OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

INF FAKULTÄT FÜR INFORMATIK

18. GI/ITG KuVS **F**ach**G**espräch **S**ensor**N**etze

FGSN 2019

PROGRAMM

19. SEPTEMBER – 20. SEPTEMBER

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Conference Chair

Prof. Dr. rer. nat. Mesut Güneş
Universitätsplatz 2
39016 Magdeburg
e-mail: mesut.guenes@ovgu.de

Organisation

Frank Engelhardt
Universitätsplatz 2
39016 Magdeburg
e-mail: frank.engelhardt@ovgu.de

Katja Nothnagel
Universitätsplatz 2
39016 Magdeburg
e-mail: katja.nothnagel@ovgu.de

Preface

It is our great pleasure to welcome you to FGSN 2019, the 18. GI/ITG KuVS Fachgespräch Sensornetze. Welcome also to the city of Magdeburg and the Otto-von-Guericke University Magdeburg (OVGU).

The FGSN Workshop series has already a long tradition to serve as a forum for the discussion of research on Wireless Sensor Networks, Wireless Multi-hop Networks, Internet of Things, and other related topics, where especially (resource constrained) wireless nodes interact with different types of environments. This tradition will be continued this year with an interesting program consisting out of 13 paper presentations, 4 demo papers, and a hands-on tutorial on RIOT OS, all covering highly relevant and recent research topics. We are convinced that this will lead to a highly interactive workshop with lively discussions and intense exchange among all participants.

We thank all those who contributed to FGSN 2019 and making this workshop possible: the authors for submitting their work to the workshop, the program committee members for reviewing the papers, and the organizing team, especially Frank Engelhardt, Katja Nothnagel, Jürgen Lehmann, Marian Buschsieweke, Kai Kientopf, Petra Duckstein, but also all the others from ComSys@OVGU who contributed to the workshop organization.

The major value of workshops is to enable discussions among researchers and to allow for the exchange of ideas, which should result in new thoughts, insights, and research ideas. We hope that the FGSN 2019 contributes to this and that you will enjoy the event.

Mesut Güneş
FGSN 2019 Chair

Program Committee

- Sebastian Feld, Ludwig Maximilian University of Munich
- Reinhardt Karnapke, Brandenburg University of Technology Cottbus
- Mesut Güneş, Otto von Guericke Universität Magdeburg
- Doreen Boehnstedt, TU Darmstadt
- Lars Wolf, TU Baunschweig
- Christian Renner, Universität zu Lübeck
- Andreas Reinhardt, TU Clausthal
- Bettina Schnor, University of Potsdam
- Anna Förster, University of Bremen
- Kay Roemer, TU Graz
- Björn Scheuermann, Humboldt University of Berlin
- Christian Bettstetter, University of Klagenfurt
- Karin Anna Hummel, JKU Linz
- Thomas Schmidt, HAW Hamburg
- Oliver Hahm, RIOT OS / Zühlke
- Torsten Braun, Universität Bern
- Matthias Wählisch, Freie Universität Berlin
- Kurt Tutschku, Blekinge Institute of Technology (BTH)
- Jochen Schiller, FU Berlin
- Joerg Nolte, BTU Cottbus
- Matthias Hollick, TU Darmstadt
- Mario Schölzel, Universität Potsdam / IHP Frankfurt (Oder)
- Ruediger Kapitza, TU Braunschweig
- Alexander von Bodisco, University of Applied Science Augsburg
- Claudia Linnhof-Popien, Ludwig-Maximilian-University Munich
- Reiner Kolla, Julius-Maximilians-Universität Würzburg

Contents

Evaluating the Suitability of LoRa for Potato Storage Monitoring

Jan Schlichter, Björn Gernert and Lars C. Wolf
Institute of Operating Systems and Computer Networks
Technische Universität Braunschweig
Braunschweig, Germany
Email: [schlichter | gernert | wolf]@ibr.cs.tu-bs.de

***Abstract*— In order to minimize the loss of crops during the storage period, food storage need to be equipped with an air conditioning system. To guarantee correct operation of the system, detailed temperature and humidity data from the inside of the stored good is required. State of the art systems only use data collected from sensors placed on top of storage boxes, which contain the crops. Therefore, they are not able to measure the conditions inside the boxes, which means that air conditioning can only be carried out on an estimated basis.**

In this paper a sensor node for food storage is introduced which can be equipped with different radios and uses delay and disruption tolerant (DTN) multihop communication to collect data from inside of the storage boxes. The evaluation of the developed sensor node is carried out exemplary inside a *real potato storage*, since the high water content in the potato (approx. 80%) creates a challenging environment for wireless communication. Of course, the sensor can also be applied to other stored goods. For the evaluation, the node was equipped with a LoRa radio and it was recorded how feasible a communication within a food storage is compared to a node equipped with a FSK radio.

