

Technical Report
IDE0924

Handover in IEEE 802.11p-based Delay-Sensitive Vehicle-to-Infrastructure Communication

Annette Böhm and Magnus Jonsson

Abstract:

Based on communication and cooperation between vehicles and roadside infrastructure, Intelligent Transport Systems (ITS) safety applications offer great potential to avoid traffic accidents or at least reduce their impact. As these applications usually are delay-sensitive, the delay introduced by waiting for access to the wireless communication channel should both be reduced and provided with an upper bound. The proposed IEEE 802.11p standard for short to medium range vehicular communication does not offer these guarantees. In previous work, we presented a MAC (Medium Access Control) enhancement supporting delay-sensitive, safety-critical V2I (Vehicle-to-Infrastructure) applications. Since the proposed enhancement requires a deterministic and fast mechanism to associate a vehicle to a roadside unit (RSU) so that it can be integrated into the centralized polling schedule, we now target the handover and connection setup between a vehicle and an RSU. Although the first connection setup with an RSU still underlies the randomness of the original 802.11p MAC method, we provide a deterministic solution to further enhance the handover procedures by introducing a fast, proactive handover mechanism. We show that the overhead of our solution is limited and still allows our MAC protocol to support safety-critical V2I applications in a densely trafficked highway scenario.

Handover in IEEE 802.11p-based Delay-Sensitive Vehicle-to-Infrastructure Communication

Annette Böhm and Magnus Jonsson
CERES (Centre for Research on Embedded Systems)
Halmstad University, Halmstad, Sweden
{annette.bohm, magnus.jonsson}@hh.se
<http://ceres.hh.se>

I. INTRODUCTION

Vehicular networks have been of special interest in the communication research area for several years now. Communication and cooperation between vehicles offer great potential in reducing the number and impact of road accidents. Recently, the allocation of a dedicated frequency band for ITS (Intelligent Transport Systems) communication in Europe and the emerging IEEE 802.11p standard [1] for short to medium range inter-vehicle communication have paved the way for future implementations of communication-based ITS safety applications.

Most cooperative ITS safety applications depend on periodic information exchange in order to keep an up-to-date view of the current traffic situation. Additionally, in case of an emergency, event-triggered warning messages need to be transmitted to other concerned traffic participants. Both types of data have strict real-time requirements in order to be of any value for the proactive safety application. We define real-time data traffic as deadline-dependent data traffic that must be delivered to its destination before a given deadline in order to be of use for its target application. A key to timely data transmission is the opportunity to access the communication medium (here, the shared wireless frequency channel) whenever needed and without experiencing long and uncertain delays. The more data that share the common communication channel, the more difficult it becomes to achieve this goal. Fast and deterministic medium access control (MAC) methods are thus needed. The upcoming IEEE 802.11p standard, however, offers only a random access MAC method, which introduces the problem of packet collisions and unbounded channel access delays. Deterministic MAC methods are typically centralized, such that a central controller polls surrounding stations. However, the IEEE 802.11p is a decentralized ad hoc network since this yields low delay, cheap infrastructure and no requirements on coverage. Nonetheless, traffic accidents are typically concentrated to certain road sections such as highway entrance ramps, intersections or areas with road work. In such areas it is justified to install a roadside unit (RSU) offering centralized vehicle-to-infrastructure (V2I) communication. In

[2-3] we therefore proposed an enhancement to the 802.11p standard based on a V2I communications. By placing a real-time layer on top of the 802.11p MAC layer we have the possibility to let a coordinator (in this case the RSU) produce a communication schedule for all vehicles in its transmission range and poll these vehicles for data accordingly. This polling-based, collision-free MAC scheme coexists with the contention-based CSMA/CA scheme of the 802.11p standard, providing safety-critical applications with guarantees for the timely delivery of real-time data.

A vehicle entering an RSU's transmission range needs to be integrated into the RSU's communication schedule. Only then will it be polled for data by the RSU and allowed to participate in the collision-free communication required by real-time safety applications. In order to become a part of the RSU's schedule, a vehicle needs to make its presence known to the RSU as soon as it enters the RSU's transmission range. To cope with the high mobility and to support V2I-based, delay-sensitive ITS safety applications, the time it takes for a vehicle to associate itself with an RSU when it enters the RSU's communication range (the connection setup delay) should be as short as possible. Handover, when leaving the transmission range of one access point and entering another, is a way of reducing the connection setup delay when associating with a new RSU. This has been studied thoroughly for IEEE 802.11b/g [4] since it is widely implemented in wireless network cards in WLANs (wireless local area networks) today. As stated in e.g. [5] and [6], current implementations of MAC layer handover do not meet the requirements of delay-sensitive real-time applications. Further, due to the ITS adaptations made in the 802.11p standard and the special properties of a vehicular network, existing WLAN handover mechanisms are not directly applicable.

