Road Surface Networks
Technology Enablers for Enhanced ITS

Wolfgang Birk, Jens Eliasson, Per Lindgren*, Evgeny Osipov and Laurynas Riliskis

Abstract—The increased need for mobility has led to transportation problems like congestion, accidents and pollution. In order to provide safe and efficient transport systems great efforts are currently being put into developing Intelligent Transport Systems (ITS) and cooperative systems. In this paper we extend proposed solutions with autonomous on-road sensors and actuators forming a wireless Road Surface Network (RSN). We present the RSN architecture and design methodology and demonstrate its applicability to queue-end detection. For the use case we discuss the requirements and technological solutions to sensor technology, data processing and communication. In particular the MAC protocol is detailed and its performance assessed through theoretical verification. The RSN architecture is shown to offer a scalable solution, where increased node density offers more precise sensing as well as increased redundancy for safety critical applications. The use-case demonstrates that RSN solutions may be deployed as standalone systems potentially integrated into current and future ITS. RSN may provide both easily deployable and cost effective alternatives to traditional ITS (with a direct impact independent of penetration rate of other ITS infrastructures - i.e., smart vehicles, safe spots etc.) as well as provide fine grain sensory information directly from the road surface to back-end and cooperative systems, thus enabling a wide range of ITS applications beyond current state of the art.

I. INTRODUCTION

Mobility is essential in today’s societies and intimately related to the prosperity and quality of life of citizens. But the increased need for mobility has led to problems like congestion, accidents and pollution, especially in urban areas [1]. These issues are further stressed by the current discussion on climate change and energy consumption.

ITS are projected to provide effective means to improve transportation efficiency and road safety, reducing travel time, and bring environmental footprint benefits in terms of reduced air pollution and fuel consumption. However, the deployment of traditional ITS is costly both in terms of the technology and infrastructure involved as well as installation and maintenance. Cooperative systems involving C2X and VANETs are projected to improve cost-benefit and efficiency of ITS, but will for the upcoming decades suffer from limited penetration of enabled vehicles and equipped road stretches [2], [3], [4].

By investigating an alternative approach based on a network of autonomous, wireless, on-road-sensor and -actuating devices we seek to overcome some of the major obstacles associated with current and proposed ITS technologies.

In our approach the road itself becomes an essential part of the ITS, hosting the wireless network of on-road devices (e.g., placed on the road surface as road mark units). The network of devices should facilitate ITS services by directly guiding the vehicles through easily understood signals, e.g., flashing light in case of danger, running light indicating preferred path and speed, etc. In addition the on-road devices should be able to provide sensory and actuator services in collaboration with current and future ITS.

Current wired road sensor technologies, have become very mature and enable the assessment of traffic properties, road conditions and characteristics of individual vehicles. In [5], different detector technologies are summarized and discussed and their potential is assessed. In a more recent research report focus was put on wireless sensor networks as the basis for the assessment of traffic properties, see [6]. As a consequence, there are now technology providers of wireless sensor nodes, which market off-the-shelf products for short term measurements. For long term measurements only a few products, with limited capability to cooperate, are yet available. Compared to wired solutions, wireless sensors have the advantage of being more cost-efficient when it comes to roll-out and maintenance, but their major drawback is the limited energy amount that the sensors have to operate on. It is the belief of the authors that a combination of energy harvesting strategies with low-power sensing, processing and communication can circumvent this shortcoming and enable networks which have a long life span and good capabilities to cooperate with their environment. This way we foresee to overcome the costly technology and infrastructure of today’s wired devices. Furthermore, we will be able to bridge the gap in between traditional ITS and upcoming cooperative systems and offer new means to ITS development.

