Applicability of IEEE 802.11s for Automotive Wireless Software Updates

Marco Steger*, Michael Karner*, Joachim Hillebrand*, Werner Rom*, Eric Armengaud†,
Martin Hansson‡, Carlo Alberto Boano§, and Kay Römer§

*Virtual Vehicle Research Center, Graz, Austria
†AVL LIST GmbH, Graz, Austria
‡Volvo Group Trucks Technology, Göteborg, Sweden
§Institute for Technical Informatics, Graz University of Technology, Graz, Austria
Email: marco.steger@v2c2.at

***Abstract*—Due to the rising number of electronic control units (ECU) in a vehicle and the growing complexity of the related software installed, a fast and efficient system for updating software is needed. Wireless software updates similar to firmware over the air updates for smartphones can be a suitable solution to solve this issue. In this paper we propose a wireless update system based on an IEEE 802.11s mesh network and describe related high-level requirements for such a system. Additionally the prototype of a wireless vehicle interface (WVI) is described. This interface is needed to maintain the wireless link as well as to forward the received data to the in-vehicle communication system and finally to the ECU. Existing diagnostic standards are applied to transfer and install the new software on the ECU.**

Furthermore, IEEE 802.11s-based network nodes and the WVI prototype are used to evaluate the applicability of IEEE 802.11s for a wireless update system used in the vehicle development phase. We performed indoor measurements as well as measurements inside two different vehicles to evaluate the influence of the shielding properties of a vehicle. The results of these measurements show that the used setup consisting of the WVI prototype and other IEEE 802.11s based nodes can be used to realize a wireless update system and is able to fulfil the defined system requirements.

I. Introduction

The number of electronic control units (ECU) in a vehicle is rising, and the used software (SW) is getting more and more complex, leading to a growing number of bugs in the automotive SW. Because of that, efficient SW updates for vehicular ECUs are getting more and more important. An emerging trend for consumer devices is to perform wireless SW updates. These so-called firmware-over-the-air (FOTA) updates can help to speed up the update process and reduce the related costs dramatically. All major mobile phone manufacturers are already using FOTA updates to provide new features and to fix bugs. This technology can help to reduce costs for customers as well as for OEMs, avoid product recalls, and increase consumer satisfaction.

In a vehicle, the size of current ECU SW can be about tens of megabytes for engine and transmission controllers, while infotainment systems (e.g., audio or navigation system) are usually the largest and most complicated software units, often exceeding 100MB [1]. Therefore, a fast and reliable wireless link to the vehicle is needed to ensure that the required data can be transferred very quickly.

To enable FOTA updates, the vehicle must be equipped with a wireless vehicle interface (WVI), which is used to transfer the received data (e.g., the new SW version) to the ECU concerned by using the in-vehicle communication system. The wireless link to the WVI can either be based on an external cellular network or use a local network infrastructure (e.g., based on Wi-Fi or Bluetooth).

For vehicle respectively ECU development a system based on a local wireless network seems to be more attractive and realistic. A development engineer will be able to use such a wireless update system to download new SW to a vehicle (via the WVI) from his office or to run wireless diagnostics.

In this paper we will introduce such a wireless update system based on the IEEE 802.11s mesh standard. Thereby we will mainly focus on the evaluation of the IEEE 802.11s-based vehicle interface and on the influence of the environment on the WVI and the wireless link (e.g., radio interference, shielding). The described wireless update system will mainly be used in the development phase of a vehicle respectively on an ECU, but in a more generalized form it will also work in workshops (vehicle maintenance) or even in the assembly line.

The rest of the paper is structured as follows. In Section 2 the system requirements are stated and different wireless technologies are discussed. Section 3 provides an overview of the related work on wireless SW updates and applications based on IEEE 802.11s. Section 4 describes the architecture of the wireless update system and the components involved. In Section 5 we describe the experimental setup and the performed measurements. The results of these measurements and an evaluation of the results can be found in Section 6. Section 7 provides a summary of the key contributions of this applied research and discusses future work.

II. System requirements and evaluation of wireless technology

In this section the requirements of the wireless update system are defined and a technology evaluation based on these requirements is performed.

A. Requirements on the wireless vehicle interface and the wireless update system

In the following the most important requirements on the WVI are stated and described. The requirements must be taken into account when the interface respectively the entire system is designed and implemented.

