VEHICULAR 2016

The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications

ISBN: 978-1-61208-515-9

November 13 - 17, 2016

Barcelona, Spain

VEHICULAR 2016 Editors

Markus Ullmann, Bundesamt für Sicherheit in der Informationstechnik (BSI) - Bonn, Germany

Khalil El-Khatib, University of Ontario Institute of Technology, Canada

VEHICULAR 2016

Foreword

The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2016), held between November 13-17, 2016 - Barcelona, Spain, continued the inaugural event considering the state-of-the-art technologies for information dissemination in vehicle-to-vehicle and vehicle-to-infrastructure and focusing on advances in vehicular systems, technologies and applications.

Mobility brought new dimensions to communication and networking systems, making possible new applications and services in vehicular systems. Wireless networking and communication between vehicles and with infrastructure have specific characteristics from other conventional wireless networking systems and applications (rapidly-changing topology, specific road direction of vehicle movements, etc.). These led to specific constraints and optimizations techniques; for example, power efficiency is not as important for vehicle communications as it is for traditional ad hoc networking. Additionally, vehicle applications demand strict communications performance requirements that are not present in conventional wireless networks. Services can range from time-critical safety services, traffic management, to infotainment and local advertising services. They are introducing critical and subliminal information. Subliminally delivered information, unobtrusive techniques for driver's state detection, and mitigation or regulation interfaces enlarge the spectrum of challenges in vehicular systems.

We take here the opportunity to warmly thank all the members of the VEHICULAR 2016 Technical Program Committee, as well as the numerous reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to VEHICULAR 2016. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the VEHICULAR 2016 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that VEHICULAR 2016 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of vehicular systems, technologies and applications.

We are convinced that the participants found the event useful and communications very open. We also hope the attendees enjoyed the charm of Barcelona, Spain.

VEHICULAR 2016 Chairs:

VEHICULAR Advisory Committee

Sriram Chellappan, Missouri University of Science and Technology, USA
João Dias, Universidade de Aveiro, Portugal
Carl James Debono, University of Malta - Msida, Malta
Johan Lukkien, Eindhoven University of Technology, The Netherlands
Matthias Uwe Pätzold, University of Agder - Grimstad, Norway
Tapani Ristaniemi, University of Jyväskylä, Finland
Hwangjun Song, POSTECH (Pohang Univ of Science and Technology) - Pohang, Korea
Kevin Daimi, University of Detroit Mercy, USA

VEHICULAR Industry/Research Chairs

Alexandre Bouard, BMW Forschung und Technik GmbH, Germany
Daniel Jiang, Mercedes-Benz Research & Development North America, USA
Peter Knapik, Volkswagen AG, Germany
An He, Qualcomm, USA
Khelifa Hettak, Industry Canada / Communications Research Centre - Nepean, Canada
Wenjing Wang, Blue Coat Systems, Inc., USA

VEHICULAR Publicity Chairs

Sangmi Moon, Chonnam National University, South Korea

VEHICULAR 2016

Committee

VEHICULAR Advisory Committee

Sriram Chellappan, Missouri University of Science and Technology, USA
João Dias, Universidade de Aveiro, Portugal
Carl James Debono, University of Malta - Msida, Malta
Johan Lukkien, Eindhoven University of Technology, The Netherlands
Matthias Uwe Pätzold, University of Agder - Grimstad, Norway
Tapani Ristaniemi, University of Jyväskylä, Finland
Hwangjun Song, POSTECH (Pohang Univ of Science and Technology) - Pohang, Korea
Kevin Daimi, University of Detroit Mercy, USA

VEHICULAR Industry/Research Chairs

Alexandre Bouard, BMW Forschung und Technik GmbH, Germany
Daniel Jiang, Mercedes-Benz Research & Development North America, USA
Peter Knapik, Volkswagen AG, Germany
An He, Qualcomm, USA
Khelifa Hettak, Industry Canada / Communications Research Centre - Nepean, Canada
Wenjing Wang, Blue Coat Systems, Inc., USA

VEHICULAR Publicity Chairs

Sangmi Moon, Chonnam National University, South Korea

VEHICULAR 2016 Technical Program Committee

Taimoor Abbas, Volvo Car Corporation, Sweden
Aydin Akan, Istanbul University, Turkey
Waleed Alasmary, University of Toronto, Canada
Marica Amadeo, University of Reggio Calabria, Italy
Andrea Baiocchi, SAPIENZA University of Rome, Italy
Irina Balan, Ghent University - IBBT, Belgium
Gaurav Bansal, Toyota InfoTechnology Center, USA
Michel Basset, Université de Haute Alsace, France
Melike Baykal-Gursoy, Rutgers University, USA
Monique Becker, Institut Mines Telecom, France
Luis Bernardo, Universidade Nova of Lisboa, Portugal
Yuanguo Bi, Northeastern University, China
Sebastian Bittl, Fraunhofer ESK Munich, Germany
Pascal Bodin, Orange Labs, France
Mélanie Bouroche, Trinity College Dublin, Ireland

Carlo Vallati, University of Pisa, Italy
Rens W. van der Heijden, Institute of Distributed Systems - University of Ulm, Germany
Wantanee Viriyasitavat, Mahidol University, Thailand
Ljubo Vlacic, Griffith University, Australia
Wenjing Wang, Blue Coat Systems, Inc., USA
You-Chiun Wang, National Sun Yat-Sen University, Taiwan
Chih-Yu Wen, National Chung Hsing University - Taichung, Taiwan
Yue Wu, Shanghai Jiaotong University, China
Weidong Xiang, University of Michigan - Dearborn, USA
Jinyao Yan, Communication University of China, China
Zheng Yan, Aalto University - Espoo, Finland / Xidian University Xi'an, China
Wei Yuan, Huazhong University of Science and Technology - Wuhan, China
Peng Zhang, Xi`An University of Posts and Telecommunications (XUPT), China
Wensheng Zhang, Iowa State University, USA
Zhangbing Zhou, China University of Geosciences - Beijing, China & TELECOM SudParis, France
Haojin Zhu, Shanghai Jiao Tong University, China
Yanmin Zhu, Shanghai Jiao Tong University, China

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

The Problem of Comparable GNSS Results – An Approach for a Uniform Dataset with Low-Cost and Reference Data

Pierre Reisdorf, Tim Pfeifer, *Julia Breßler, Sven Bauer, Peter Weissig, Sven Lange, Gerd Wanielik, Peter Protzel

Technische Universität Chemnitz
Reichenhainer Str. 70, 09126, Chemnitz, Germany
Email: firstname.lastname@etit.tu-chemnitz.de, *julia.bressler@wirtschaft.tu-chemnitz.de

***Abstract*—Localization and navigation are two key factors for our globalized world. Driven by cost-effective end-user devices, position estimation using Global Navigation Satellite Systems (GNSS) is common sense. Using the pseudorange measurements as input, many research groups developed their own approaches for estimating position information and evaluated it in simulation or real-world scenarios. Surprisingly, a common publicly available dataset for comparing such algorithms against each other has not been established. We pursue the idea of a uniform, free to use dataset collected by a low-cost receiver in conjunction with associated reference data originating from a high-precision device. For creating representative datasets, we chose four challenging scenarios within two different cities with various influences of urban canyons and surroundings. Based on this, we present first preliminary results from our Factor Graph approach. Our datasets are associated with the smartLoc project and are available online at: www.mytuc.org/GNSS**

Keywords–GNSS; Low-cost Sensor; NLOS; Reference Data; Urban Canyon

I. INTRODUCTION

Localization around the globe and in real time with satellites is a big accelerator to a globalized traffic and trade. The technique behind is called Global Navigation Satellite System (GNSS). In more detail, different satellite systems like the North American Global Positioning System (GPS), the Russian Glonass, the European Galileo or the Chinese BeiDou could be used for the localization process already. All these global systems and other local systems, like the Japanese QZSS (to mention just one), enable a fast localization under an open sky. However, satellite navigation is based on the transmission of electronic waves with its typical characteristics and drawbacks. That is, if we have a limited view to the sky, the localization process is faulty. Well-known examples are places in the proximity of high buildings or with dense and high vegetation. Hence, the localization process in urban scenarios was addressed by many research activities. Within urban areas, Non-line-of-sight (NLOS) and multipath are the largest challenges for an accurate and available position fix.

Existing research activities (see Table I) encounter these challenges in different ways with various approaches. All these activities base on simulated or real world data in static or dynamic scenarios [1]. Unfortunately, a major restriction of all published and founded work is the incomparability of the results. Thus, all existing works are only comparable with itself. It should be noted that the reasons for this fact could be diverse. That starts with additional sensors like cameras, light detection and ranging (LiDAR), radio detection and ranging (Radar), etc., special prepared maps with different content and ends with cooperative approaches to improve the position quality. To cover all the various approaches is impossible with one dataset. All approaches in context of GNSS use calculated position fixes or raw measurements (more known as pseudoranges) delivered by a receiver. At this point, we would like to publish a common dataset in typical scenarios, which addresses the mentioned challenges. We provide within this paper complete datasets with low-cost GNSS data, reference GNSS data, associated broadcasted ephemeris data, as well as ego motion data like yaw-rate and velocity. These datasets enable the user to calculate a position fix, compare with the reference data and fuse the data with ego motion output.

This paper is categorized in four main parts. After a brief introduction in the field of GNSS and a motivation to the question—*Why do we need a uniform dataset for GNSS data?*—a short state of the art overview regarding available datasets is shown. In the subsequent section, the methodology is introduced in detail. The following section presents the output data and explains each data type. In Section VI, we present first results from the project smartLoc [2]. The paper will end with a conclusion as well as an outlook. After all, the license terms for the given datasets will end the paper.

II. MOTIVATION

A major challenge of GNSS based systems in urban environments are NLOS measurements. These result from reflections of the received signals, which especially can occur in narrow streets between tall buildings, so-called urban canyons. Figure 1 shows such an urban canyon with the negative effects on the availability of satellites. For a better understanding of the challenges in the scene at hand, we added a sky plot (left side) with GPS (green) and Glonass (red) showing the reduced availability of satellites (in ideal view 16 satellites).

The common Kalman filter-based approach to fuse the measured pseudoranges uses a Gaussian distributed noise as error model. Through the geometrical elongation case of NLOS measurements, this error model becomes invalid, which leads to a large distortion of the position estimator. To prevent these distortions, the common filter approach has to be replaced with an algorithm that is better suited for non-Gaussian errors. For the simultaneous localization and mapping (SLAM) problem in robotics, a variety of robust optimization back-ends have been proposed in the recent past [3]–[10]. These back-ends can be applied to solve generic estimation problems like in GNSS

 ISBN: 978-1-61208-515-9

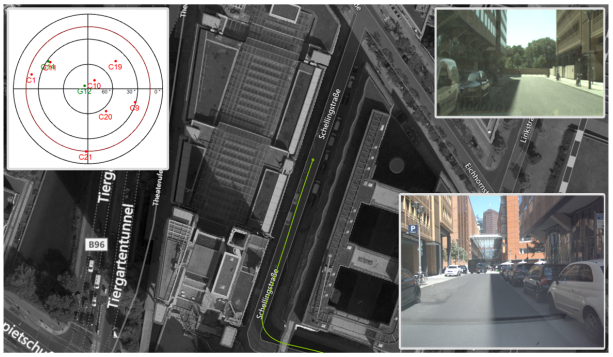


Figure 1. Birds eye view of an urban canyon including a front and rear view example (right side) from the scenario *Potsdamer Platz* in Berlin.

TABLE I. NUMBER OF PUBLICATIONS GROUPED BY ITS DATASET CHRACTERISTIC BASED ON [1]

Real Data collection	**Static measurement**	**Dynamic measurement**
Via vehicle	7	19
Via person	2	4
(No information)	11	—
Simulation	**Static measurement**	**Dynamic measurement**
Via vehicle	1	6
Via person	—	—
(No information)	4	

if they are formulated as factor graphs, a kind of Bayesian network. While for SLAM scenarios, multiple comparisons of robust graph optimization approaches like [11] and [12] exist, there are none for GNSS-related applications. For this reason, our first comparison in [13] was limited to synthetic data, but already showed the potential of this class of algorithms. To create a first foundation for a comparison under real world conditions, we decided to share the required data in form of a public available dataset, because none of the examined datasets (see Table I) fulfilled all our requirements in terms of surroundings and the necessary measurement data.

III. STATE OF THE ART

In science, it is necessary to compare various results against each other or to have a same base to build comparable conclusions. In the field of vision systems like training sets for different classifiers, there are serious datasets. For vision systems exist some databases, e.g., the Daimler Database for pedestrians [14] or the Nordland dataset [15] from a drive in a train over different seasons. In the field of mobile robotics, specifically SLAM, many real and synthetic datasets exist, like the well-known dataset of the Intel Research Lab. The spirit of providing datasets for competing algorithms is present in the community and online resources like [16], [17] or [18] provide collections of datasets and sometimes specific benchmarks for scoring results or more generic evaluations. Other datasets contain data about Naturalistic Driving Studies (NDS) from the project UDRIVE [19] and Strategic Highway Research Program 2 [20]. Another well-known source in the field of autonomous driving, including datasets and benchmarks, is the *Kitti Vision Benchmark Suite* [21] with focus on stereo processing, optical flow, visual odometry, object and lane detection and tracking. Still others focus on semantic understanding of urban street scenes like Cityscapes Dataset [22], different kind of published data from the INRIA Grenoble Rhône-Alpes team [23] or synthetic images of urban scenes [24]. The focus of all these datasets are different from a dataset addressed for the GNSS field (raw measurements and reference data). In our view the conditions of a uniform dataset are:

- Low-cost GNSS position
- Smoothed Reference GNSS position
- Odometry data (yaw-rate and velocity)
- Ephemeris data

Some datasets contain localization information, but neither includes precise data as well as low-cost data. The focus of the majority of the introduced datasets are vision systems. At this point, we would like to fill the gap with real data from urban scenarios including low-cost GNSS data and an associated reference data.

IV. METHODOLOGY

In this section, we describe in detail all conditions to the data recording procedure used to create the four proposed datasets located in Frankfurt/Main and Berlin. Ground-truth information is generated in post-processing mode, as described later on. It is based on the high-precision reference system's measurements.

A. Precondition on Data

After the taxonomy of the multipath/NLOS problem by [25] there are some preconditions to the kind of data. Different approaches use external map data as an additional sensor. Other approaches use *Quality parameters* like Signal-noise-ratio, Doppler frequency or Carrier phase. Still others use additional sensors like camera, laser or radar for data fusion approaches. No dataset is able to cover all possible setups. Hence, we focus on a good selection of the measurement tracks, where data for buildings and environments are available. For Berlin, there is public data in the project *Berlin 3D* [26] available. For the city of Frankfurt am Main, the *Stadtvermessungsamt* [27] published some inner city data. Likewise, the open project osm-3D [28] provides city data, but for many cities. The above mentioned quality parameters are supported by our low-cost receiver. They are included within our data accordingly. However, as the current work has its focus on GNSS-based position estimation, we neglect camera data for now, even if we have recorded some. The dataset is recorded with our test vehicle Carai1, which will be described later on.

B. Measurement Tracks

Based on the aspects detailed above, we examined possible environments suiting our demands for a challenging dataset. Especially, we focused on Urban Canyons, where NLOS and multipath are present to a large extend. Looking for a suitable route, we first extracted the cities, which have a large amount of high-rise buildings. Thus, we identified the cities of Frankfurt/Main and Berlin. We designed our test tracks to lie preferably within areas with high-rise and densely populated buildings as well as narrow streets. Naturally, these properties are met more or less during one scenario. An overview of all four scenarios with its tracks is given in Figure 4.

Within the city of Berlin, we located one track around the *Potsdamer Platz* (Scenario 1). It has a length of about 1.6 km

 ISBN: 978-1-61208-515-9

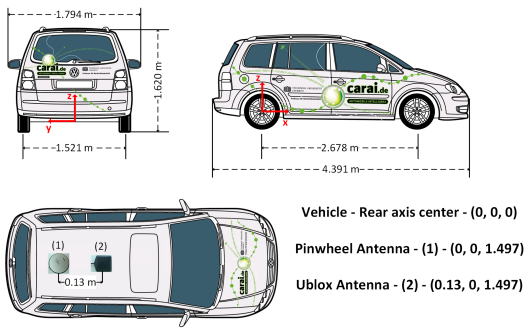


Figure 2. Schematic view in all dimensions of our test vehicle Carai1.

and is accompanied with 70 m to 100 m high buildings (Forum Tower, Kollhoff Tower, etc.). The road width varies between 13 m to 17 m and according to the approach in Sec. IV-F, we got 49 % NLOS measurements. The example view of an *Urban Canyon* in Fig. 1 originates from this scenario. The second track within Berlin is centered around the Friedrichstrasse and is referred to as *Gendarmenmarkt* (Scenario 2). The track is roughly 5 km long and includes 13 blocks. The streets are framed by 20 m to 60 m high buildings and the road width is about 20 m to 23 m. Here we have an NLOS ratio of about 37 %.

Within the city Frankfurt am Main, the first track is referred to as *Main Tower* (Scenario 3), which includes the highest tower of Germany. Here, the Urban Canyon is characterized by 110 m to 259 m high buildings. The route is about 3 km long with 46 % NLOS measurements. The second track within Frankfurt is called *Westend Tower* (Scenario 4), which includes three high-rise buildings (208 m, 200 m, 142 m). The track is measured to 2.3 km and the road width varies between 10 m to 70 m while the NLOS ratio is about 32 %.

C. Sensor Setup

We use both a high-cost GNSS sensor (for reference or ground truth position) and a low-cost GNSS sensor for localization. Additionally, we recorded odometry data (yaw-rate and velocity) from the test vehicle Carai1 [29]. The low-cost data can be divided in two categories. On the one hand side calculated position fixes and on the other hand side raw measurements. We get the reference position as a calculated position fix from the NovAtel sensor. Table II describes the sensors, which were used during the recording process. All GNSS sensors are market products without any adaption from our side.

TABLE II. SENSORS FOR RECORDING

Sensor	*Description*
1) Low-cost GNSS sensor	u-blox EVK-M8T (u-blox M8 GNSS Evaluation Kit *Precision Timing*) with ANN-MS antenna
2) Reference GNSS sensor	NovAtel SPAN Differential (Model CDJRPRT-TNS2) GPS, GLO, BeiDou with RTK and IGM-S1 Inertial Measurement Unit (IMU) and Pinwheel-Antenna (Model GPS-703-GGG [30])
3) Odometry	For obtaining ego motion data over the CAN gateway.
4) Carai1	One of our three test vehicle equipped with different sensors [29]. This test vehicle is a VW Touran.

The positions of the antennas on top of the roof of our test vehicle Carai1 [29] are shown in Figure 2. The figure illustrates the schematic view of all antennas. The Pinwheel antenna is mounted 1.497 m above the origin of the vehicle coordinate system. The centers of antenna one and antenna two are on the same height. All units in this figure are in meter. By virtue of a firmware update of the u-blox sensor during the both measurement campaigns, we have a different availability of satellite systems in the scenarios. Table III shows the different constellation for each scenario in Berlin and Frankfurt.

TABLE III. SATELLITE SYSTEMS IN SCENARIOS AT GLANCE

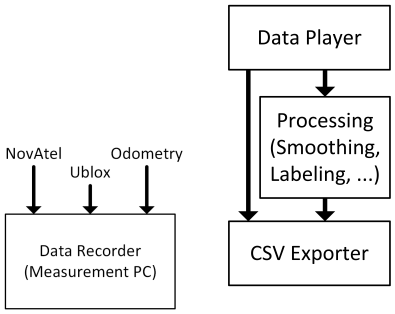
Satellite system	*GPS*	*GLO*	*GAL*
Potsdamer Platz	x	x	
Gendarmenmarkt	x	x	
Main Tower	x	x	x
Westend Tower	x	x	x

D. Procedure of Sensor Data

Our software base for recording, processing and analysis of the data are the system development framework vADASdeveloper by Vector [31] and the sensor fusion development library BASELABS Create [32]. We divide our procedure to handle and processing the data in three steps. Figure 3 illustrates these three steps, which are necessary to get a complete comparable dataset.