Based on previous work in the iRoad project [7], we present a Road Surface Network (RSN) architecture that facilitates both stand alone ITS applications as well as integration to ITS infrastructures as discussed in section II. In section III we describe the design methodology for mapping a desired ITS functionality onto the RSN. In order to demonstrate the applicability of our suggested approach, section IV describes the queue-end warning use-case scenario, along with communication protocol design and discussion of different detection approaches. The selected use-case shows that the RSN architecture can be deployed stand-alone without additional infrastructure support, as well as complementing the functionality of cooperative ITS and opening up for novel applications where the road itself becomes an active part. The paper is concluded in Section VI where we also outline topics for future RSN research.
composed of a number of subsystems, i.e.:

- Capabilities for extended operational lifetimes. The RMUs are consumption of the RMUs, combined with energy harvesting is not possible. This results in the need of ultra-low power

- Consumption of the RMUs, combined with energy harvesting is not possible. This results in the need of ultra-low power

- Provide more accurate real-time traffic information to users and ITS infrastructure than current systems and achieve its interoperability with information exchanged in cooperative systems and in the backend systems.

The RSN architecture is illustrated in Figure 1. It is built upon three principle entities: road marking units (RMU), road-side units (RSU) and an open platform server (OPS) for enabling new RSN services in larger ITS systems. RMUs are autonomous on-road devices (shown in Figure 2) that may work independently or cooperatively to carry out sensing and actuating tasks. RMUs will be capable of wireless communication with RSUs as well as communicating with each other forming a wireless sensor and actuator network. RSUs are the gateway nodes for conveying data between RMUs and the ITS backend system. With additional C2X communication interfaces, RSUs also directly interact with vehicles, thus combining WSANs with VANET communications. The open platform features a set of open interfaces that connects RMUs to a backend ITS and front ends (e.g., CVIS RSUs).

**A. Road marking units**

A road marking unit, depicted in Fig. 2, situated on the road surface must endure the toughest of conditions: being overrun by cars, trucks, heavy vehicles, and harsh weather with rain and snow. At the same time, it must, with a very limited power supply, sense passing vehicles and use wireless communication to propagate the aggregated information. Because the RMUs are deployed in the harsh environment mentioned above and the large number of installed devices, changing drained batteries is not possible. This results in the need of ultra-low power consumption of the RMUs, combined with energy harvesting capabilities for extended operational lifetimes. The RMUs are composed of a number of subsystems, i.e.:

- Sensors and signal processing are used to detect passing vehicles as well as properties of the environment, such as temperature and light. Actuators are used to communicate with drivers directly.

- Power management is necessary in order to deliver a level of dependable performance.

- Wireless communication enables a RMU to create a wireless network to transmit sensor data to RSUs or other RMUs.

The RMUs are also required to support wireless software updates so that new features can be added even after the network is deployed. Security is another important issue, since a road surface sensor network in an ITS application to prevent intrusion and malfunction of the system.

One of the most challenging issues with deploying a sensor network on a road surface for vehicle detection is the power consumption. The network’s sensor nodes must be able to perform sensing, processing, and communication on a very limited energy budget. Energy scavenging, through the use of solar panels and rechargeable batteries, can address this issue to some extent. During spring and summer, the sun will be able to recharge the battery and hence allow operation during night without any constraints on power consumption. However, during the autumn and winter, the sun will produce drastically less power, and no new energy might be scavenged by the sensor nodes for several months. This is especially true for arctic regions that will receive a great deal of snow which will cover the solar panels.

In the remainder of the article we present a methodology for mapping an ITS application onto a RSN, and show its applicability the example of RSN-extended queue warning.

**III. DESIGN METHODOLOGY**

The proposed road surface network architecture implies the selection and composition of numerous hardware and software components in order to realize the desired ITS functionality. In this paper we focus on the design methodology of the road surface network (RSN) proper and leave details on the RSU and Open platform out. In the following we sketch a V-like design process.

- RSN requirements: The RSN is a distributed real-time system of communicating RMUs. Hence to map an ITS application onto a RSN, we first have to formulate the functional and extra functional (lifetime, cost etc.) requirements of the RSN.