- Throughput: as described above the size of the SW installed on an ECU node is growing and can be between dozens and hundreds of megabytes. Therefore, the link requires high throughput to ensure a fast data transfer. In practice, diagnostic protocols like UDS [2] are used to handle the SW update on the in-vehicle communication system and confine the maximum response time of an ECU node. This time is also influenced by the end-to-end latency of the link (e.g., round-trip time for 'tester present' messages to keep programming session alive: wireless link + in-vehicle communication consisting of bus transmission times and the time the gateway(s) need to forward the data + the time the ECU needs to react on the request $\leq$ 2000ms).
- Parallel updates and scalability: the wireless update system shall be able to handle updates in parallel. This means that several vehicles can receive new SW at the same time. Therefore, one update (one SW version for a specific ECU) can be transferred to several vehicles (multi-cast, e.g., the same type of car/ECU) and the system shall be able to distribute the required data (different vehicle types, ECUs, and SW versions) via the wireless link in an efficient, fast way (e.g., using different channels per vehicle).
- Reliability: the wireless link may operate in harsh environments (e.g., concerning temperature, vibration) and will also be impaired by different sorts of radio interferences.
- Extendability: the distance to the vehicle, which shall receive new SW versions, will vary and may exceed the current transmission range of the wireless update system. In such a case there must be an easy way (with less or without any additional configuration) to extend the transmission range of the system (e.g., several hundred meters to cover the whole area of a company or a test track).
- Compatibility: laptops, smartphones, tablets, or dedicated hardware devices (in the context of automotive SW updates also called diagnostic tester devices) will be used to interact with the vehicle via the WVI and therefore the used technology shall be available for consumer electronics.
- Security: updating the SW of an ECU and adding a WVI to the existing vehicle architecture can be very critical and therefore the integrity of the transferred data as well as the integrity of the vehicle must be ensured. This paper focuses on the wireless system architecture as well as on the properties of IEEE 802.11s, not on the security layer on top of it. We will use the SHIELD methodology proposed in [3], [4] to continuously evaluate our system regarding security, privacy as well as dependability issues and to find the best configuration of the core components of our wireless update system. Additionally, security on higher network layers will be addressed as part of future research carried out within our project.
- Functional safety: for embedded automotive SW functional safety is an important issue and must also be considered when the SW of an ECU shall be updated. ISO 26262 [5] defines a safety life cycle by delineating different levels of safety requirements [6]. Regarding our wireless update system we will start from a higher level of functional abstraction (safety goal, functional safety requirements) to the more detailed levels of the technical realization of the system (technical safety requirements), down to the software (software safety requirements) and hardware levels (hardware safety requirements). For the implementation we will use knowledge about functional safety methods and work flows which we developed in several projects (e.g., SafeCer [6], VeTeSS [7], [8]) to identify all relevant functional safety requirements as well as continuously analyze and improve our system w.r.t. functional safety.
- Interconnection with other networks respectively (re)use of existing infrastructure: the interconnection to other networks (e.g., the network of a company) would be very beneficial for the wireless SW update scenario. The WVI or the diagnostic tester can connect to the network infrastructure of a company (via WLAN, Ethernet) to enable remote updates or to increase the range of the entire system.

B. Wireless technology evaluation

Based on the requirements stated above, a suitable wireless standard has to be chosen as the communication technology for our wireless update system. IEEE 802.15.4 is a very power-efficient protocol and is used in many different wireless sensor network (WSN) applications. However, this standard would be too slow for our purposes [9], [10] (raw bit rate of 250 Kbps, with a measured throughput $<$50Kbps). The throughput of Bluetooth Low Energy (BLE) is quite similar to IEEE 802.15.4 [11] (maximum application layer throughput is 236.7Kbps, typically $<$60Kbps), which also makes it unsuitable for our wireless update scenario.

A lot of research regarding vehicle-to-vehicle communication (IEEE 802.11p [12]) has been carried out in the last decades, but it is not clear when respectively if IEEE 802.11p will be integrated into vehicles. Currently, IEEE 802.11p platforms and interfaces are quite expensive compared to Bluetooth or IEEE 802.11 components. Laptops or hand-held devices such as smartphones or tablets probably won't be equipped with IEEE 802.11p hardware at all. So the availability of IEEE 802.11p components is currently insufficient. Additionally, the interconnection to other IEEE 802 networks is hard to realize because current automotive IEEE 802.11p stacks are not IP-based and a dual-stack solution would be needed to interconnect IEEE 802.11p and other infrastructural networks (e.g., a corporate network via Ethernet or Wi-Fi). Current IEEE 802.11 networks offer typically enough bandwidth to satisfy the needs of the described SW update scenario.

The IEEE 802.11b/g/n hardware is integrated in nearly every recent laptop and hand-held device, and a good fraction of this hardware can also be used for IEEE 802.11s (e.g., several Atheros and Qualcomm chips already support IEEE 802.11s).

IEEE 802.11 protocols are designed for large networks and therefore satisfy the scalability requirement. Extending the communication range of IEEE 802.11b/g/n network is possible but dedicated hardware is required. IEEE 802.11s networks can be extended easily by adding relay nodes (forwarding data to other nodes, multi-hop) without any configuration effort (in Section 3, an example regarding the range of the wireless update system is presented). Additionally, IEEE 802.11s was designed in a way that gateway nodes can be easily used to forward data to other IEEE 802 networks.

III. Related work

The use of FOTA updates in the automotive domain was already addressed in several works, which we summarize is this section. Additionally, some applications based on IEEE 802.11s are described to show the potential of IEEE 802.11s.

A. Wireless SW updates

A white paper from Redbend [1] summarizes the benefits of using FOTA updates in the automotive domain and shows the benefits of this technology for both OEMs and end users. In [13] the basic idea and the benefits of a dynamic SW update system are demonstrated. The system provides high-level abstractions for sensing and tuning automobile parameters. Using these abstractions, developers can achieve fuel efficiency, responsiveness, or safety goals and users can tune their vehicles at the granularity of individual trips, a capability we call personalized tuning. Several other scientific papers regarding SW updates over the air are available. These papers are mainly focusing on security and verification issues but the question of how the data can be transferred to the vehicle was neither addressed nor resolved.

A system where vehicles can be updated using an Internet connection to a portal server is proposed in [14]. The authors mainly focus on the secure data link between the vehicle and the portal and no in-depth information on how the data is transferred to the ECU or how a vehicle can connect to the network is provided. However, an overview on desired security properties for the network traffic of such an automotive system is given.