1) Record real data during a measurement campaign
2) Post processing the data for generating of ground truth
3) Generation of export data

Step one consists of both recording the data and check the data for consistency of the desired recording setup. Step two contains the processing of all data and create a ground truth for each position related data to export. The last step generates the export data in form of different *Character Separated File (CSV)* files.



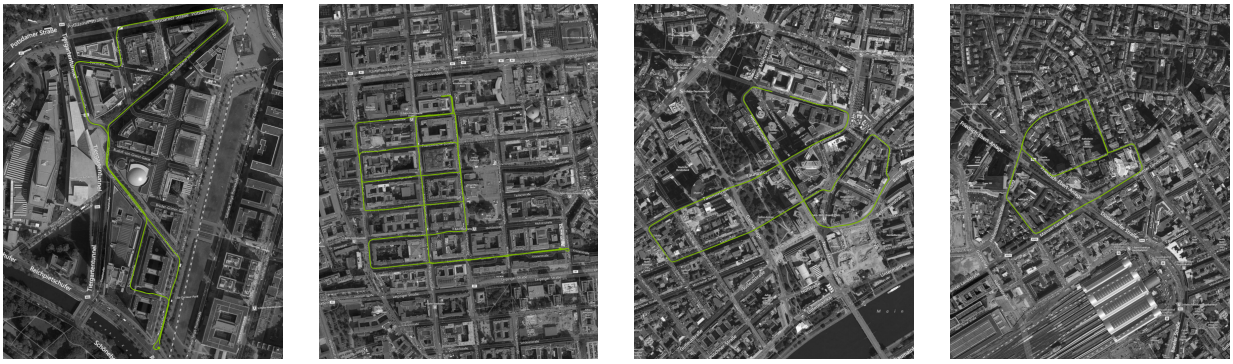
(a) Recording (b) Post processing and export

Figure 3. Schematic representation of the procedure for recording, post processing and generation of export data.

Which messages from the sensors did we recorded? Table IV gives an overview about the messages with the associated frequency for each sensor. For more details, take a look into the manuals of the sensor (u-blox [33] and [34], NovAtel without IMU [35] and with IMU [36]). The log type indicates the type of a messages, continuous or when a new message available. The messages BestPos and BestVel from NovAtel can used for the generation of ground truth and is also a part of the exported data.

A worldwide common coordinate system for localization is the World Geodetic System 1984 (WGS 84). A definition

 ISBN: 978-1-61208-515-9



(a) Berlin 1 - Potsdamer Platz (b) Berlin 2 - Gendarmenmarkt (c) Frankfurt 1 - Main Tower (d) Frankfurt 2 - Westend Tower

Figure 4. Aerial view of the selected scenarios. We chose two different tracks (visualized as green line) in the city of Berlin and Frankfurt am Main (Germany). They are representative examples for a so called *Urban Canyon*.

TABLE IV. DATA FROM SENSORS

Sensor	*Data type*	*Log type*	*Frequency (Hz)*
Low-cost GNSS sensor	NAV-POSLLH	Sync	5
	RXM-RAWX	Sync	5
High-cost GNSS sensor	BESTPOS	Sync	20
	BESTVEL	Sync	20
Odometry	YAWRATE	Sync	50
	VELOCITY	Sync	50

of the WGS 84 system is done by the National Imagery and Mapping Agency [37] or in the *Global Positioning System Standard Positioning Service Signal Specification* [38]. This coordinate system can be called as the standard coordinate system and all our position information refer to it.

E. Parameters for Data

This section includes some explanations and details about the exported data. In detail, some hints about the time format, the ground truth format as well as both ephemeris data formats for GPS and Glonass.

GPS time: The first and second column of each exported data file describe the GPS time. This time is the measurement time on the sensor side. The GPS time is divided into the GPS week (first column) and the GPS seconds of week (second column). More explanations to GPS time in section V-C.

Ground truth: The base of our provided ground truth is BestPos message from NovAtel sensor [35] and odometry data (velocity and yaw-rate). Hence, the coordinate system is WGS 84 in the format of Longitude, Latitude and Height (above mean sea level) too. In subsection V-C there are more details and explanations about the ground truth.

Ephemeris data: For a complete set of data, we use the ephemeris data from the German Research Centre for Geosciences (GFZ) [39], which provide data to the Multi-GNSS EXperiment (MGEX) of the International GNSS Service (IGS). This service provides orbit data in the Extended Standard Product 3 Orbit Format (SP3) for the most common satellite systems in Europe. SP3 format is a standard format in GNSS field and gives a fast access to this data without any special adaptions.

F. Label for LOS/NLOS

The NovAtel receiver is also able to provide raw measurement (pseudorange) information like the u-blox receiver. The u-blox receiver provide information about all received satellite signals. The NovAtel receiver seems to exclude some satellites in harsh environments, which might be affected by NLOS. NovAtel used for receiving a Pinwheel antenna and internally different algorithms. Hence, we use this information to build a NLOS detection based on different satellites availabilities in both receivers. Therefore, we remember the last received set of satellites from NovAtel and time of data. When we receive in next step a set of satellites from u-blox, we compare the availability of each satellite and time span since the last update from the NovAtel. If the time span is too high or the satellite was never seen before, the pseudorange measurement or satellite marked as NLOS. In the other case, the measurement marked as LOS. This approach gives a hint for the type of LOS or NLOS of a given measurement and we export this information to complete the datasets.

V. OUTPUT OF DATA

This section describes in the first part the structure of the data and gives some comments for a fast implementation of an importer for the data. The second part explains in more detail the creation of the ground truth data, which is the base for a comparison of each algorithm based on the low-cost data.

A. Structure of Exports

There are six message types, which are exported in separate files. The name of the messages and the log type as well as the frequency are described in Table IV. Additionally, the SP3 file is provided by the GFZ and we add this to our exports. All exports have the same structure and the delimiter used in the CSV-files are semicolons. Each line starts with the measurement GPS time of the sensor, followed by the structure described in the data manuals. Additionally, the exports for the messages NAV-POSLLH and RXM-RAWX have information about the ground truth included – more details are described in Section V-C. That means, the structure of both file types follows this structure:

NAV-POSLLH and RXM-RAWX: GPSWeek; GPSSeconds; GTLongitude; GTLongitude Cov; GTLatitude; GTLatitude Cov; GTHeight; GTHeight Cov; GTHeading; GTHeading Cov;

 ISBN: 978-1-61208-515-9

GTAcceleration; GTAcceleration Cov; GTVelocity; GTVelocity Cov; GTYawRate; GTYawRate Cov; next entries followed by manual for each message... GT means in this context ground truth.

Other exports: GPSWeek; GPSSeconds; next entries followed by manual for each message...

One full export of a scenario consists of the following data files (same order like in Table IV):

1) NAV-POSLLH.csv
   A Geodetic Position Solution calculated by the low-cost receiver.
2) RXM-RAWX.csv
   Multi-GNSS raw measurements for GPS and Glonass from the low-cost receiver.
3) YAWRATE.csv
   Yaw-rate data from the ego motion sensor of the test vehicle Carai1.
4) VELOCITY.csv
   Velocity data from the ego motion sensor of the test vehicle Carai1.
5) SP3 file
   Includes the post-processed ephemeris data for all relevant satellite systems.
6) BESTPOS.csv and BESTVEL.csv
   The BestPos is the raw ground truth message from the reference system. We use this message for our smoothing process to build the post-processed ground truth. The BestVel includes best available velocity data from the reference system.

All datasets are published under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 license on the project website of smartLoc – http://mytuc.org/GNSS. A complete package of each message types for all scenarios is available there.

B. Challenges of selected scenarios

As described in section IV-B, we have decided us for urban scenarios with harsh environments for satellite reception. The challenges are the ever changing satellite availabilities. To get a better understanding of NLOS influence in urban areas, we chose the fourth scenario (Westend Tower) to show some details. In Figure 5, two diagrams are shown to visualize the challenge within this urban canyon. The lower diagram shows the theoretically possible number of satellites currently visible in relation to the satellites classified as NLOS. Accordingly, the upper diagram shows the NovAtel receiver's estimated standard deviation. It is easy to see, that if the number of NLOS measurements is increasing, the estimated accuracy is decreasing in consequence. Indeed, we have situations with less than four LOS satellites. Thus, the IMU supports the reference system to stabilize the localization. This is important to note and restricts the quality of the assumed ground truth originating from the receivers BestPos messages. Later on, we describe how to support the ground truth by post-processing it with a smoother and additional odometry information. All other recorded scenarios show the same effects between NLOS and standard deviation of the reference system.

C. Merge all Data - Smoothing

During the measurement campaigns multiple sensors were used. In detail, the sensor output of a u-blox EVK-M8T low-cost GNSS receiver, a NovAtel INS SPAN reference GNSS system and the vehicle's odometry has been recorded. As the sensors are not synchronized, we have to align them first to a common timescale, before using them as input to our smoothing algorithm.

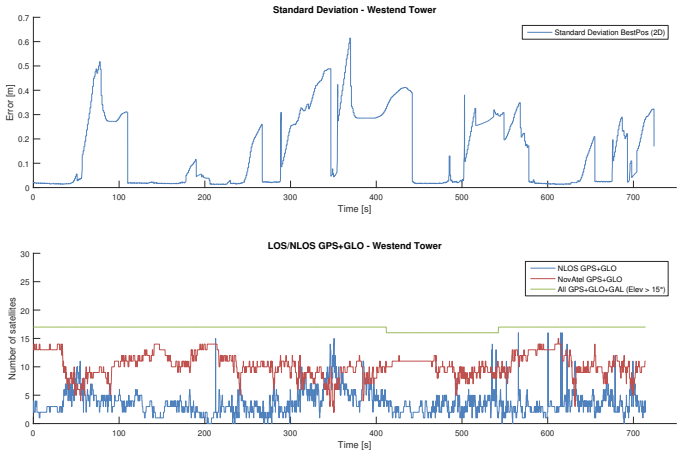


Figure 5. Influence of satellite numbers and NLOS to standard deviation of BestPos message from reference system. The number of NLOS was created after the strategy described in section IV-F. Both diagrams show the Frankfurt Westend Tower scenario.

The given system timestamp of each measurement denotes the time of arrival according to the computer's system clock. The NovAtel and u-blox measurements also include the actual time of measurement in GPS time. As the computer clock is quite unstable in general and the timestamping is also influenced by variable delays due to the operating system's thread scheduling, the time of arrival jitters a lot. To get the highest quality ground truth, the data fusion has been performed using GPS time as the reference. As the vehicles odometry sensor lacks a GPS timestamp, it has been estimated as follows:

- Estimate the relation between NovAtels GPS time of measurement and time of arrival.
- Estimate the relation between an idealized odometry time of measurement and time of arrival.
- Combine the two relations to transform the idealized time of measurement to GPS time.
- Correct the time offset to account for different processing delays.

In the first step the NovAtels GPS time of measurement was compared to the time of arrival, estimating the bias and drift between both clocks using a first order polynomial curve fit.

Following this, a stable internal clock that triggers odometry measurements every $20\,\mathrm{ms}$ was assumed for the odometry sensor. An idealized hardware timestamp was computed for each odometry measurement as the product of the measurements successive number and this period time. This hardware timestamp was then related to the time of arrival the same way as the NovAtels GPS time before. This yielded the bias and drift between the idealized measurement time and the computers system time.

Combining these two relations allowed then the computation of the odometries apparent period time within the GPS timescale and its time offset, so suitable GPS timestamps could be derived.

 ISBN: 978-1-61208-515-9

At last, the time offset needed to be adjusted as the previous steps implicitly assumed that both sensors have the same time delay between taking the measurement and applying the system timestamp. An optimizer was used to tune the time offset minimizing the average error between the odometries and NovAtels velocity measurements. As a second optimization parameter, the odometries velocity scaling error was determined too. This scaling error is caused by a changed wheel diameter due to tire wear in respect to the wheel diameter that the revolution counter assumes.

Finally, a Rauch-Tung-Striebel smoothing filter is applied, which uses an unscented Kalman filter in a two-way-smoothing fashion. It used a constant turn-rate and acceleration (CTRA) motion model to estimate the vehicle movement. This motion model was chosen as it is one of the most advanced curvilinear motion models commonly used for vehicle state estimation. Further improvements – like the constant curvature and acceleration model (CCA) – offer only minor benefits but lead to fresnel integrals requiring numerical approximations increasing the implementation complexity and computational cost. More commonly, even simpler motion models like a constant turn-rate and velocity (CTRV) or even constant velocity (CV) are used. As their respective state spaces are subsets of the CTRA state space, smoothing using the CTRA model creates a ground truth that allows the evaluation of those as well.

TABLE V. PROCESS NOISE PARAMETERS USED BY THE CTRA MODEL BASED FILTERS

Parameter	*Value*
Angular acceleration	0.2 rad/s
Jerk	2.0 m/s^3
Altitude acceleration	0.04 m/s^2
Yaw-rate bias drift	0.0001 rad/s

A comparison of the mentioned motion models including their basic state space definitions and state transition equations can be found in [40]. Extending this, the CTRA model has been augmented to use 3D coordinates. While the original horizontal position estimation was left unchanged, the positions Z component was added as well as an additional altitude velocity to model the altitude assuming a constant climb rate. To optimally include the odometry measurements, the scaling error that had been estimated by the optimizer during the time synchronization process is applied within the odometry velocity measurement model. The odometry yaw-rate bias, however, was estimated online by the filter assuming it to be constant. The used noise parameters for the resulting process model are shown in Table V. The angular acceleration and jerk being noises for the otherwise constant turn-rate and acceleration, the altitude acceleration for the constant altitude velocity and drift for the estimated yaw-rate bias.

VI. FACTOR GRAPH OPTIMIZATION

In the following section we want to give an example of the result of state-of-the-art algorithms with the provided dataset. For the estimation of a trajectory based on a set of pseudo-ranges, a sensor fusion algorithm has to be applied. Similar to our former benchmark [13], we use a factor graph as graphical representation of a non-linear least squares minimization problem. In its general topology the same graph as proposed in [41] is used, including atmospheric (Ionosphere and Troposphere) and satellite clock corrections. The robust

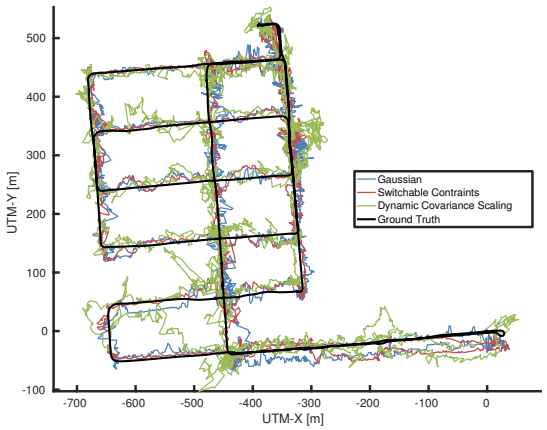


Figure 6. Resulting trajectory of an online factor graph optimization with the GTSAM library for the Berlin Gendarmenmarkt dataset.

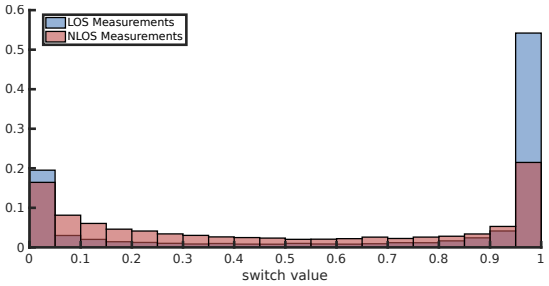


Figure 7. Normalized distribution of the switch variables of the switchable constraints algorithm for the Berlin Gendarmenmarkt dataset. These weights should be 1 for LOS measurements an 0 for NLOS, if the algorithms works perfect.

algorithms Switchable Constraints (SC) [3] and Dynamic Covariance Scaling (DCS) [4] were implemented within the GTSAM framework [42] and solved online with the provided iSAM2 algorithm [43]. For further algorithmic details, we refer to our earlier descriptions in [13] or the original papers of each algorithm. A constant position model is used to avoid the more complex handling of the odometry, which has a different measurement rate than the satellite system.

The estimated trajectory of the Berlin Gendarmenmarkt data stream at Figure 6 shows the strong distortion that is most likely caused by NLOS Observations. Table VI summarizes the 2-dimensional UTM-X/Y position error for all data streams. This error can be described as the Euclidean distance between the estimated position and the ground truth. Similar to our former comparison at high NLOS ratios, the DCS algorithm shows bad results. The high NLOS amount over 30% in combination with the lack of odometry could be the reason for the insufficient performance of this algorithm. Especially with the missing odometry and the simplified motion model, there is no possibility to set the new initial position values different from the previous ones. Such a suboptimal initialization can be a problem for robust algorithms, like shown in [44] or [45].

Switchable Constraints on the other side is able to improve the position estimate over the results of the pure Gaussian factor graph. Nevertheless, is the improvement smaller than we would expect based on our former work. To investigate the problem of the SC algorithm, we visualized the switch values, a kind of continuous weights for each measurement, with Figure

 ISBN: 978-1-61208-515-9

TABLE VI. RESULT OF THE FACTOR GRAPH BASED POSITION ESTIMATION

	Gaussian			Switchable Constraints			Dynamic Covariance Scaling		
	Absolute Position Error [m]								
Dataset	mean	median	max	mean	median	max	mean	median	max
Berlin Potsdamer Platz	23.70	21.16	72.24	25.11	19.89	78.17	32.92	25.05	111.4
Berlin Gendarmenmarkt	17.04	15.86	62.90	15.32	13.06	54.21	22.84	19.26	118.5
Frankfurt Main Tower	19.68	12.74	158.1	18.02	10.32	137.9	61.95	29.50	763.1
Frankfurt Westend Tower	16.10	11.86	105.2	14.57	10.43	90.41	32.30	11.68	284.0

7. A perfect distribution would show all LOS values on the right side around 1 and all NLOS values around 0 at the left. Although the NLOS values are more on the left side than the LOS one, the histogram is far from ideal. So, a high amount of NLOS pseudoranges is included in the optimization process, which explains the results. However, for final conclusions about the performance of robust algorithms on these datasets there is still a lot to do.

VII. CONCLUSION & OUTLOOK

Challenging datasets for the evaluation and application of GNSS based position estimation algorithms have been presented in this work. The selected tracks cover ordinary situations typically encountered in urban environments, such as limited satellite visibility, uncounted reflections and satellite signal outages caused by buildings. As our aim is the reusability of our dataset for the evaluation of competing algorithms within the GNSS field, we gave detailed information about our experimental setup as well as an analysis of our datasets including a description of the provided file types.

The included results of a factor graph based position estimation provide a first baseline to compare future implementations. For further improvements, the online estimation of the underlying error distribution seems to be an important next step. With a good representation of this distribution, we will be able to apply other robust sensor fusion algorithms like Max-Mixture [9] or generalized iSAM [46]. Also, we have to invest more efforts to characterize the error distribution of this dataset and the differences to our previous synthetic test.

Another point is the handling of information inside the datasets. Currently, some expert knowledge is needed for extracting the satellite positions from the SP3 file or to estimate different errors, e.g., ionospheric or tropospheric delays, which influence the accuracy of the ego position result. The extension of our datasets for such information facilitate the access to the information inside the dataset.

Within varying published work, some approaches use camera information for NLOS detection [47], traffic sign recognition for additionally landmarks [48] or lane mark recognition to stabilize the localization [49], to address just some examples. Due to publishing camera information, the dataset could be more interesting for variety of other approaches using camera information.

