Post-print of: M. Tarkowski et al., "Validation of a virtual test environment for C2X communication under radio jamming conditions," 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), Graz, Austria, 2019, pp. 1-5, doi: 10.1109/ICCVE45908.2019.8964938.

Validation of a virtual test environment for C2X communication under radio jamming conditions

Michal Tarkowski, Mateusz Rzymowski, Lukasz Kulas, Krzysztof Nyka, Marcin Borawski, Przemysław Kwapisiewicz, Wojciech Piechowski
Department of Microwave and Antenna Engineering
Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics
Gdansk, Poland

Gerald Temme, Saifullah Khan, Danny Behnecke, Mohamed Mahmod
Institute of Transportation Systems
German Aerospace Center
Braunschweig, Germany

***Abstract*—In this paper, we propose a novel car-2-x communication security testing methodology in the physical layer of wireless systems. The approach is dedicated to automated testing of autonomous vehicles and it is essential for such complex systems operation, especially with regard to safety and security issues. It is based on scenario-driven testing in virtual and real test environments created from collected or simulated data. The presented approach is dedicated for reducing the time and costs of testing and generates a number of potential situations to examine the autonomous system behavior with regard to the wireless communication security. The conducted test results compare some exemplary scenarios, which involve 802.11p C2X communication in presence of intentional interferences, which are realized in different configurations: SiL, HiL and in-field measurements.**

Keywords—wireless communication, C2X, signal interference, jamming attacks, verification and validation, CAD.

I. INTRODUCTION

Automotive industry is considered as one of the most essential industries in Europe. In last decade, different Research and Technological Development (RTD) organizations invested tremendous efforts in the development and demonstration of the Connected and Automated Driving (CAD) systems. A convenient progress has been made in key technologies for innovative CAD functions and applications such as vehicle location and detection system, advance vehicle control system, relative data processing and human-machine interaction etc. However, there are still many challenges which need to be tackled in order to make it promising for social and economic benefits. In this context, C2X communications is one of the important technologies for future road safety that can cope some of the automated driving challenges. The C2X technology provides new possibilities for enhancing active safety and traffic efficiency at a large scale. Utilizing the C2X communication, risky situations are detected and shared with other road users in single or multiple hops. In consequence, the approaching vehicles may react to potentially dangerous situation well in advance and adapt their driving behavior accordingly. Among many possible wireless standards, IEEE 802.11p [1] is the protocol that has been well tested and has been ratified as a standard to provide wireless access in vehicular environment which enables time critical safety applications at very low data transmission delay. In this context, the European Commission has allocated 30 MHz spectrum (5.875–5.905 GHz) of three channels with 10 MHz each are assigned exclusively for safety related communication [2].

One of the most critical and challenging aspects related to the C2X testing is the communication security. The growing number of cars that are able to communicate to each other increases the risk of potential interferences between them [3] The other problem is related to the intentional attacks (e.g. jamming attacks) on the communication link. Due to the technological development and considerable reduction of cost, the sophisticated software defined radio (SDR) platforms that could be used for eventual attacks on C2X radio links are available for amateur users. Although, the cars are equipped with different sensors that increase their awareness, the affected communication link may influence the safety-related decision undertaken by a reasoning system. This brings up a need to extend existing verification and validation methods for automotive systems with analysis of the physical layer of wireless communication links including interferences, possible jamming attacks and propagation-related problems.

Before their deployment for public use, all CAD systems, including C2X communication, have to show their safety and reliability. This means testing mechanisms and processes for independent licensing authorities have to be developed and defined. On one side, these mechanisms and processes have to be sophisticated enough to cover every necessary sufficiently complex test case with acceptable accuracy and granularity. On the other side, they also have to be feasible and usable. Therefore, some kind of automation in testing for modern driving systems is required. This necessarily leads to the simulation of traffic scenarios and the question how to digitally validate driving systems in order to obtain the quality control needed for autonomous driving systems to be approvable for public use.

Such digital validation has a couple of advantages: it speeds up the development and validation process, it enables a more thorough quality inspection and quality control possibility and improves financial efficiency of the whole process, from development to verification by appropriate licensing authority and maintaining the systems through its life-cycle. An example of such financial efficiency improvement is incorporation of simulations performed in earlier stages of model development. This enables early detection of software errors and therefore reduces costs spent on testing. However, currently the interchangeability of real proving ground tests and simulations are still under research. It is not defined what tests can be made virtually and what tests have to be done by real test drivers. Furthermore, the standards for this virtual

validation are still under development and are not yet streamlined into an operational toolchain.