In [15], a security hardware module for vehicular ECUs, to handle the verification of new SW updates, is proposed. The module can also be used for data encryption respectively decryption, digital signatures, and authentication. The wireless interface and the wireless link are not described.

The authors of [16] focus on how transferred SW can be verified when it is flashed to the ROM. Therefore, an additional control system (as part of the ECU), which is responsible to handle the verification procedure, is defined. In [17] a classification of ECUs is stated and described. This approach is based on the assumption that different ECUs may require different levels of security. The idea is that an ECU, which was classified as very critical, is not allowed to be updated using FOTA updates.

All these articles focus on how wireless updates can be performed and on how the required data can be transferred to the vehicle in a secure way. However, no information about how the wireless link actually can be realized and which additional components and requirements are needed for such a system are given.

FOTA updates play a crucial role also in wireless sensor networks, as they allow to extend the software with additional features and to fix existing bugs. Over-the-air programming techniques for wireless sensor networks typically exploit their multi-hop communications to transfer the new software to all nodes in the network and need to meet also the limited power, processing, and storage capabilities of sensor nodes [18]. The same principles can be used in vehicular settings by using multi-hop capabilities to carry out a fast and efficient firmware update on several vehicles situated in a large area.

B. IEEE 802.11s applications and performance analysis

We will use IEEE 802.11s as communication media for our wireless update infrastructure. Therefore we carried out a literature research to get a better overview on the performance and on the possibilities, as well as on the limitations of IEEE 802.11s. In the following, we present the results of our literature research.

In [19] an overview on IEEE 802.11s is given. The paper starts with a brief explanation of IEEE 802.11 networks and then focuses on 11s mesh networks. Frame structure, channel selection, power management, security, and path selection are described. Additionally, measurements in a test-bed consisting of ten nodes (basic performance measurements, enforced multi-hop) were performed.

In [20] and [21], IEEE 802.11s is used as a backbone network for V2X[1] networks. The main idea is to replace the wired connections between the RSUs (road side units) and the V2X servers by wireless ones. The authors of both papers use simulation to verify the system performance.

An evaluation of the impact of uncontrolled traffic sources on real-time communication in IEEE 802.11s networks is described in [22]. The results are based on simulations using the *ns-3* simulator. The idea is to set up a WSN with real-time constraints and simulate the impact of radio interference (simulated HTTP traffic).

Other papers focus on improving the standard Hybrid Wireless Mesh Protocol (HWMP), the routing protocol used in IEEE 802.11s mesh networks, to increase the fairness in mesh networks and to make IEEE 802.11s networks more energy efficient. In [23] an energy efficient HWMP scheme (eHWMP) is proposed, which shall help to increase the overall network lifetime. Simulations are carried out to show the positive impact of eHWMP on network lifetime. The authors of [24] propose an energy-optimization-based path selection algorithm which can be incorporated in the standard HWMP. Simulations are carried out to evaluate the performance of the path selection algorithm. The authors of [25] propose a power efficient mesh application with nearly identical throughput as

[1]General term for vehicle to vehicle and vehicle to infrastructure communication.

normal 11s. The performance of the system was evaluated based on simulation results.

In [26] the implementation of IEEE 802.11s nodes based on open80211s[2] is explained and test-bed measurements (throughput vs. hop-count) were carried out. The authors also address the gateway functionality of 802.11s to other (wireless) networks. In [28] a campus-wide mesh network was used to test new mesh application. A proprietary mesh network (no IEEE 802.11s) based on madWIFI[3] was defined. The results of the experiments (a very basic evaluation of a video streaming application) are also briefly described.

A big portion of the mentioned articles use network simulators to validate the described applications. In the automotive domain, the environment can be quite rough for a wireless network architecture (e.g., regarding vibrations, temperature, and radio interference). Therefore, in this work, we perform real-world measurements instead of simulations to evaluate the performance and the applicability of an IEEE 802.11s based wireless update system in a vehicular setting.

IV. System description

The wireless update system shown in Figure 1 is based on a IEEE 802.11s mesh network infrastructure, where several vehicles, hand-held devices such as smartphones and tablet and diagnostic tester devices (the data source, where the new ECU SW version is stored) like laptops, PCs or dedicated hardware devices (mainly used in workshops) are connected to each other either directly or via another device/node. Because of the mesh characteristic of the IEEE 802.11s standard, additional devices can be used as relay nodes (e.g., a parked vehicle or a placed relay node) between two end nodes. If there is no direct connection between the source (e.g., the diagnostic tester) and the target (e.g., the WVI), a relay node can be placed in between without any extra configuration of the network and the nodes. This also means that the transmission range of the wireless system can be extended easily by (temporarily) adding/placing relay nodes. If a development engineer wants to download SW to an ECU of a vehicle parked outside he can either directly connect to the WVI (if in transmission range) or place a relay node (e.g., at a window near the parking position of the vehicle) and use this node to extend the range to ensure the connection with the WVI.

The hand-held devices can be used to schedule, trigger, and monitor the update process and to run wireless diagnostics. The diagnostic tester can be seen as the data source. The data (SW binary) can be located directly on the device or the device can be connected to a backbone network (e.g., OEM SW server) via an Internet link. The SW binary is sent to the WVI via the IEEE 802.11s link using TCP or UDP. In the next step the WVI will forward the data to the ECU, which shall be updated using the in-vehicle communication system.