ACKNOWLEDGMENT

This evaluation was done as part of the smartLoc project, which is funded by the "Bundesministerium für Wirtschaft und Energie" (German Federal Ministry for Economic Affairs and Energy). For this evaluation and generation of ground truth data, precise real-time corrections provided by the AXIO-NET service (www.axio-net.eu) were used.

REFERENCES

[1] J. Breßler, P. Reisdorf, M. Obst, and G. Wanielik, "Gnss positioning in non-line-of-sight context - a survey," 2016, manuscript submitted for publication at 19th International IEEE Conference on Intelligent Transportation Systems (ITSC).

[2] Retrieved: Sept. 2016. [Online]. Available: https://www.smartLoc.eu/

[3] N. Sünderhauf, "Robust optimization for simultaneous localization and mapping," Ph.D. dissertation, Technischen Universität Chemnitz, 2012.

[4] P. Agarwal, G. D. Tipaldi, L. Spinello, C. Stachniss, and W. Burgard, "Robust map optimization using dynamic covariance scaling," in Proc. of Intl. Conf. on Robotics and Automation (ICRA), 2013, pp. 62 – 69.

[5] P. Agarwal, G. Grisetti, G. Diego Tipaldi, L. Spinello, W. Burgard, and C. Stachniss, "Experimental analysis of dynamic covariance scaling for robust map optimization under bad initial estimates," in Proc. of Intl. Conf. on Robotics and Automation (ICRA), 2014, pp. 3626 – 3631.

[6] P. Agarwal, "Robust graph-based localization and mapping," Ph.D. dissertation, PhD thesis, University of Freiburg, Germany, 2015.

[7] Y. Latif, C. Cadena, and J. Neira, "Robust loop closing over time for pose graph slam," The International Journal of Robotics Research, vol. 32, no. 14, 2013.

[8] G. H. Lee, F. Fraundorfer, and M. Pollefeys, "Robust pose-graph loop-closures with expectation-maximization," in Proc. of Intl. Conf. on Intelligent Robots and Systems (IROS), 2013, pp. 556 – 563.

[9] E. Olson and P. Agarwal, "Inference on networks of mixtures for robust robot mapping," The International Journal of Robotics Research, vol. 32, no. 7, 2013, pp. 826–840.

[10] D. M. Rosen, M. Kaess, and J. J. Leonard, "Robust incremental online inference over sparse factor graphs: Beyond the gaussian case," in Proc. of Intl. Conf. on Robotics and Automation (ICRA), 2013, pp. 1025 – 1032.

[11] N. Sünderhauf and P. Protzel, "Switchable constraints vs. max-mixture models vs. rrr – a comparison of three approaches to robust pose graph slam," in Proc. of Intl. Conf. on Robotics and Automation (ICRA), 2013, pp. 5198 – 5203.

[12] Y. Latif, C. Cadena, and J. Neira, "Robust graph SLAM back-ends: A comparative analysis," in Proc. of Intl. Conf. on Intelligent Robots and Systems (IROS), 2014, pp. 2683 – 2690.

[13] T. Pfeifer, P. Weissig, S. Lange, and P. Protzel, "Robust factor graph optimization – a comparison for sensor fusion applications," in Proc. of Intl. Conf. on Emerging Technologies and Factory Automation (ETFA), 2016.

[14] Retrieved: Sept. 2016. [Online]. Available: http://www.gavrila.net/Datasets/datasets.html

[15] Retrieved: Sept. 2016. [Online]. Available: http://www.nrkbeta.no/2013/01/15/nordlandsbanen-minute-by-minute-season-by-season/

[16] Retrieved: Sept. 2016. [Online]. Available: http://radish.sourceforge.net

[17] S. Ceriani, G. Fontana, A. Giusti, D. Marzorati, M. Matteucci, D. Migliore, D. Rizzi, D. G. Sorrenti, and P. Taddei, "Rawseeds ground truth collection systems for indoor self-localization and mapping," Autonomous Robots, vol. 27, no. 4, 2009, pp. 353–371.

[18] Retrieved: Sept. 2016. [Online]. Available: http://projects.asl.ethz.ch/datasets

[19] Retrieved: Sept. 2016. [Online]. Available: http://www.udrive.eu/

[20] Retrieved: Sept. 2016. [Online]. Available: https://insight.shrp2nds.us/

[21] Retrieved: Sept. 2016. [Online]. Available: http://www.cvlibs.net/datasets/kitti/

[22] Retrieved: Sept. 2016. [Online]. Available: https://www.cityscapes-dataset.com/

 ISBN: 978-1-61208-515-9

[23] Retrieved: Sept. 2016. [Online]. Available: http://lear.inrialpes.fr/data

[24] G. Ros, L. Sellart, J. Materzynska, D. Vazquez, and A. Lopez, "The synthia dataset: A large collection of synthetic images for semantic segmentation of urban scenes," in IEEE Conference on Computer Vision and Pattern Recognition, 2016.

[25] M. Obst, "Bayesian Approach for Reliable GNSS-based Vehicle Localization in Urban Areas," Ph.D. dissertation, Technische Universität Chemnitz, 2015.

[26] Retrieved: Sept. 2016. [Online]. Available: http://www.businesslocationcenter.de/en/downloadportal

[27] Retrieved: Sept. 2016. [Online]. Available: https://www.frankfurt.de/sixcms/detail.php?id=3027

[28] Retrieved: Sept. 2016. [Online]. Available: http://www.osm-3d.org/

[29] R. Schubert, E. Richter, N. Mattern, P. Lindner, and G. Wanielik, Advanced Microsystems for Automotive Applications 2010 - Smart Systems for Green Cars and Safe Mobility. Springer, 2010, ch. A Concept Vehicle for Rapid Prototyping of Advanced Driver Assistance Systems, pp. 211 – 219.

[30] GPS-703-GGG and GPS-703-GGG-N User Guide, 4th ed., NovAtel, April 2014.

[31] Retrieved: Sept. 2016. [Online]. Available: http://www.vector.com/vi_vadasdeveloper_en.html

[32] Retrieved: Sept. 2016. [Online]. Available: https://www.baselabs.de/data-fusion-algorithm-design/

[33] U-blox 6 Receiver Description, GPS.G6-SW-10018-F ed., u-blox, April 2013.

[34] U-blox 8 / u-blox M8; Receiver Description; Including Protocol Specification, R10 (111670) ed., u-blox, February 2016.

[35] OEM6 Family of Receivers - Firmware Reference Manual, 9th ed., NovAtel, March 2016.

[36] SPAN® on OEM6® Firmware Reference Manual, 7th ed., NovAtel, January 2015.

[37] National Imagery and Mapping Agency, "Department of Defense World Geodetic System 1984: its definition and relationships with local geodetic systems," National Imagery and Mapping Agency, St. Louis, MO, USA, Tech. Rep. TR8350.2, January 2000. [Online]. Available: http://earth-info.nga.mil/GandG/publications/tr8350.2/tr8350_2.html

[38] Global Positioning System Standard Positioning Service Signal Specification, 2nd ed., United States Coast Guard Navigation Center, Juni 1995. [Online]. Available: http://www.navcen.uscg.gov/pubs/gps/sigspec/gpssps1.pdf

[39] M. Uhlemann, G. Gendt, M. Ramatschi, and Z. Deng, GFZ Global Multi-GNSS Network and Data Processing Results. Cham: Springer International Publishing, 2016, pp. 673–679. [Online]. Available: http://dx.doi.org/10.1007/1345_2015_120

[40] R. Schubert, E. Richter, and G. Wanielik, "Comparison and evaluation of advanced motion models for vehicle tracking," in Information Fusion, 2008 11th International Conference on, June 2008, pp. 1–6.

[41] N. Sünderhauf, M. Obst, S. Lange, G. Wanielik, and P. Protzel, "Switchable constraints and incremental smoothing for online mitigation of non-line-of-sight and multipath effects," in Proc. of Intelligent Vehicles Symposium (IV), 2013.

[42] Retrieved: Sept. 2016. [Online]. Available: https://collab.cc.gatech.edu/borg/gtsam

[43] M. Kaess, H. Johannsson, R. Roberts, V. Ila, J. J. Leonard, and F. Dellaert, "isam2: Incremental smoothing and mapping using the Bayes tree," Intl. Journal of Robotics Research, vol. 31, no. 2, Dec. 2012, pp. 216–235.

[44] D. M. Rosen, C. DuHadway, and J. J. Leonard, "A convex relaxation for approximate global optimization in simultaneous localization and mapping," in 2015 IEEE International Conference on Robotics and Automation (ICRA), May 2015, pp. 5822–5829.

[45] J. Wang and E. Olson, "Robust pose graph optimization using stochastic gradient descent," in 2014 IEEE International Conference on Robotics and Automation (ICRA), May 2014, pp. 4284–4289.

[46] D. M. Rosen and J. J. Leonard, "Nonparametric Density Estimation for Learning Noise Distributions in Mobile Robotics," in Workshop on Robust and Multimodal Inference in Factor Graphs, ICRA, 2013.

[47] P. D. Groves, Z. Jiang, M. Rudi, and P. Strode, "A Portfolio Approach to NLOS and Multipath Mitigation in Dense Urban Areas," in Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2013), 2013, pp. 3231 – 3247.

[48] A. Welzel, P. Reisdorf, and G. Wanielik, "Improving urban vehicle localization with traffic sign recognition," in 2015 IEEE 18th International Conference on Intelligent Transportation Systems, Sept 2015, pp. 2728–2732.

[49] N. Mattern, M. Obst, R. Schubert, and G. Wanielik, "Simulative analysis of accuracy demands of co-operative localization in the COVEL project," in Intelligent Vehicles Symposium (IV), 2011 IEEE, June 2011, pp. 516 – 521.

 ISBN: 978-1-61208-515-9

Sensor Calibration and Registration for Mobile Manipulators

Steven Legowik
Robotic Research, LLC
Gaithersburg, MD , USA
email: legowik@roboticresearch.com

Roger Bostelman[1,2] and Tsai Hong[1]
[1]Intelligent Systems Division
National Institute of Standards and Technology
Gaithersburg, MD, USA
[2]IEM, Le2i, Université de Bourgogne,
Dijon, France
email: roger.bostelman@nist.gov and tsai.hong@nist.gov

***Abstract*—This paper describes the methods used to register a mobile manipulator to a workstation to perform assembly tasks. The nonlinear, least square model of the system is formulated and Ceres Solver is used to compute the position of the robot arm relative to the mobile base. The use of non-contact fiducials to test the accuracy and repeatability of the mobile manipulator positioning in the context of an assembly operation is also discussed. Using mathematical methods and indirect measurements it is possible to compute the offset between physical components of the system where direct measurement is not feasible.**

Keywords- robot; AGV; mobile manipulator; collaborative robotics; registration; Ceres Solver; calibration.

I. INTRODUCTION

Industry is making increasing use of robotics for material transport and processing. These robotic systems make use of many innovative sensing technologies [2]-[5] and control techniques [6]-[9] to improve their versatility and agility. The traditional approach to flexible manufacturing is to use mobile robots to transport materials [10][11] between workstations containing stationary robotic manipulators [6]. Another approach is to move the robotic manipulators between the workstations [12] using an Automatic Ground Vehicle (AGV). This configuration is referred to as a mobile manipulator in this paper. The use of mobile manipulators can be advantageous in a number of situations. It can result in cost savings when a single mobile manipulator can be used to replace several stationary manipulators. The use of mobile manipulators is also useful in cases where the item being worked on is too large to be easily moved. Throughout this paper the term manipulator will refer to the robotic manipulator arm mounted on the mobile base, and the mobile base will be referred to as the AGV. The combination is referred to as a mobile manipulator.

The use of mobile manipulators in manufacturing presents new challenges [6]. The use of intelligent sensing systems such as computer vision or light detection and ranging (LADAR) sensors [13] can be used to measure a workpiece's location and orientation relative to the manipulator. To effectively act on sensor information, the systems need to know precisely where those sensors are located with respect to the other elements of the system. The calibration of a new sensor involves the determination of the position and orientation of the sensor relative to other sensors and manipulators. These parameters are difficult, or even impossible, to measure directly. Sometimes the only way of determining these unobservable system parameters is through the mathematical analysis of the sensor's own data. The calculation of arm-mounted camera offsets using images from the camera has been widely discussed in the literature [14]-[25]. In most of these methods, a key feature is the simultaneous solution of two sets of independent transformations. These transformations are typically the desired offset of the sensor and the pose of a calibration target. The solution of the calibration target pose is typically incidental to the solution of the desired offset. Similar methods can be applied to determining other system offsets.

The focus of this paper is on indirect methods for determining the mounting offset of a robot manipulator on a mobile base. Section II discusses the need to calibrate the offset between the manipulator base and the AGV's coordinate system. It also describes the equipment and methods used to collect the data and evaluate the results of the mounting offset calibration. Section III. discusses two methods of computing the mounting offset: the first using measurements taken at selected positions around a test artifact, and the second a method of computing the offset using Ceres Solver and a selection of measurements from a random set of positions around the test artifact. Section IV. discusses the effectiveness and accuracy of the two calibration methods discussed in Section III. Section V discusses the relative merits of using Ceres Solver for solving this type of calibration problem and the effects of measurement noise on the procedure.

II. WORKSTATION REGISTRATION

This section describes the workstation registration problem, the NIST mobile manipulator testbed, a novel registration artifact, and the use of the artifact for registration.

A. Description of the problem

The goal is to be able to use the AGV to move the manipulator to a workstation and be able to accurately assemble items in that workspace [26]. To perform this task, it is necessary to accurately determine the location of the manipulator relative to the workspace. Two crucial components of this are determining: (1) the actual (not just the commanded) position of the AGV and (2) the position of

 ISBN: 978-1-61208-515-9

the manipulator relative to the AGV. For component one, we need to be able to get the position of the AGV from the navigation system in near real time. All our prior research to this point has involved off-line, AGV position data processing from log files. For the current task, we must be able to pass the position information directly to the computer system that is controlling the manipulator.

The second requirement is to establish the offset between the AGV and the base of the manipulator. This will allow the AGV's position to be used to determine the global location of the manipulator when the AGV stops at a particular work station.

B. NIST Mobile Manipulator Testbed

The mobile manipulator used for the work described in this paper is a part of the National Institute of Standards and Technology (NIST), Robotic Systems for Smart Manufacturing Program. It was assembled as a platform for developing and testing performance standards [26][27] for mobile manipulators in industry.

The mobile manipulator consists of a six-axis manipulator mounted on top of an AGV. The AGV is an electrically-powered, all-wheel drive, automatic forklift designed for material transport in an industrial setting. The AGV navigates from location to location using a path network that is preprogrammed off-line. The AGV location is measured using a navigation system that uses a rotating laser range sensor to detect the locations of reflectors strategically mounted throughout the work area. The positions of the reflectors are surveyed during the initial setup of the system. During operation the position and orientation of the AGV is calculated based on the range and angle to reflectors within range of the navigation sensor.

In order to test the positioning accuracy and repeatability of the mobile manipulator, a laser retro-reflector sensor was mounted as the end-of-arm-tool (EOAT) of the manipulator. A digital signal is output from the sensor when the laser is emitted and reflected to the sensor. The signal is then read by the manipulator controller. Less intense reflections off of other objects in the workstation are ignored. The laser is used to interact with the Reconfigurable Mobile Manipulator Artifact (RMMA) described in the next section.

C. Reconfigurable Mobile Manipulator Artifact

The RMMA [26]-[28] is a test fixture developed at NIST to emulate the environment that would be encountered by a mobile manipulator. It was designed primarily to emulate the positioning requirements of an assembly task, specifically the peg-in-hole insertion task. It does this by providing a set of precisely positioned mount points for reflective targets. The targets are detected using a non-contact, laser retro-reflector sensor designed to detect the presence of retro-reflective targets in line with the laser beam. The sensor is mounted as the EOAT. The targets are designed to determine if the manipulator position is accurate enough for successful peg-in-hole insertion. The RMMA provides a way to test and verify the performance of mobile manipulator systems without the use of expensive 3D tracking systems [29].

The target fiducials are constructed using a piece of reflective material fixed behind a circular aperture. In some of the targets a fixed radius aperture is used, in others a variable aperture is used. A top down view of a target fiducial is shown in Fig. 1. The laser retro-reflector sensor is used to detect the alignment of the manipulator with the fiducial. A signal is returned by the sensor when the laser beam is reflected back by the fiducial. The position accuracy can be adjusted by varying the size of the aperture used to expose the reflector. In addition, a tubular collimator is added to the fiducial to restrict the detection angle of the fiducial. The position of a fiducial can be determined by performing a search starting somewhere near the fiducial's actual position. By performing a spiral grid search with a step size of half the aperture diameter, the position of the fiducial can be determined with an accuracy bounded by the

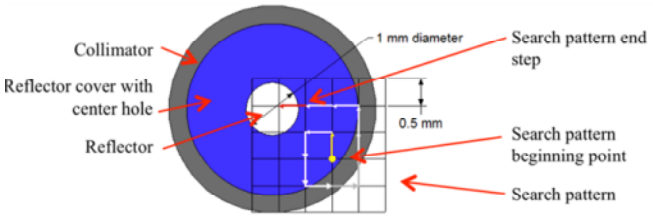
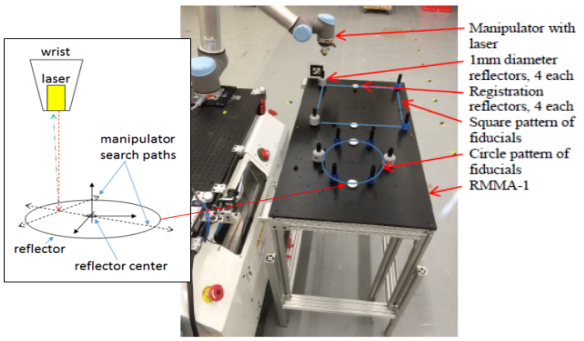


Figure 1. Top down view of an RMMA fiducial showing grid spiral search pattern.

aperture diameter. Fig. 1 illustrates the path followed during a spiral grid search.

Large circular reflectors can also be mounted on the RMMA to aid in mobile manipulator localization. The center of the large reflectors is measured by performing a bisecting search starting from a point within the radius of the reflector. The center is found by searching outward to find the reflector edges and bisecting that chord. After locating the center along one axis, a search for the reflector's edges is performed along an axis perpendicular to the first. After the endpoints of this second chord are determined, the center position of the reflector can be calculated. The bisection search is illustrated in Fig. 2(a). After the centers of two reflectors have been measured, the position and orientation of the pattern can be determined. Then the positions of all the other target reflectors in the pattern can be calculated based on their position relative to the registration reflectors.

 ISBN: 978-1-61208-515-9



(a) (b)

Figure 2. (a) Bisection search concept, and (b) the mobile manipulator positioned next to the RMMA, the RMMA square and circle patterns, and the large reflectors within each pattern.

D. *Registration to RMMA Patterns*

The RMMA has a number of precisely-positioned, threaded holes into which the fiducials and reflectors can be mounted to exercise the system. There are two main target configurations: a square target and a circular target as shown in Fig. 2(b). These are used to test the positioning accuracy and repeatability of the mobile manipulator after bisecting the large reflectors.

The two dimensional (2D) pose of the square and circle pattern of small reflectors can be determined by measuring the locations of two reflectors, large or small, on each pattern. The other small reflector locations in the pattern can be calculated based on their relative offsets when given the pattern pose. Either a pair of small reflectors using the search method or a pair of large reflectors using the bisect method can be used to register the mobile manipulator with the workspace represented by each pattern. For example, after moving to the calculated reflector positions, if the small reflector is not immediately detected, a search is performed. The distance between the initial position of the manipulator and the position at the end of the search can be used to provide information on the accuracy of the mobile manipulator's position and the accuracy of the registration.

III. MANIPULATOR CALIBRATION

Calibration of the manipulator onboard the AGV is critical for understanding how to position and orient the manipulator to a workstation. This section describes manual and Ceres Solver methods.

