Proceedings of ITS World Congress and Exhibition, New York, USA, November 2008

VEHICLE-TO-VEHICLE AND ROAD-SIDE SENSOR COMMUNICATION FOR ENHANCED ROAD SAFETY

Andreas Festag, Alban Hessler, Roberto Baldessari,
Long Le, Wenhui Zhang, Dirk Westhoff
NEC Laboratories Europe, Network Research Division
Kurfürsten-Anlage 36, D-69115 Heidelberg
Phone: +49/(0) 6221/4342-0, Fax: +49/(0) 6221/4342-55
Email {festag|hessler|baldessari|le|zhang|westhoff}@nw.neclab.eu

Abstract

We propose a hybrid ITS safety architecture that combines vehicle-to-vehicle communication and vehicle-to-roadside sensor communication. Opposed to dedicated roadside units, which require major investments for purchase, installation and maintenance, roadside wireless sensor and networking technology represents a cost-effective solution and can leverage the deployment of the system as a whole. Among the various services of the hybrid communication system, the paper introduces accident prevention and post-accident investigation. We present a system and protocol architecture with a fully distributed concept for efficient and secure storage of sensor data. For deployment, this architecture will likely be combined with an alternative approach using dedicated road-side units as a centralized network element for communication and data storage. For the proposed system, we describe the main components (radio, networking and services, security). Finally, we describe our prototype implementation and experimental testbed featuring hardware and software platforms for vehicle on-board units and sensor nodes.

Keywords: vehicular communication, wireless sensor networks, accident prevention, post-accident investigation

I. INTRODUCTION

In order to make roads safer, cleaner and smarter, sensor and communication technologies are increasingly considered in research, standardization and development. While today's vehicles are already able to sense the surrounding environment, we expect that future cars will communicate with a roadside communication infrastructure and with each other. Connected vehicles create a fundamental building block of intelligent transport systems (ITS) and can provide numerous application services to improve safety and comfort of driving.

Among the various wireless technologies for vehicular communication, we can identify a clear trend n the usage of Wireless LAN adapted to vehicular conditions in Europe and North America [1], [2], [3]. The upcoming standard IEEE 802.11p [4] as well as the frequency band allocations in the higher 5.8 GHz band for various public safety services clearly indicate the next step towards deployment. For vehicle-to-infrastructure communications, the system architecture assumes access points with IEEE 802.11p network interfaces to be set up at least in dedicated locations (such as road intersections), whereas the system is still able to deliver information even when no access point is available within the communication range of a vehicle. A particular technology is *vehicular ad hoc networking* (VANET), which enables communication over multiple wireless hops, potentially but not necessarily including roadside access points.

While the development of vehicular communication technology based on IEEE 802.11p has considerably progressed in the past years, the introduction and wide-scale deployment

of such a system has not been decided yet. In a purely vehicular communication system, i.e. without roadside access points, a minimum market penetration of equipped vehicles is required for applications to work. This can at best be achieved a few years after an initial commercial roll-out. To accelerate the revenue of such investment, a roadside infrastructure could be installed along major road across a country. However, costs for purchase, installation and maintenance represent a major investment and in turn can be an obstacle for a successful introduction.

A complementary solution to the deployment of road-side access points consists of road-side wireless sensors. These devices represent a cost effective solution and allow to create *wireless sensor networks (WSN)*, but are subject to energy and processing constraints. For battery-powered sensor nodes, IEEE 802.15.4 [5] is a well-established radio technology that permits embedded systems to function up to years on a simple pair of AA batteries. WSN islands could be rolled out along the road, such as on the road surface or at road boundaries (curves, tunnels and bridges), and even on a much wider scale. They can be used to measure physical data like temperature, humidity, light, or detect and track movements.

In this paper, we propose and analyze a hybrid architecture that combines vehicle-to-vehicle communication and vehicle-to-roadside sensor communication. From the wide range of possible use cases, we have chosen *accident prevention* and *post-accident investigation*, which we regard as important future services.

For accident prevention, roadside sensor nodes measure the road condition at several positions on the surface, aggregate the measured values and communicate their aggregated value to an approaching vehicle. The vehicle generates a warning message and distributes it to all vehicles in a certain geographical region, potentially using wireless multi-hop communication. For post-accident investigation, sensor nodes continuously measure the road condition and store this information within the WSN itself. When a accident occurs, road condition data stored over a sufficiently long duration can be used for forensic reconstruction of road accidents. In contrast to the accident prevention service, such a liability service needs to be restricted to a well specified group of end-users, e.g. insurance companies or the road patrol. Information stored within the WSN can also be utilized to judge a driver's driving style according to the road condition at the moment of an accident.