- RSN design: Here we make an overall RSN design meeting the requirements of the ITS application. From the RSN requirements, we take (initial) decisions on distributed information retrieval, (precision and pace) together with decision on network design (density, topology, bandwidth, latency) .
• RMU requirements: From the RSN design we derive requirements for the RMUs functionality in terms of sensing, processing logic, actuating, and communicating.
• RMU function design: From the RMU requirements we take (initial) decisions on sensors, actuators, detection algorithms together with node logic.
• RMU communication design: From the RSN design we take (initial) decisions on radio technology, and protocol(s).
• RMU HW design: From the RMU function and communication design we take (initial) selection of hardware and software components.
• RMU verification: Verify the requirements with respect to both functional and extra functional properties. Sub-system testing in lab and on road.
• RSN verification: Verify the ITS system requirements in simulator, lab and on road.

In comparison to the traditional V process, design choices are made at several stages opening up for an iterative process re-designing and improving the system without going all the way to a complete design. In the following section we will see how the design methodology can be applied to the use case of queue end detection, where we discuss two alternative vehicle detection methods based on the assumption that detection can be performed using local data only. Furthermore the communication protocol is detailed on basis of the RSN design.

IV. USE CASE: QUEUE WARNING

Queue warning systems are not new and have been thoroughly discussed already, both from their potential impact and accident statistics and implementation characteristics, [8]. In a recent study, [9], it is also suggested that queue warning systems have the potential to reduce accident rate with up 16%. Thus, such an ITS system contributes to the safe property of transport. A queue warning system aims at making a road user aware of an upcoming queue end, which might be invisible due to adverse weather conditions or due to constructive properties of the road.

The RMUs detect traffic properties like vehicle speeds and detects queue end by fusing information from several RMUs. In case that a queue end is detected, RMUs that are located upstream provide visual warnings/information to the drivers using flashing LEDs. Thereby, drivers in vehicle without transponders or VANET capabilities can receive warnings. Additionally, the warning information which is composed of geo-location of the queue-end and its speed is propagated into the VANET using a gateway that replicates the information of the road surface network. In Fig. 3, the information flow is depicted using red arrows and flash arrows for intra surface network communication. The yellow car is a vehicle without VANET capability.

Following the outlined design methodology, we derive RSN requirements from the application, and from that a tentative RSN design. For this specific case make the assumption that vehicle detection can be carried out based on RMU sensor data only.

A. Sensing and estimation concept

Several sensors can be integrated into the RMU, namely accelerometer, magnetometer, temperature sensor. The first two have already successfully been used for the detection of vehicles and estimation of traffic flows characteristics, [10] and [11]. These sensors have different characteristics, which results in that accelerometers are able to detect vehicle axles, while magnetometers can detect the magnetic length of vehicles. Both sensors can detect passing vehicle reliably and sensor fusion would result in the best estimation concept, but with high energy consumption. A standard way to estimation vehicle passages is the assessment of the signal energy in certain frequency ranges. Here, the estimation concept for the accelerometer source is summarized. The accelerometer can detect vibration in the surface of the road which are vibration waves that originate from the contact of the wheel with the road surface. The waves are propagated to the sensor, where different frequencies are more or less damped during the propagation in the tarmac. In Fig. 4, the intensity of different frequency of the vibration signal over time is depicted. Clearly, there are certain regions that show clear peaks when a vehicle is passing. These frequencies will be extracted using a band-pass filtering scheme, which yields a time domain signal according to Fig. 5.

Now the envelope of the energy signal can be estimated which yields the input signal for the vehicle detector, see Fig. 6. Applying a CUSUM algorithm to the envelope of the signal yields a detection of the vehicle passages. The same estimation scheme can be applied to a magnetometer signal.
to detect vehicles. Using the vehicle detection algorithm a queue-end can be detected in two ways: By combining two subsequent vehicles detection events of two RMUs in the driving direction, or by estimating the event of too slow vehicle speed in one RMU.

The latter concept is the preferred one as communication between units is reduced and thereby less energy consumed for sensing and estimation. But this comes with more computational complexity since a coarse vehicle speed estimate needs to be derived. Having more than one sensor in one housing with known displacement it is straight forward to determine the vehicle speed.