A. *Manual calibration method*

We experimented with methods to allow strictly manual calibration of the manipulator mounting offset using a number of simple measurements. The idea was to select pairs of calibration data measurements that would lead to the simple calculation of a single value of the manipulator mounting offset. This was done by selecting pairs of positions around the target where the other parameters of the manipulator mounting offset would effectively cancel each other out.

The AGV positions were chosen to cancel out the effects of the other base offset parameters, or to minimize their effect on the computation. In testing, these values were good enough to come up with rough values of the offset, but not good enough for precise positioning of the manipulator. There were some interactions between the calibration variables that could not be completely eliminated using this method. However, the method works well as a sanity check for the other computation methods.

The equations below describe the manipulator offset calibration in a 2D plane. The value being determined is the 2D translational offset and rotation offset of the manipulator relative to the AGV. The reason for doing the calculations in 2D is that the method for taking the measurements using the laser sensor only constrains the position in 2D, and the AGV navigation solution is only 2D.

Fig. 3(a) illustrates a pair of mobile manipulator locations that isolates the x offset of the manipulator base.

$$A_{x1} + O_x - P_{x1} = A_{x2} - O_x + P_{x2}, \quad (1)$$

$$O_x = \tfrac{1}{2} (A_{x2} - A_{x1} + P_{x1} + P_{x2}), \quad (2)$$

where:

P is point in manipulator coordinates (P_x, P_y)
A is AGV coordinate (A_x, A_y, A_a=angle)
O is the manipulator mounting offset (O_x, O_y, O_a=angle)

Fig. 3(b) illustrates a pair of mobile manipulator locations that isolates the y offset of the manipulator base.

$$A_{y1} + O_y - P_{y1} = A_{y2} - O_y + P_{y2}, \quad (3)$$

$$O_y = \tfrac{1}{2} (A_{y2} - A_{y1} + P_{y1} + P_{y2}), \quad (4)$$

Fig. 3(c) illustrates a pair of mobile manipulator locations that isolates the angular offset of the manipulator base.

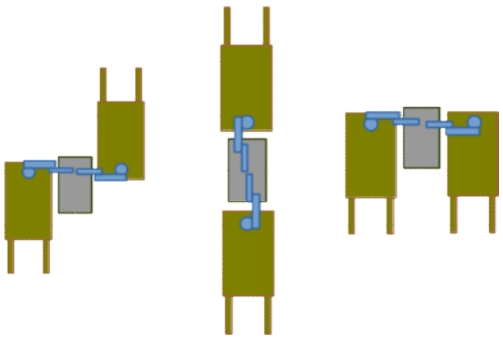
$$A_{x1} + O_x - P_{x1} + R_1 \sin O_a = A_{x2} + O_x - P_{x2} + R_2 \sin O_a, \quad (5)$$

where

$$R_n = (P_{xn}^2 + P_{yn}^2)^{1/2} \quad (6)$$

and

$$O_a = \sin^{-1}((A_{x1} - A_{x2} - P_{x1} + P_{x2}) / (R_2 - R_1)) . \quad (7)$$



(a) (b) (c)

Figure 3. Mobile manipulator (green) positions relative to the RMMA (gray) selected for manual calibration of manipulator (blue) mounting offset.

These formulas assume the manipulator is mounted on the AGV with its positive y-axis pointing toward the rear

 ISBN: 978-1-61208-515-9

(fork-end) of the AGV (in the direction of the AGV's negative x-axis).

There are a number of issues that limit the effectiveness of this approach for determining the manipulator base location. One issue is that despite the best efforts to position the AGV as described, there will be some errors in alignment. The result is that the other offset terms will not cancel out exactly, and there will be some interaction between the parameters that will affect the results of the calibration.

Another issue with this method is that it does not deal well with measurement error. Each parameter is calculated using a single pair of AGV positions. So any errors in the measurements are reflected directly in the calculated mounting parameters. The effects of measurement noise can be compensated for by averaging together a number of measurements at a given location.

B. Calibration using Ceres Solver

A better way to solve for the manipulator base offset is to express it in terms of a non-linear minimization problem. This allows all the interactions between the base offset parameters and the calibration measurements to be explicitly modeled. After the interactions between the calibration parameters and the calibration data have been modeled, the calibration parameters can be solved using iterative methods. The tool used to compute the iterative solution was the Ceres Solver library [1].

The calibration data consists of paired AGV and manipulator position data taken at various locations around the RMMA. The only constraint on the data is that it needs to be collected at a number of different AGV positions and angles in order for the solver to converge properly. Data from multiple target points can also be used as long as the association is maintained in the data model.

The mobile manipulator system model is formulated as:

$$wp(k) = agvPose(t) * robotPose * rp(k,t), \quad (8)$$

where:

- wp(k) is the estimated position of the *k*th target point in world coordinates;
- agvPose(t) is the measured pose of the AGV in world coordinates at time t;
- robotPose is the estimated pose of the manipulator in AGV vehicle coordinates;
- rp(k,t) is the measured location of the *k*th target point in manipulator coordinates at time t.

The agvPose(t) and robotPose are 2D transformations consisting of a translation and a rotation. The points wp and rp are 2D points. Individual calibration targets are enumerated by *k*, and individual calibration measurements are enumerated by *t*.

The program adjusts the values of wp(k) and robotPose to minimize the residual between the estimated world coordinates of the target points and the position value computed in (8) above using the calibration data. The estimate of the manipulator mounting offset is calculated using the data collected for the manual calibration augmented with additional samples not used in the manual calibration.

The relationship between the calibration data and the free variables is established in Ceres Solver by the creation of *residual blocks*. The residual is defined as the difference between the estimated value of wp and the value of wp calculated by (8). The Ceres Solver then iteratively solves for the values of wp and robotPose that minimize the sum of the squares of all the residuals defined by the residual blocks. Ceres can also make use of a loss function, which can be used to minimize the effect of outliers. When the loss function is $\rho(x) = x$, Ceres minimizes the mean squared error of the residuals. The encapsulation of the residual computation in the residual blocks also allows Ceres to automatically compute the partial derivatives of the modeling equations. This eliminates a potential source of user error.

This problem bears a close similarity to the three-dimensional (3D) simultaneous, robot-world, hand-eye calibration discussed in [14][15][16]. The camera calibration problem is typically expressed as AX = ZB, where X is the 3D pose representing the camera offset and Z is the 3D pose representing the location of the calibration target. It is easy to see that (8) can be manipulated into this form. Both X and Z are unknowns that have to be solved simultaneously. A number of closed-form solutions [14][25] have been proposed to solve for these values. The principle difference between the different solutions is how they resolve the weighting between the positional and rotational components [11] of the residual that defines the 'best' solution to the problem. Given the 2D nature of the current problem, it is probable that a closed-form solution to the problem can be formulated. However, since the calibration parameters do not need to be computed in real time, the iterative solution implemented with Ceres Solver is sufficient. The iterative solution method is also easily adapted to solve for other calibration constants, some of which may not be solvable with a closed-form solution.

More data is generally better data. Unlike the manual calibration approach, the iterative minimization approach can use additional data to minimize the effects of measurement noise. However, care must be taken to provide a suitably rich set of input data. For example, if all the samples were taken at different positions around the workspace, but with the same orientation, it is not possible to determine the orientation offset of the manipulator base. The iterative solution would either not converge, or would converge to an unstable value.

Care must also be taken in the construction of the system model used for iterative minimization. If two or more of the free variables are correlated, the model will be under constrained, and may not be able to converge to an answer. A high degree of correlation between variables can also lead to a high degree of sensitivity to the input data.

IV. RESULTS OF TESTING

The initial set of calibration data was collected manually. The AGV was moved manually to various locations around the RMMA and its position was recorded. Then the

 ISBN: 978-1-61208-515-9

manipulator was moved manually to the positions of the first and second reflectors of the square target. The manipulator was moved until the retro-reflector sensor detected the reflectors. Then the position of the manipulator was manually recorded.

The reflectors used to collect the calibration data had a 3.2 mm (1/8 in) aperture. The positions of the AGV relative to the RMMA for the manual data collection are shown in Fig. 4. A subset of these measurements, shown in Fig. 3, was used to perform the manual calibration described in Section III.A. The orientation of the EOAT was maintained constant relative to the manipulator base so that any lateral offset of the sensor from the tool center could be ignored. Any offset at the tool becomes part of the base offset for the purposes of this calibration. A subsequent calibration of the base offset using all of the collected data was performed using Ceres Solver.

Testing of the manipulator base calibration was performed using an automated test program and the RMMA. A program was set up to drive the AGV to ten different positions around the RMMA as shown in Fig. 5. At each docking location, the position of the AGV, the world coordinate of the reflector, and the manipulator base offset were used to compute the robot coordinates of the reflectors using (8). After positioning the sensor, a search was performed to determine how far off the position calculation was.

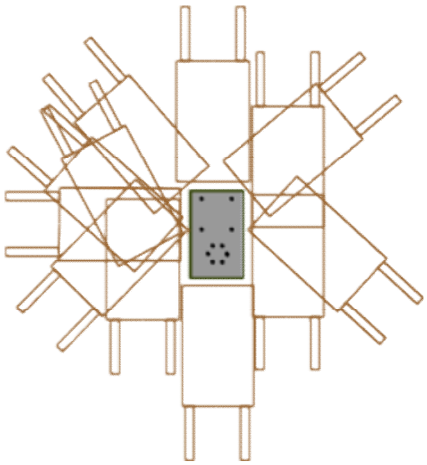


Figure 4. Position and orientation of AGV relative to the RMMA from manually collected calibration data.

Ideally, it should be possible to move the manipulator directly to the reflector based on the position of the AGV. Unfortunately, noise and systematic errors in the AGV position data prevent this. Fig. 6 shows a plot of consecutive samples of the AGV's *x*-axis position as the AGV sits motionless. The graph also shows a plot of the average value of samples 1 through n. This shows roughly how many samples need to average together to produce a reasonably stable position value. The *y* position and the orientation angle exhibit similar noise. The AGV position data is available at about 16 Hz, so it requires about 6.25 seconds to collect 100 samples. In this 2D case a simple average of the orientation angles is sufficient. In the general case of 3D orientations, greater care needs to be observed in averaging the orientation [32][33]. In addition to the random noise, tests also indicate that there are some systematic biases in the AGV position data depending on the location of the AGV.

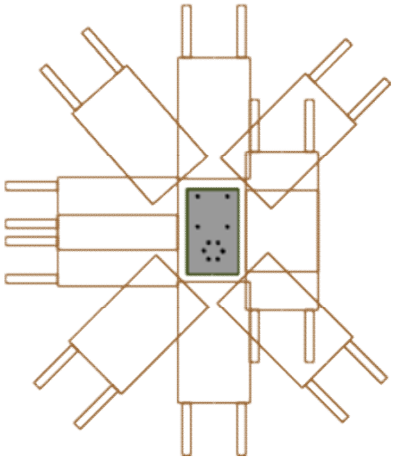


Figure 5. Docking locations used for automated data collection and system evaluation.

The goal is to be able to align the manipulator with the workspace in the minimum amount of time. The ideal situation is to be able to perform the insertion task immediately on arrival at the workstation. However, in this case it is necessary to compensate for the unavoidable measurement errors. It becomes a tradeoff between time spent averaging the position data to produce a stable value vs. time spent searching for registration points in the workspace.

The manual calibration method described in section III.A generated a base offset of (x = 831.5, y = - 7.5) mm and a rotation of 90.6°, yielding a mean square error of 1.25 mm and a maximum residual of 6.3 mm. The Ceres Solver came up with an offset of (x =833.637, y = -8.22223) mm and a rotation of 90.5314°, yielding a mean square error of 1.19 mm and a maximum residual of 10.7 mm. The Ceres Solver was seeded with a variety of initial conditions, including setting all the variable parameters to 0, and had no problems with convergence. The resulting offset positions agreed with each other within 0.1 mm

V. CONCLUSIONS

With care, Ceres Solver has proven to be a valuable tool in calibrating a variety of hard to measure constants in our robotic systems. It provides an easy to use framework for solving difficult non-linear problems iteratively. The main issues that have to be observed are that the model cannot be either over or under constrained if Ceres Solver is to converge properly.

 ISBN: 978-1-61208-515-9

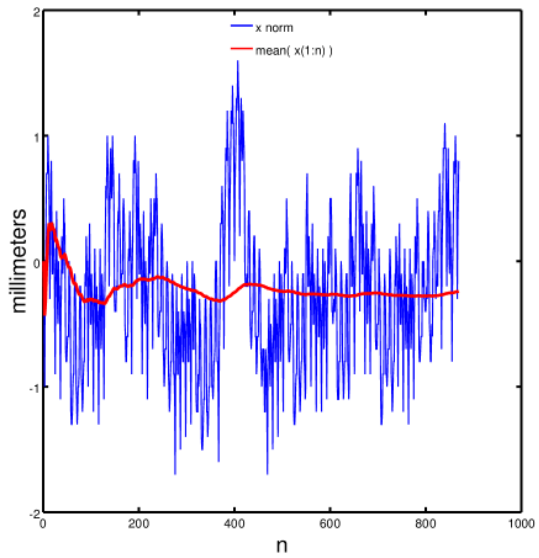


Figure 6. (blue)AGV position along x-axis, normalized to the first sample, x(1); (red) the mean of the normalized x value from x(1) to x(n).

Using Ceres Solver, we were able to compute the base offset of the manipulator mounted on a mobile platform despite the fact that the location of the AGV origin was not directly measureable. Using the computed offset and the location of the AGV, we were able to position the manipulator end effector within a few millimeters of the target regardless of the position and orientation of the AGV. While perfect initial positioning was not possible, the search time required to achieve the desired alignment accuracy was greatly reduced by improving the initial positioning of the manipulator.

The limiting factors in being able to accurately position the end effector are the noise and systematic errors in the AGV navigation sensor. This affects both the final position calculation and the accuracy of the manipulator base transform. The AGV position errors in the measurement used to compute the base offset affect the quality of the solution derived. The quality of the solution can be assessed by examining the residuals left after the model has converged to a solution for the free parameters. Large residuals indicate corresponding errors in the calibration data, either random or systematic.

We plan on pursuing other methods to increase the speed of the workspace registration. The spiral grid search increases in time proportional to the square of the initial error. Performing a bisecting search on the large reflectors goes up approximately linearly with the size of the maximum expected error, since the size of the reflector needs to be scaled up to encompass the maximum initial positioning error. In the future, we are planning to investigate the use of camera-based position estimates to improve the alignment time.

DISCLAIMER

Commercial equipment, software, and materials are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials, equipment, or software are necessarily the best available for the purpose.

REFERENCES

[1] S. Agarwal and K. Mierle, “Ceres solver,” http://ceres-solver.org [retrieved August, 2016].

[2] B. Hamner, S. Koterba, J. Shi, R. Simmons, and S. Singh, “Mobile robotic dynamic tracking for assembly tasks,” IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 2489-2495, 2009.

[3] R. Bostelman, T. Hong, and G. Cheok, "Navigation Performance Evaluation for Automated Guided Vehicle," 2015 IEEE International Conference on Technologies for Practical Robot Applications (TePRA), pp. 1-6 , 2015.

[4] R. E. Mandapat, “Development and evaluation of positioning systems for autonomous vehicle navigation,” Florida University Gainesville Center for Intelligent Machines and Robotics, pp. 1-277, 2001.

[5] A. Kelly, B. Nagy, D. Stager, and R. Unnikrishnan, "Field and service applications an infrastructure free automated guided vehicle based on computer vision an effort to make an industrial robot vehicle that can operate without supporting infrastructure." IEEE Robotics & Automation Magazine, pp.24-34, 2007.

[6] B. Hamner, S. Koterba, J. Shi, R. Simmons, and S. Singh, “An autonomous mobile manipulator for assembly tasks,” Autonomous Robot, pp.131-149 , 2010.

[7] J. Vannoy and J. Xiao, “Real-time Adaptive Motion Planning (RAMP) of mobile manipulators in dynamic environments with unforeseen changes,” in IEEE Trans. on Robotics, pp.1199-1212 , 2008.

[8] H. Martínez-Barberá and D. Herrero-Pérez, "Autonomous navigation of an automated guided vehicle in industrial environments." Robotics and Computer-Integrated Manufacturing, pp.296-311, 2010.

[9] R. C. Arkin and R. Murphy, "Autonomous navigation in a manufacturing environment," IEEE Transactions on Robotics and Automation, pp.445-454 ,1990.

[10] H. F. Durrant-Whyte, "An autonomous guided vehicle for cargo handling applications." The International Journal of Robotics Research, pp.407-440, 1996.

[11] H. Martínez-Barberá and D. Herrero-Pérez, "Autonomous navigation of an automated guided vehicle in industrial environments." Robotics and Computer-Integrated Manufacturing, pp.407-440, 2010.

[12] S. Bøgh, M. Hvilshøj, M. Kristiansen, and O. Madsen, "Autonomous industrial mobile manipulation (AIMM): from research to industry." In 42nd International Symposium on Robotics. Pp. 1-9, 2011.

[13] M. Hvilshøj and S. Bøgh, “Little Helper-An autonomous industrial mobile manipulator concept,” International Journal of Advanced Robotic Systems, pp.80-90, 2011.

[14] M. Shah, “Solving the Robot-World/Hand-Eye Calibration Problem Using the Kronecker Product,” ASME Journal of Mechanisms and Robotics, Vol. 5, 031007, pp. 1-7, 2013.

[15] F. Dornaika and R. Horaud, “Simultaneous robot-world and hand-eye calibration, “IEEE Transactions on Robotics and Automation, pp.617-622 ,1998.

[16] H. Zhuang, Z. Roth, and R. Sudhakar, “Simultaneous robot/world and tool/flange calibration by solving

 ISBN: 978-1-61208-515-9

homogeneous transformation of the form AX = YB," IEEE Trans. Robot. Automat, pp.549-554, 1994.

[17] A. Geiger, F. Moosmann, O. Car, and B. Schuster, "Automatic calibration of range and camera sensors using a single shot," ICRA, pp. 3936-3943, 2012.

[18] H. S. Alismail, D. Baker, and B. Browning, "Automatic calibration of a range sensor and camera system," Second International Conference on 3D Imaging, Modeling, Processing, Visualization & Transmission. IEEE, pp. 286-292 ,2012.

[19] Z. Zhang, "A flexible new technique for camera calibration," IEEE Transactions on pattern analysis and machine intelligence, pp.1330-1334, 2000.

[20] J-Y. Bouguet, "Camera calibration toolbox for matlab," < http://www.vision.caltech.edu/bouguetj/calib_doc/> [retrieved August, 2016].

[21] J. Weng, P. Cohen, and M. Herniou. "Camera calibration with distortion models and accuracy evaluation," IEEE Transactions on pattern analysis and machine intelligence 14.10, pp.965-980, 1992.

[22] O. D. Faugeras, Q.-T. Luong, and S. J. Maybank, "Camera self-calibration: Theory and experiments," European conference on computer vision, Springer Berlin Heidelberg, pp. 321-334, 1992.

[23] Y. Huang, X. Qian, and S. Chen, "Multi-sensor calibration through iterative registration and fusion, " Computer-Aided Design, pp.240-255, 2009.

[24] S. Spiess, V. Vincze, and M. Ayromlou, "On the calibration of a 6D laser tracking system for contactless, dynamic robot measurements," Instrumentation and Measurement Technology Conference, pp. 1203-1208 ,1997.

[25] M. Shah, R. D. Eastman, and T. Hong, "An overview of robot-sensor calibration methods for evaluation of perception systems," In Proceedings of the Workshop on Performance Metrics for Intelligent Systems, pp. 15-20, ACM, 2012.

[26] R. Bostelman, T. Hong, and J. Marvel, "Performance Measurement of Mobile Manipulators", SPIE 2015, Baltimore, MD, Vol. 9498, pp. 1-9, April 2015.