In this paper, we describe a fast connection setup mechanism for V2I communication based on the 802.11p random access protocol. Taking a broader perspective, we also investigate the handover process between several, non-overlapping RSUs and suggest a position-based, proactive handover method to reduce the handover delay. This solution

goes along with our previous assumptions and results, and completes our system design for safety-critical real-time applications with infrastructure support.

This paper is organized as follows. Section II we describe the target application scenario and give an overview of our assumptions and adaptations to the 802.11p MAC layer introduced in previous work. Section III describes the basics of standard 802.11 handover and its shortcomings, the special properties of the 802.11p ITS-adaptation and related works on how to reduce the delay introduced by the handover process. Section IV focuses on our proposed solution for fast connection setup to an RSU and proactive handover between several RSUs. Section V concludes this paper.

II. SYSTEM DESCRIPTION

We assume a common 10 MHz frequency channel, shared by both driving directions, used for both safety-critical and best-effort services. For financial reasons, a seamless RSU coverage along the roadside cannot be expected and we therefore see our solution as an addition to vehicle-to-vehicle (V2V) applications at particularly dangerous road sections. A merge assistance application at a highway entrance ramp was chosen as the type scenario for the system which is described in detail below.

A. V2I-based Application Scenario

The merge assistance scenario is based on V2I communication involving an RSU at a highway entrance ramp that supports both entering and passing vehicles with heterogeneous communication services covering a variety of Quality of Service (QoS) classes. Through short, periodic heartbeat messages from the vehicles, the RSU is informed about individual positions, states and intentions. The RSU broadcasts recommendations concerning the merging process back to the vehicles. Moreover, vehicles passing an RSU are provided with updates on e.g. current road, traffic or weather conditions. Vehicle heartbeats, RSU recommendations and road information updates are all considered safety-critical. At the same time, bandwidth should be reserved to support ongoing V2V applications or various, V2I-based, best-effort data traffic classes as e.g. digital map updates or commercial services. 802.11p-based V2V applications (e.g. collision avoidance) are maintained while the vehicle moves through a region with an RSU without involvement of the RSU. Therefore, V2V data traffic concerning these applications, although safety-critical in their nature, is not part of what we handle as real-time data traffic. The data traffic classes are summarized in Table 1.

B. The IEEE 802.11p MAC standard

In the highly mobile environment, especially concerning V2V communication, the time interval during which vehicles are in communication distance of each other is very limited.

Therefore, the proposed 802.11p MAC protocol only offers a limited subset of the original 802.11 MAC functionality. Only the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) random access scheme is assumed for 802.11p. This MAC phase is referred to as contention-based phase (CBP). The polling-based, collision-free phase (CFP) present in other versions of 802.11 is not part of 802.11p and therefore no guarantees for the timely delivery of real-time data packets can be offered.

TABLE 1: DATA TRAFFIC CLASSES

	Safety-Critical	Best-Effort
Vehicle → RSU	▪ Vehicle heartbeat	▪ CSR messages
RSU → Vehicle	▪ RSU recommendation ▪ Road information updates	▪ Non-safety-critical RSU-based services
Vehicle → Vehicle		▪ RSU-independent V2V communication

The contention-based phase in 802.11p uses the enhanced distributed channel access mechanism (EDCA) originally provided by IEEE 802.11e. Four priority classes ensure four different QoS levels. Fixed waiting times (Arbitrary Inter Frame Spacings - AIFS) of different lengths are used to make sure that high priority packets get access to the medium first. Within the respective priority classes, however, packet collisions are still possible. After a packet collision has occurred, a back-off time is randomly chosen from an interval (the Contention Window – CW). The window size is also coupled to the priority level, giving high priority packets the higher probability of channel access after a collision. The initial size of the CW is given by the factor CW_{min} . Each time a transmission attempt fails, the CW size is doubled until reaching the size given by the parameter CW_{max} . Table 2 summarizes the parameter set defined for EDCA in 802.11p, where 1 denotes the highest priority level and 4 the lowest. The parameters are given in time slots where one slot is defined as $8\mu s$. Although these priorities can be used to increase the probability of certain packets to get access to the wireless channel, there are no guarantees that this will happen before a predefined deadline.