I. Introduction

Many agricultural products are stored for several month after the harvest, so they can be sold over longer time periods. During the storage period it is important to carefully adjust the storage conditions to minimize the loss due to diseases e.g. soft rot and other factors like waterloss, which results in a lower selling price. In potato storage various harmful conditions like a small change in temperature, which can lead to a loss of over 3% [1], can be detected by sensors. This also applies to diseases like soft rot, which can be detected by measuring the CO_2 concentration inside of the potato storage [2].

Up to now it is common practice to use wired temperature and humidity sensors outside of the boxes or clamps in which potatoes are stored. The size of modern storage warehouses implies the difficulty to comprehensively monitor the storage conditions.

To solve this problem *StorageLogger* is introduced, a wireless sensor node which is able to measure storage conditions directly in the boxes or clamps. Radio communication through potatoes is difficult due to the high water share of the potatoes and implies that measured data needs to be forwarded from one node to another to collect all data at a sink. Furthermore it is common that boxes, which contain the potatoes and sensor nodes, are restacked multiple times in a different order during a storage period. This means that a static network topology is not given and the nodes must act based on their current location.

Another factor, which needs to be considered, is energy consumption. It is impossible to change the battery of the deployed sensor nodes without manually pouring them, and accordingly also potatoes, out of the storage box. This makes it impractical to replace batteries during the storage period. Thus, the aim is to monitor a whole storage period with one set of batteries.

Due to a modular design the sensor node can be equipped with different radios. The focus of this paper is to evaluate the suitability of using a LoRa radio for communication between the sensor nodes. To achieve this two versions of the sensor node were considered, one with a $433\,\mathrm{MHz}$ frequency-shift keying (FSK) radio and one with a $433\,\mathrm{MHz}$ LoRa radio.

The paper is organized as follows. First, an overview about the related work and groundwork for this paper in section II is given. The different versions of sensor node and the used components are described in section III. Section IV shows the results of a real-world evaluation for which different versions of the nodes were deployed at the "Versuchsstation Dethlingen"[1] (VSD), a research station specialized on potatoes. Finally section V concludes this paper.

II. Related Work

This paper is based on the findings and experiences published by the authors in [3]. In this paper different radio frequencies for data transmission in potato warehouses were examined. First a wall of potatoes was simulated and hit with a planar incident wave at different frequencies to look at the attenuation caused by the potatoes. The simulation results were then validated by building a real wall of potatoes and trying different frequencies to penetrate the wall. The setup is shown in Figure 1 and consists of 16 potato boxes (each $1.2\,\mathrm{m}$ x $1\,\mathrm{m}$ x $0.85\,\mathrm{m}$ (WxDxH)) and two Vivaldi antennas. The simulation and experimental setup have shown that the attenuation of potatoes is quite high and that the path of the radio waves does not necessarily go directly through the potatoes but through the small gaps between the stored potatoes. In regards to the design of the *StorageLogger* node the possible frequencies

[1] http://www.vsd-dethlingen.de

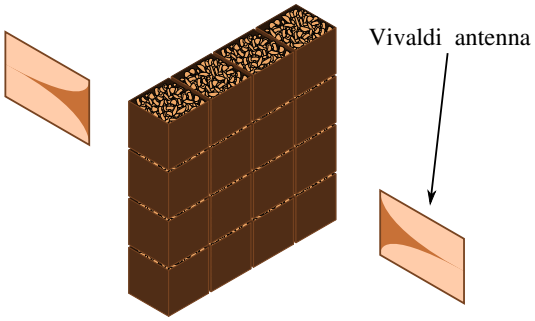


Fig. 1. Test setup used in [3]

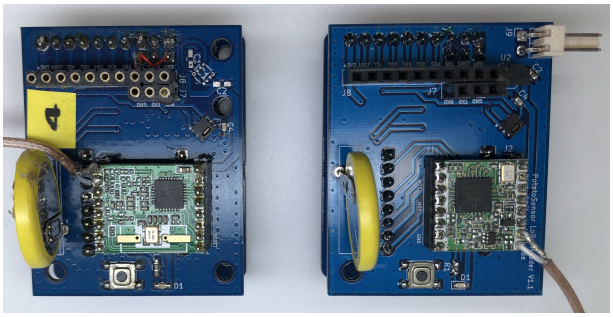


Fig. 2. *StorageLogger* node version 1 (left), version 2 (right)

which can be used are limited to the ISM band. The previous work conclude that 433 MHz, with a attenuation of 22 dB per meter, yields the best results for this constraint.

Based on this findings *StorageLogger* can be used with two different 433 MHz radios. The first one uses the FSK modulation scheme and the second one the LoRa modulation scheme. The differences are described in section III.