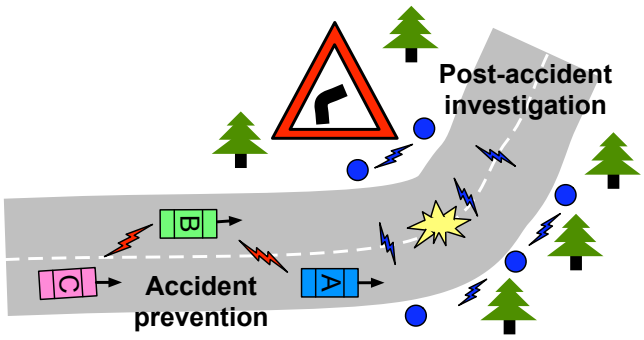


Fig. 1. Use cases for vehicle-to-vehicle and roadside sensor communication

The hybrid, road-side WSN – VANET communication architecture assumes that vehicles are equipped with an *on board-unit* (OBU) and two wireless network interfaces; namely IEEE 802.11p and IEEE 802.15.4. The sensor data are stored in a distributed and redundant database in the sensor nodes. Data are also transmitted to approaching vehicles, which can inject hazard

warnings into the VANET. As compared to the alternative systems architecture, the one just presented allows to reduce costs for ITS road-side communication facilities. In such a setting (this corresponds to the protocol design depicted in Fig 3(a)), no road-side equipment other than the sensor nodes themselves is required. We argue that the WSN hardware, roll-out and maintenance costs are a crucial success criterion for a real WSN island penetration in the context of vehicular communication since the roll-out of WSN islands with high probability is an investment of a single or few providers. Maintaining the costs for road-side equipment low also motivates our decision not to use tamper resistant modules in the sensor nodes. Consequently, the best achievable security is achieved by applying pure software solutions.

An alternative system architecture is also presented in this paper. In the system depicted in Fig. 3(b) we do not consider costs for road-side equipment as primary design criterion and therefore add a more powerful RSU to each road-side WSN island. Such a setting is beneficial with respect to a straightforward storage of monitored data, but also paves the way to an optional WSN and/or VANET communication over the Internet. As an example, live environmental information could be pushed to the car navigation system. The coexistence of both approaches is also likely since it provides a good compromise between costs and connectivity, giving a road operator the choice between two systems.

The remaining sections of the paper are organized as follows: In Sec. II we introduce scenarios and use cases, focusing on accident prevention and post-accident investigation. Sec. III presents the system and protocol architecture and Sec. IV describes technology components of the proposed system. In Sec. V we outline our prototype implementation and experimental testbed and conclude in Sec. VI.

II. Scenario and Use Cases

Roads have always been dangerous, and a lot of efforts have been undertaken to improve their safety. Vehicles, education, road signs have been improved throughout generations. Nevertheless, dangers remain and with the rise of computer and wireless technologies, new solutions are available to assist the driver in hazardous situations and to decrease road dangers.

We envision that in a near future, vehicles will be equipped with wireless devices, so that they can communicate with each other. The primary application of this technology is to let vehicles exchange about their current context. In detail, the information exchanged can be of two types, *(i)* periodic exchange of status messages among the vehicles in direct communication range and *(ii)* safety messages triggered by a critical event and distributed in a geographical region. In the same time frame of the VANET deployment, we expect that WSN technologies would have reached the necessary maturity to be rolled out in a large scale at an affordable cost. We foresee that WSN roadside islands will be installed in specific dangerous locations to support drivers with current road and weather condition. Typically, WSN technologies help where neither the vehicle's sensors nor the driver can detect the danger, e.g. very localized road condition, animal crossing the road out of a forest, etc. The roadside WSN islands significantly extend the sensing range of a vehicle. Hence, either the driver or the vehicle itself could initiate appropriate reactions according to the current environmental conditions with the overall aim to increase the driver's safety.

The scenario of a combined WSN and VANET architecture aims at the provisioning of two complementary services:

1) **Accident prevention.** When a car passes by a sensor network, it retrieves fresh environmental data collected by the roadside sensors. Data can include various physical quantities, such as temperature, humidity and light, and also detect moving obstacles (such as animals); optionally, it can be processed within the WSN network, in order to

acquire higher level information. The received information are processed in the vehicle's OBU and potentially displayed to the driver. Hence, wireless sensor nodes complement other sensors installed in a car (such as radar). However, wireless sensor nodes are external devices that in principle can measure road conditions data more accurately than an on-board sensor. In addition, the data of the wireless sensor node may include a set of data covering a period of quantities collected over a time-span and make the data more plausible.

Once a vehicle has processed the sensor data, it may interpret the data as a dangerous situation and trigger a safety warning message. For this message, the vehicle determines a geographical region defined by a geometric shape and broadcasts the message to its neighbor vehicles. The communication system of the vehicles ensures that the data packets is reliably distributed to all vehicles located within a region. As a result, vehicles that receive the information are warned about dangerous spots ahead of time and can take appropriate countermeasures.