TABLE 2: EDCA PARAMETERS

QoS class	CWmin	CWmax	AIFS
4	15	1023	9
3	7	15	6
2	3	7	3
1	3	7	2

C. IEEE 802.11p MAC Layer Enhancements

We base our non-intrusive solution on an RSU and an additional real-time layer, placed on top of the unaltered

IEEE 802.11p protocol, such that a deterministic, polling-based MAC method is introduced. This real-time layer divides the access to the available bandwidth into two different phases: in the contention-based phase (CBP) nodes compete for access to the medium according to the original IEEE 802.11p MAC method, but in the collision-free phase (CFP) the RSU assumes the responsibility for scheduling the data traffic and polls the mobile nodes for data. As previously presented by the authors [2], this real-time layer guarantees the timely delivery of safety-critical data, as long as the CFP is long enough. We apply real-time schedulability analysis to determine the minimum length of the CFP such that all deadlines are guaranteed and the remaining bandwidth is maximized to cater for best-effort services, figure 1. In [3], we further enhanced our solution by introducing geographical priority zones around an area of hazard (e.g. an intersection), defining different levels of priority and, thereby, determining a vehicle's communication parameters based on its geographical position.

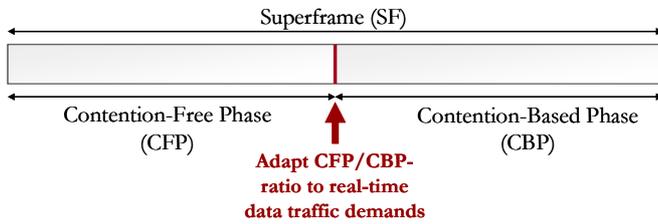


Figure 1: Adaptable ratio between CFP and CBP.

III. HANDOVER IN IEEE 802.11

In a WLAN, mobile nodes (MN) are associated with an access point (AP) as long as a satisfactory communication quality with that AP can be maintained. If the MN is about to leave the transmission range of the AP, a handover process is initiated such that an association with a new AP can be established.

A. Standard Handover in IEEE 802.11

Wireless networks based on 802.11 are made up of areas, WLANs, each determined by the communication range of a fixed AP. The AP and all MNs associated with it constitute a Basic Service Set (BSS) where the AP acts as a bridge for all communication involving the MNs in the BSS. A handover implies the process when a MN leaves a BSS to join another. The process leading up to and executing a handover can be divided into three phases, figure 2:

- **Detection phase** – The need for a handover must first be detected by the MN. How this should be done is not specified in the standard, but usually it is accomplished by monitoring the amount of consecutive un-acknowledged data packets or by detecting when the signal strength or the signal-to-

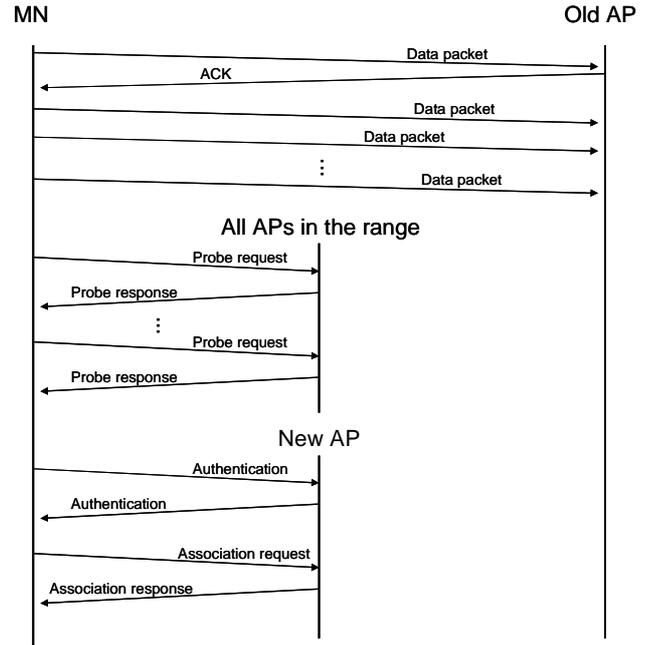


Figure 2: The handover process in 802.11a/b.

noise ratio drops under a specified threshold. The detection phase stands for approximately 85% of the total handover duration.

- **Search phase** – In the search phase, corresponding to about 15% of the handover time, a MN attempts to find a new AP. This can either be done passively by listening for a beacon from an AP. Depending on the beacon period and the number of frequency channels the MN has to tune to during its search, this phase can take up to 1 second. Active scanning allows the MN to broadcast probes in each frequency channel and await a response from an AP. This usually reduces the search time.
- **Execution phase** – Here, the actual handover takes place through the exchange of authentication and association requests and responses by the MN and the new AP. The evaluation of handover delays for different 802.11b WLAN cards made in [5] shows that the execution phase only stands for about 0.1% of the total handover delay.

These three phases define MAC layer handover within a single IP subnet. In larger networks, handover between subnets affects even the network layer and the address that associates a MN to a subnet needs to be changed. Implications of that change are described and taken care of in e.g. mobile IP [7] or its enhancements. In this paper, our focus lies on MAC layer handover.