In this paper, a novel approach for verification and validation of the car-to-x communication link has been proposed. The physical link analysis between the car and relevant infrastructure in presence of a jamming signal has been performed with a dedicated simulation tool called PhyWiSe Tool and proved in real environment experiments. To this end, the physical layer of 802.11p standard has been implemented and investigated. The unique architecture of the proposed approach allows for interchangeable use of software (simulated) and hardware (commercial) modules. The proposed tool has built-in self-contained test scenario controller as well as a convenient API to be utilized in a co-simulator environment (such as Model.CONNECT™[1]). To verify the effectiveness and reliability of the proposed approach, real measurements were collected and replicated in the tool. The communication between the crossroad controller and the approaching vehicle was examined under different jamming conditions. Measurement and simulation results were compared and additional applications (e.g. data augmentation) were demonstrated.

II. PROPOSED APPROACH

Testing methods relying on validation and verification are a popular approach that is used extensively in automotive domain [4]. Although, the method is very popular in testing software, it has also been successfully extended to model- (MiL), software- (SiL) and hardware-in-the-loop (HiL) testing [5], which is illustrated in fig. 1, and has also been recently chosen to cover CAD systems testing [6].

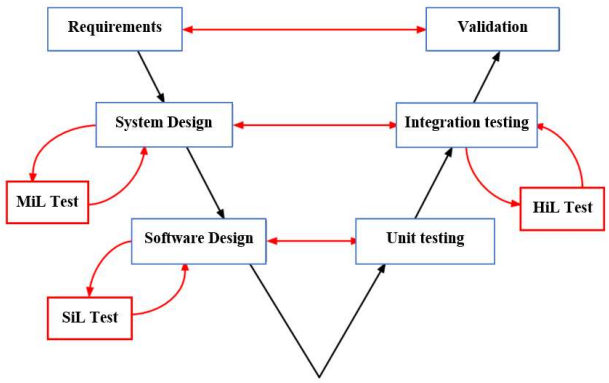

Fig. 1. Simplified illustration of V&V testing methodology.

In order to simulate the real-world scenarios one has to develop a fully virtual counterpart of a communication link. This nontrivial task has led to development of the test framework for validation and verification of wireless communication - Physical layer Wireless Security Tool (PhyWise Tool). The emphasis was put on the physical layer of wireless systems, because of its importance in the investigation of interferences and jamming influence on link quality. PhyWiSe Tool was created and developed in ENABLE-S3 project within a European consortium for automotive, aerospace and maritime domains[2]. The tool allows for performing tests of different communication systems in two main modes: hardware-in-loop (HiL) and software-in-loop (SiL). It was crucial to maintain consistency between those two methods in order to allow for combining blocks from hardware and software domain in a single simulation/verification tool.

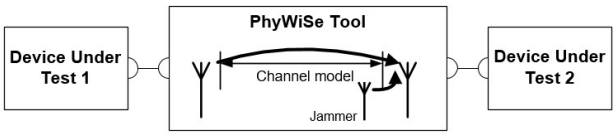

Fig. 2. HiL mode configuration of PhyWiSe Tool

HiL operation mode in PhyWiSe Tool (fig. 2) is used for testing the real RF equipment like off-the-shelf radio transceivers, sensors, modems, microcomputers with wireless cards, etc. In this mode, PhyWiSe Tool acts as a middle-box between two parties to alter RF signals that are sent between them to mimic particular programmed upfront conditions including antennas, signal propagation effects and external interferences (like jamming). Devices can be connected using convenient RF connectors, which are connected to antennas in real deployments. The core of PhyWiSe Tool in this setup is a software-defined radio (SDR) unit with fast field-programmable gate array (FPGA) realizing baseband signal processing. Dealing with real RF signals imposes frequency limitations depending on SDR properties.