The detection scheme has been verified in both experimental setups where controlled vehicle passage occurred, as well as on real-life motorway with large traffic density, [10]. Similarly, the detection using a magnetometer source has been tested.

B. Low-power operation

Depending on available energy levels, traffic load, and required performance in terms of delay and sensing accuracy, a sensor node must be able to maintain a high level of awareness while still minimizing the power consumption. Using a 750 mAh battery and the requirement to be able to operate during the winter, ranging from November to March (a total of 3360 hours), a sensor node cannot have a higher power consumption than approximately 220 micro amps, assuming that the battery’s performance drop in low temperatures and self-discharge are neglectable.

The concept of energy-aware operation implies that knowledge of the energy system is utilized to improve system operation, which allows a device to dynamically adjust its mode of operation to optimize the entire network’s robustness, as opposed to sub-optimize individual devices. The use of distributed energy-aware operation can therefore drastically extend the dependability of the network. Raghunathan et. al reported in [12] the advantages of using energy awareness in wireless sensor networks. The term power-aware operation is used to describe a system that can keep track of power usage, as well as monitor the energy harvesting system. This approach allows a device to perform energy-consuming tasks such as data compressing, encryption, or firmware updates, at no additional cost in terms of energy. A sensor node’s power consumption also depends on how its different sub systems interact. Vehicle speed estimation can for example be obtained using two RMUs by detecting the vehicle with a low-power magnetic sensor and measuring the time it takes for a vehicle to pass the (known) distance between them. This yields a very low power consumption for the sensing and processing sub system, but a high consumption on communication. Another approach is the use the more power consuming vibration sensor and extracting a passing vehicles’ speed using more advanced signal processing. This yields a very high power consumption for the sensing subsystem but no extra energy is needed for the communication.

C. Network architecture and protocols

When designing communication protocols for the RSN architecture it is of primary importance to satisfy dependability requirements of envisioned ITS applications. In general, dependability of a computing system is an integrated property jointly characterized by its attributes: availability, reliability, security and maintainability [13]. The concept of dependability also includes justification of an ability of the system to perform according to the requirements on the above listed attributes given in the system specification.

In this section we present a summary of the dependability analysis performed for the selected show-case application. In the case of the RSN architecture, the availability requirement concerns maximizing the energy efficiency of the communication system for prolonging the time of autonomous network operation. With respect to maintainability requirements, the target communication system should possess self-* properties excluding as much as possible human involvement in its configuration and management, since the network will be deployed by non-experts in communication systems. This requirement also motivated us to search for the simplest possible solution to network protocols following the Occam’s razor principle “plurality should not be posited without necessity”.

Fig. 5: Band pass filtered vibration signal for a passenger car with two axles passing by the sensor

Fig. 6: Envelope of the energy signal for a passenger car with two axles passing by the sensor
1) Application requirements on topology: Obviously, the accuracy of the location of the queue-end depends on the distance between the RMUs and their sensing capabilities. Efficient detection of vehicles can be achieved by using either magnetometers or accelerometers, see [10] and [11]. It is assumed that an installation distance of the RMUs of 50 m is sufficient, which would yield an detection uncertainty of a little less than 50 m, depending on the detection range of the sensors.

The specifics of the installation environment, i.e. a road with lanes in the opposite directions allows suggesting a simple addressing scheme which would intern facilitate the choice of the routing protocol. For the queue-end warning application we decided that the RMUs’ addresses are assigned in an increasing order along the direction of the particular lane. Thus the address spaces for road lanes with opposite traffic directions are not intersecting. This decision implies our choice of a simple implicit geocast routing protocol where each node is preconfigured with two default routes: upstream and downstream. Obviously, when the queue end is detected the message should be propagated upstream.

2) Application requirements on timing and reliability: Depending on the relative speed and distance between queue and approaching vehicle, different levels of intervention need to be considered. In the most severe case when the vehicle is rather close at a high differential speed, an emergency brake need to be initiated. In order to get an understanding of the warning range, some numbers are needed. It can be assumed that a vehicle could achieve an average deceleration of 7 m/s² under good friction conditions. On a motorway, the relative speed, can easily reach 42 m/s, which would yield an intervention range of 126 m.