B. Handover in IEEE 802.11p

The proposed IEEE 802.11p standard is part of the Wireless Access in Vehicular Environments (WAVE) protocol suite and defines layer 1 and layer 2 adaptations to the 802.11 WLAN standard. The focus of 802.11p lies on fast adaptation to the rapid changes occurring in a highly mobile vehicular network, sacrificing identification and authentication procedures that are usually part of the 802.11 WLAN standard. For more efficient data exchange between high speed vehicles or between a vehicle and an RSU, IEEE 802.11p therefore specifies a minimized set of parameters for the execution phase of the handover process. In the 802.11p standard, a WAVE Basic Service Set (WBSS) is built around an RSU (or, in V2V communication, around any vehicle assuming the role of a WBSS leader). The existence of a WBSS is announced through the WAVE Service Announcement (WSA), a beacon from the WBSS leader (or the RSU in the case of V2I communication). A vehicle that hears this beacon configures itself according to the information contained in the beacon frame and is immediately ready to communicate with the RSU according to its rules. No authentication or association is required. This ensures that the vehicle is ready to start communicating with the RSU much quicker than in the original WLAN standard.

For privacy reasons, a MN in a vehicular network changes its MAC address regularly. At system startup, a new MAC address is randomly determined to make it more difficult to track the movements of a certain vehicle. As there is no association phase when a vehicle enters the WBSS of an RSU, the MAC address will not be passed to the RSU, further enhancing the driver's privacy. On the other hand, the lack of an association and de-association process means that the RSU has no means of identifying a vehicle or to know if it has left its transmission range.

C. Handover in Vehicular Networks and Related Work

In vehicular networks, the MN is a vehicle, while the AP is an RSU. Even in networks where the MNs move relatively slowly, as e.g. an office environment with WLAN APs, the delay introduced by handover is considered a problem for real-time applications. In a highly mobile vehicular network, this delay is of special concern as vehicles only stay in the transmission range of an RSU for a relatively short time span (approximately 20s for a transmission radius of 400m and a vehicle speed of 40 m/s). Additionally, ITS safety applications benefit from very short connection setup times with guaranteed delay bounds, so that the deadlines of the real-time data traffic are not compromised.

Handover between RSUs in a vehicular network differs from a normal WLAN in several ways. Vehicles have access to their speed and typically also to their geographical position through a GPS receiver. Further they are bound to a predefined road network and thus their movements are more easily predicted. RSUs are usually static and placed

strategically along a road such that the number of RSUs that are appropriate for a handover is limited and often predictable.

Further, the number of available frequency channels in dedicated ITS bands are limited. In Europe for example, only 30 MHz are set aside for ITS applications and only one 10 MHz control channel will be used initially [8]. This further reduces the complexity of finding a new AP as no probing and scanning over multiple channels is required.

Another criterion that distinguishes handoff between RSUs from normal 802.11 handover is that full coverage of the road network with RSUs can typically neither be expected nor called for. Therefore, there is no need for seamless handover but instead connection setups to rather irregularly spaced RSUs. Communication between closely located RSUs can be assumed (either through cables along the road or some other wireless communication technology), so that an RSU can presumably exchange information with its neighboring RSUs.

Existing solutions and research work to reduce handover delays are mostly targeting the detection and search phases of the handover process. Most authors assume a regular WLAN with several APs operating on various frequencies and a relatively slow mobility amongst the MNs. In [6], the idea of periodic scanning is presented, where a MN performs scans for possible new APs already while being connected with good channel quality to an AP. Short probes sent out on varying channels will interfere with the ongoing data traffic but, on the other hand, the MN is ready for the handover execution phase as soon as the need for a handover arises. This solution is however, less beneficial when the choice of suitable APs are limited and predictable.

In order to eliminate the search phase and speed up the execution of a handover, Tseng *et al.* [9] propose a location-based solution where a MN, knowing its own position and direction of movement, gets information on nearby APs from a location server. The server also performs proactive authentication and association on behalf of the MN, reducing the handover duration even further. Montavont and Noel [10] describe a similar solution where a so called GPS server collects movement updates from the MNs and compares them with a known topology of APs in order to recommend the handover to a specific AP. These are examples of solutions that are directly applicable in our V2I traffic scenario.

Shimizou *et al.* [11] target an 802.11 enhancement for communication between high speed vehicles and RSU without considering the proposed 802.11p standard. The authors assume a multitude of APs to be present at the same time, operating on different frequency channels. Their solution, to limit the number of scanned channels to achieve a reduction in handover delay, although interesting is not applicable to our case where only one control channel is available, regardless of the number of AP.

In [12], Paik and Choi take advantage of the fact that the mobility in vehicular networks is fairly predictable and chose the next AP and the best time for handover based on a vehicle's known mobility pattern. Their solution targets public transport vehicles like busses and trains, running on a known and tight schedule along a predefined path. Based on their mobility prediction-based WLAN enhancement, fast handover between hot spots is performed and passengers experience seamless connectivity. Note however, that seamless connectivity is less likely to be needed or expected in a V2I scenario where RSU can be expected to be sparsely located.