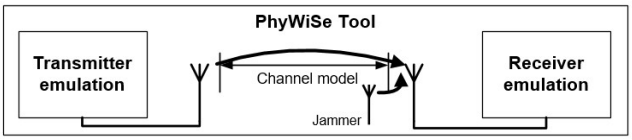

Fig. 3. SiL mode configuration of PhyWiSe Tool

In SiL operation mode (fig. 3), every component is realized by a software block in the digital domain. It allows for running the simulation without specialized equipment and without a physical device under test. Test scenarios with a simple channel models can be executed faster than using hardware. Software emulations of the real devices have to be implemented according to their specifications, hence PhyWiSe Tool includes transmitter and receiver models for IEEE 802.11p [7][8] standard. Such implementation has a form of software LabVIEW module. It supports all bit rates specified by the IEEE standard and includes all required signal processing stages, including OFDM modulation, Viterbi decoder, bit interleaving and scrambling. An OFDM symbol consists of 4 pilot subcarriers and 48 data subcarriers. Single data subcarrier can be modulated by 1 to 6 bits of data, which corresponds to BPSK, QPSK, 16QAM, 32QAM and 64QAM modulation. Variable rate forward error correction provides some degree of immunity to transmission impairment. As all the calculations are taking place in the digital domain, signals frequency is taken into account only with simulation of propagation effects.

[1] See: https://www.avl.com/-/model-connect-

[2] See: https://www.enable-s3.eu/

In the simplest model for free-space propagation, the communication link budget model is based on Friis transmission formula [9]:

$$P_r = P_t + D_t + D_r + 20\log_{10}\frac{\lambda}{4\pi d},$$

where P_r – is power delivered at a receiver's terminal, P_t – power from a transmitter to an isotropic antenna, D_t, D_r – transmitter's and receiver's antenna gain respectively, λ – signal's wavelength, d – distance between transmitter and receiver. Communication analysis is performed from the receiver's point of view for two signal paths: transmitter-receiver and jammer-receiver being added at the receiver's terminal. Additional components, like additive noise or more realistic channel models, can be implemented for better accuracy. In SiL mode all processing is performed on a host computer, and in HiL mode FPGA unit is used for this task. PhyWiSe Tool takes into account the directional patterns of the antennas as well.

Beside a transmitter and receiver, PhyWiSe Tool introduces a third party – radio jammer. It is in fact an additional transmitter aimed at disrupting the communication between the former two. The jammer signals can realize some statistical distributions in the particular bandwidth or can have unique properties to impair a specific modulation or standard. It can simulate the ongoing transmission following a legitimate protocol too. It allows for wide variety of experiments showing test system behaviour under various unexpected conditions. Currently, 16 different jammer types are implemented in the tool.

Because PhyWiSe Tool works specifically in physical layer, no higher-level error correction mechanisms were implemented. Therefore, to evaluate the communication quality in a presence of jamming signal the Packet Loss Ratio (PLR) is calculated. This metric is commonly used to measure network reliability and can be obtained conveniently in both real-world measures and the simulation especially when the number of transmitted packets is known beforehand. Despite its limitations it can be successfully applied when packet size and data rate are constant [10].

III. Experimental scenario

A. In-field verification

For optimization and verification of the jamming model, an experiment on a test field was conducted to collect reference jamming data. The experimental setup was based on Enable-S3's Use Case 2 "Autonomous left turn on intersection" in which the DLR as UC leader has been involved. Therefore, the DLR test field was used. In this setup, an autonomous cyber physical system (ACPS) drives towards an intersection. The ACPS detects oncoming vehicles via LiDAR and receives additional information about oncoming vehicles from an infrastructure sensor pole equipped with cameras via C2X. Based on the received information, the ACPS decides how to turn left and controls the autonomous left turning on the intersection. Fig. 4 depicts the arrangement of the setup on the test field. The test site provides a typical four-leg intersection and is located at a traffic training area in the North of Brunswick.

The functional setup of the experiment is presented in Fig. 5. The sensor pole was placed at the beginning of an s-curve and is even able to detect oncoming vehicles inside the s-curve around the corner. The sensor pole is placed in such a way that there is still a direct line-of-sight connection toward the incoming ACPS vehicles from the western leg of the intersection. For the collection of jamming data, a C2X jammer provided by Gdansk University of Technology (GUT) was installed in the test field. The jammer was located in such a way that the jamming signal affects the C2X communication between the sensor pole and ACPS in the area before the intersection. Accordingly, the data about obstacles sent from the sensor pole become less accurate in the most important functionality of the ACPS for planning the turning behaviour. In case of perfectly effective jamming the ACPS will lose its more forward looking obstacle information's from the pole completely and has to plan the left turn based on its internal LiDAR sensors.