Figure 1 shows a higly simplified model of the in-vehicle communication system. In reality, a vehicular communication system consists of dozens of ECUs, several different bus systems (e.g., CAN, FlexRay, LIN) and a central gateway device,

[2]open80211s is an open-source implementation of the recently ratified IEEE 802.11s wireless mesh standard [27].

[3]http://madwifi-project.org/

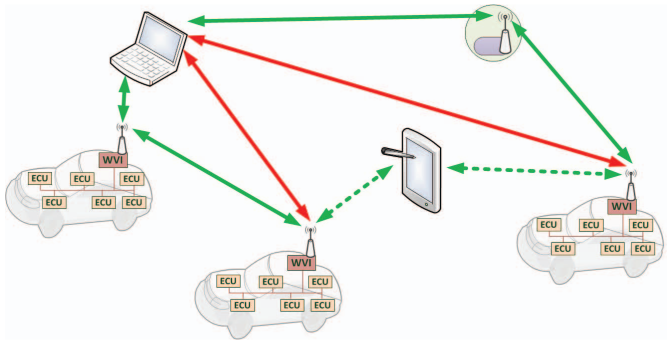

Fig. 1. The top-level communication model of the wireless update system.

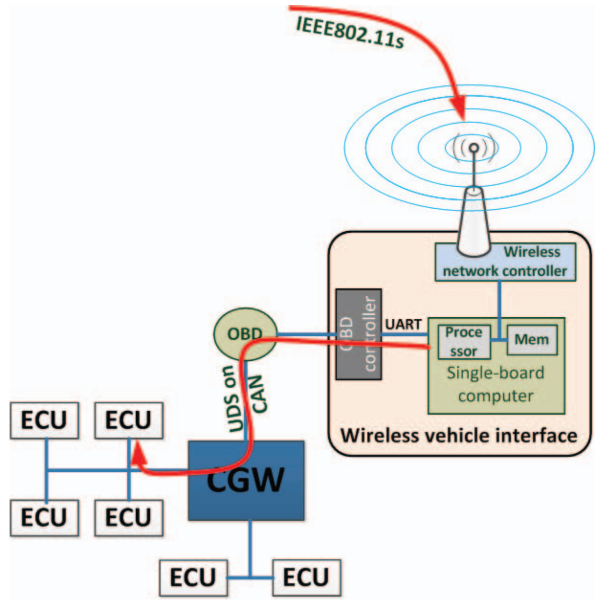

Fig. 2. Simplified block diagram of the WVI and the links to the in-vehicle communication system and the IEEE 802.11s mesh network.

which is used to interconnect all bus systems and the ECUs. The in-vehicle communication system can be accessed from outside via the OBD interface. The interface is mainly used for vehicle diagnostics (e.g., reading error codes) but can also be used to transfer data (in our case the new SW version) to an ECU inside the vehicle. Therefore diagnostic standards like Unified Diagnostic Services (UDS) or Universal Measurement and Calibration Protocol (XCP), which are running on top of buses such as CAN or automotive Ethernet, can be used.

It is important that such a diagnostic standard is used to guarantee the backward compatibility and the system acceptance inside the automotive domain of our solution.

The first prototype of our WVI consist of a Beaglebone black (BBB), a single-board computer, a IEEE 802.11(s) Wi-Fi stick (TL-WN722N) and an OBD-Controller and is implemented according to the system requirements stated in Section 2. In Figure 2 the block diagram of the WVI prototype is presented. Additionally, the connection to the in-vehicle communication system (via the OBD interface) as well as to the ECU node is shown.

V. Experimental setup

In the considered scenario the test vehicle is parked in front of the building where the office of the development engineer is located. To test a new SW version the engineer wants to download new SW to the vehicle from the office.

The prototype of the WVI described above was used to perform some measurements to evaluate the feasibility of our system setup. The basic idea was to get a feeling about the range of the TL-WN722N sticks using IEEE 802.11s in and around a vehicle. Additionally, the stick was used to perform a spectral scan (in the 2.4GHz band) in two different cars.

In the following the measurement setup is described in more detail. The results of the measurements are stated and discussed in the next section.

A. Indoor Measurements

In the first step we used two nodes to measure the transmission range of the system inside a building. Therefore we performed indoor measurements in the Virtual Vehicle office building. The first node was used as static node (NodeB) and second node (NodeA) was moved around in the building (on second floor, both nodes on the same floor for the whole measurement, a mix of thin wooden and concrete walls). Thereby we evaluated the impact of the distance between the nodes on the link quality. Among others, we measured the signal strength and used iperf[4] to evaluate the link quality. For the measurement, the Debian default rate control algorithm (Minstrel[5]) was enabled, but the rate remain at 54Mbps all the time. The multi-hop ability of 11s based network was not used in this measurement setup. This means that no relay nodes were used to increase the transmission range.

B. The impact of a vehicular environment on the IEEE 802.11s link

The WVI prototype was placed inside a vehicle (BMW X3) and the link properties to other nodes located inside as well as outside the vehicle was measured.