2) **Post-accident investigation**: In this use case, sensor nodes continuously measure and store the environmental data. These data include the collected quantities (e.g. temperature) and also event data, such as previously detected obstacles and vehicles. Storing these information over a long time period may be of interest for a forensic team. In contrast to the accident prevention service, such a liability service will be limited to a well specified group of end users, e.g. insurance companies or the road patrol. These authorized users can retrieve the sensor data from the roadside WSN islands from (nearly) any time in the past for forensics purposes. Typical examples are retroactive discovery of accident causes and assessment of drivers' behavior with respect to the road conditions at the time of the accident.

The two scenarios described above pose various functional and performance-related requirements for the data communication and storage. A fundamental assumption is that a communication system for vehicle-to-roadside communication will only be rolled out if the costs for the roadside equipment, installation, and maintenance are minimal. This leads to a system architecture with extremely low cost autonomous sensor networks and without the deployment of dedicated roadside units. Since sensor nodes may disappear over time due to their restricted energy capabilities, both communication among sensors and data storage need to be distributed and redundantly organized. Likewise, sensor nodes' data transmission to approaching vehicles and dissemination of data for persistent storage require energy-efficient communication protocols. The main requirements for the security is to ensure the reliability and the trustworthiness of the data being communicated from the WSN to the vehicles. In addition, as the data are stored for a relative long duration within the roadside WSN, they shall not be stored in plain-text. In turn, in order to minimize costs, software-based security solutions are preferred over costly hardware components or tamper-resistant modules on sensor nodes.

III. System and Protocol Architecture

While VANETs and WSNs have common characteristics, such as network self-organization, they also have important differences. VANET nodes are typically equipped with relatively powerful computing devices. Further, since VANETs node are connected to the power supply of a car or are located at the roadside, they usually do not have constraints on energy consumption. In contrast, sensor nodes have extremely small physical dimensions and strong constraint in the processing and energy capabilities. VANET nodes are also highly mobile, resulting in frequent topology changes of the network, whereas sensor nodes are assumed to

be static. The different characteristics of VANETs and WSN have led to the development of different technology components for radio, networking, middleware and applications.

Radio. For VANETs, IEEE 802.11 [6] represents a cost-efficient and widely deployed solution that will be applied in OBUs and RSUs of future VANETs. More specifically, its variant IEEE 802.11p [4] is designated for safety applications. The basic data rate of IEEE 802.11p is 3 Mbps for a 10-MHz channel but higher data rates up to 27 Mbps are also possible. In WSNs, IEEE 802.15.4 realizes a low costs, energy-optimized radio technology for small, $\sim$250 kbps data rates.

Routing. For routing in VANETs, Geocast [7] supports wireless multi-hop communication utilizing geographical positions for addressing and packet forwarding. Geocast allows scalable packet transport with frequent topology changes and the efficient and reliable distribution of packets in geographical areas. A previous study demonstrated that position-based routing such as Geocast significantly outperformed topology-based routing protocol in vehicular environments [8]. The assumption in Geocast is that vehicles are equipped with a GPS device and are aware of their geographical positions. In contrast, WSNs are typically not equipped with GPS to provide geographical positions and therefore apply other routing schemes that are better suited for static scenarios and optimized for energy-efficiency. For example, tinyLUNAR [9] is a reactive, topology-based multi-hop routing scheme with minimal signaling overhead by applying a label-switching technique. Efficient coding label-switching is important for WSNs where bandwidth is scarce and precious. Topology-based multi-hop routing scheme is also well suited for WSNs because sensor nodes are usually stationary.

Middleware. In both, VANETs and WSNs, a *middleware* collects, aggregates and stores collected data, but applying different concepts. In VANETs, the middleware collects all data from different sources, such as sensors inside of a car (radar, camera, etc.) as well as by communication from other cars or the communication infrastructure, often combined with a digital map[1]. In WSNs the middleware collects and stores the monitored data in a distributed way. Since the sensor nodes may disappear over time, WSNs use methods for a replicated, yet space- and energy efficient data storage. Moreover, the monitored data need to be encrypted in order to protect them from unauthorized access.

Applications. VANETs wants to achieve delivery of safety messages with low delay and high reliability. On the other hand, WSNs want to achieve a reliable collection of precise environmental data. As sensor nodes are self-powered, the protocols must be energy-efficient, and the WSN must be able to reorganize itself in case of node failures.

From our aforementioned discussion, it is difficult to design a common system architecture for both VANETs and WSNs. For this reason, we propose a hybrid system architecture that combines the best of two worlds, VANETs and WSNs (Fig. 2): We use IEEE 802.15.4 as a low-cost and energy-efficient radio technology in sensor nodes along the road side that communicate over small distances and geographical areas. IEEE 802.11p is applied in the VANET – it is more expensive but able to send data over medium distances and to distribute the information in geographical regions via multi-hop communication. The main benefit of the proposed architecture is the fact that it does not rely on dedicated RSUs and saves the investment for installation and maintenance. The absence of dedicated RSUs results in some specific requirements for the system design, such as the need for IEEE 802.15.4 radio technology in vehicles, distributed and persistent data storage balanced over multiple nodes, and an efficient protocol for energy-efficient injection of sensor data into the VANET.