IV. FAST HANDOVER IN V2I COMMUNICATION

A vehicle entering an RSU's transmission range needs to be integrated into the communication schedule of the RSU as soon as possible. Only then will it be polled for data by the RSU and be part of the collision-free communication required by real-time safety applications. Our centralized approach requires the RSU to know about and identify the vehicles currently residing within its transmission range and their communication needs. This makes a connection setup between vehicle and RSU necessary. One option is to let the vehicles send out connection setup requests (CSR) as soon as they can hear the RSU. Even if the RSUs along a road might be widely spaced, we can view this chain of connection setup and disconnection as a series of handover procedures. We thus consider two protocol components: fast connection setup with a RSU and proactive handover between consecutively located RSUs.

A. Fast connection setup with an RSU

As mentioned above, the search phase, accounting for a majority of the handover delay in regular WLAN, does not come into play at all in a network where all access points operate on the same frequency channel. No scanning is required and a vehicle merely listens for the WSA (in our case the beacon announcing the start of a CBP in the beginning of a superframe) and replies with a CSR. A vehicle enters the RSU's transmission range and as soon as it hears the WSA beacon, it will try to make its presence known to the RSU. This is done in the CBP and therefore, no guarantees for a successful channel access can be given. Nevertheless, the four priority levels provided in the CSMA/CA-based MAC protocol of 802.11p limit the number of competing data channels. We assign the following applications classes to the four available priority levels:

- **Priority level 1** (highest): Safety-critical V2V alert messages, e.g. collision avoidance applications
- **Priority level 2**: Connection setup request (Vehicle to RSU)
- **Priority levels 3**: Periodic V2V Cooperative Awareness Messages

- **Priority level 4**: Best effort comfort/entertainment application data

Only safety-critical V2V application data (as e.g. alert messages from collision avoidance applications) have a higher priority than the CSR. As these V2V alert messages only occur in the rare case of an emergency, CSR of a vehicle usually only competes with other CSRs from other vehicles entering the transmission range at approximately the same point in time.

To keep the overhead at a minimum, IEEE 802.11p defines no association, authentication or disassociation process. For our system solution, however, the RSU needs to be able to uniquely identify each vehicle and address it with individual polling messages. According to the standard, at system startup, i.e. whenever a vehicle is started, a temporary MAC address is randomly determined. We assume that this MAC address is communicated to the RSU in the CSR and then used by the RSU to address the vehicle. It should be noted though, that we do not introduce any authentication data exchange in conjunction with the connection setup. The disassociation from an RSU happens automatically after a threshold of unanswered polling messages to a vehicle or based on the RSU's knowledge of the vehicles current position relative to the RSU's own approximate transmission range.

Anastasi et al. [13] conducted measurements with 802.11p enabled devices. They measured when (at what distance from the AP) a mobile node starts receiving beacons from the AP and experienced considerable differences in their series of measurements even at moderate mobility. This indicates that changes in the surrounding environment, weather conditions etc. influence an AP's actual, experienced transmission range. Adding high mobility and a constantly changing environment (moving vehicles) around an RSU to the equation, we can assume that different vehicles, approaching an RSU at the same time, will hear the RSU's WSA beacons at different distances to the RSU. Vehicles lying close behind a large bus or truck might experience radio shadow, hindering the reception of the WSA. How much these individually experienced transmission ranges differ must be further investigated and field measurements using 802.11p-enabled platforms are thus planned. However, to acknowledge the problem we assume here that this difference in experienced RSU transmission range might be as high as 100 m. A worst case scenario for an RSU at a 3-lane highway would therefore be a total of 36 vehicles hearing the WSA for the first time and trying to send out a connection setup request approximately simultaneously. Here we assume very dense traffic with a vehicle spacing of 20 m. Although unlikely to occur, this scenario shows that it is possible that a high number of vehicles attempt a connection setup at the same time. This would lead to an increased probability of packet collisions during the contention-based random access phase and delay the association of vehicles to the RSU. As the

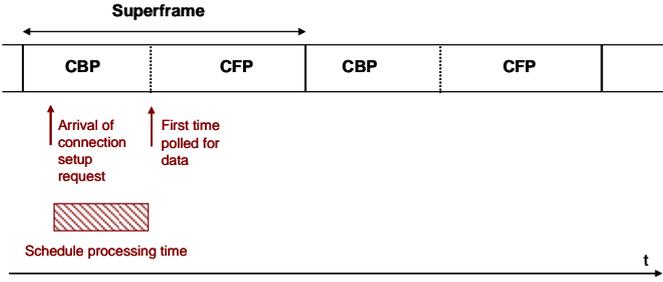


Figure 3: Best case waiting time between successful CSR and first polling message.

connection to the RSU is a prerequisite to take part in the collision-free exchange of safety-critical data, this delay should be reduced as much as possible; ideally, it should have a guaranteed upper bound.