[27] R. Bostelman, T. Hong, and S. Legowik, "Mobile Robot and Mobile Manipulator Research Towards ASTM Standards Development", SPIE 2016, Baltimore, MD, pp. 98720F-98720F , 2016.

[28] R. Bostelman, S. Foufou, S. Legowik, and T. Hong "Mobile Manipulator Performance Measurement Towards Manufacturing Assembly Tasks", 13th IFIP International Conference on Product Lifecycle Management (PLM16), Columbia, SC, July 11-13, Vol. 9892, pp. F1-F10, 2016.

[29] R. Bostelman, J. Falco, M. Shah, and T. Hong, "Dynamic Metrology Performance Measurement of a Six Degree-of-Freedom Tracking System Used in Smart Manufacturing", Autonomous Industrial Vehicles: From the Laboratory to the Factory Floor, ASTM Book chapter 7, 2016.

[30] R. Bostelman, R. Eastman, T. Hong, O. A. Enein, S. Legowik, and S. Foufou, "Comparison of Registration Methods for Mobile Manipulators," CLAWAR, 2016.

[31] M. Shah, "Comparing Two Sets of Corresponding Six Degree of Freedom Data," Computer Vision and Image Understanding, Volume 115, Issue 10, pp. 1355-1362. 2011.

[32] R. Hartley, J. Trumpf, Y. Dai, and H. Li, "Rotation averaging," International journal of computer vision, 103(3), pp.267-305, 2013.

[33] F. L. Markley, Y. Cheng, J. L. Crassidis, and Y. Oshman, "Averaging quaternions," Journal of Guidance, Control, and Dynamics, pp.1193-1197, 2007.

 ISBN: 978-1-61208-515-9

Plausibility Checks in Automotive Electronic Control Units to Enhance Safety and Security

Martin Ring, and Reiner Kriesten

University of Applied Sciences Karlsruhe
76133 Karlsruhe
Emails: {martin.ring, reiner.kriesten}@hs-karlsruhe.de

Abstract— **Automobiles nowadays consist of multiple Electronic Control Units (ECUs) and bus systems. Attacks on these critical infrastructure elements have increased a lot over the last years, especially since remote exploitation is possible due to wireless connectivity. Most of these attacks targeted standard services implemented in cars. These services, e. g., allow the activation of the headlights or turning of the steering wheel via the parking assist. All these services have to be secured so they can only be executed when it is safe to do so. These checks for a safe state are plausibility checks, which nowadays only utilize the vehicle speed. In this paper we motivate the need for other values that have to be authentic and integrous. We want to utilize immanent signals, derived from hard wired sensors, for each ECU that utilizes plausibility checks.**

Keywords–Automotive Security; Vehicular Attacks; Plausibility Checks.

I. INTRODUCTION

Modern automobiles feature a myriad of cyber physical systems. These systems are composed of up to 100 microprocessors (called ECUs) with up to 100 million lines of code [1]–[3]. These systems are prone to attacks. Since the introduction of bus systems to cars they are vulnerable to attacks that require a physical connection (e. g., car theft). With the introduction of wireless interfaces, these attacks and many more can now be performed from the basement of hackers [4]. Thus the most acclaimed attacks on automotive networks nowadays have been remote attacks. These attacks alone have little to no effect on cars, only combined with flaws in the internal networks security risks can arise. Miller and Valasek come to the same conclusion and argue that their work "shows that simply protecting vehicles from remote attacks isn't the only layer of defence that automakers need." [5]. An defense in depth concept is necessary. One part of such a concept are the proposed plausibility checks in this paper. In earlier publications [4]–[8] a lot of the attacks able to compromise the safety of a car were limited to low speeds. These limitations stem from plausibility checks in ECUs that try to determine if the execution of the requested service is safe. These plausibility checks only rely on the speed of the vehicle. With this paper, new approaches for such checks will be introduced.

In the following, we will first give an introduction to plausibility checks and outline the requirements for the used signals. Section III then describes the method for advanced plausibility checks and the assessment process to determine suitable functions to safeguard. Next Section IV gives an evaluation of our method and its applicability, and finally Section V concludes this paper.

II. STATE OF THE ART

As researchers noticed in their attempts to compromise cars, most of the time the last barrier to safety critical functions is a plausibility check. These are simple checks that verify if the prerequisites to execute a function safely are met. All found checks use the speed of the car as a signal to check against [5]. All but one ECU (the Antilock Brake System (ABS)/Electronic Stability Control (ESC)-ECU) obtain this information from a bus system. The check only determines if the speed is below a predetermined threshold. This threshold is usually 5 mph or 8 kph depending on whether the country uses imperial or metrical units, respectively. Above these thresholds, ECUs change their internal state to one with very limited triggerable functions. The problem with this mechanism is not its principle function but that everything depends on the speed of the car, which is received by bus messages and can thus be sent by any host in the same subnet in current automobiles. If no network separation is present the signal can basically be sent by any host in the network even by ones plugged in externally.

In order to provide the necessary protection, the signals used for plausibility checks have to be authentic and integerous. The approach used nowadays and presented in a recent publication [9] is the applications of cryptographic functions to ensure that these preconditions are met. A possible way to ensure the authenticity and integrity of a message is the use of an Keyed-Hash Message Authentication Code (HMAC). This type of message protection can not be found in production vehicles nowadays. The maximum security offered is the use of an alive counter and a simple checksum.

III. ADVANCED PLAUSABILITY CHECKS

As stated before, plausibility checks can be applied as part of a defense in depth concept to prevent attacks on safety critical functions. Figure 1 shows the method that can be used to determine if our proposed checks can be used for a certain application.

In advance to this assessment, a hazard and risk analysis has to be conducted. This analysis is part of every automotive development lifecycle and demanded by the functional safety standard ISO 26262 [10]. The objective of this analysis is the identification and classification of the hazards of an item ("a

 ISBN: 978-1-61208-515-9

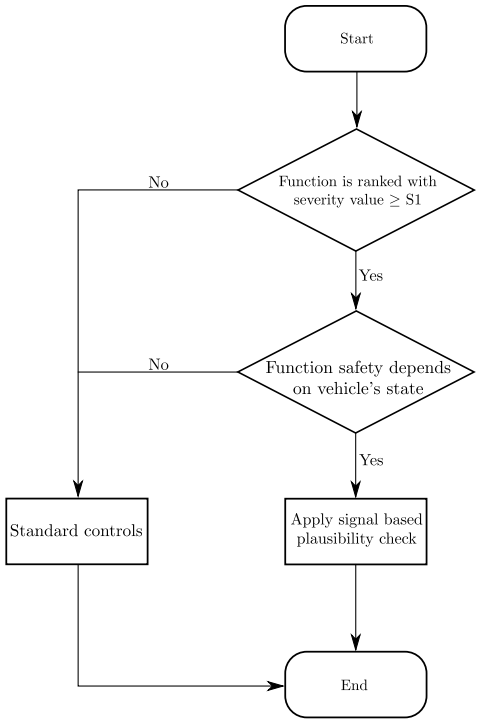


Figure 1. Methodology for applying plausibility checks

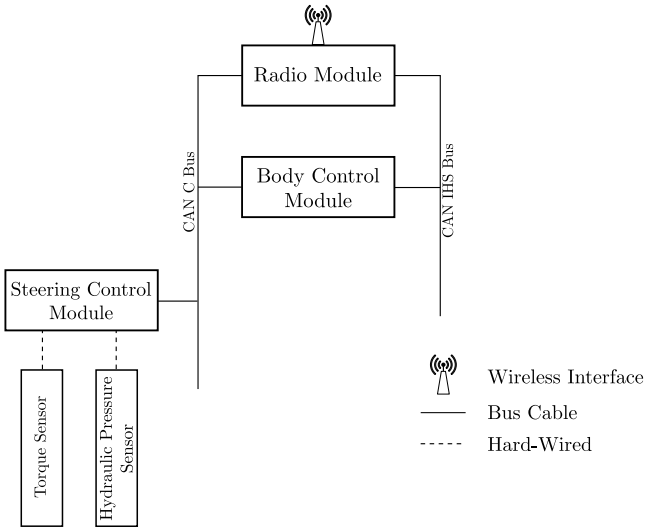


Figure 2. Sub-architecture of a Jeep Cherokee 2014 [4]

system that implements a function at a vehicle level" [10]). Such an item could, e. g. , be the airbag. In addition, safety goals related to the prevention and mitigation of the found hazards have to be drafted. For each hazard, an Automotive Safety Integrity Level (ASIL) has to be calculated. The inputs for this calculation are the expected loss in case of an accident (*severity*) and the probability of the accident occurring (*exposure and controllability*). For this contemplation only the severity as the consequences of a malfunction are considered. With levels from S 0 to S 3, functions with a severity equal or above S 1 (light to moderate injuries) are deemed meaningful. These considerations are embodied by the first decision in the design structure chart pictured in Figure 1. The next necessary decision is to determine if the function in question depends on the state of the vehicle.

When these requirements are met, advanced plausibility checks should and can be used to safeguard functions. As mentioned before, inputs to these plausibility checks have to be authentic and integrous. These protection goals can be met by applying cryptographic functions, e. g. , using HMAC [9]. This type of cryptographic measure ensures the desired protection goals with an acceptable demand for computational performance. Nevertheless there also exist a few drawbacks using HMACs. In particular the key management and reduced bandwidth on the bus by attaching an HMAC to each message are problematic. Is there another method to ensure the needed protection goals without the drawbacks of HMACs? To answer this question we took a deeper look into automotive architectures like the one presented in Figure 2.

Figure 2 represents a part of a Jeep Cherokee 2014 network architecture which was the target of the latest attacks of Miller and Valasek on a car [4], [5]. The figure shows different ECUs and gateways that are interconnected by bus systems. Furthermore, some hard-wired sensors are apparent delivering relevant information about the state of the vehicle. This information can be used to derive ECU immanent signals for plausibility checks without the need for cryptographic algorithms.

ECU immanent signals should be used for plausibility checks whenever possible. These signals can be signals produced in the ECU, like the regulated torque in the engine ECU that is calculated by adding up all the torque demands of the engine auxiliaries and the driver requirement. The other possibility for such signals are hard-wired sensor signals like the rotational speed sensors for the ABS / ESC ECU. With the help of Figure 3 we want to show how an immanent signal of an ECU can be used to make a plausibility check for a requested function. The latest hacks applied on the Jeep [5] jammed the signal of another ECU that normally would have been used to make the plausibility check. In this case the plausibility check would verify if the car is in reverse and slower than 5 mph. The check for the driving direction is not easily possible but we can check for the speed constraint. We can assume a known level of hydraulic pressure in the steering system because we have a hard-wired sensor for this signal to the Steering Control Module (SCM). This module also evaluates the signal of the torque sensor. With this information we can determine the speed of the car within small limits. With the help of the information in Figure 3 it is possible to determine the speed of a car. As a small example we will show the determination of the threshold for the steering torque for the conditions the Jeep has to meet to execute the steering angle change. With a supposed threshold of 20 kph for the Jeep and an assumption of 20 bar for the hydraulic pressure brings us to the conclusion that a steering moment of more than 2.9 Nm is equivalent to a speed above the defined threshold and thus the execution of the requested function has to be refused. An implementation according to this technique would have prevented the attack on the steering system as described in [5]. Such immanent signals can be found and utilized on almost any safety critical ECU in a car. Only if such signals are not existent signals from other ECUs should

be used. As mentioned before these signals have to fulfill some preconditions, namely being integrous and authentic. Only if these prerequisites are fulfilled, such bus signals can be used for plausibility checks of functions with a severity value of S 1 or above.

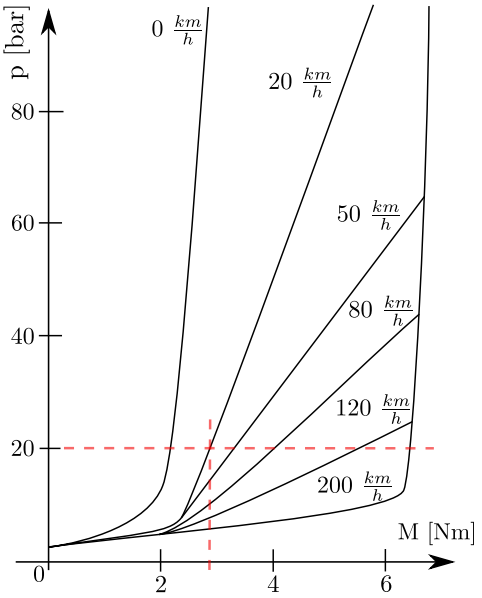


Figure 3. Plot of steering moment dependent on hydraulic pressure and vehicular speed [11]

The other attacks presented in the latest release of Wired [5] are more problematic as they use legitimate messages to request certain functions. The *slamming on the car's brakes* is a standard function that is executed while the driver presses the switch for the electronic parking brake. While pressing the switch the pump for the ABS / ESC system gets activated and provides the pressure to engage the brakes of the car. Such a brake maneuver is comparable with an emergency braking. As Miller and Valasek were able to request and execute this function it is reasonable to assume that the switch for the electronic parking brake is directly connected to the bus system of the car. The same thing can be concluded for their last attack, the unintended acceleration of the car. They used the standard function to enable Apdative Cruise Control (ACC) and then increase the target speed of the cruise control. This is possible by replaying messages of the switches embedded in the steering wheel. We were able to observe the same situation in an electric vehicle produced by a German manufacturer. Therefore, safety critical functions with an ASIL of D should not be able to be activated by bus messages. For all requests of such functions direct connections should be used (peer-to-peer); although these connections can be network connections, like Controller Area Network (CAN) or Ethernet, they should not be routed over gateways.

IV. Evaluation

To demonstrate the validity of this method in this section we present other examples of instances where plausibility checks with immanent signals can be used. First, we further evaluate the examples in Section II. After these examples other published attacks on safety critical functions (lighting, engine,

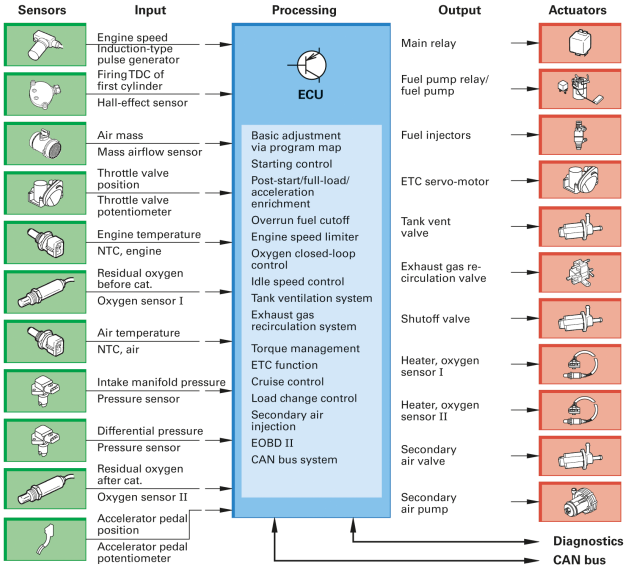


Figure 4. Engine ECU with its hard-wired sensors (green) and actuators (red) [13]

gearbox, brakes and suspensions [4], [6], [8], [12]) and the possibility to apply plausibility checks with ECU immanent signals are evaluated.

We start with the engine example. There are multiple attacks published on the engine of a car [6]–[8], [12]. Most attacks completely disable the engine and shut it down. To achieve this result standard services were used to reset the ECU, deactivate fuel injectors or initiate a flash session. Every service should use a plausibility check as the safety of its execution is widely dependent on the vehicles state. There are multiple immanent sensor values or processed signals that could be used for these plausibility checks. An extensive overview is presented in Figure 4. The easiest signal to use is the rpm-signal of the engine. If this signal is unequal zero no service that compromises the operation of the engine should be able to execute. Not necessarily forbidden should be services that help mechanics with diagnostics of the engine in a workshop, like reading out live data. Besides the aforementioned rpm-signal there are a host of other sensor signals which could be used, like the readout of the air mass sensor, exhaust temperature sensor, fuel pressure sensor and more. A processed signal that could be used is the calculated torque of the engine. This torquer is calculated by adding the demands of all auxiliaries of the engine, like the AC compressor, the alternator or the hydraulic steering pump as well as the driver demand. If this signal is unequal zero it can also be concluded that the car is in use and any execution of service that compromises the operation of the engine can be deemed unsafe.

The second and probably most critical point of attack is the braking system, which was also the target of multiple attacks [4]–[6], [12]. The executed attacks include wheel selective braking as well as disabling the braking system all together. Here it is also possible to use ECU immanent signals. All wheel speed sensors are hard wired to the ECU. Modern wheel speed sensors can determine speeds as low as

 ISBN: 978-1-61208-515-9

0.1 kph [14]. As soon as any speed is detected all safety critical services should stop their execution. However, the speed signal is not the only one that can be used, as an alternative the hard wired three-axis acceleration sensor can be evaluated. As soon as these sensors signals show any acceleration the car is not in a safe state to execute safety critical functions.

Our research shows vulnerabilities in active suspension systems. The ECUs controlling such systems also use a vast amount of sensors and signals to control the ride of a vehicle. Two possible immanent signals of such a system are acceleration sensors or sensors for the level of each wheel. If the signals of the level sensors of the car change or an acceleration unequal zero is detected it can be concluded that the car is in motion and thus safety critical functions should not be able to perform their task of, e. g. , resetting the ECU.

A way to utilize immanent signals to check the safe state of the car with immanent signals of the steering system was presented in Section III. This shows that these systems could be safeguarded in their current implementation with our method. Furthermore, these examples show that this method allows it to safeguard every ECU responsible for lateral or longitudinal behavior of a vehicle.

An instance where an odd sensor signal could be used were attacks on the headlights of cars [6], [8]. These attacks spoofed messages of the light sensor or used diagnostic messages to deactivate the headlights of a car. The sensor signal of the light sensor is evaluated in the vehicle supply system control device. This device also powers the electric fuel pump, see, e. g. , the schematic in [15]. This pump is only active when the engine is running and during a short time after unlocking the car or switching on the ignition. The signal is thus also a good indicator if it is safe to execute the inquired function. As the sensor is in the mentioned schematic hard wired to the executing ECU it can determine if the message was spoofed or issued by the correct sender.

V. Conclusion

In this paper, we have motivated the need for security plausibility checks. Such checks are already implemented but rely on bus messages of the vehicle speed which can be jammed or spoofed. As they are one crucial part of a defense in depth approach, a secure implementation is crucial.

With the use of immanent signals a secure way for plausibility checks is found. This approach can be used in modern cars without any need to change the architecture or wiring; all that has to change is the software and that can be achieved by a simple software update. We have discussed that many of the published attacks can be prevented by the presented approach.

References

[1] R. N. Charette, “This Car Runs on Code,” 2009. [Online]. Available: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

[2] G. Serio and D. Wollschläger, “Vernetztes Automobil Verteidigungsstrategien im Kampf gegen Cyberattacken,” ATZelektronik - 06/2015, 2015.

[3] SAE, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” 2016. [Online]. Available: http://standards.sae.org/wip/j3061/

[4] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle.” [Online]. Available: http://illmatics.com/Remote Car Hacking.pdf

[5] ——, “CAN Message Injection – OG Dynamite Edition.” [Online]. Available: http://illmatics.com/can%20message%20injection.pdf

[6] ——, “Adventures in Automotive Networks and Control Units,” 2014. [Online]. Available: http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf/

[7] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” 2011.

[8] “Gehackte Mobilität,” Apr. 2016. [Online]. Available: https://www.3sat.de/mediathek/?mode=play&obj=58732

[9] K. Beckers, J. Dürrwang, and D. Holling, “Standard Compliant Hazard and Threat Analysis for the Automotive Domain,” Information, vol. 7, no. 3, 2016, p. 36. [Online]. Available: http://www.mdpi.com/2078-2489/7/3/36

[10] ISO, “ISO 26262 Road vehicles – Functional safety,” 2011.