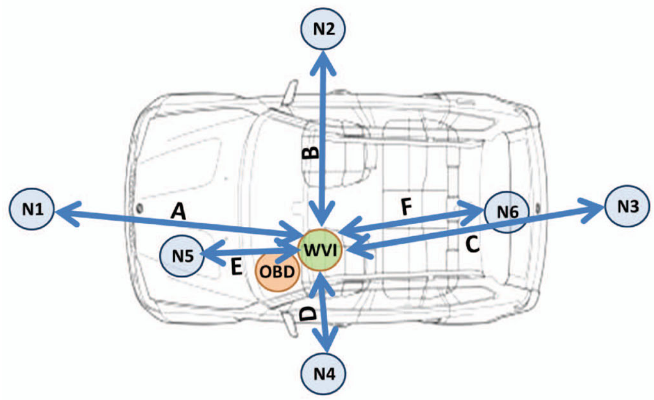

Fig. 3. Position of the used 11s node inside and around the BMW X3 and the measured links.

[4]https://iperf.fr/

[5]See https://wireless.wiki.kernel.org/en/developers/documentation/mac80211/ratecontrol/minstrel for more information

TABLE I. The indoor link properties between a two nodes

Distance [m]	Signal_{NodeA} [dBm]	Signal_{NodeB} [dBm]	Metric
0	-16	-17	152
10	-42	-44	152
20	-46	-51	152
30	-66	-66	152
40	-59	-64	152
50	-68	-73	152
60	-64	-65	152
70	-69	-73	152

In Figure 3 the location of the WVI (near the OBD interface) and the other nodes is shown. The WVI as well as the other nodes consists of a BBB and a plugged in TL-WN722N stick. The distance between the vehicle and the nodes outside the vehicle (N1-N4) were about 5m and the data rate was 54Mbps (fixed rate with disabled rate control) for all performed measurements.

C. Spectral scan of the 2.4 GHz band performed in two different vehicles

The actuators in a vehicle will create different kinds of interference. These interferences may also influence the link quality between the WVI and other nodes in the transmission range of the wireless update system. To get a better feeling of how this interference can look like, we performed some measurements in a conventional diesel car (BMW X3) and also in a electric car (Citroen C-Zero). In practice, additional interferences because of other wireless networks (e.g., WLAN and Bluetooth) from outside but also inside the vehicle (e.g., electronic devices of the passengers or the infotainment system) can occur and may also influence the link quality. However, in this paper we focus on the evaluation of the influence of the vehicle itself (infotainment off). Therefore, we first measured a baseline (no vehicle-based interferences, ignition and engine off) to check that no other sources of interference will influence our spectral scans.

The hardware used to collect the data consisted of a BBB and the TL-WN722N stick (especially the ability of the built-in Atheros ATH9K_HTC chip to perform a spectral scan in the 2.4GHz band). An adapted version of the open source spectrum analyzer tool FFT_eval[6] was used to create the plots shown in the following section. The resulting plots are mainly influenced by 1) the signal strength and 2) the density over several measurements. Hence, the blurry look of the plots is an additional level of information.

VI. Measurements and Evaluation

In this section the measurement results are described and evaluated.

A. Indoor measurements

The first measurements with 802.11s-based nodes was done indoors in the Virtual Vehicle office building. In Table I the link properties as a function of the distances between the nodes is shown.

Along with the hop count (number of hops respectively other nodes between the sender and the target node) the link

[6]https://github.com/simonwunderlich/FFT_eval

metric is used to find the best path through a mesh network between two nodes. In IEEE 802.11s networks the metric is a combination of the frame error rate and the bit rate. In our measurements, the metric remains constant because the frame error rate (error rate at the MAC layer, retries on HW are not counted) stays 0 during the measurement and the metric remains unchanged. In Figure 4 the plots of the received signal strength are shown.

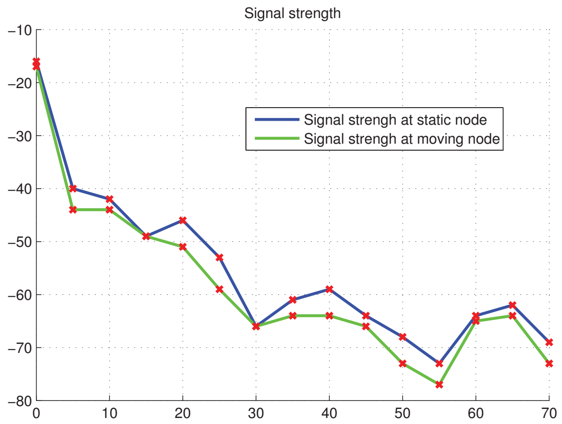

Fig. 4. The indoor link between a static and a moving node.

The measured curves are quite similar to access-point-based Wi-Fi like IEEE 802.11b/g/n and the indoor transmission performance (0 transmission errors at 70m distance and 54Mbps) is sufficient for the described scenario.

B. IEEE 802.11s based nodes inside and around a BMW X3

In Table II the results of the measurement are stated. For each link marked in Figure 3 the signal strength and the link metric is stated.