In the proposed architecture, the sensor nodes in the WSN monitor environmental data, store

[1]For vehicles, the data aggregation is also called 'sensor data fusion'.

the collected information with timestamp and geo-information ('sectors'), and communicate the data to passing vehicles via IEEE 802.14 (left cloud in Fig. 3(a)). The storage is encrypted and distributed over multiple nodes in a persistent way. For communication among the sensor nodes, the WSN is randomly divided into clusters, where each cluster is managed by a cluster head. The sensor nodes transmit data to their cluster heads, which transmit the aggregated data to other cluster heads. Data from the WSN are injected into the VANET by vehicles in the communication range of a sensor. The data transmission from a sensor to a vehicle can either be periodic, solicited by the passing vehicle, or both. Once the vehicle has received the sensor data, it can distribute the information to relevant in a geographical region by the Geocast protocol. Clearly, the OBU of a vehicle plays an important role in the architecture since it acts as a gateway between the WSN and the VANET and decides about injection and forwarding of relevant sensor data.

As an alternative to the WSN with a distributed data storage, a RSU may act as a gateway between WSN and VANET (right cloud in Figure 3(b)). In this architecture, the RSU collects all sensor information, maintains the collected, aggregated data in a local database, and injects the data into the VANET.

The resulting protocol architecture is shown in Fig. 3(a). A vehicle's OBU has a dual protocol stack. For communication in the VANET the OBU executes Geocast and IEEE 802.11p beneath the VANET middleware and application. It is worth noting that a vehicle does not need to implement full tinyLUNAR, but the minimal functionality required to access the WSN. In Fig. 3(a) this is expressed by tLI (tinyLUNAR Interface). A sensor node executes IEEE 802.15.4 and tinyLUNAR as radio and networking protocol, the middleware tinyPEDS [12] and applications. The alternative protocol stack for centralized data storage is depicted in Fig. 3(b). Compared to the proposed architecture, the RSU has the same stack as the OBU in the previous figure, whereas the OBU has a simple stack.

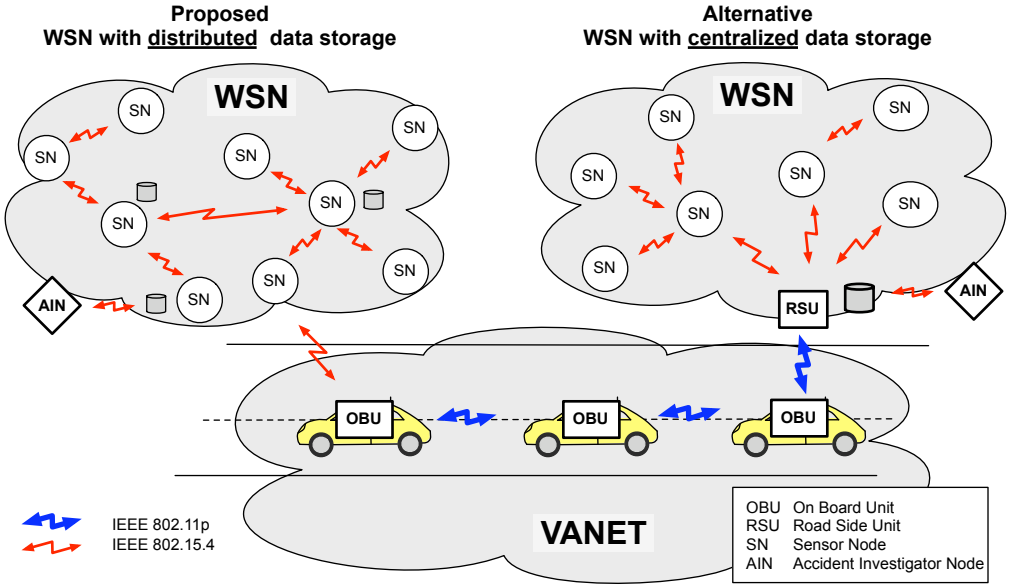
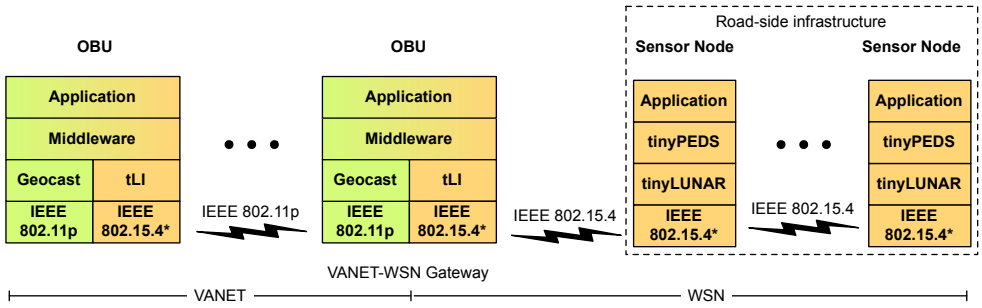


