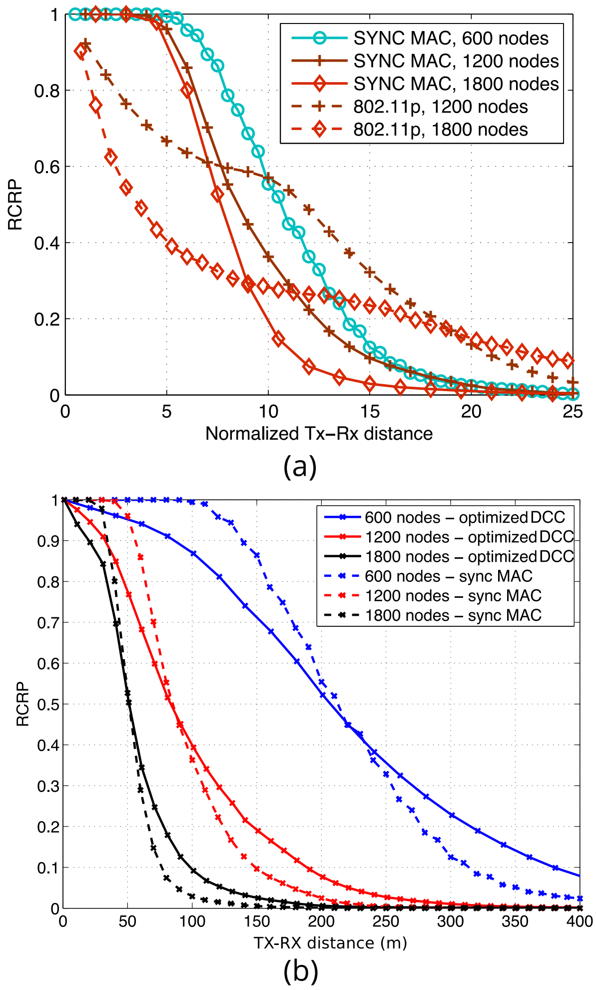


Fig. 10. Performance comparision of the proposed SYNC MAC. (a): Packet reception performance of the SYNC MAC with the normalized TX-RX distance on the x-axis and the RCRP on the y-axis. (b): Comparision between SYNC MAC and the optimized DCC with TX-RX distance on x-axis and the RCRP on the y-axis. Adapted from: [5].

In [4] the congestion issue in CSMA-based broadcast networks, especially the IEEE 802.11p MAC layer issue, is mathematically analyzed using stochastic geometry. It was proved that the network degrades for high densities to an ALOHA type behaviour [4] as presumed in [5]. Furthermore [4] establishes lower and upper bounds on the critical density where the behaviour changes from CSMA to ALOHA. [4] obtained metrics (e.g. the number of discoveries) and demonstrated how to optimize these metrics by adjusting the system parameters.

For the future it is expected that the DSRC technology is deployed into the public road traffic and new cars [1], [5]. But the author of this article could not find any latter substantial research results than the presented paper [5]. A work from 2015 [15] is concerned in general with an improvement of power control algorithms in DSRC. Another recent work [16] from 2014 presents a new analytical approach based on stochastic geometry like [4]. In particular [16] creates a model to consider concurrent transmissions from nodes within the carrier sense range. This way they lead to a more accurate and realistic analysis.

The paper [17] is published in the same year as [5] and approaches the congestion issue of IEEE 802.11p in another way. In the proposed scheme the transmit power or the transmission frequency of packets is reduced only in case of a confirmed congestion [17]. In order to confirm a congestion a set of metrics (e.g. *average waiting time* or *collision rate*) is created which reflect the current state of the VANET [17]. Therefore the performance is kept high since the parameters of the transmit power and frequency are only changed for a small amount of time when a congestion arises [17]. The computer simulation of [17] showed that this scheme is very efficient.

Despite this analytical and simulated results there are no research results of data accumulated on real hardware; only simulations are considered in the literature.