TABLE II. THE IEEE 802.11S LINK PROPERTIES BETWEEN THE WVI AND A SECOND NODE

Link	Distance [m]	Signal_{WVI} [dBm]	Signal_{Node} [dBm]	Metric_{WVI}	Metric_{Node}
A	7	-61	-63	152	152
B	6	-59	-62	152	152
C	7.5	-58	-69	152	152
D	5.5	-55	-59	152	630
E	1.5	-46	-49	152	152
F	2	-45	-47	152	152

Except for link D the metric still remains constant because no frame errors occurred during the measurement. For link D one frame error occur during our measurements (frame sent to the WVI) and because of that the metric is higher. We also did this measurement with reduced data rate (1Mbps) and got a constant metric value (8193) for all links. So the metric value stays constant but the value is way higher because of the reduced data rate (1Mbps compared to 54Mbps). The shielding properties of the vehicle significantly influence the received signal strength. The distance between the nodes outside the vehicle and the WVI node is just about 5m but the measured signal strength is between -45 and -69dBm. Compared to the results of the indoor measurements this range equals a node distance between 20 and 50m. As presented in Table II the emitted signal strength measured at two nodes located inside a vehicle (links E and F) is quite low compared to the other results (links A-D).

C. Spectral scan inside a BMW X3

In the previous section the shielding properties of a vehicle were measured and explained. The results show that the shielding due to the metal, glass, etc. significantly reduces the signal strength at the receiving node. Additionally, the actuators in a vehicle will create all kinds of interference which will also influence the robustness of wireless update systems operating in the 2.4Ghz band. The following spectral scans shall help to understand how this interference can look like. In Figure 5 the spectral scan of the BMW X3 (Diesel) during the start process (ignition off to engine started) is shown. Some significant peaks can be found in the spectrum. The results of several scans show that these peaks can appear in all channels of the 2.4GHz band.

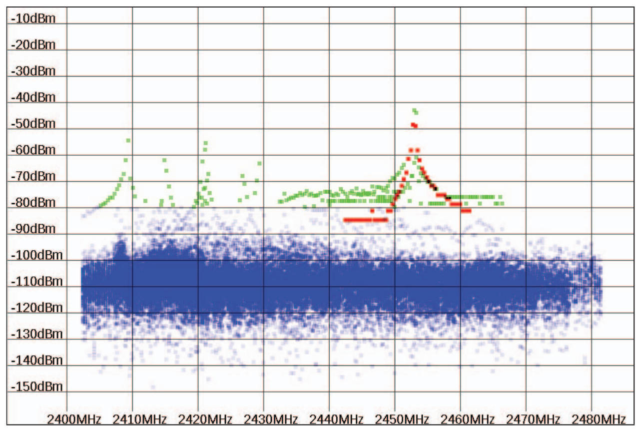

Fig. 5. Starting the engine of our BMW X3 (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

The same kind of peaks can also be found in the scans shown in Figures 6 and 7, where scans of the same BMW with running engine are presented. These scans clearly reveal that interference can appear in all channels of the 2.4GHz frequency band. Although, temporary there are channels without significant interferences (see, e.g., Figure 7: no significant interference between 2460 and 2480MHz).

D. Spectral scan inside a Citroën C-Zero (e-car)

In an electric car quite different actuators may be in use and therefore the occurring interference may also differ. Because of that we decided to create the same kind of spectral scans also for an electric car. In Figure 8 the spectral scan of Citroën C-Zero in parking mode (ignition on but vehicle in standstill) is shown. In the collected frequency spectrum similar peaks can be found but there are more peaks and more interference in general distributed over the whole spectrum.

In the next step we collected spectral data while driving around with the e-car (constant speed, approximately 30km/h) to find out if the interferences are different than in standstill. The results of these measurements are shown in Figures 9 and 10.

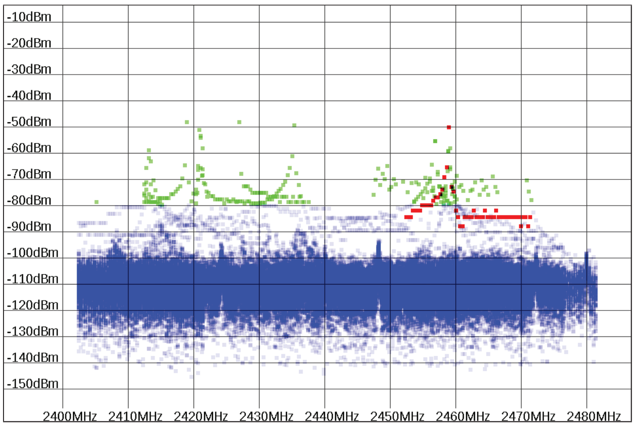

Fig. 6. First spectral scan of the BMW X3 with running engine (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

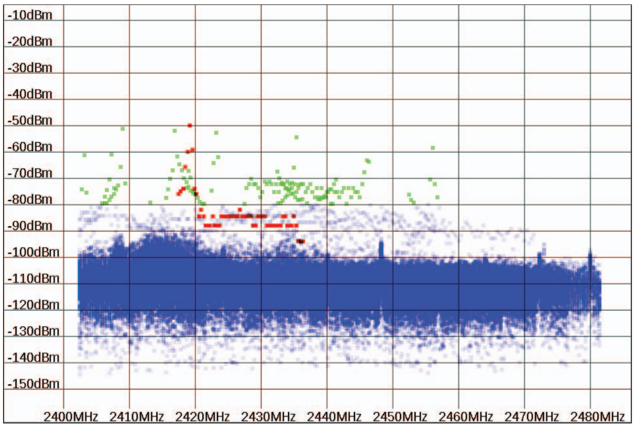

Fig. 7. Second spectral (approximately 1 minute after the first scan) scan of the BMW X3 with running engine (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

The scans show that there is no significant difference between vehicle in standstill and the vehicle driving at constant speed. Compared to the scans of the BMX X3 the frequency spectrum of the e-car contains more samples above the -80dBm limit. Although there are also some regions with less interference (see 2430-2440MHz in Figure 9 and 10).