[11] H. Felder, “Autoelektrik – Grundlagen- und Fachwissen.” [Online]. Available: http://www.fahrzeug-elektrik.de/

[12] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., “Experimental Security Analysis of a Modern Automobile,” Symposium on Security and Privacy, 2010.

[13] R. H. Gscheidle, Ed., Modern automotive technology : fundamentals, service, diagnostics, 2nd ed., ser. Europa reference books for automotive technology. Haan-Gruiten: Verl. Europa-Lehrmittel, 2014.

[14] “Raddrehzahlsensoren im Kraftfahrzeug Funktion, Diagnose, Fehlersuche.” Tech. Rep. [Online]. Available: http://www.hella.com/ePaper/Raddrehzalsensoren/document.pdf

[15] “STG. Bordnetz - Control Mains Power Supply.” [Online]. Available: http://www.seatforum.de/uploads/DRAFT01%5B1%5D244.jpg

 ISBN: 978-1-61208-515-9

Test Results for V2V and V2I Optical Camera Communications

Byung Wook Kim

Dept. of ICT Automotive Engineering
Hoseo University, Asansi, Korea 30332
Email: bw-kim@hoseo.edu

Hui-Jin Jeon, Soo-Keun Yun, Sung-Yoon Jung

Dept. of Electronic Engineering
Yeungnam University, Kyungsansi, Korea 30332
Email: {huijin,ysk1438,syjung}@yun.ac.kr

***Abstract*—Autonomous vehicles require the integration of multiple communication systems. This paper presents test results of vehicle-to-vehicle (V2V) and vehicle-to-infra (V2I) optical camera communications (OCC). The flicker-free light emitting diode (LED) light sources, providing illumination and data transmission simultaneously, and a high speed camera are used as transmitters and a receiver in the OCC link, respectively. Test results showed that vehicle information sent by tail lamps of a running car ahead and absolute location data sent by streetlights were successfully received at a vehicle's camera via the OCC link.**

Keywords–Optical camera communications (OCC); vehicle-to-vehicle (V2V); vehicle-to-infra (V2I).

I. INTRODUCTION

Recently, many people demonstrate great interests in self-driving technology and car makers move toward offering fully autonomous vehicles. Although recent vehicles are equipped with cameras, sensors, and software essential for driving assistance, the advanced level of self-driving requires the functionality of V2V and V2I communication [1]. The future self-driving cars will talk to each other and also talk to any road-side infrastructure equipped with dedicated short-range communications (DSRC) and wireless access in vehicular environment (WAVE) devices [2][3].

There exist some issues concerning the vehicle communication reliability of DSRC and WAVE devices because they use radio frequency (RF) bands, which are vulnerable to multipath fading and channel congestion. This issue is significant when data transmission of road/vehicle safety messaging and vehicle safety control is required. Therefore, autonomous vehicles require the integration of information transmitted via multiple communication mediums.

With the widespread use of LED lights, optical camera communications (OCC) technology [4][5] has gained interests in a variety of fields. An OCC system is a new trend of optical communication using a camera receiver at visible light spectrum. As a back-up system to RF based vehicle communications, OCC technology can be applied to V2V and V2I communication for self-driving vehicles. Because the implementation of an OCC system is based on pre-installed LED lamps and cameras, an OCC system for vehicle communication requirea no substantial additional costs. Along with the advantages of OCC, several researches related to wireless communication in smart traffic systems based on OCC have been conducted recently [6][7].

This paper presents test results of flicker-free OCC for V2V and V2I communications. The flicker-free light sources of car tail lamps and streetlights were used as data transmitters. OCC data can be received by a high speed camera via the OCC link. Test results showed that reliable V2V/V2I communications were provided using the OCC technology.

The remainder of this paper is organized as follows. Section II outlines OCC data communication process. Section III shows test results of OCC based V2V and V2I communications and Section IV reports the discussion.

II. DATA COMMUNICATION PROCESS

This section explains the process of data communications via the OCC link. LED light sources, such as car tail lamps and streetlights, offer both communication and illumination performance. Because the human eye cannot perceive the light pulses blinking at 200 Hz or higher frequency, a manchester encoding method with a flickering rate of greater than or equal to 200 Hz was used. We set a data frame consisting of 8 bits of synchronization data and 16 bits of information data.

At a receiver-side, a high speed camera captures images with LED light sources containing OCC data and other light noises. To extract the image pixel regions containing OCC data, differential images were obtained and cumulated. An image binarization process was then performed using an appropriate intensity thresholds. To remove the additional noise induced by a camera equipped in a moving vehicle, a morphology erosion scheme was used. Then, region of interests (ROIs) containing OCC data were obtained and symbolic label were added to every ROIs. Because we set the same level of the camera sampling rate and LED flickering rate, a camera captures successive images containing "On" and "OFF" patterns of OCC data. By analyzing the intensity of ROIs in successive images, it is possible to obtain synchronization and information bits.

III. TEST RESULTS AND DISCUSSION

In this section we show test results of what we achieved during OCC field tests. For the OCC data transmitter, LED light sources controlled by an AVR microcontroller (ATmega128) were used. As a receiver, a high speed camera (FL3-U3-20E4C-C) with global shutter was used. In subsection III-A, we illustrate the test process and results of V2V OCC. Subsection III-B shows the results of V2I OCC and performance of vehicle location estimation.

A. V2V optical camera communication

In a V2V OCC scenario, LED tail lamps of a running car ahead (sedan) transmit data containing the car brake information (No brake, brake level 1, 2, 3) and the distance between tail lamps. Note that distance between tail lamps can be used for vehicle width estimation, the distance estimation from the car ahead and lane keeping assistance. As an OCC receiver, a high speed camera was equipped in the following

 ISBN: 978-1-61208-515-9

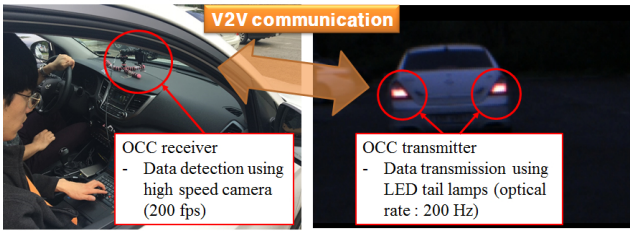


Figure 1. V2V communication scenario

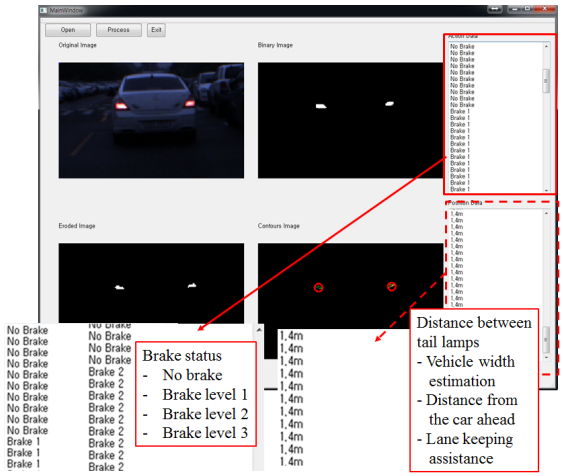


Figure 2. V2V OCC data acquisition

SUV car. As shown in Fig. 2, the camera frame rate and LED flicker rate were set to 200 Hz. The vehicles run within a speed of 40 km/hr. Fig. 3 shows that OCC data including the car brake information and the distance between tail lamps were received successfully even in a moving vehicle.

B. V2I optical camera communication

In a V2I scenario, we consider 6 LED streetlights transmitting their absolute 3D location information. By receiving these information using a high speed camera, the location of a moving vehicle can be estimated. As shown in Fig. 4, the camera frame rate and LED flicker rate were set to 250 Hz. It can be seen from Fig. 5 that the location estimation error lies within a range of $1m$. This means that an OCC system can provide lane-level services for self-driving cars. When the distance from the closest LED was approximately $27.5m$, a change point on the graph was observed due to the change in the number of total observed LEDs sending OCC data.

C. Discussion

Test results of V2V OCC scenario proved that the information from the running car ahead can be transmitted using LED tail lamps and enhance the car safety aspect of self-driving vehicles. In the results of V2I OCC case, absolute location information was transmitted by LED streetlights and captured images containing OCC data provided the estimated vehicle location, with the location estimation error less than $1m$.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(2016R1C1B1013942)

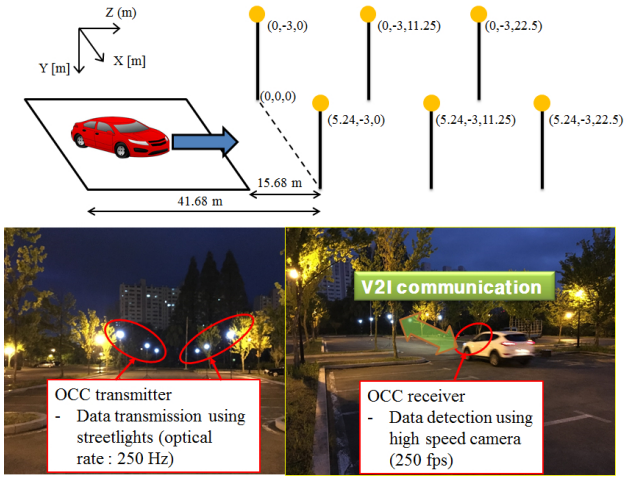


Figure 3. V2I communication scenario

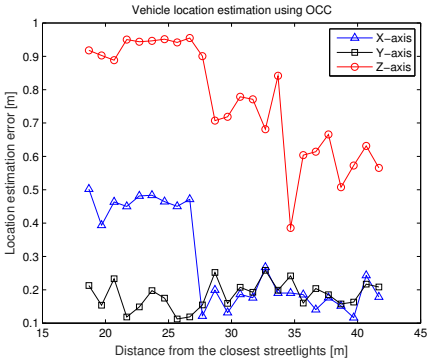


Figure 4. Location estimation error using the received V2I OCC data

REFERENCES

[1] A. Conti, A. Bazzi, B. Masini, and O. Andrisano, "Vehicular Networks: Techniques, Standards, and Applications," Boca Raton, FL, USA: Auerbach Publications, vol. 4, pp. 63-107, 2009.

[2] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," IEEE Vehicular Technology Conference, IEEE, May 2008, pp. 2036-2040.

[3] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," IEEE Vehicular Technology Conference, IEEE, Oct. 2007, pp. 2199-2203.

[4] The IEEE 802.15.7a Study Group, [Online]. Available from: https://mentor.ieee.org/ 802.15/documents?is dcn=DCN%2C%20Title%2C%20Author% 20or%20Affiliation & is group=007a.

[5] S. Rajagopal, R.D. Roberts, and S.-K.Lim, "IEEE802.15.7 visible light communication: modulation schemes and dimming support," IEEE Communications Magazine, vol. 50, no. 3, pp. 7282, 2012.

[6] I. Takai, S. Ito, K. Yasutomi, K. Kagawa, M. Andoh, and S. Kawahito, "LED and CMOS image sensor based optical wireless communication system for automotive applications," IEEE Photonics Journal, vol. 5, no. 5, 2013.

[7] T. Nguyen, N. T. Le, and Y. M. Jang, "Asynchronous Scheme for Optical Camera Communication-Based Infrastructure-to-Vehicle," International Journal of Distributed Sensor Networks vol. 2015, http://dx.doi.org/10.1155/2015/908139

 ISBN: 978-1-61208-515-9

Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication

Markus Ullmann* †, Thomas Strubbe,* and Christian Wieschebrink*
* Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann, thomas.strubbe, christian.wieschebrink}@bsi.bund.de
† University of Applied Sciences Bonn-Rhine-Sieg
Institute for Security Research
D-53757 Sankt Augustin, Germany
Email: markus.ullmann@h-brs.de

***Abstract*—A deployment of the Vehicle-to-Vehicle communication technology according to ETSI is in preparation in Europe. Currently, a Public Key Infrastructure policy for Intelligent Transport Systems in Europe is in discussion to enable V2V communication. This policy set aside two classes of keys and certificates for ITS vehicle stations: long term authentication keys and pseudonymous keys and certificates. We show that from our point of view the periodic sent Cooperative Awareness Messages with extensive data have technical limitations and together with the pseudonym concept cause privacy problems.**

Keywords–Vehicular Ad hoc Networks; Vehicle-to-Vehicle Communication; Intelligent Transport System; Cooperative Awareness Message; Pseudonym Concept; Privacy

I. INTRODUCTION

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I) (consolidated V2X) have been discussed intensively in recent years. The deployment of this technology requires accepted standards. The neccessary specification and standardization in Europe is done by the European Telecommunications Standards Institute (ETSI) based on considerations of the Car2Car Communication Consortium[1]. This includes the security standardization as well [2].

The ETSI specifications define an architecture for Intelligent Transport Systems (ITS). This architecture defines different ITS stations (e.g., ITS roadside stations, and ITS vehicle stations) and wireless communication between the ITS stations. The wireless communication technology for cooperative V2X communication is based on the IEEE 802.11p standard. A frequency spectrum in the 5.9 GHz range has been allocated on a harmonized basis in Europe in line with similar allocations in US.

The ETSI communication model defines broadcast communication between ITS stations. Different message types are defined for information exchange. Primary, these are the Cooperative Awareness Message (CAM) and the Decentralized Environmental Notification Message (DENM). These messages are disseminated via broadcast. According the ETSI specifications messages shall be digitally signed by the sender (ITS vehicle station or ITS roadside station) to guarantee message integrity and authenticity. In order to issue and authenticate the corresponding cryptographic keys, a suitable public key infrastructure (PKI) has to be established.

At the moment, the deployment of V2X technology is in preparation in large scale intelligent mobility infrastructure projects, for example SCOOP@F [3] in France, the C-ITS corridor Rotterdam-Frankfurt-Vienna [4] and the Nordic Way [5], a joint project of Denmark, Finland, Norway, and Sweden.

Research and development of the V2V communication has started 15 years ago. In the meantime, the IT architecture of vehicles has significantly changed. A lot of components to assist driving are available: lane keeping support, traffic jam assist, automatic parking assistant, remote parking assistant and so on. This is a prestage of automatic driving, which is one of the main challenges in automotive engineering at the moment. Already the mentioned systems to support driving require specific sensor systems to detect objects (e.g., road lanes, other vehicles and/or static traffic signs) as well as pedestrians and bicycles by capturing the environment. Many modern vehicles are already able to deduce a specific environmental traffic situation based on the captured information of the sensor elements without any V2V communication. But the integration of further sensor elements in vehicles is an ongoing activity due to automated driving in the near future. We argue that due to this deployment the relevance of the V2V communication will change over time. So on the one side, the importance of the periodically sent CAM, to deduce a specific environmental traffic situation, will decrease to more or less additional information in consequence of the integration of sensor systems in vehicles. On the other side, the signing of the CAM data and the integration of the certificate expands the message size tenfold, which can cause message collisions on the wireless communication cannel.

In the final report of the C-ITS platform (January 2016) of the EC DG MOVE the data elements of CAM and DENM messages of ITS vehicle stations are rated as *personal data* [6]. To put it briefly, each ITS vehicle station leaves a signed trace of its geographic location. Each entity within the communication range of the ITS communication technology can receive that data.

In this paper, we show that it is easy to link CAMs of a vehicle to a CAM trace even in case of a pseudonym switch. The effect of cryptographic signed CAMs is that the existance of the CAM data is not disputable. The applied cryptographic ECC domain parameter (NIST P-256 [7], BrainpoolP-256r1 [8]) are such that ECDSA signatures are not foregable within

 ISBN: 978-1-61208-515-9

the next years. Assuming, an attacker can plot a CAM trace of a vehicle. Is there any evidence that only one CAM of the whole CAM trace can be bound to a specific vehicle then the whole CAM trace can be bound to this vehicle. The attack to capture CAM traces and to bind these to a specific vehicle respective driver is described in [9]. So, CAMs provide side effects which can totally jeopardize the privacy of motorist. The technical limitations and the privacy shortcomings are raised by the usage of electronic signatures to assure message integrity and authentication.

Besides sensor elements, modern vehicles are equipped with wireless interfaces, e.g., bluetooth to connect devices (smart phones, tablets, etc) to the multimedia component of the vehicle. Initially, these wireless interfaces have nothing to do with the V2V communication. But from an attacker perspective these interfaces enable to bind captured CAM data traces to a specific vehicle. Therefore, these wireless vehicular interfaces has to be regarded in a holostic security analysis of the V2V technology as well.

The following sections of this paper are organized as follows: Section II is a description of related work. Next, Section III provides a brief overview of the secure V2V communication specified in the ETSI standards. Especially, the suggested pseudonym concept for securing CAM and DENM messages is presented in detail. Subsequent, identifiers for ITS vehicle stations are presented in Section IV. Next, technical limitations and privacy shortcomings of the current V2V communication approach are illustrated in Section V. Finally, in Section VI we summarize our results.

II. Related Work

A detailed overview of attacks in VANETs is given by Ghassan Samara et al. in [10]. A security and privacy architecture for pseudonymous message signing is described in [11]. Here, a public key infrastructure is regarded, too. In [12], Julien Freudiger et al. suggested mix zones for location privacy in vehicular networks. Giorgio Calandriello et al. propose on-board, on-the-fly pseudonym certificate generation and self-certification. The autors developed this approach to alleviate one of the most significant limitations of the pseudonym-based approach: the need for complex management. To achieve this, the use of group signatures is proposed. A survey on pseudonym schemes in vehicular networks is given in [13].

A detailed analysis of privacy requirements and a comparison with the security requirements in VANETs is given in [14]. Wiedersheim et al. [15] analyzed the location privacy in a specific communication scenario. Vehicles send beacon messages periodically. The beacons only carry the geographic position and an identifier. To support location privacy, the vehicles use pseudonymous identifier, which are changed regularly. Assuming a passive attacker who is able to eavesdrop the communication in a specific region the attacker is able to track the vehicles with an accuracy of almost 100% if he uses the approach in [15]. To perform this attack in a larger area an infrastructure of receivers is necessary to collect the CAM data. This can be done, e.g., by

- ITS roadside stations or
- an ITS vehicle fleet (e.g., truck fleet)

The fleet of ITS vehicle stations is equipped with additional V2V communication gateways only for monitoring the ambient V2V communication. All the collected data is sent to a centralized server infrastructure to analyze the data. Primary use case can be the analysis of traffic flow for the fleet to perform optimized navigation for individual ITS vehicle stations.

Besides the identification of ITS vehicle station based on licence plates or cryptographic certificates the identification based on noise features (individual noise spectrum) are discussed. That is a very active research area and different studies are presented [16] [17]. They differ in concerning single or multi sensor usage and concrete feature extraction. Surprisingly, neither common security nor privacy analyzation of the V2V communication consider this issue. Also, Bluetooth MAC IDs of vehicular multi-media devices are already used to develop route specific origin-destination tables and to perform vehicles counting on specific roads. In [18], an analysis in Jacksonville, Florida, is described. Therefore, a set of Bluetooth receivers was located at the roadside on specific streets to capture the Bluetooth MAC ID of crossing vehicles. But no paper is found, which analyze the ultimate problem of the usage of signatures to assure CAM integrity and authenticity. That issue is addressed here.

III. Secure V2X Communication

The ETSI specification [19] defines a basic set of applications for ITS, like active road safety (e.g., emergency vehicle warning), co-operative traffic effiency (e.g., regular speed), co-operative local services (e.g., automatic access control), and global internet services (e.g., fleet management).

To date, V2X broadcast communication based on IEEE 802.11p is provided. So, V2X is a short range communication technology with a communication range of about 600 m in open space.

The ETSI ITS architecture [19] distinguishes 4 different ITS station types: ITS roadside stations (typically termed road side unit), ITS vehicle stations, ITS central stations (e.g., traffic operator or service provider), and ITS personal stations (e.g., a handheld device of a cyclist or pedestrian such as a smart phone).

The ITS stations exchange information based on two different specified message types: Cooperative Awareness Message, and Dezentralized Environmental Notification Message.