If a CSR was sent successfully to the RSU, the vehicle is integrated into the RSU's schedule for channel access and polled for data in the upcoming CFP. CSRs that are sent out in the beginning of a CBP might lead to a first polling message from the RSU already during the same superframe, figure 3. Ideally, the connection setup delay d_{CS} (i.e. the delay between the arrival of the CSR at the RSU and the point in time when the first polling packet is sent out) is:

$$d_{CS}^{\min} = (T_{CBP_end} - T_{CSR_arrival}), \quad (1)$$

$$\text{iff } d_{sched} \leq d_{CS}^{\min}, t_{CBP},$$

where d_{sched} denotes the time required for scheduling, $T_{CSR_arrival}$ is the point in time when the CSR arrives at the RSU, T_{CBP_end} is the point in time when the current CBP ends and t_{CBP} is the duration of the CBP. This implies that if the request reaches the RSU in the end of a CBP (or in the case of a short CBP), it will not leave the RSU enough time to schedule the data packets for the next CFP and the node will first be polled in the following superframe. For periodic real-time data traffic, our framework assumes a deadline that is equal to the period. An Earliest Deadline First (EDF) scheduling policy makes sure that the packet with the tightest timing requirements is sent first. During the connection setup process, the first time a vehicle's heartbeat message is scheduled by the RSU, its deadline is set equal to the end of the ongoing superframe. EDF scheduling thereby ensures that the vehicle is polled within this superframe, assuming a real-time analysis as proposed in [2]. After that, the deadline of heartbeat messages is set equal to their period, which is dependent on the vehicle's location within the RSU's communication range (as explained in detail in [3]). In the worst case, the time span between an acknowledged CSR and the first time a new node is polled for data is therefore, figure 4:

$$d_{CS}^{\max} = (T_{CBP_end} - T_{CSR_arrival}) + t_{SF} + t_{CFP} - (t_{trans} + t_{prop}),$$

$$\text{iff } d_{CS}^{\max} < d_{sched},$$

(2)

where t_{SF} is the duration of a superframe, t_{CFP} is the duration of the CFP and t_{trans} and t_{prop} denote the transmission delay and the propagation delay of a data packet to be sent by the MN.

Since the delay until a connection setup request results in a successful access to the shared frequency channel in the CBP cannot be bounded, there are still no guarantees that a vehicle is able to connect to an RSU within a predefined time span from entering its transmission range.

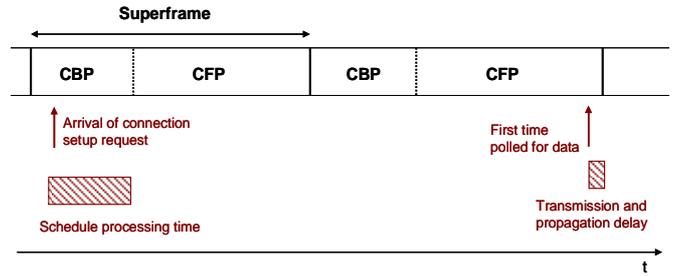


Figure 4: Worst case waiting time between successful CSR and first polling message, when the CSR arrives when the scheduling process for the next CFP just started.

B. Proactive handover between RSUs

As long as we depend on the random access MAC protocol of 802.11p, we cannot guarantee that a vehicle will be integrated into the collision-free infrastructure-based communication within a certain delay bound. We therefore need an alternative way to let the RSU know that a new vehicle has entered its communication range.

Through heartbeat messages, an RSU is informed about a vehicle's position, speed and direction of movement. On a highway or rural road, a vehicle will only have one RSU further down the road to choose from when a handover becomes necessary. This next RSU is known to the old RSU before the vehicle leaves the transmission range. Thanks to the knowledge of the vehicle's speed, its approximate arrival time at the next RSU can be predicted. A new RSU can now integrate the vehicle into its schedule and start polling it proactively before it even enters the RSU's transmission range. In order to prevent proactive polling from taking away too much bandwidth from application data transfer, a threshold of 10% of the length of an entire superframe is introduced for proactive polling. Figure 5 shows the introduction of the proactive polling phase (PPP) into the superframe structure. A worst case connection setup delay can then be calculated as:

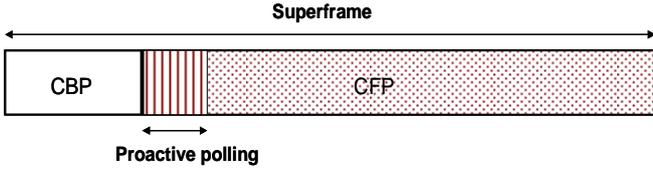


Figure 5: Proactive Polling Phase (PPP) as part of the collision-free phase of the superframe

$$d_{CS_proactive}^{\max} = t_{SF} + \frac{1}{10} \cdot t_{SF}, \quad (3)$$

i.e. the length of one superframe (t_{SF}) plus 10% of a superframe, figure 6. This case occurs when a vehicle just misses its proactive polling message when it enters the new RSU's transmission range in the beginning of the PPP and has to wait until the end of the next PPP to receive the next proactive polling packet. The delay for connection setup with the new RSU therefore has an upper bound, i.e. we can guarantee that the vehicle is ready to participate in the collision-free safety-critical communication after not more than $d_{CS_proactive}$.

Assume that vehicles leave the transmission range of their current RSU at an initial speed v_{init} of 30m/s. In order to allow for changes in the vehicle's speed until it reaches the next RSU, a margin of 20% is introduced, i.e. even though the vehicle is expected to arrive at the following RSU at a certain instance in time (based on a constant speed of 30 m/s), the RSU starts polling early enough to account for a 20% increase in average vehicle speed over the distance between the two access points. In our example, this means an increased average speed of 36 m/s. The new RSU starts polling t_{poll_start} seconds after the vehicle left the old RSU's transmission range:

$$t_{poll_start} = \frac{d - r_{oldRSU} - r_{newRSU}}{1.2 \cdot v_{init}}, \quad (4)$$

where d is the distance between the RSUs and r_{oldRSU} and r_{newRSU} is the transmission radius of the old and the new RSU respectively. The transmission and propagation delay of the information sent between the old and the new RSU are negligible.

When a vehicle experiences a significant decrease in average speed (e.g. as a consequence of a traffic jam building up in between the RSUs) or leaves the highway entirely, the RSU cannot continue sending out proactive polling messages indefinitely. We allow a decrease in average speed of 20%. t_{poll_stop} seconds after the vehicle left its old RSU, the new RSU stops the proactive polling to save bandwidth, assuming the vehicle has left the road, parked or been delayed. A vehicle that reaches the new RSU after this threshold has to go through the regular connection setup process by sending a

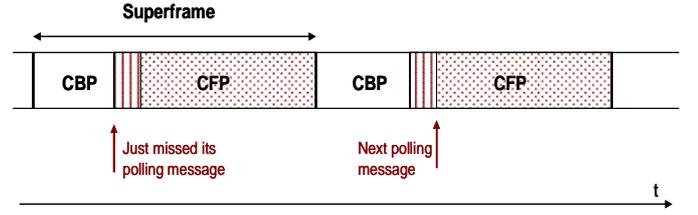


Figure 6: Worst case waiting time until connection setup for proactive polling.

CSR and waiting to be scheduled. t_{poll_stop} is calculated as follows:

$$t_{poll_stop} = \frac{d - r_{oldRSU} - r_{newRSU}}{0.8 \cdot v_{init}}. \quad (5)$$

Equation (3) assumes a dense but normal road traffic flow. If, in the case of road congestions, the 10% of the bandwidth cannot support a proactive polling packet per expected vehicle and superframe, the PPP will be distributed over two or more consecutive superframes. The worst case delay for connection setup will thereby be increased to:

$$d_{CS_proactive}^{\max} = k \cdot t_{SF} + \frac{1}{10} \cdot t_{SF}, \quad (6)$$

where k is the number of superframes appropriate as the total period for the polling. Despite the increased delay, there is still a guaranteed upper bound. Our handover method therefore fits perfectly with our deterministic MAC protocol developed for safety-critical RSU-supported applications.

C. Evaluation of proactive handover

Based on the simulation results of [3], we can determine how many vehicles that can be supported in the RSU's schedule when a maximum of 10% of the superframe is dedicated to proactive polling. Figure 7 shows the results for bit rates of 6, 12 and 24 Mbit/s when applying position-based priorities with three priority zones (see [3] for more details). A minimum of 20% of a superframe is reserved for best-effort traffic in the CBP, while a maximum of 10% is used for the proactive polling introduced above. The figure shows that, even at low bit rates, we can guarantee the support of 80 vehicles in the collision-free MAC phase used for delay-sensitive real-time data traffic. We assume that an RSU covers about 800m of road and even for a 3-lane highway with bidirectional traffic, this means that dense road traffic can be supported (with a distance of approximately 50 m between vehicles in the same lane). For bit rates of 12 and 24 Mbit/s, the number of supported vehicles increases to 150 and 280 respectively.