In case that the vehicle is equipped with an emergency brake assist the reaction time on a warning is shorter, than for the driver. Assuming a reaction time of 1 s already yields a range of 168 m. Adding an additional 1 s for detection and warning propagation, would mean that the vehicles headway to the queue is 210 m.

Naturally, these distances increase in case that the vehicle should receive a warning for a comfortable deceleration, which is assumed to be less than 3 m/s², yielding an intervention range of 294 m and a warning range of at least 378 m.

These numbers suggest that a visual warning by the RMUs would require 4 hops of communication within the road surface network and a rather acceptable broadcasting range for a VANET.

Table I summarizes the identified reliability, throughput and delay requirements. In summary, it is important to note that with respect to reliability the optimization objective function for the queue-end warning application is binding the packet loss rate and the end-to-end delay. Due to the specifics of the topology and the error-prone wireless transmission medium we decided to address reliability requirements on the hop-by-hop basis, i.e. designing an appropriate MAC protocol.

3) Security requirements: It is well known that securing an initially insecure communication protocol is a complex task. In many cases this process would lead to modification of the protocol functionality. Therefore, the design of a dependable protocol should start from selection of communication components, which address the security requirements. Table II presents the results of the security analysis for a general class of RSN functions.

D. Selecting MAC protocol components for addressing reliability and security requirements

Amongst the attacks presenting the highest risk for the queue-end warning application (see Table II) jamming and deployment of rogue nodes require active involvement of the MAC layer for implementing the countermeasures. The resulting MAC protocol should implement secure bootstrapping and authentication as means of protecting the network from illegitimate nodes. These procedures, however, do not have specific dependencies on the choice of the medium access technique. Protection against jamming attacks, however, requires a specific support from the MAC and physical layer. If jamming is done with the highest power and the attacker does not care to be detected, the MAC layer does not have any active countermeasures. The MAC layer at nodes located at the edge of the jammed region can notify upper layer protocols about permanent link failures. For the target protocol this implies an inclusion of the link-quality reporting functionality. When dealing with sophisticated jamming attacks, however, channel hopping, message fragmentation and redundant encoding are possible countermeasures [14]. Several protocols e.g [15], [16], [17] and references therein are multichannel schemes, (further on referred to as FDMA access), designed specifically for single radio WSN.

In the scope of our discussion it is important that choosing a class of multichannel MAC schemes with random access to the medium and on-fly channel negotiation was out of consideration due to poor overall energy efficiency of the channel scanning operation. We resort our search to the class of multichannel schemes which rely on slotted transmission in the time domain (further on referred to as TDMA access). The performance properties of either separate FDMA and TDMA components or their combination are determined by the quality of the established access schedules. The scheduling procedures fall into two major classes: centralized and distributed. The centralized approach requires the presence of a dedicated coordinator node. Since in our applications the coordinator nodes are not present we did not develop this thread further and concentrated on the analysis of distributed approaches. The distributed approaches could be in their turn divided into eavesdropping methods, cooperative assignment of exclusive schedules and implicit consensus methods (see [17] for more elaborative description). In the scope of our discussion it is

---

1For the critical communication the 1% packet loss rate is commonly used.
2Much less than the available end-to-end capacity.

<table>
<thead>
<tr>
<th>Application</th>
<th>Queue-end warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet loss rate, %</td>
<td>≤ 1</td>
</tr>
<tr>
<td>Data delivery order</td>
<td>Not applicable</td>
</tr>
<tr>
<td>End-to-end delay, s</td>
<td>≤ 1</td>
</tr>
<tr>
<td>Throughput, b/s</td>
<td>≤ 100</td>
</tr>
</tbody>
</table>
TABLE II: Analysis of security threats in a general class of RSN applications.