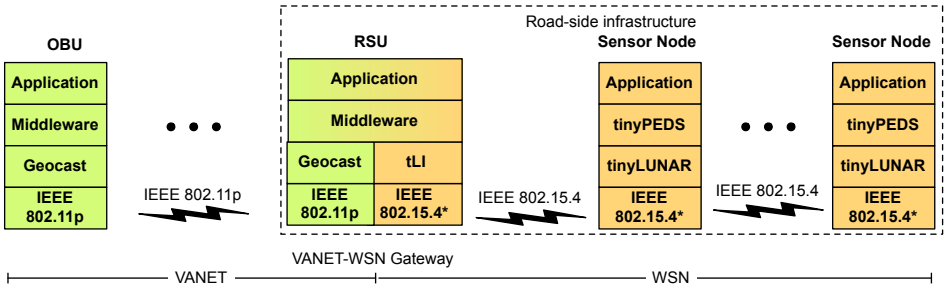
Fig. 2. System architecture with distributed and centralized data storage

IV. Technology Components

This section describes the core technological components of the hybrid VANET-WSN architecture.



(a) Proposed protocol design for distributed data storage



(b) Alternative protocol design for centralized data storage

Fig. 3. Protocol design

IEEE 802.15.4*. 802.15.4 defines PHY and MAC layers targeting low bit-rate personal area networks and is also the basis for *ZigBee* specification. At the unlicensed 2.4 GHz band, it is based on direct sequence spread spectrum and it can achieve a data rate of 250 kbps using OQPSK modulation. At this frequency range, the band is divided into 16 non-overlapping channels.[2] The MAC layer provides access to the physical medium by through a CSMA/CA protocol, management for association of nodes and security. IEEE 802.15.4 can provide guaranteed time slots when using a beaconing mode. However, we use B-MAC [10], a tinyOS variant of IEEE 802.15.4 (indicated by *), which defines a MAC layer based on CSMA/CA, but no management for security nor node association, i.e. node joining the network.

IEEE 802.11p. IEEE 802.11p is a draft amendment to the IEEE 802.11 standard dedicated to vehicular environments. It is derived from IEEE 802.11a standard, but PHY and MAC layers are modified to support low-latency communication among vehicles. IEEE 802.11p operates at a frequency band specifically allocated for road safety, such as 5.850–5.925 GHz (75 MHZ) in the US and 5.875–5.90 GHz (30 MHz) in Europe with possible future extension, defines data rates from 3 to 27 MHz for 10 MHz channels (optionally 6 to 54 MHz for 20 MHz channels), OFDM modulation and maximum power levels of 44.8dBm. The basic MAC is the same as the well known IEEE 802.11 Distributed Coordination Function (DCF). It adopts concepts from Enhanced Distributed Channel Access (EDCA) of 802.11e, like Access Category (AC) and Arbitrary Inter-Frame Space (AIFS), in order to differentiate priorities among applications. IEEE 802.11p is designed as a multi-channel scheme, where nodes can switch between channels (US) or transceive on multiple channels simultaneously (dual transceiver in Europe). For advanced networking algorithms, we use standard-compatible extensions to control radio parameters (transmit power and others) on a per-packet basis.

[2]Note that other PHY layers for IEEE 802.15.4 are defined, with other frequencies and modulation schemes.

tinyLUNAR. tinyLUNAR[3] offers a low-overhead, topology based, reactive routing for WSNs. Based on the label switching mechanism, nodes maintain simple and small forwarding tables, while the overhead for data packets is only one byte. Routes are discovered by flooding route requests, which can address nodes according to flexible criteria; e.g. node role, content, position, etc. Our WSN middleware, *tinyPEDS* [12], takes advantage of this addressing to easily build a transmission overlay for the tinyPEDS sectors.