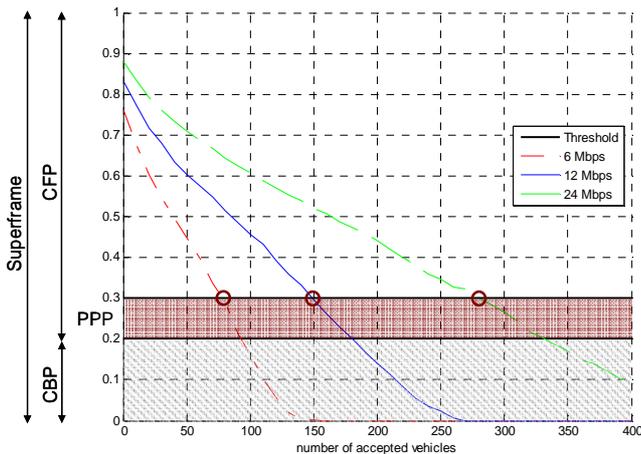


Figure 7: Number of vehicles supported for various bit rates under the assumption of a 20% CBP and a 10% Proactive Polling Phase (PPP).

V. CONCLUSION

In this paper, we target fast connection setup and handover between vehicles and RSUs. An earlier developed enhancement of IEEE 802.11p developed by the authors – supporting safety-critical, delay-sensitive ITS applications – requires a deterministic and fast mechanism to associate a vehicle to an RSU and integrate the vehicle into the centralized polling schedule. We propose and analyze a random access-based connection setup mechanism during the contention-based phase of an 802.11p superframe. As packet collisions are possible, this mechanism itself does not offer a guaranteed delay bound for connection setup and we therefore propose further improvement by proactively forwarding information about approaching vehicles to the next RSU along the road. Thus, vehicles are already part of the communication schedule even before they enter the next RSU’s transmission range, thereby providing an upper bound on the connection setup (or handover) delay. An analysis of this proactive handover mechanism is provided, showing that, even for dense road traffic, the bandwidth requirements to support our proactive handover solution do not compromise our previously proposed system design for infrastructure-based ITS safety applications.

REFERENCES

- [1] Task Group p. *IEEE 802.11p: Wireless Access in Vehicular Environments (WAVE)*, draft standard, IEEE Computer Soc., 2007.
- [2] A. Böhm and M. Jonsson, “Supporting real-time data traffic in safety-critical, vehicle-to-infrastructure communication,” *Proc. IEEE LCN Workshop on User Mobility and Vehicular Networks*, Montreal, Canada, Oct. 2008.
- [3] A. Böhm and M. Jonsson, “Position-based data traffic prioritization in safety-critical vehicle-to-infrastructure communication,” *Proc. IEEE ICC Vehicular Networks & Applications Workshop*, Dresden, Germany, June 2009.
- [4] IEEE, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” *IEEE Standard 802.11*, 1999.
- [5] H. Velayos and G. Karlsson, “Techniques to reduce the IEEE 802.11b handoff time,” *Proc. Int. Conf. on Communications (ICC 2004)*, Paris, France, June 2004, vol. 7, pp. 3844-3848.
- [6] J. Montavont, N. Montavont, and T. Noel, “Enhanced schemes for L2 handover in IEEE 802.11 networks and their evaluations,” *Proc. 16th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC '05)*, Berlin, Germany, Sept. 2005, vol. 3, pp. 1429-1433.
- [7] R. Koodli (Ed.), *Fast Handovers for Mobile IPv6*, RFC 4068, July 2005.
- [8] T. Kosch et al., “European ITS Communications Architecture,” COMESafety deliverable D31, version 2.0, October 2008. Available at: <http://www.comesafety.org/index.php?id=systemarchitecture>.
- [9] C.-C. Tseng, K. H. Chi, M. D. Hsieh, and H. H. Chang, “Location-based fast handoff for 802.11 networks,” *IEEE Communications Letters*, vol. 9, pp. 304-306.
- [10] J. Montavont and T. Noel, “IEEE 802.11 handover assisted by GPS information,” *Proc. IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob '06)*, Montreal, Québec, Canada, June 2006, pp. 166-172.
- [11] A. Shimizu, S. Fukuzawa, T. Osafune, M. Hayashi, and S. Matsui, “Enhanced functions of 802.11 protocol for adaptation to communications between high speed vehicles and infrastructure,” *Proc. 7th IEEE Int. Conf. on ITS Telecommunications (ITST '07)*, Seattle, WA, USA, Oct. 2007, pp.1-3.
- [12] E. K. Paik and Y. Choi, “Prediction-based fast handoff for mobile WLANs,” *Proc. 10th IEEE Int. Conf. on Telecommunications (ICT '03)*, Tahiti, Feb. 2003, vol. 1, pp. 748-753.
- [13] G. Anastasi, E. Borgia, M. Conti, and E. Gregori., “IEEE 802.11 ad hoc networks: performance measurements,” *Proc. 23rd Int. Conf. on Distributed Computing Systems Workshops (ICDCSW '03)*, 2003.