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Risk in RSN applications</th>
<th>Countermeasure, implementation place</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismounting and stealing nodes (including destruction of nodes)</td>
<td>High</td>
<td>Periodic network self-diagnostic, reporting the fault in presence of connectivity to the control center, graceful WSN service degradation. Network management component using support from network and MAC layers.</td>
</tr>
<tr>
<td>Jamming</td>
<td>High</td>
<td>Channel hopping combined with packet fragmentation and redundant encoding ([14] are only efficient in the case when the attacker has limited energy resources and does not use full transmission power to perform the attack. MAC layer.</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Low</td>
<td>Encryption of the message content (medium risk). Application layer.</td>
</tr>
<tr>
<td>Replay of protocol messages</td>
<td>High</td>
<td>Authentication Network layer (routing) or MAC layer.</td>
</tr>
<tr>
<td>Injection of crafted protocol messages</td>
<td>High</td>
<td>Authentication Network layer (routing) or MAC layer.</td>
</tr>
<tr>
<td>Remote code injection including installing rogue software on nodes</td>
<td>Medium</td>
<td>Secure code distribution. Network layer (routing) Application layer, network management component with authentication support from the MAC layer.</td>
</tr>
<tr>
<td>Deployment of rogue nodes</td>
<td>High</td>
<td>Authentication, secure bootstrapping procedures. Network layer (routing) and MAC layer.</td>
</tr>
</tbody>
</table>

important that the eavesdropping method requires continuing monitoring (at least during certain time) of activities on available communication channels, this obviously results in energy wastage in the “Listen” state of the transceiver. The cooperative negotiation requires an exchange of candidate schedules in the two-hops neighborhood, which also consumes energy. The most energy efficient way from the point of view of the communication overhead is suggested in [18]. There, the nodes independently agree on the communication channel number by computing common to all nodes hash function based on their own ID and the IDs of the neighboring nodes. We choose this approach as a candidate for schedule establishment both in frequency and time domains based on its both lowest overhead and low implementation complexity properties. Aiming at finding the simplest solution we remove the schedule conflict resolution functionality, by this substantially reducing the communication overhead. As the analysis presented below shows, even this simplest version provides the required performance characteristics.

E. MAC Protocol

For the sake of further discussion we assume that the nodes share a pre-deployed secret, their clocks are synchronized with one-second precision. This initialization is made off-line before the deployment of nodes at a centralized point. During the protocol’s operations all nodes re-synchronize with substantially higher precision in bootstrap phase. The protocol is designed for low-power radio transceivers with 16 available radio channels (out of which 8 are orthogonal). Each node is equipped with only one radio interface and is pre-configured with a unique identifier.

The time line for the protocol is divided into epochs. The duration of one epoch is a configurable parameter and may span over the duration of one or several superframes. A superframe contains a broadcast subframe during which transceivers of all nodes are on and a slotted unicast subframe during which only communicating nodes are on. The length of the broadcast subframe is a configurable parameter. The duration of a unicast slot equals the time to transmit one maximum size data unit plus a short acknowledgement generated by the recipient of the data packet. This is a configurable parameter of the protocol.

The epochs are enumerated and all sensor nodes have a unified understanding of the current epoch number. The structure of the time primitives is illustrated in Figure 7.

Fig. 7: Epochs, superframes, subframes and slots.

Fig. 8: MAC operations in time and frequency domains.

1) Establishment of the channel hopping and time division patterns: The FDMA and TDMA schedules are constructed in each node independently in probabilistic manner. As a con-
sequence the schedules in one node may partially overlap with other schedules in the two-hop neighborhood. The schedules’ establishment happen at the beginning of each epoch and is based on computation of a cryptographic hash function \( f_1 = Hash(e, ID_s, ID_d) \mod N \). Note that we use the same hash function both for computation of the transmission schedules and for authenticating data packets as described below. For computation of the transmission schedule we construct a data block which includes the epoch number \( e \), identifiers of the source and destination nodes \( ID_s \) and \( ID_d \) correspondingly. The resulting hash value maps either into a channel number \( CH \in [1, N_{ch}] \) or a slot number \( S \in [1, N_{slots}] \) depending on the purpose of its computation, by taking \( hash \mod N \). The broadcast channel is computed similarly using function \( R_{BCAST} = Hash(e, 0 \times FF) \mod N_{ch} \). In the time domain the broadcast communications always happen in the beginning of the superframe. Figure 8 presents an overview of separating the concurrent transmissions both in frequency and the time domains.