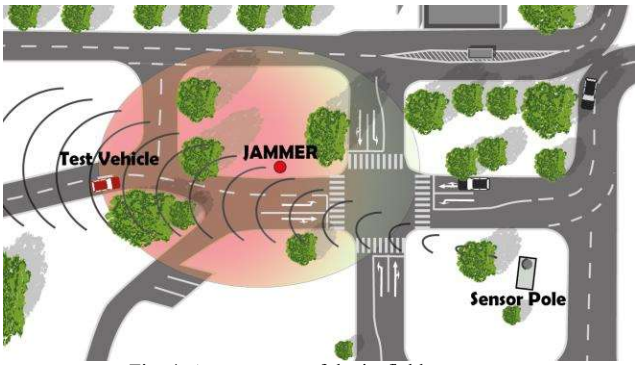

Fig. 4. Arrangement of the in-field test setup

To conduct the tests, NEC Linkbird-MX was equipped on each side which is a custom-built unit for vehicular communications [11]. The operating frequency for these Dedicated Short Range Communication (DSRC) devices was set to 5.9GHz (CH 180) and IEEE 802.11p standard was implemented. The data rate is set to 100 packets per second and the transmission power on both sides i.e. transmitter and receiver is set to 21dBm for all the tests. The omni-directional antennas were mounted on both sides i.e. Mobile Mark ECO12-5900 on the sender side and Mobile Mark SMW-305 on the receiver side. With GPS receiver added to each Linkbird-MX the units have also built-in beacon functionality. The tests were based on 16 trials and throughout different parameters are recorded such as Received Signal Strength (RSSI), Packet Loss Ratio (PLR) and locations on the receiver side. C2X Jamming device was designed especially for in-field tests and consists of a dedicated application running on a single-chip Intel NUC microcomputer connected to the NI USRP-2922 Software Defined Radio (SDR) by an Ethernet cable with 1Gb/s throughput. The jamming device can be remotely controlled by a tablet that is connected via wireless network to the microcomputer to facilitate the tests. The purpose of the jamming device is to transmit the signals in a 10MHz band that disturbs the communication in the IEEE 802.11p standard. The device is able to transmit various signals in 5.9GHz frequency band. The particular signal used during the measurements aims at disrupting 48 subcarriers that are summed into one signal. It is possible to adjust the gain and SNR level of the waveform. The phase of each subcarrier is

randomly selected in a range of 0-90 degree. Distance between subcarriers is 0,15625MHz.

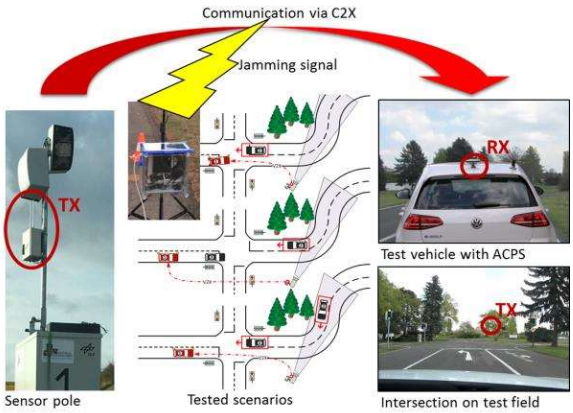

Fig. 5. Functional scheme of the experimental setup

B. *Test representation in simulator*

In order to reproduce the real-world tests, PhyWiSe Tool was setup in software-in-loop (SiL) mode, so the whole test has taken place in the virtual domain. The transmitter and corresponding receiver were configured to support IEEE 802.11p physical layer at 10 MSa/s sample rate but bit rate was 6 Mb/s with 2 bits per OFDM subcarrier and coding rate is 1/2. The jamming transmitter was configured to emit the signal that disrupts data subcarriers. The applied propagation channel model consists of free-space path loss (FSPL) model and statistical Average White Gaussian Noise (AWGN) added at the receiver. The noise level was experimentally determined at -69 dBm. The antennas' gain was set according to the manufacturer specification: $D_r = 5\ dBi$ for the receiver and $D_t = 12\ dBi$ for the transmitter.