VII. Conclusions and Future Work

In this paper we described the design and the high-level requirements for an IEEE 802.11s based wireless update system for automotive software. Additionally, a prototype of a wireless vehicle interface (WVI) was presented. Different measurements and an evaluation of an IEEE 802.11s based network in an automotive context was performed, and the result were presented in the previous sections.

Our experimental results clearly show that IEEE 802.11s can be used as the basis technology for a wireless SW update system. Indoor measurements prove that a robust and reliable link between two nodes in a distance of up to 70m can be realized. Shielding properties of vehicles significantly influence the transmission range and the signal strength. However, a reliable IEEE 802.11s based link between the WVI inside the vehicle and a diagnostic device (e.g., a laptop, tablet or

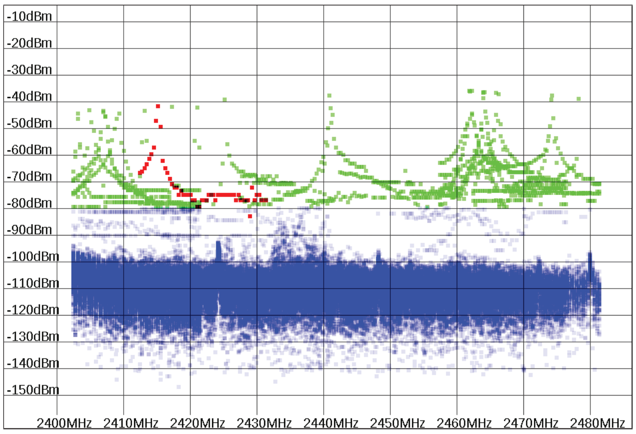

Fig. 8. Citroën with ignition on but in standstill (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

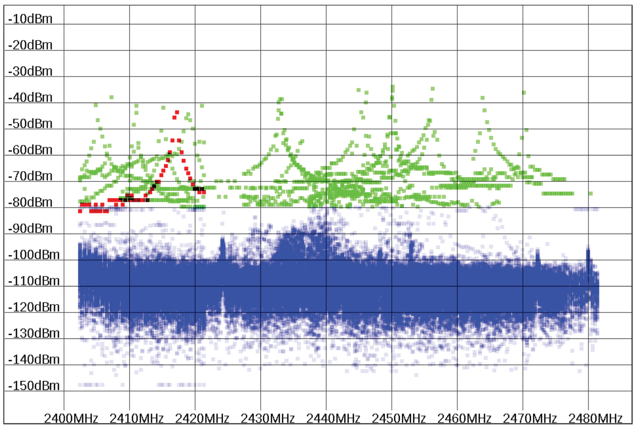

Fig. 9. First scan of Citroën e-car at 30km/h (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

smartphone) or a relay node (nodes outside the vehicle) can be achieved. Based on our experiments, we were able to show that an IEEE 802.11s-based wireless update system can be realized with the components used (mainly the WVI consisting a single-board computer and a Wi-Fi stick). Additionally, we also measured and analyzed the frequency spectrum of a conventional car (BMW X3) and an e-car (Citroën C-Zero). The results show that there is interference in the 2.4GHz band which must be taken into account. Especially for nodes with smaller antennas (e.g., a PCB antenna instead of the rod antenna of the TL-WN722N) these interferences together with the shielding properties of a vehicle can be critical.

In the next step we plan to test such a node with a smaller (PCB) antenna and to evaluate if it still can be used for our purpose. This smaller solution can then be used as plug-in device for wireless updates and diagnostics. Additionally, we will also think about an integrated solution, where the WVI is part of the in-vehicle communication system, thereby being able to use the antenna(s) of the vehicle. The antenna diversity will help to improve the link quality and to avoid attenuation issues. In the next months we will focus on the advancement of the WVI including the implementation of the gateway functionality to forward data received from the wireless update system to the ECU node. A security layer will also be added

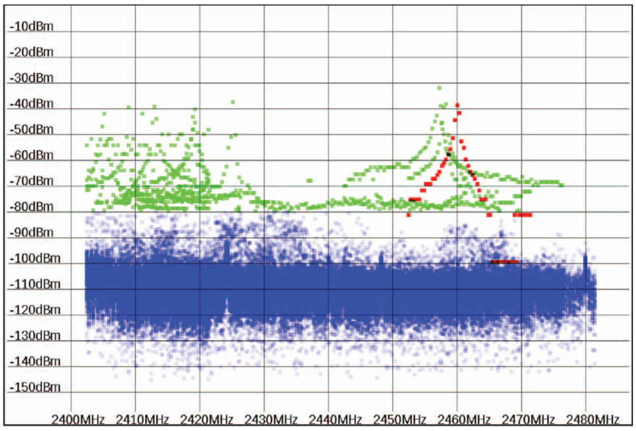

Fig. 10. Second scan (approximately 1 minute after the first scan) of Citroën e-car at 30km/h (blue: samples below -80dBm, green: -80dBm and above, red: one specific sample).

to ensure the integrity of the transferred data as well as the integrity of the vehicle.