2) Protocol operations: In order to allow self-configuration of the new nodes during the protocol operation the bootstrapping phase repeats with a configurable period of \( N_{conf} \) epochs. During the bootstrapping phase, the entire superframe is replaced with the configuration frame, and the application operates in a default safe mode (not specified in this article). The exact specification of the bootstrapping phase procedures falls outside the scope for this article. The two major outcomes of the bootstrapping phase are: 1) Synchronization of nodes’ clocks with the highest precision, and 2) the securely exchanged current epoch number. As soon as a new node is deployed it turns its transceiver on and tunes it to the bootstrap channel computed as \( CH_{BOOT} = Hash(round(t_{cur}, (N_{conf} \cdot t_{epoch}), Secret)) \mod N_{ch} \). There \( t_{cur} \) is the current pre-configured time on the node; \( t_{epoch} \) is the duration of one epoch, specific for the particular application; and \( Secret \) is the shared pre-established secret. The computation of \( round(t_{cur}, (N_{conf} \cdot t_{epoch})) \) rounds the current time to the precision of the size of the interval between the subsequent bootstrap phases. The transceiver remains in the ON state until the configuration of the node is complete. Assuming that the new node is deployed at the end of the current bootstrap phase its configuration will end within \( N_{conf} \) epochs.

During the main operation phase the actual exchange of control and data messages happen. The MAC communications are guided by a forwarding table, with the following format of the entries \(< Slot number, Channel number, Node ID, Direction>\). The direction field indicates whether the transceiver will transmit or receive data in the particular time slot over a specific channel. The Node ID field is used as an index field when looking up the time slot and the transmission channel for locally generated packets. When receiving a packet this field uniquely identifies the source node since the joint probability of collision in time and frequency domains is negligible. This allows to include the source and destination addresses in the header of each protocol data units. The message authentication procedure described below enables an extra control on the identities of the communicating nodes.

By default we specify that all nodes compute FDMA and TDMA schedules and fill in the forwarding table at the beginning of each epoch. This means that the nodes will be in the active state during all scheduled slots even if there is no data to transmit (or receive). This operating mode does not require exchange of any messages and minimizes the protocol’s reaction time when the data to transmit becomes available.

3) Message identification and authentication:: Packet sequence numbering is left to the upper layer services directly adjacent to the MAC protocol. Therefore, this field should be present in the structure of upper layer payload. In the specified MAC protocol all messages are authenticated by means of AEAD security services, i.e. Simultaneous Combined Mode Algorithm, SCMA, [19] running on the ID’s of the source and destination nodes and the payload. The SCMA provides the means for both encryption and message authentication. Therefore, we reuse functionality for message authentication to compute hash for establishment of channel-hopping and time division patterns. The message authentication code is truncated to 32 bits, which represents a trade-off between security and byte overhead. The size of the Message Authentication Code field can of course be increased, however at the cost of increasing the communication overhead.

V. PERFORMANCE ASSESSMENT

The analysis of collision probability both in time and frequency domain is similar due to the same procedure of schedule negotiation. In the following discussion we commonly refer to time slots and available radio channels as a resource to distribute. The sequence of pseudo-random channel numbers computed by the corresponding hash functions \( f_1 \) follow a uniform distribution. Denote \( p_r = 1/N \) a probability of choosing resource \( r \ (r \in [1..N]) \) by two communicating nodes. Since all other nodes compute hash function independently, several pairs of nodes may select the same resource resulting in the collision either in frequency or time domain. An event that a particular resource is not collided is the event when either no one node selects \( r \) or \( r \) is selected by only one pair of nodes. Formally: \( p_{no-collision} = (1 - p_r)^M + M \cdot p_r \cdot (1 - p_r)^{M-1} \), where \( M \) is the number of contenders for the resource. The probability of collision is therefore \( p_{collision} = 1 - p_{no-collision} \).