B. Conclusion

For high node densities a congestion issue arises with IEEE 802.11p. This congestion interfers with the usage of IEEE 802.11p in WAVE for safety applications in a vehicular topic since safety messages are transmitted very often in this application. Therefore the solution approach DCC was introduced which uses a state machine to set the parameters of IEEE 802.11p according to the current state. This way it improves the ratio of correctly received packets. According to the empirical simulation it turned out that DCC works well but has a major downside: it reduces the number of transmitted packets and thus reduces congestion. Because of the fact that this is impractical [5] optimized DCC by using a finer state machine and adjusting only the transmit power. Therefore the number of transmitted packets was preserved and the results are promising. But the downside is that the proposed solution is an asynchronous protocol.

To overcome this downside a synchronous protocol was developed. It is based on time division multiplexing (*TDM*) by dividing the time into slots in which each node can send its packet. This scheme is enriched with a distributed contention algorithm which decides locally on every node if a time slot can bew acquired. The synchronization of the clocks of the different nodes is achieved using GPS which is most likely available in a vehicular scenario. This approch performed much better than the optimized DCC variant. Besides that synchronous schemes are deterministic which can be handled and analyzed in an easier way [5].

Despite these results, further research should be done on the topic of inter-operability with asynchronous and legacy devices to support a wide variety of devices [5]. For the synchronous protocol approach a further study on off-the-shelf WiFi chipsets could bring good results because some Atheros chipsets are able of injecting messages into the MAC layer based on external input [5].

References

[1] W. Fehr, *Dedicated Short-Range Communications (DSRC) - The Future Of Safer Driving*, U.S. Department of Transportation (U.S. DOT), October 2015.

[2] The CAMP Vehicle Safety Communications Consortium, “Vehicle safety communications project task 3 final report - identify intelligent vehicle safety applications enabled by dsrc,” U.S. Department of Transportation (U.S. DOT) & National Highway Traffic Safety Administration (NHTSA), Tech. Rep., May 2005.

[3] “ETSI TS 102 687: Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 ghz range; access layer part,” European Telecommunication Standard Institute, Tech. Rep., July 2011.

[4] T. V. Nguyen, F. Baccelli, K. Zhu, S. Subramanian, and X. Wu, “A performance analysis of CSMA based broadcast protocol in VANETs,” in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2805–2813.

[5] S. Subramanian, M. Werner, S. Liu, J. Jose, R. Lupoaie, and X. Wu, “Congestion control for vehicular safety: Synchronous and asynchronous mac algorithms,” in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, ser. VANET ’12. New York, NY, USA: ACM, 2012, pp. 63–72.

[6] U.S. Department of Transportation (U.S. DOT), “Its infographics,” as consulted online on 16 January 2016. [Online]. Available: http://www.its.dot.gov/infographs/DoNotPass.htm

[7] *IEEE802.11-207 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, 2007.

[8] N. Mahalik, *Sensor Networks and Configuration: Fundamentals, Standards, Platforms, and Applications*. Springer Berlin Heidelberg, 2007.

[9] S. Eichler, “Performance evaluation of the ieee 802.11p wave communication standard,” in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, Sept 2007, pp. 2199–2203.

[10] H. Hartenstein and K. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164–171, June 2008.

[11] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, “Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks,” in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET ’04. ACM, 2004, pp. 10–18.

[12] Z. Wang and M. Hassan, “How much of dsrc is available for non-safety use?” in *Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, ser. VANET ’08. ACM, 2008, pp. 23–29.

[13] “The network simulator - ns-2,” University of Southern California, http://www.isi.edu/nsnam/ns/.

[14] T. Singal, *Wireless Communications*. McGraw-Hill Education (India) Pvt Limited, 2010.

[15] J. Jose, C. Li, X. Wu, L. Ying, and K. Zhu, “Distributed rate and power control in dsrc,” in *Information Theory (ISIT), 2015 IEEE International Symposium on*, June 2015, pp. 2822–2826.

[16] Z. Tong, H. Lu, M. Haenggi, and C. Poellabauer, “A stochastic geometry approach to the modeling of ieee 802.11 p for vehicular ad hoc networks.”

[17] S. Djahel and Y. Ghamri-Doudane, “A robust congestion control scheme for fast and reliable dissemination of safety messages in vanets,” in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, April 2012, pp. 2264–2269.