Geocast. Geocast is a networking protocol using geographical positions for addressing and routing. It supports the addressing of individual nodes and of geographical areas. Core protocol components of Geocast are beaconing, location service, and forwarding. With beaconing, nodes periodically broadcast short packets with their ID, current geographical position, speed and heading. The *location service* resolves a node's ID to its current position based on a flooding request/reply scheme. *Forwarding* basically means relaying a packet towards the destination: *Geographical Unicast* provides packet transport between two nodes via multiple wireless hops. *Geographical Broadcast* distributes data packets by optimized flooding, where nodes re-broadcast the packets if they are located in the geographical region determined by the packet. *Geographical Anycast* is similar to the broadcast scheme but addresses a single (i.e., any) node in a geographical area. *Topologically-scoped broadcast* provides re-broadcasting of a data packet from a source to all nodes in its n-hop neighborhood. Single-hop broadcast are a specific case of TSB, which are used to send periodic messages. Various extensions adapt the basic addressing and forwarding scheme to vehicular environments and application requirements, such as algorithms for efficient and reliable communication (e.g transmit power and rate control), advanced flooding schemes to avoid so-called 'broadcast storms' and minimize overhead, security and privacy to prevent attacks and preserve the drivers' anonymity, and Internet integration [11].

WSN data retrieving. In order to efficiently retrieve environmental data collected by the WSN, we need to define an appropriate protocol. We assume that the amount of information collected by the WSN is relatively small due to data aggregation, and its packet size does not exceed 20 bytes. The objectives of the protocol are: *(i)* In normal conditions, every vehicle entitled to get the WSN information should receive it. *(ii)* The energy consumption for the WSN should be as small as possible. We consider the energy consumption of a mobile router as negligible for a vehicle. *(iii)* The solution should be cost-effective for WSN operators.

From the requirements listed above, we believe that the best solution for the vehicle would be to pull the information by broadcasting a triggering message when approaching to a WSN island. Assuming that in the future the positions of roadside safety WSN islands are integrated to navigation systems, vehicle thus may be informed when to start scanning for WSN information. This would allow the sensor nodes of the WSN to use low-power listening (LPL) techniques with a trade-off between service delay and network lifetime. As road-safety is a critical application, the sleep period of the node should be rather short (one second maximum). Upon reception of the triggering message, an aggregator sends back to the vehicle road-safety data. In our case, that data consists of aggregated environmental information such as light, humidity and temperature. Based on these raw data, a vehicle could for example infer if there is ice on the road.

tinyPEDS tinyPEDS[4] [12] is a distributed data collection and storing scheme with security enhancements for WSNs. It used concealed data aggregation techniques in order to minimize the size of the data transmitted in the network, thus increasing the system lifetime. The

[3] Leightweight Underlay Network Ad hoc Routing

[4] tiny Persistent Encrypted Data Storage

network is divided in a few sets of sectors defined by the WSN operator at the time of deployment. For example, in our scenario, there could be 'north of the road' and 'south of the road' sectors. In each sector, there is an elected aggregator which is in charge of collecting the data for the sector. Data is encrypted before being stored, in order that an attacker cannot read it out if it corrupts a node. Stored data can later be used by an authority for forensics purposes. *tinyPEDS* has further reliability and security enhancements, such as access control and sensor reading outliers detection, as presented in [13]. To balance the memory and power load over the whole network, we use a non-manipulable node election protocol, SANE[5] [14]. Furthermore, the protocol increases the robustness of our solution, since the network can re-organize itself if the aggregator is out-of-order.

VANET middleware. The VANET middleware is the main data repository in a vehicle, which is a dynamic representation of the vehicle's environment. It maintains the fused sensor data, information exchanged with other vehicles and static data (such as a digital map). The stored data are utilized by control algorithms for driver assistance and communication applications. Typical example of a VANET middleware is the *'local dynamic map'* [15]. In addition to data storage, the middleware has important tasks for cross-layer communication exchange, security and privacy [16], [17], [18].

WSN application. On top of tinyPEDS, there is a small application that is responsible of communicating warnings for the vehicle. The cluster heads of tinyPEDS analyze the data collected by tinyPEDS, and infer if there is an actual danger for incoming vehicles. In that case, it will transmit that data to the vehicle, otherwise it will sleep in order to increase the system lifetime.

VANET applications. VANET safety applications provide the application logic and algorithms for the driver information via the HMI utilizing the VANET middleware. The applications also implement the application communication protocol, typically based on SAE J2735 [19] for message encoding and TPEG for event encoding [20].

V. Prototype Implementation and Experimental Testbed

We have implemented a software prototype and set up an experimental testbed as proof-of-concept of the proposed architecture including the integrated communication system for VANET and WSN, as well as a security middle-ware secure distributed storage in sensor nodes. The testbed was presented in a live demonstration at the 14th ITS World Congress and Exhibition in Beijing in 2007.

A. Setup

For the VANET node, we used the hardware NEC LinkBird-MX, an embedded system specially designed for vehicle. For the wireless sensor network, we tested the system on commercially available TelosB platforms [21]. Tab. I gives an overview of the hardware of our testbed.

The protocol stack of the vehicular communication system is implemented in C for the Linux OS, which results in high performance and good portability to embedded systems [22]. We tested our roadside application in two setups. In an indoor lab setup the network is deployed over a small area as a proof-of-concept. In in the road setup, we have deployed the WSN to cover an outdoor area in order to show the feasibility of WSN-to-vehicle communication. In both experiments, the post-accident investigation feature of our WSN application was also demonstrated and tested.