In order to assess the suitability of the identified component to the queue-end warning application we first compute the minimum number of time slots needed to ensure 1 second end-to-end propagation delay for a given transmission rate at the physical layer. In this application the relay nodes do not inject new traffic into the network. In order to reduce the per-hop delay we specify that each node will reserve \( M \) transmission slots in each superframe. The signal message, therefore, can be sent/relayed during any of the \( M \) slots. Having four hops as the maximum distance between the queue-end detecting RMU and the warning RMU’s the per-hop delay should be less than 100ms (this is twice less than the required limit). In the worst (and the very improbable) case \( M \) slots in one superframe will be scheduled at its beginning and \( M \) slots in the subsequent superframe will be scheduled at its end. In order to assure the 100 ms delay for a packet being received at the last slot of the first superframe and being send during the first possible slot in the subsequent superframe, the number of
slots in between is calculated as $d_{\text{per-hop}} \cdot R_{\text{PHY}} / L$, where $L$ is the size of the transmitted signal message. In the case when $L = 10B$, $R_{\text{PHY}} = 100kb/s$, the maximum number of slots between two subsequent transmissions is 125. This makes the number of slots in a superframe $N_{\text{slots}} = 125/2 + M$. Now we need to find the value of $M$ such that the resulting collision probability and the probability of having empty slots (energy saving) are less than 1% and greater than 90% respectively. These characteristics are achieved for a superframe size of 67 slots, 5 of which will be scheduled in each superframe for data transmission. The achievable collision probability in time domain is then 0.002, and the system will be in the OFF mode 93% of time. Since the result of computation of a hash function is a sequence of uniformly distributed pseudorandom numbers, $M$ transmission slots will be distributed evenly inside the superframe. This implies the per-hop delay of much less than 100 milliseconds.

VI. SUMMARY AND CONCLUDING REMARKS

ITS will play a key role to improve transportation efficiency and safety. However, cost-benefit of deploying traditional ITS is retarded by expensive equipment, infrastructure, installation and maintenance, while cost-benefit of cooperative systems involving C2X and VANET communication is suffering from limited penetration.

In this paper we have studied the use of networked on-road devices, with the outset to improve functionality and cost efficiency of traditional ITS as well as bridging the gap towards future cooperative ITS solutions. Key features of the Road Surface Network architecture have been described, and a methodology for mapping ITS applications onto the RSN has been demonstrated on a queue-end warning use-case. Results so far manifest the overall applicability of our approach. However, the study also pin-points areas for future research.

Although the sensing and estimation schemes have been tested in both lab and real-life settings, the confidence in the detection is still too low for a safety system. This requires more verification efforts to be put on the vehicle detection. Additionally, the vehicle speed estimation is still in a conceptional state and requires further research efforts for both accelerometer based and magnetometer based estimation. This is motivated from a power consumption perspective it is important to estimate the traffic flow speed with rather high accuracy in one RMU. Another important challenge is to extend the performance of the wireless communication. Near ground communication results in severely limited range and an increase of packet loss.

The presented specification of a communication protocol is specific for the selected use case. While other RSN application would require other application-tailored solutions it is important to highlight the integrated design process which should be adopted when creating road sensor network architecture. This process on the one hand which include joint analysis of reliability, performance and security requirements for selecting appropriate protocol components. On the other hand the design process should be overlaid on top of accurate and energy efficient real-time traffic characterization and available mechanisms of energy harvesting and scavenging, which together call for simplest possible and energy efficient solution yet satisfy the requirements of the application. Enabling such an integrated design methodology is a complex and challenging process.

Despite the remaining challenges it is the authors believe that RSN represent a beneficial complement to targeted VANET strategies. Moreover, it can be concluded that the available technology pieces can already be combined to use WSNs on road surfaces.

REFERENCES