ITS stations will be equipped with two classes of key pairs/certificates:

1) Long term key pairs (certificates) based on elliptic curve cryptography (ECC)
2) Pseudonymous ECC key pairs (certificates)

Based on the long term key pair an ITS vehicle station is able to authenticate itself, e.g., against a certification authority (Pseudonym Certification Authority termed Authorization Authority according to ETSI). Pseudonymous keys are used to secure the CAMs and DENMs mentioned in Section III-A respective Section III-B. It is assumed that pseudonymous keys and certificates are not directly linkable to an identity of an ITS vehicle station.

A. Cooperative Awareness Message

Cooperative Awareness Messages are comparable to beacon messages. They are broadcasted periodically with a packet generation rate of 1 up to 10 Hz. Based on received CAM

 ISBN: 978-1-61208-515-9

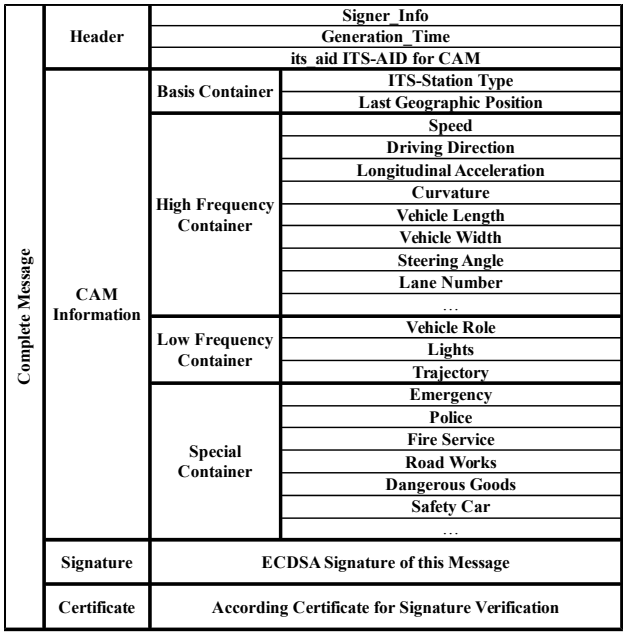


Figure 1. Examplary message format of a CAM. The CAM consists of a header, different data containers, e.g., the basis container, a signature and the appropriate certificate

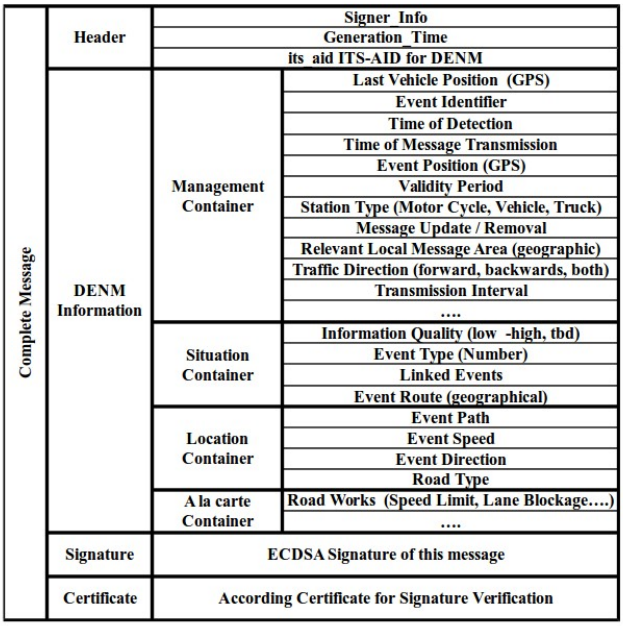


Figure 2. Examplary message format of a DENM. The DENM consists of a header, different data containers, e.g., the management container, a signature and the appropriate certificate.

messages, ITS vehicle stations can calculate a local dynamic traffic map of their environment. A CAM reveals a lot of dynamic information about the associated ITS vehicle station: geographic position, speed, driving direction, etc at a specific time. In addition, static information, e.g., the confidence levels of heading, speed, acceleration, curvature and yaw rate and the length and width of the ITS vehicle station are given. Length and width are stated with a precision of 10 centimeters.

To assure message integrity and authenticity CAMs contain an electronic signature and the appropriate certificate. As signature algorithm ECDSA, which operates on elliptic curves, is chosen. Then the receiver is able to cryptographically verify the message and check the temporal validity (temporary freshness).

It is not planned to forward CAM messages hop-to-hop. Figure 1 illustrates the structure of a Cooperative Awareness Message. The CAM is specified in detail in [20].

Regarding ECDSA based on the ECC domain parameter NIST P-256 a CAM without special container has a size of about 2 kbit. These 2 kbit are splitted into 200 bits for coding the basic -, high frequency - and low frequency container, 750 bits for the header and the ECDSA signature and nearly 1 kbit for a certificate according to the ETSI format [2]. So, only about 10 % of the whole CAM message size are needed for the data elements. The remainder 1,8 kbit are necessary for coding the CAM header, the ECDSA signature and the certificate of the appropriate public key.

B. Dezentralized Environmental Notification Message

In contrast, the second message type, Dezentralized Environmental Notification Messages (DENMs), are event-driven and indicate a specific safety situation, e.g., road works warning (from an ITS roadside station) or a damaged vehicle warning (from an ITS vehicle station). The DENM message format is specified in detail in [21]. DENM messages can be transmitted hop-by-hop. Figure 2 illustrates the structure of a Dezentralized Environmental Notification Message.

C. Pseudonymous Signatures

CAMs and DENMs should not reveal the identity of ITS vehicle stations (sender anonymity). Furthermore, it should not be possible to link messages of an ITS vehicle station (message unlinkability) over longer time periods. Both requirements shall be sufficient to assure location privacy of the ITS vehicle stations. Due to these privacy requirements, CAMs and DENMs are signed using pseudonymous ECC keys, which are not publicly linked to a vehicle. The pseudonymous ECC keys are randomly chosen. The used key for signing and the appropriate certificate are periodically changed during operation. Therefore, an ITS vehicle station needs a set of pseudonymous keys and certificates valid for some period of time. The set size of pseudonymous keys and certificates and the pseudonym change frequency are not specified in [22].

Moreover, the applied elliptic curve domain parameters (NIST P-256 or BrainpoolP-256r1) are such that ECDSA signatures are not foregable within the next years. Therefore, the effect of cryptographic signing of data is that the existence of this data is non-disputable. Especially, this means that sent CAMs are non-disputable.

Figure 3 depicts the usage of the pseudonyms. At time point t_0 pseudonym “1” is still used for signing the CAM. Then the used pseudonym is switched to pseudonym “2”. So, in contrast to time point t_0 at time point t_1 pseudonym “2” is used for signing during the next time frame.

 ISBN: 978-1-61208-515-9

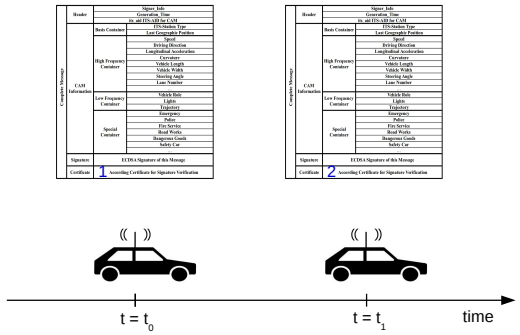


Figure 3. Switch pseudonymous keys for signing CAMs respective DENMs (pseudonym concept)

IV. ITS VEHICLE IDENTIFIER

Here, we categorize the available identifiers of vehicles into three classes. Primary vehicle identifier represent such identifiers which will be typically regarded today, e.g., the Vehicle Identification Number (VIN). Secondary vehicle identifier come up with new information technologies used in modern vehicles. Tertiary vehicle identifier are not sufficient to directly identify a vehicle but to link CAM respective DENM messages of an ITS vehicle station.

A. Primary Vehicle Identifier

To date, each vehicle is identifiable based on the distinct VIN. In some areas the VIN is integrated as human readable information in the windscreen of vehicles.

Besides the VIN, vehicles are marked with a licence plate. This is a further primary vehicle identifier, which is already used for identification.

With the deployment of the V2V technology vehicles will be equipped with a long term ECC key pair and an appropriate certificate. This certificate becomes an additional primary vehicle identifier.

B. Secondary Vehicle Identifier

Besides these obvious primary vehicle identifiers, vehicles have further identifiers. Modern vehicles are equipped with multi-media components, which are able to etablish communications with electronic devices of the driver or passengers. Typically, wireless communication technologies, e.g., bluetooth are used for that purpose. A bluetooth multi-media device emits a static 48 bit MAC identifier. The MAC ID is composed of two parts: the first half is assigned to the manufacturer of the device, and the second half is assigned to the specific device. In addition, each bluetooth device emits a “User-friendly-name” which is typically alterable. Bluetooth devices operate in the ISM band (2.4 to 2.485 GHz).

Moreover, vehicle-based wireless routers allow any Wi-Fi equipped laptop, tablet or mobile phone to access the internet within the ITS vehicle station while travelling if the router has mobile communications. But routers configured as access point need an unique Service Set Identifier (SSID) or network name to connect devices. According to the IEEE 802.11 workgroup, Wi-Fi can be used in following distinct frequency ranges: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands. Each range is divided into a multitude of channels. Countries apply their own regulations to the legitimate channels and maximum power levels within these frequency ranges. In addition, each wireless router has an unique MAC address. This is a further secondary vehicle identifier.

A Wi-Fi access point is accompanied by mobile communication. Mobile communication requires an International Mobile Subscriber Identity (IMSI). That is an unique identification number to identify a mobile device within the network. In addition, a SIM card with an assigned mobile phone number is needed for mobile communication.

Since the 1th of November 2014, vehicles and motorhomes have to be equipped with a Tyre Pressure Monitoring System (TPMS) within Europe. There exists direct and indirect TPMS. Direct TPMS means that specific physical sensors measure the air pressure of the tyres. These sensors communicate wireless with the vehicle and transmit an identifier of 28 to 32 bit length. There are different wireless technologies available for 125 kHz or 315 kHz respective 433 MHz. A detection range of up to 40 m for direct TPMS is mentioned in [23].

Initially, secondary vehicle identifier have no formal character in contrast to a licence plate or VIN. But it is technically very easy to capture Bluetooth MAC IDs and SSIDs of a vehicle and to link them to a vehicle because their primary application is to establish a communication with other devices. So, attacker can use them for their purpose.

C. Tertiary Vehicle Identifier

CAMs contain a lot of static information, like the vehicle length and vehicle width and the confidence level of heading, speed, acceleration, curvature, and yaw rate. These static information enable to link CAMs only based on the CAM data elements.

V. ANALYZATION OF THE V2V COMMUNICATION

From our point of view the main technical- and privacy problems arise with the periodically broadcasted CAMs. So, here in our analysis only CAMs are addressed.

A. Technical Issues

1) CAM data elements: A lot of CAM data elements are results of sensor measures, like: speed, driving direction, longitudinal acceleration, curvature. But sensors have only a defined precison level.

The geographic position is typically calculated based on satellite systems, like GPS. But spoofing attacks on GPS to influence the geographic position are possible. This issue is intensively analyzed in Tippenhauer et al. [24]. Open source code for software definded radio makes GPS spoofing attacks very realistic. The tool GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as bladeRF, HackRF, and USRP [25]. In addition, spoofing attacks on GPS can also influence the time synchronization for ITS vehicle stations.

For that, the data elements of received CAMs can only be regarded as additional information, which have to be verified by internal sensor measurements of the ITS vehicle station. Even when a receiver can cryptographically verify a

 ISBN: 978-1-61208-515-9

CAM respective DENM then the receiver only knows that the received data is broadcasted by an authentic ITS station and no error happend on the wireless transmission path of the data. Nevertheless the receiver can not really trust the CAM data due to the sensor accuracy and possibly attacks on the time value and geographic position as well as modifications of vehicular components.

2) Capacity of the IEEE802.11p channel: As shown in III-A only about 10% of the CAM size is used for coding the data, the remainder to assure integrity and authenticity of the data (ECDSA signature and certificate). So, the used technology to assure message authentication and integrity is very costly especially considering the fuzziness of the CAM data as shown in V-A1.

Even today collisions on the IEEE802.11p channel are feared in case of a large number of communicating ITS vehicle stations in a local area because all ITS station share only one frequency channel for the whole broadcast communication. But obviously we have to adapt the used key length to perform the ECDSA signature in future. Today, the NSA does not recommend to use the ECC domain NIST P-256 any more, due to the progress in quantum computing [26]. The next existing ECC domain parameters have key length of 384 bit. This extends the size of ECDSA signature from 512 to 768 bit. This means the CAM size will be increased from 2 kbit to 2,5 kbit because the signature of the certificate is affected, too. This will worsen the collision problem. Looking in the remote future (20 year ahead) we have to regard that quantum computers can possibly attack elliptic curve cryptography. There is large progress in research and construction of quantum computers based on semiconductors at the moment. Because vehicles have an operation time of about 15 - 20 years that issue has to be regarded in future, too. Although, no broadly accepted alternative post-quantum public key cryptography is ready for application, one consequence is very certain: in future new post-quantum public key cryptography have to use much longer keys compared to ECC today. This worsen the collision problem if ECDSA signatures should be replaced by post-quantum signatures algorithms.

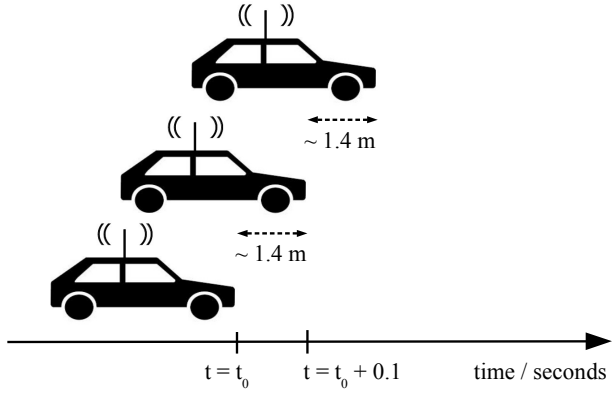
B. Security Issues

1) Jamming the IEEE802.11p channel: An attack, which can be performed very easy is jamming the 5.9 GHz wireless channel (with a strong sender). As consequence, it can not be assured that CAM and DENM messages reach the surrounded ITS vehicle stations in time.

2) Security Shortcomings of the ETSI Specifications: The ETSI certificate format provides only elliptic curve cryptography based on the NIST prime curve P-256. No mechanism is provided to securely adapt the key length or ECC domain parameters or cryptographic algorithms if necessary. In the meantime this issue is already termed: cryptographic agility. Additional security shortcomings concerning the necessary Public Key Infrastructure are explained in detail in [27].

C. Privacy Issues

1) Linkability of CAMs based on Certificates: Each CAM includes a pseudonymous certificate. The appropriate secret key is used to sign the CAMs for a short time frame, e.g., 15 minutes. As long as the same key for signing is used the appropriate certificate is static. So, this static information at the end of each CAM can be easily used to link CAMs of an ITS vehicle station. The pseudonym concept (change keys during operation) is applied to prohibit the linkability of CAMs after a pseudonym switch. But a linkability of CAMs is even possible based on the (static) CAM data elements shown next.



Assumptions: Speed: 50 km / h, CAM transmission frequency: 10 Hz

Figure 4. Movement of an ITS vehicle station within 100 ms based on a speed of 50 km/h

D. Linkability of CAMs based on the CAM data

The requested transmission rate for CAMs are 10 messages per second. Figure 4 illustrates that an ITS vehicle station moves on nearly 1.4 m in this case if the speed is 50 km/h. 50 km/h is the permitted speed in towns in Europe. Assuming an ITS vehicle station has a minimum length of 3 m: In that case the length of an ITS vehicle station overlaps at least 50% of the movement (1.4 m). If the ITS vehicle station is longer than 3 m it overlaps much more than 50%. So, no other ITS vehicle station can physically be at the same geographic position. This means, a linkability of CAMs of a specific ITS vehicle station is constituted only based on the geographic position of the CAMs respective DENMs. In addition, further static CAM data elements (e.g., vehicle length and vehicle width, and the confidence level of heading, speed, acceleration, curvature, and yaw rate) and the current speed (minor change within a time frame of 100 ms) are helpful to link the CAMs if the ITS vehicle station is much faster then 50 km/h. Furthermore, the trajectory (included in the low frequency container of the CAM) can be used to link CAMs of an ITS vehicle station.

These linkability of CAMs can be exploited to plot complete CAM traces of drives of a specific vehicle described in detail in [9].

Also, CAM traces can be bound to a vehicle, e.g, based on secondary identities. First practical measurements show that, e.g., bluetooth multi-media devices of analyzed vehicles of a specific german OEM have the “User-friendly-name” *OEM name* followed by a *figure space* and an individual five-figure number. The *five-figure number* are the last 5 figures of the VIN.

 ISBN: 978-1-61208-515-9

VI. CONCLUSION

Modern vehicles are already equipped with a lot of sensor elements to support driving assistance. That will be an ongoing process due to automated driving. ITS vehicle stations can trust data of internal vehicular sensors much more than the information contained in the received CAMs as shown in V-A. Additionally, an ITS vehicle station can not be sure that sent CAMs can be received in time, due to jamming or collisions on the wireless communication channel. For the reasons listed above, we argue that the V2V communication, especially CAMs, will not have this importance then expected. CAM data can only be an additional information, e.g., in invisible situations which have to be checked by the internal sensors. In addition, the concept to secure messages (ECDSA signature) and to verify them is very time consuming. In addition, a complex key management system is necessary to enrole the needed pseudonymous keys and certificates. Moreover, the signing of the data increase the CAM message size by a factor of 10. Finally, the mechanism to solve the privacy requirements (pseudonym concept) allows attackers to plot CAM traces of specific vehicles and drivers, which are non-disputable, due to the applied signatures with unique keys. So, the suggested pseudonym concept neglects the privacy requirements. In summary, it can be stated that a new V2V approach for the day-2 deployment of ITS vehicle stations is needed, which addresses the whole analyzed technical limitations and privacy shortcomings of the periodic sent CAMs. One possible direction is to use symmetric cryptography (message authentication codes) instead of electronic signatures, mentioned in [13].

In this paper, only the V2V communication, especially CAMs, are analyzed. In contrast, the adaptation of the ETSI communication to ITS roadside station - vehicle-2-infrastructure (V2I) - constituted in [27] is sound and can be broadly applied that way.

REFERENCES

[1] Car 2 Car Communication Consortium, “Mission, News, Documents,” 2015, https://www.car-2-car.org/, access date: November 02, 2016.

[2] ETSI, “Intelligent Transport Systems (ITS);Security; Security header and certificate formats, ETSI TS 103 097 V1.2.1,” 2013, http://www.etsi.org/, access date: November 02, 2016.

[3] European Commission, “SCOOP@F,” 2013, http://inea.ec.europa.eu/en/ten-t, access date: November 2, 2016.

[4] BMVI, “Cooperative its corridor rotterdam-franfurt-vienna joint deployment,” 2014, http://www.bmvi.de, access date: November 2, 2016.

[5] Vejdirektoratet, “NordicWay,” 2016, http://vejdirektoratet.dk/EN/roadsector/Nordicway/Pages/Default.aspx, access date: November 2, 2016.

[6] C-ITS Platform of the EC DG MOVE, “Final Report,” 2016, http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf, access date: November 2, 2016.

[7] Recommended Elliptic Curves For Federal Government Use, National Institute of Standards and Technology, 1999. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf, access date: November 02, 2016

[8] Brainpool.

[9] M. Ullmann, T. Strubbe, and C. Wieschebrink, “V2V Communication - Keeping You Under Non-Disputable Surveillance (Short Paper),” in Proceedings of the IEEE Vehicular Networking Conference(VNC), to appear. IEEE, 2016.