During the simulation, the position of the vehicle was updated each second according to the GPS data acquired during the measurements and the path-loss was recalculated respectively. At the same time information about the amount of correctly received packets since last update was sent to PhyWiSe for PLR calculation. The transmitter was sending packets at 100 packets per second with power set to 21 dBm, which is the same as during the real measurements.

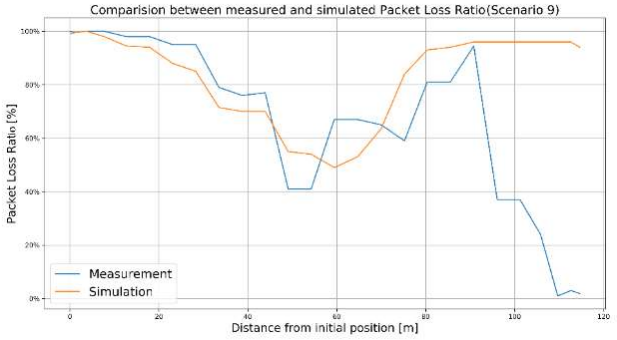

Fig. 6. Comparison between measured and simulated Packet Loss Ratio

IV. TEST RESULTS

Among 16 of examined scenarios, three of them were found corrupted due to GPS acquisition failure. The rest of them were used for test replication PhyWiSe Tool. In Fig. 6, a comparison of measured and simulated Packet Loss Ratio is presented in scenario #9 (jamming transmitter output power level at 15 dB). As can be seen, the scenario reproduction in PhyWiSe Tool captured the loss of signal due to distance and disturbances introduced allegedly by signal jamming. In Fig. 7, measured and simulated Packet Loss Ratio was depicted in a terrain map. The latter was moved down for a better visibility. The vehicle's movement was marked by the black line. C2X jammer and the transmitter (sender) positions were depicted by red and blue markers, respectively. The empirical cumulative distribution function of absolute error of the Packet Loss Ratio was presented in Fig. 8. The comparison comprises 362 samples examined and mean simulation error stands at 21.4 percent points with standard deviation at 26.8 percent points. Less than 50% of analysed samples exceed 8 percent points error.

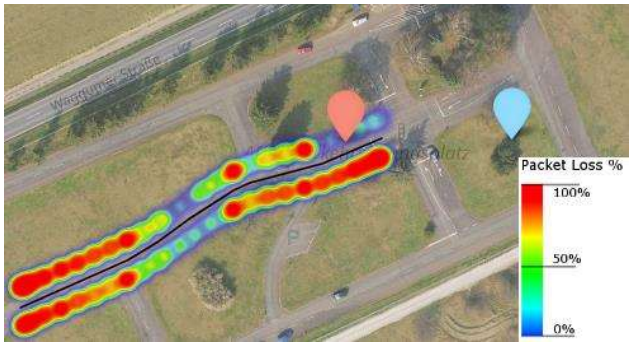

Fig. 7. Comparison of measured and simulated Packet Loss Ratio presented in a terrain map (see detailed explanation in text)