[5] Secure Aggregator Node Election

	VANET node (NEC LinkBird-MX)	**WSN node** (Crossbow TelosB)
Physical size	153 mm x 118 x 43 mm	65 x 31 x 6 mm
Processor	64 bits MIPS@266 MHz	16 bits MCU@8 MHz
Memory	512 MB + 16 MB program flash and 128 MB RAM	10 kB RAM, 48 kB program flash, 1 MB for data logging
Power suppy	5.4–22 VDC@400 mA max.	3 VDC@25 mA (active, sending) 6 μA (sleep)
Network interfaces	Fast Ethernet, IEEE 802.11p draft 3.0, IEEE 802.15.4 (only RSU)	IEEE 802.15.4
Connectors	UART (GPS, CAN), USB, MOST, VICS	UART, I2C, SPI
Antenna	External, omni-directional, diversity	Nearly omnidirectional (on-board) or directional (external)
Operating system	Linux 2.6	TinyOS
On-board sensors	None	Temperature, humidity, light

TABLE I

EXPERIMENTAL PROTOTYPE PLATFORMS FOR VANET AND WSN NODES

B. Indoor Setup and Tests

The goal of the indoor tests was to observe the capability of every vehicle inside the Geobroadcast range to receive warning signals initiated by the WSN. Three VANET nodes run a application that displays hazard warnings to drivers via a visual HMI. Each VANET nodes run Geocast as part of the communication protocol stack. The positions of the vehicles are mocked by a 4th control PC, which feeds the VANET nodes with position information and permits to reset, pause or start the experiment at every time. Because of the proximity of the equipment, packet dropping is also emulated based on the distance between communication nodes. In the experiment, one of the VANET nodes is connected via IEEE 802.15.4 to a sensor note that acts as a gateway to the sensor network. If this node is in the vicinity of the sensor network, it will receive sensor data, and forward to other VANET nodes nearby using Geobroadcast.

C. Road Setup and Tests

In the road setup, we have deployed the WSN to cover an area of about 900 m^2 close to a road. The sensor nodes that may potentially can communicate with vehicles are put on poles standing about 45 cm above ground. Nodes lying on the ground suffer from poorer connectivity due to a higher degree of ground reflection and scattering. In the test, a vehicle – equipped with an on-board unit and an 802.15.4 interface – is driving toward the WSN with a Line-of-Sight (LoS) communication path. During the test, the vehicle periodically sends requests to retrieve WSN information. When the vehicle's OBU receives data from the WSN, the warning is graphically shown to the driver via screen and HMI together with the measured distance between the vehicle and the WSN.

For the demonstration of the accident prevention service we drove the vehicle in direction of the roadside WSN with varying velocities up to 70 km/h. Higher velocities could not be managed safely on our test spot due to the limited road length. We measured approximately the distance at which the vehicle received the safety information from the WSN for the first time, which would determine the time left for a driver to react to the incoming danger. The

Velocity [km/h]	Omni-directional antenna [m]	Directed antenna [m]
30	78	150, 165 163
40	79	158, 161 163
50	68	150, 164 155
60	71	140 150, 155
70	72	151, 155, 161

TABLE II

COMMUNICATION RANGE FOR WSN-TO-VEHICLE COMMUNICATION WITH DIFFERENT ANTENNA TYPES AND VELOCITIES IN A LOS SCENARIO WITH AGGREGATOR NODES 45 CM ABOVE THE GROUND.

vehicle sent a message to the roadside WSN every 200 ms. An aggregator node receiving such a message responded by sending the actual aggregated value of their cluster.

Tab. II documents our measurements in a LoS setting for different velocities and antenna types (directed antenna, omni-directional antenna). In this measurement campaign the four aggregator nodes have been placed 45 cm above the ground. Whereas the antenna type has significant impact on the transmission range and thus on the reaction time of a driver the chosen velocities in our setting do only effect the measured transmission range to a minor degree. For the setting with the directed antenna we made three measurements per velocity, whereas we did only one for each velocity when using an omni-directional antenna. In turns out that under such (surely simplified conditions since no obstacles are in place and only one vehicle is sending 'hello'-messages at one point in time) our measurements defend the design choice to directly communicate between the roadside WSN and the vehicle's OBU via IEEE 802.15.4. To recall, in order to save hardware costs in a real large-scale deployment of roadside WSNs for an IEEE 802.11 enabled RSU per each WSN roadside, we decided not to involve any devices on the roadside which are more powerful and costly than sensor nodes themselves.

D. Post-Accident Investigation

As *Accident Investigator Node (AIN)* (see Fig. 3(a)) we used a standard laptop with a tinyPEDS client to retrieve past data from the WSN. In our setting, sensor nodes had the capability to store data for 50 days, which appears to be sufficient for a typical post-accident investigation.