[10] G. Samara, W. A. Al-Salihy, and R. Sures, “Security analysis of vehicular ad hoc nerworks (vanet),” in Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on. IEEE, 2010, pp. 55–60.

[11] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for secure and private vehicular communications,” in Telecommunications, 2007. ITST’07. 7th International Conference on ITS. IEEE, 2007, pp. 1–6.

[12] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos et al., “Mix-zones for location privacy in vehicular networks,” in Proceedings of the first international workshop on wireless networking for intelligent transportation systems (Win-ITS), 2007.

[13] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” IEEE communications surveys & tutorials, vol. 17, no. 1, 2015, pp. 228–255.

[14] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” in Computational Science and Engineering, 2009. CSE’09. International Conference on, vol. 3. IEEE, 2009, pp. 139–145.

[15] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on. IEEE, 2010, pp. 176–183.

[16] S. S. Yang, Y. G. Kim, and H. Choi, “Vehicle identification using discrete spectrums in wireless sensor networks,” Journal of Networks, vol. 3, no. 4, 2008, pp. 51–63.

[17] S. Astapov and A. Riid, “A multistage procedure of mobile vehicle acoustic identification for single-sensor embedded device,” International Journal of Electronics and Telecommunications, vol. 59, no. 2, 2013, pp. 151–160.

[18] C. Carpenter, M. Fowler, and T. Adler, “Generating route-specific origin-destination tables using bluetooth technology,” Transportation Research Record: Journal of the Transportation Research Board, no. 2308, 2012, pp. 96–102.

[19] ETSI, “ETSI EN 302 665 V1.1.1: Intelligent Transport Systems (ITS) - Communications Architecture,” 2010, http://www.etsi.org/, access date: November 02, 2016.

[20] ——, “ETSI EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service,” 2015, http://www.etsi.org/, access date: November 02, 2016.

[21] ——, “ETSI TS 102 637-3 V1.2.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service,” 2010, http://www.etsi.org/, access date: November 02, 2016.

[22] N. Bissmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, “A generic public key infrastructure for securing car-to-x communication,” in 18th ITS World Congress, 2011.

[23] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, “Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study,” in 19th USENIX Security Symposium, Washington DC, 2010, pp. 11–13.

[24] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful gps spoofing attacks,” in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 75–86.

[25] T. Ebinuma, “Gps-sdr-sim,” GitHub, 2015, https://github.com/osqzss/gps-sdr-sim, access date: Novemver 2, 2016.

[26] National Security Agency, “Cryptography today,” 2015, https://www.nsa.gov/ia/programs/suiteb_cryptography, access data: November 02, 2016.

[27] M. Ullmann, T. Strubbe, C. Wieschebrink, and D. Kügler, “Secure Vehicle-to-Infrastructure Communication: Secure Roadside Stations, Key Management, and Crypto Agility,” in International Journal On Advances in Security, vol 9 no 12. IARIA, 2016, pp. 80–89.

 ISBN: 978-1-61208-515-9

Evaluating the Impact of Electric Vehicles on the Smart Grid

Roozbeh Jalali, Zachary Hills, Khalil El-Khatib,
Richard W. Pazzi, Daniel Hoornweg
University of Ontario Institute of Technology
Oshawa, Ontario, Canada
(Roozbeh.Jalali, Zachary.Hills, Khalil.El-Khatib,
Richard.Pazzi, Daniel.Hoornweg)@uoit.ca

Kevin Myers
Veridian Connections
Ajax, Ontario, Canada
Kmyers@veridian.on.ca

***Abstract*— With the 23% of total global GreenHouse Gas (GHG) emissions coming from the transport sector, many initiatives have been suggested to address this emissions sector, including reducing the number of vehicles on the roads using ridesharing programs, and switching from Internal Combustion Engine Vehicles (ICEV) to battery powered Electrical Vehicles (EV). While many governments around the world have started various programs to help increase the adoption of EVs, including incentive to purchase, introducing new policies, increasing public awareness, and installing charging infrastructures, the impact of EVs on the electric grid (load, harmonic, line and transformer lifespan) is still not completely understood. In this paper, we present a literature review about the impact of EV on the electric grid, and the evaluation results carried on the grid on a small community in the Greater Toronto Area (GTA). The results of the evaluation show a 12.5% increase in overloaded transformers within the simulated city.**

Keywords-Electrical vehicle; Energy management; Smart grid.

I. INTRODUCTION

Over the last few decades, there has been an increase in GHG emission from various sectors, because of fossil fuel use. This increase in GHG has resulted in an increase of some 0.8°C and likely over 2°C this century, and the amount of GHG emission is expected to double by 2050 if fossil burning continues at the current rate. Much of the emission is attributed to vehicles that use fossil fuel in their internal combustion engines. In Canada, GHG emission from the transport sector accounts for around 23% of the total GHG emissions in Canada in 2013, second only to the oil and gas sector.

To help reduce greenhouse emissions from the transport sector, several new technologies (e.g., Plug-in Electrical Vehicles (PEVs) and buses, natural gas fueled buses) and community services (e.g., ridesharing) are currently proposed and being tested. Each of these alternatives has social, economic, technical, and environmental impacts, as well as business opportunities. Of interest to this paper is the PEVs. These vehicles can use electricity stored in battery packs instead of fuel, and can be recharged from the electrical grid. These vehicles have potential for lower cost for operation, with minimal or no air pollution and GHG emissions [1]. In addition, using EV can also improve the efficiency, stability, and reliability of the grid [2].

While EV's can help reducing GHG, their effect on the electric grid is still not yet completely understood. The main objective of this paper is to present literature review about the impact of EV on the electric grid, and the evaluation results carried on the grid on a small community in the GTA. The rest of the paper is organized as follow: Section 2 presents a literature review on the effect of EV on smart grid. The results of a simulation exercise on a small community smart grid is provided in Section 3, and a conclusion is presented in Section 4.

II. LITERATURE REVIEW

Electrical Vehicles have been recognized as an alternative that can diminish toxin and gas emissions. Because of their high-energy capacity and potential mass production, electrical vehicles will have critical impact on power networks, electricity cost, power transmission and distribution. Since this kind of vehicles are not popular yet, it is important to study their energy consumption and their impact on the electricity infrastructure, which can help in to plan for development of the infrastructure. Studies show that increasing number of EVs have significant impact on transformer life specially in residential area and may require more investment on electricity infrastructure [3].

There has been some research work on the impact of EVs on smart grid in the literature. General effects of EVs on grid surveyed by [4] upon their characteristics. These characteristics are divided into two different categories: vehicle characteristic and charging characteristics. Most of the research is geared toward considering three main factors when they estimate the impact of EVs on grid. These three factors are charging location, charging demand and charging moment [5]. Charging location indicates the site where the EV connect for charging. It can be residential area, working place, urban area or even rural area. Charging demand reflects the model that is used by EVs to consume electricity, which was stored on their batteries. Charging moment represents the model that is used to charge the vehicle. There are also additional factors that can have indirect effects on the grid, such as driving habits, mobility pattern, etc.

Early research work used simple methods to model vehicle behavior, mobility pattern and charging demand [6][7][8][9]. For instance, the Shao et al. [9] reviewed the

 ISBN: 978-1-61208-515-9

impact of EVs on distribution network at Blacksburg residential area. They considered five houses and two electrical vehicles and applied different charging strategies to see the effect of charging on transformer. The study showed that in the worst-case scenario, charging the EVs can increase transformer load by 68 percent. They also show that if quick charging is used, it can easily overload the transformer.

Recent research studies use complex methods and more factors to model the effect of EVs on the grid [10][11][12] [2]. For example, Razeghi et al. [2] modeled the residential electricity demand based on household and EVs data. Household factors which used are average daily miles travel, arrival and departure time, number of available vehicle per household and number of trips per day. EVs data is also categorized based on the type of charging and consumption model. Razeghi et al. [2] then developed a thermal model to find the grid hot spots and calculate the loss of life of all transformers. Based on the simulation on southern California residential neighborhood, they claimed that uncontrolled level 1 charging has a little effect on transformers life but uncontrolled level 2 charging will result high transformer aging rate and probably transformers failure.

Hilshey, et al., [13] have similar findings to [2] with some little differences. The authors used Monte Carlo model to predict transformers life and aging when EVs charged with level 1 and level 2 charging in Phoenix and Burlington residential area. In addition to prediction model, Hilsey et al. [13] presented a new strategy for decentralized autonomous charging. This autonomous charging model can keep the transformers power to nominal or acceptable limit value.

Clement-Nyns, et al., [14] used driving pattern and road traffic to find the impact of vehicles on Belgium distribution network. They considered two different scenarios for charging. In the first scenario vehicles are charged between 6:00 to 8:00 pm and in the second scenario they are charged at the midnight (2:00am). The paper concluded that charging pattern and charging characteristic can significantly effect on transformers load and consequently effect on distribution network.

The impact of EVs on the smart grid was also studied in different areas worldwide such as the work presented in [15][16][17]. In Canada, Maitra et al., [18] evaluated the impacts of EVs on Hydro- Quebec power network. They considered multiple factors in their evaluation such as battery type, charging scenario, demands, etc.

Some research work proposed the use of statistical information to model household characteristic such as the work in [19], which considered area population, people per house, number of vehicle each household has and EVs penetration rate as a simulation factor. Other research used historical data as load profile and quadratic programming to forecast transformer failure and overloading [14].

III. SIMULATION RESULTS

In this section, we will present the design of a simulation tool that was used by Veridian Connections, a local distribution company, to evaluate how their electric grid performs under various degrees of EV adoption rates. Based on mobility models of residents, the work investigated the EV specific requirements, and local grid system capabilities, in one community in the GTA communities as personal transportation is electrified. The work focused on assessing the grid performance, as personal vehicles move to electric vehicles, EVs, by 5%, 15% and 50% of total fleet over 20 years. A simulation tool was developed and used to inform projections for a GTA-wide roll-out of EVs in terms of grid capacities, life-cycle impacts, and specific household impacts under a province-wide carbon tax or Emissions Trading System (ETS) [20].

To identify the effect of various percentage of EV penetration on the electric grid (load, harmonic, line and transformer lifespan), data about how people commute in the designated community, as well as information about the electric grid needed to be modeled and used to run different simulations using various simulations tools (ns-2 and CYME). The details of the work included the following ordered steps:

- Step 1: Analysis of current traffic and driving patterns from the Transportation Tomorrow Survey (TTS) database and building mobility models of drivers, which include the number and mode of trips (use standard engineering practice, and modeling tools to enable replication across jurisdictions).
- Step 2: Gathering information on different various charging/discharging models for various electric vehicles. Vet (and possibly obtain) data through Local Distribution Companies (LDC), Veridian Connections and Toronto Hydro.
- Step 3: Running various simulations using the *ns-2* simulation tool to incorporate the mobility and charging/discharging models, and various EV penetration rates to compute the load that electric vehicles can add to the grid.

Running the simulation, we have performed the following tasks:

A. *Loading Traffic and Transformers Profile*

The simulated area was divided into four wards; each ward has its own traffic behavior. Based on the traffic data, electrical vehicles were loaded into the map and given a destination for their route that relates to the data (Fig. 1). For this simulation, the highest load period in December was selected and the hourly transformer data was loaded into the simulation as the base load. The simulation covered a 24-hour period. Maps are constructed based on OSM files, for the purposes.

B. *Electrical vehicle specifications*

The simulation was set so that each electrical vehicle begins with a full charge. The simulation had a range of battery capacities depending on the type of vehicle. The batteries range from 18 kWh to 80 kWh. The vehicles supported are: Tesla, Volt, Leaf, Kia Soul.

 ISBN: 978-1-61208-515-9

TRIPS MADE BY RESIDENTS OF TOWN OF AJAX																
Time Period	Trips	% 24 hr	Trip Purpose				Mode of Travel						Median Trip Length (km)			
			HB-W	HB-S	HB-D	N-HB	Driver	Pass.	Transit	GO Train	Wlk & Cy	Other	Driver	Pass.	Transit	GO Train
6-9 AM	59,700	25.4%	41%	22%	23%	14%	62%	13%	5%	9%	7%	3%	9.0	2.7	14.5	36.8
24 Hours	235,000		31%	13%	39%	17%	67%	16%	4%	5%	5%	2%	5.3	3.7	14.2	36.7

Figure 1. Traffic Profile for Simulated Area.

C. Assumptions

Most people will charge their vehicles after work or before they go to bed. Therefore, it is a reasonable assumption that most cars will be plugged in from 6:00 pm to 5:00 am. Due to technical restraints, this simulation will have no electrical vehicles from other cities commuting to the simulated city to charge. All the electrical vehicles will be residents of the town of Ajax.

D. Charging

Vehicles are assumed to connect to a transformer that is within 250 meters away or less to the charge. If no transformers are near, that vehicle is disregarded from the simulation. All vehicles are under the assumption that they use stage 2 charging. There are 118 potential transformers used in our simulation. The rate of charging specific to a car is added to the base load depending on the battery level.

E. Simulation Scenario

Vehicles are loaded into the simulation beginning at hour 24:01. The simulation covers a 24-hour period. Simulated vehicles have normal behaviors and routes, waiting at red lights, obeying traffic speed limits, traffic congestion. The collected traffic data is confined to four wards; the simulation was built with wards to emulate the data. Vehicles are brought into the simulation based on the data from that ward. For this simulation, 10% of vehicles are electric (penetration rate). Electrical vehicles behaved the same as combustion vehicles, however at the end of their route, electric vehicles check to see if a transformer is nearby to charge.

F. Experimental Results

Out of the 118 transformers in the simulated area, the largest amount with EV connected to was 48 (Fig. 2), among those 48 there was an average load increase of 27.222 kW. Out of the 48 transformers, 12.5% were overloaded (Fig. 3). The results represent the highest peak of transformer loads within the 24-hour simulation.

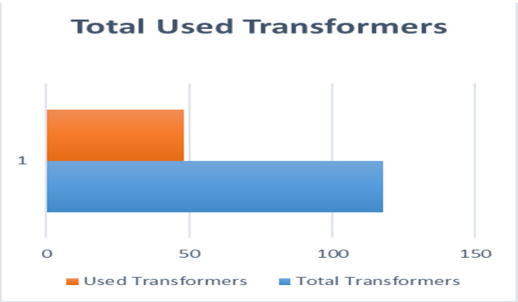


Figure 2. Total used transformer.

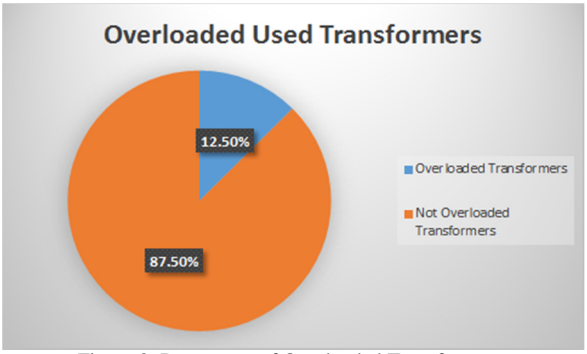


Figure 3. Percentage of Overloaded Transformers.

IV. CONCLUSION

To help curb GHG emissions, governments around the world started considering various ways to reduce the number of ICEV on the roads, including improving public transport, introducing High Occupancy Vehicle (HOV) lanes, and tolls on vehicles. However, the results of these approaches are not well documented. This paper presented a literature review on the impact of EV on the electric grid and the preliminary experimental results of varying degree of penetration rate on the electric grid of a local community in the GTA.

ACKNOWLEDGMENT

This research was partially supported by The George Cedric Metcalf Charitable Foundation.

REFERENCES

[1] G. Razeghi, T. Brown, and G. S. Samuelsen, "The impact of plug-in vehicles on greenhouse gas and criteria pollutants emissions in an urban air shed using a spatially and temporally resolved dispatch model," Journal of Power Sources, vol. 196, pp. 10387-10394, 2011.

[2] G. Razeghi, L. Zhang, T. Brown, and S. Samuelsen, "Impacts of plug-in hybrid electric vehicles on a residential transformer using stochastic and empirical analysis," Journal of Power Sources, vol. 252, pp. 277-285, 2014.

[3] C. Roe, E. Farantatos, J. Meisel, A. Meliopoulos, and T. Overbye, "Power system level impacts of PHEVs," in System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on, pp. 1-10, 2009.

[4] S. W. Hadley, "Impact of plug-in hybrid vehicles on the electric grid," ORNL Report Oct 2006 [Online]. Available: http://apps.ornl.gov/~pts/prod/pubs/ldoc3198-plug-in-paper-final.pdf.

[5] P. Grahn, "Electric vehicle charging impact on load profile," BSc. Thesis, Department of Electrical Engineering, Royal Institute of Technology, Stockholm, Sweden, 2013

[6] S. W. Hadley and A. A. Tsvetkova, "Potential impacts of plug-in hybrid electric vehicles on regional power generation," The Electricity Journal, vol. 22, pp. 56-68, 2009.

[7] K. Parks, P. Denholm, and A. J. Markel, "Costs and emissions associated with plug-in hybrid electric vehicle charging in the Xcel

 ISBN: 978-1-61208-515-9

Energy Colorado service territory," ed: National Renewable Energy Laboratory Golden, CO, 2007.

[8] D. Lemoine, D. Kammen, and A. Farrell, "Effects of plug-in hybrid electric vehicles in California energy markets," in 86th Annual Meeting of the Transportation Research Board, Washington, DC, 2007.

[9] S. Shao, M. Pipattanasomporn, and S. Rahman, "Challenges of PHEV penetration to the residential distribution network," in 2009 IEEE Power & Energy Society General Meeting, pp. 1-8, 2009.

[10] A. Ashtari, E. Bibeau, S. Shahidinejad, and T. Molinski, "PEV charging profile prediction and analysis based on vehicle usage data," IEEE Transactions on Smart Grid, vol. 3, pp. 341-350, 2012.

[11] Q. Gong, S. Midlam-Mohler, V. Marano, and G. Rizzoni, "Study of PEV charging on residential distribution transformer life," IEEE Transactions on Smart Grid, vol. 1, pp. 404-412, 2012.

[12] D. Wu, D. C. Aliprantis, and K. Gkritza, "Electric energy and power consumption by light-duty plug-in electric vehicles," IEEE transactions on power systems, vol. 26, pp. 738-746, 2011.

[13] A. D. Hilshey, P. Rezaei, P. D. Hines, and J. Frolik, "Electric vehicle charging: Transformer impacts and smart, decentralized solutions," in 2012 IEEE Power and Energy Society General Meeting, pp. 1-8, 2012.

[14] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug-in hybrid electric vehicles on a residential distribution grid," IEEE Transactions on Power Systems, vol. 25, pp. 371-380, 2010.

[15] A. Karnama, "Analysis of integration of plug-in hybrid electric vehicles in the distribution grid," Master's thesis, Royal Institute of Technology, Stockholm, Sweden, 2009

[16] M. Galus R. A. Waraich M. Balmer G. Andersson K. W. Axhausen "A framework for investigating the impact of PHEVs," in Proceedings of International Advanced Mobility Forum (IAMF), March 2009.

[17] M. D. Galus and G. Andersson, "Demand management of grid connected plug-in hybrid electric vehicles (PHEV)," in Energy 2030 Conference, 2008. ENERGY 2008. IEEE, pp. 1-8, 2008.

[18] A. Maitra, K. S. Kook, J. Taylor, and A. Giumento, "Grid impacts of plug-in electric vehicles on Hydro Quebec's distribution system," in IEEE PES T&D 2010, pp. 1-7, 2010.

[19] S. L. Judd and T. J. Overbye, "An evaluation of PHEV contributions to power system disturbances and economics," in Power Symposium, 2008. NAPS'08. 40th North American, pp. 1-8, 2008.

[20] C. Kennedy, N. Ibrahim, and D. Hoornweg, "Low-carbon infrastructure strategies for cities," Nature Climate Change, vol. 4, pp. 343-346, 2014.

 ISBN: 978-1-61208-515-9