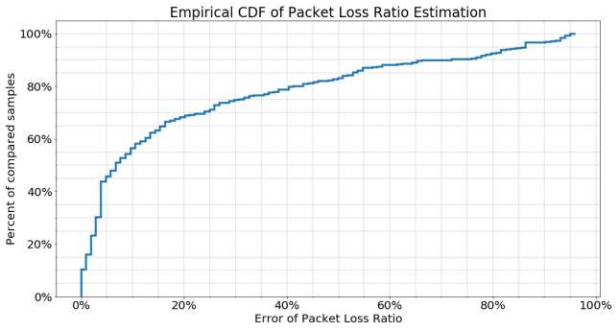

Fig. 8. CDF of absolute error of the Packet Loss Ratio

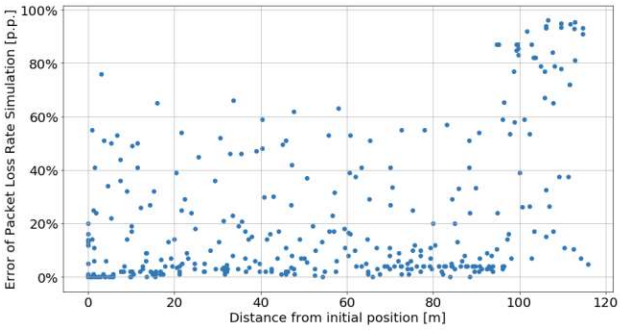

Fig. 9. Error distribution in the function distance from the initial position

It was observed that the highest error comes from samples very close to the jammer. In Fig. 9., an analysis of error distribution against the distance from the initial position (the further position, the closer to the jammer) was presented. This effect most probably comes from lack of antennas' vertical radiation pattern calculation in the simulation, as there were differences in height between transmitter, receiver and

jammer in real-world set-up. In close proximity, the influence of non-isotropic elevation characteristic is getting emphasised and effectively reduce interference signal. From the application point of view this kind of error is irrelevant because the most critical analysis applies to further distance from interference source. However, this behaviour would require more elaboration in the future.

V. CONCLUSION

A novel approach for reliable virtual testing of the C2X communication has been proposed. It is based on extended V&V approach where SiL and HiL operation modes are available. The full 802.11p communication link has been realized within the virtual environment and its operation quality in presence of interfering signal has been examined with regard to the real autonomous driving scenario. The simulated results are comparable with the corresponding in-field experimental results. The research proved that reliable virtual testing of wireless communication under jamming conditions is feasible and the inconsistences can be reduced by implementation of more accurate propagation channel model in future. A proper definition of the communication system components (e.g. antennas, transmitters, receivers etc.) models is required due to its impact on the estimation accuracy.

ACKNOWLEDGMENTS

This work has been conducted within the ENABLE-S3 and SCOTT projects that have received funding from the ECSEL Joint Undertaking under Grant Agreement no. 692455 and Grant Agreement no. 737422. This Joint Undertaking receives support from the European Union's HORIZON 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Sweden, Norway. This work was also partially supported by Polish Ministry of Science and Higher Education grant for statutory activities at Faculty of ETI, Gdansk University of Technology.

REFERENCES

[1] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments

[2] CEPT ECC, ECC Decision (08)01,The harmonised use of the 5875-5925 MHz frequency band for Intelligent Transport Systems (ITS) , approved 14 March 2008, Amended 3 July 2015

[3] P. Papadimitratos, G. Calandriello, J. Hubaux and A. Lioy, "Impact of vehicular communications security on transportation safety," IEEE INFOCOM Workshops 2008, Phoenix, AZ, 2008, pp. 1-6.

[4] "Postionspapier Hochautomatisierte Systeme - Testen, Safety und Entwicklungsprozesse," Peter Heidl, Werner Damm (Hrsg.), 2017. [Online]. Available: http://www.safetrans-de.org/de/Aktivitaeten/Roadmapping.php.

[5] V. Levardy, M. Hoppe, and E. Honour, Verification, Validation & Testing Strategy and Planning Procedure, Proceedings of the 14th Annual International Symposium of INCOSE, Jun. 2004.

[6] S. Moten, F. Celiberti, M. Grottoli, A. van der Heide, and Y. Lemmens, X-in-the-loop advanced driving simulation platform for the design, development, testing and validation of ADAS, IEEE Intelligent Vehicle Symposium, 2018

[7] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," VTC Spring 2008 - IEEE Vehicular Technology Conference, Singapore, 2008, pp. 2036-2040.

[8] IEEE Standard for 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," in IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) , vol., no., pp.1-2793, 29 March 2012

[9] H. T. Friis, "A Note on a Simple Transmission Formula," in Proceedings of the IRE, vol. 34, no. 5, pp. 254-256, May 1946.

[10] A. Vlavianos, L. K. Law, I. Broustis, S. V. Krishnamurthy and M. Faloutsos, "Assessing link quality in IEEE 802.11 Wireless Networks: Which is the right metric?," 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes, 2008, pp. 1-6.

[11] A. Festag, R. Baldessari, W. Zhang, L. Le, A. Sarma, and M. Fukukawa, "CAR-2-X communication for safety and infotainment in Europe,"NEC Technical Journal, vol. 3, no. 1, 2008