In the experiment we let the AIN query the WSN about past monitored values, which was successfully able to retrieve and decrypt the data. We demonstrated security features such as DoS resilience using access control mechanisms developed in the UbiSec&Sens project by showing that reader devices that do not possess the key are not able to decrypt the stored data.

VI. SUMMARY

We presented a hybrid architecture of vehicular ad hoc networks (VANETs) and roadside wireless sensor networks (WSN) that relies on a fully distributed approach without centralized infrastructure elements for coordinating of communication and data storage. Among the manifold opportunities of such a system we focus on accident prevention and post-accident investigations. Main technology components of the architecture are *(i)* radio interfaces

IEEE 802.11p and IEEE 802.15.4, *(ii)* routing protocols Geocast and tinyLUNAR, *(iii)* middleware for VANETs and tinyPEDS for WSNs, and *(iv)* applications. The components are well adapted to the specific requirements of VANETs and WSN, respectively.

We argue that for the deployment of a vehicular communication system, the costs for purchase, installation and maintenance of the required infrastructure can become a major barrier for the introduction of such a system. A fully distributed approach for the roadside WSNs without a dedicated roadside unit per WSN considerably reduces the costs for the WSN and can therefore leverage the overall system. WSN with dedicated RSUs are still beneficial in order to provide full service and connectivity to access networks, but we expect that the majority of the deployed systems will operate fully autonomously.

REFERENCES

[1] Car-to-Car Communication Consortium, "C2C-CC Manifesto, Version 1.1," August 2007, http://www.car-to-car.org.

[2] US Vehicle Safety Communications (VSC) Consortium, ," http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm.

[3] "Vehicle Infrastructure Integration (VII)," http://www.its.dot.gov/vii/.

[4] IEEE, "Wireless Access in Vehicular Environments (WAVE). IEEE 802.11p Draft Version 4.0.," March 2008.

[5] IEEE, "MAC and PHY Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs). IEEE 802.15.4-2006," July 2006.

[6] "IEEE Std 802.11, 1999 Edition," Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[7] L. Le, A. Festag, R. Baldessari, and A. Festag, *Handbook on Vehicular Networks*, chapter CAR-2-X Communication in Europe, Taylor & Francis, M. Weigle and S. Olariu (edts.), October 2008.

[8] A. Festag, H. Füßler, H. Hartenstein, A. Sarma, and R. Schmitz, "FleetNet: Bringing Car-to-Car Communication into the Real World," in *Proc. 10th ITS World Congress and Exhibition*, Nagoyoa, Japan, November 2004.

[9] E. Osipov, "tinyLUNAR: One-Byte Multihop Communications Through Hybrid Routing in Wireless Sensor Networks," in *Proc. NEW2AN*, St. Petersburg, Russia, September 2007, pp. 379–392.

[10] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in *Proc. SenSys*, 2004, pp. 95–107.

[11] A. Festag, W. Zhang, L. Le, and R. Baldessari, *Vehicular Networks: Techniques, Standards and Applications*, chapter Geocast in Vehicular Networks, Taylor&Francis, H. Moustafa and Y. Zhang (edts.), December 2008.

[12] J. Girao, D. Westhoff, E. Mykletun, and A. Araki, "TinyPEDS: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks," *Ad hoc Networks*, vol. 5, no. 7, pp. 1073–1089, September 2007.

[13] J.-P. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A Secure and Resilient WSN Roadside Architecture for Intelligent Transport Systems," in *Proc. WiSeC*, Alexandria, VA, USA, March/April 2008, pp. 161–171.

[14] M. Sivrianosh, D. Westhoff, F. Armknecht, and J. Girao, "Non-Manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," in *Proc. WiOpt*, 2007.

[15] Z. Papp, C. Brown, and C. Bartels, "World Modeling for Cooperative Intelligent Vehicles," in *Proc. IEEE Intelligent Vehicles Symposium*, June 2008.

[16] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication," in *Proc. WMAN*, Bern, Switzerland, March 2007.

[17] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," in *Proc. VTC*, Baltimore, MD, USA, Oct. 2007.

[18] M. Torrent-Moreno, A. Festag, and H. Hartenstein, "System Design for Information Dissemination in VANETs," in *Proc. WIT*, Hamburg, Germany, March 2006, pp. 27–33.

[19] DSRC (Dedicated Short Range Communication) Technical Committee, "Dedicated Short Range Communications (DSRC) Message Set Dicti onary," SAE Standard J2735, work in progress, March 2006.

[20] "TISA Forum," http://www.tisa.org.

[21] Crossbow Technology Inc., "TelosB Mote TPR2420," http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf.

[22] "NEC Car-2-X Communication SDK (C2X SDK)," http://c2x-sdk.neclab.eu.