Acknowledgments

The research from DEWI project (www.dewi-project.eu) leading to these results has received funding from the ARTEMIS Joint Undertaking under grant agreement n° 621353. The authors acknowledge the financial support of the COMET K2 - Competence Centres for Excellent Technologies Programme of the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), the Austrian Federal Ministry of Science, Research and Economy (BMWFW), the Austrian Research Promotion Agency (FFG), the Province of Styria and the Styrian Business Promotion Agency (SFG).

References

[1] Redbend Software, "Updating Car ECUs Over-The-Air (FOTA)," *White Paper*, p. 14, 2011.

[2] ISO, "Road vehicles Unified diagnostic services (UDS) Specification and requirements," ISO 2006, Tech. Rep., 2006.

[3] J. Noll, I. Garitano, S. Fayyad, E. Åsberg, and H. Abie, "Measurable security, privacy and dependability in smart grids," *Journal of Cyber Security*, vol. 3, pp. 371–398, Apr. 2015.

[4] I. Garitano, S. Fayyad, and J. Noll, "Multi-metrics approach for security, privacy and dependability in embedded systems," *Wireless Personal Communications*, vol. 81, no. 4, pp. 1359–1376, 2015.

[5] ISO, "Road vehicles – Functional safety – Part 1: Vocabulary," ISO, Tech. Rep., 2011.

[6] H. Martin, M. Krammer, B. Winkler, and C. Schwarzl, "Model-based engineering workflow for automotive safety concepts," *SAE 2015 World Congress and Exhibition*, 2015.

[7] M. Karner, M. Krammer, and A. Fuchs, "System level modeling, simulation and verification workflow for safety-critical automotive embedded systems," *SAE 2015 World Congress and Exhibition*, 2014.

[8] M. Krammer, P. Stirgwolt, and H. Martin, "From natural language to semi-formal notation requirements for automotive safety," *SAE 2015 World Congress and Exhibition*, 2015.

[9] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of IEEE 802.15.4 using measurements and simulations," *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, vol. 1, no. c, pp. 487–492, 2006.

[10] F. Mieyeville, W. Du, I. Daikh, and D. Navarro, "Wireless Sensor Networks for active control noise reduction in automotive domain," *2011 The 14th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 1–5, 2011.

[11] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors (Switzerland)*, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[12] I. S. for Information technology, "Local and metropolitan area networks-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY):Wireless Access in Vehicular Environments," IEEE, Tech. Rep., 2010.

[13] T. Flach, N. Mishra, L. Pedrosa, C. Riesz, and R. Govindan, "CarMA: Towards Personalized Automotive Tuning," University of Southern California, Tech. Rep. 11-921, 2011.

[14] D. K. Nilsson and U. E. Larson, "Secure firmware updates over the air in intelligent vehicles," *IEEE International Conference on Communications*, pp. 380–384, 2008.

[15] M. S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger, "Secure automotive on-board protocols: A case of over-the-air firmware updates," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6596 LNCS, pp. 224–238, 2011.

[16] D. Nilsson, L. S. L. Sun, and T. Nakajima, "A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs," *2008 IEEE Globecom Workshops*, pp. 1–5, 2008.

[17] D. Nilsson, P. Phung, and U. E. Larson, "Vehicle ECU classification based on safety-security characteristics," *Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference, IET*, pp. 1–7, 2008.

[18] S. Brown and C. J. Sreenan, "Software updating in wireless sensor networks: A survey and lacunae," *Journal of Sensor and Actuator Networks*, vol. 2, no. 4, pp. 717–760, 2013.

[19] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11s: The WLAN mesh standard," *IEEE Wireless Communications*, pp. 154–160, 2010.

[20] D. T. Tuan, S. Sakata, and N. Komuro, "Priority and admission control for assuring quality of I2V emergency services in VANETs integrated with Wireless LAN Mesh Networks," *ICCE 2012*, pp. 91–96, 2012.

[21] S. Chakraborty and S. Nandi, "IEEE 802.11s mesh backbone for vehicular communication: Fairness and throughput," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2193–2203, 2013.

[22] C. M. D. Viegas, F. Vasques, and P. Portugal, "Evaluating the Impact of Uncontrolled Traffic Sources upon Real-Time Communication in IEEE 802 . 11s Mesh Networks," *Industrial Informatics (INDIN), 2014 12th IEEE International Conference*, p. 4, 2014.

[23] M. A. Ng and K.-l. A. Yau, "An Energy-Efficient Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s Mesh Networks," pp. 17–21, 2013.

[24] M. M. Mhlanga and T. O. Olwal, "Energy Optimization based Path Selection Algorithm for IEEE 802 . 11s Wireless Mesh Networks," no. September, pp. 13–15, 2011.

[25] S. Chen and G. M. Muntean, "E-Mesh: An energy-efficient cross-layer solution for video delivery in wireless mesh networks," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, BMSB*, 2012.

[26] P. Pandey, S. Satish, J. Kuri, and H. Dagale, "Design & implementation of IEEE 802.11s mesh nodes with enhanced features," *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS '09*, pp. 639–644, 2009.

[27] "open80211s – an open-source implementation of the recently ratified ieee 802.11s wireless mesh standard," http://open80211s.org/open80211s/.

[28] M. Cesana, L. Fratta, M. Gerla, E. Giordano, and G. Pau, "C-VET the UCLA campus vehicular testbed: Integration of vanet and mesh networks," *2010 European Wireless Conference, EW 2010*, pp. 689–695, 2010.