Another example for a food storage monitoring system is described by Tervonen in [4]. The author equipped sensor nodes with a 868 MHz radio and three AA-batteries. They were used to measure the temperature and humidity inside a warehouse for seed potatoes every 16 min over a period of ten weeks. The main difference between this system and the *StorageLogger* nodes is the placement of the nodes and the resulting network topology. Tervonen placed the sensor nodes outside of the potato boxes on different levels of the storage warehouse and was able to build a star with one sink wirelessly connected to all other nodes. Since in the case of the *StorageLogger* the nodes were placed inside the boxes, a direct communication with the sink is way more challenging and simply not possible for some of the placed nodes. Apart from the changes of the used radio to increase the range of the nodes inside of the boxes, a network protocol is needed to deliver the multihop communication for the *StorageLogger* setup. However, as this is out of scope of this paper, the definition of a corresponding protocol is left out at this point.

In view of the overall vision that one sensor node could be used to monitor the whole lifecycle of a potato from the field to the storage, it is important to keep applications outside of monitoring the storage in mind. There are many authors like Heble et al. [5], who proposed LoRa based networks for monitoring large agriculture fields. The usage of LoRa for our *StorageLogger* nodes enables an easy adaption of such a network architecture increasing the possible applications beyond storage monitoring.

III. The StorageLogger Node

This paper discusses two different versions of the *StorageLogger* node. It features a modular design consisting of a baseboard and a headerboard. The baseboard remains the same for both versions and was developed on the basis of the INGA [6]. It features a Atmega MEGA1284P-MU which runs Contiki OS.

The difference between the versions is the usage of a different headerboard. They both have a shared set of components like a real time clock and an SHT21 temperature and humidity sensor, enabling the basic functionality of the *StorageLogger*. This functionality includes measuring the temperature and humidity in a configurable time interval and going to sleep between those measurements. Aside from the shared set of components and some minor design changes between the versions, the big difference is the usage of a different radio. The first version, shown on the left side in Figure 2, features a RFM69 433 MHz FSK radio, while the second version (on the right of Figure 2) supports a RFM96 433 MHz LoRa radio.

To specify which version is used, a simple compiler flag can be set which causes Contiki to use the proper driver.

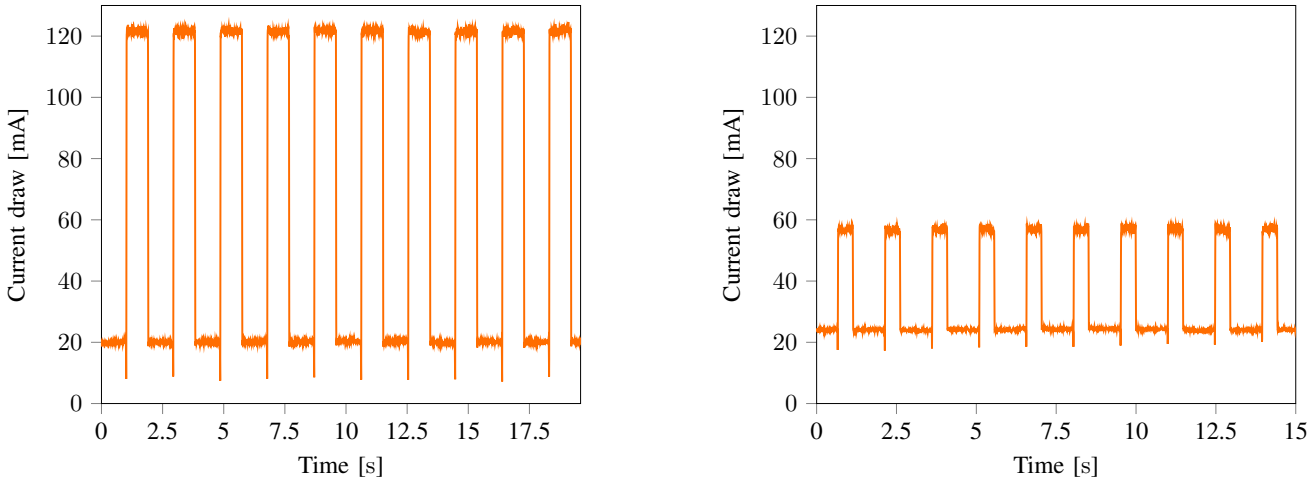
IV. Evaluation

For the evaluation of the suitability of using a LoRa radio for communication inside of a potato storage facility, a comparison of the two versions of the *StorageLogger* sensor node was carried out. Both radios were equipped with a 18 cm dipole antenna, which roughly translates to $\frac{\lambda}{4}$ for the wavelength $\lambda = 69cm$ of a 433 MHz wave.

A. Comparison of the Radios

First the two radios were compared outside of the storage monitoring scenario by three metrics: transmission speed, transmission range and current draw.

The transmission speed and range varies greatly based on the configuration of the radios. To make the results comparable the same configuration was used for both radios as far as possible. Due to the LoRa modulation scheme the RFM96 has more configuration possibilities with additional settings like coding rate (CR) and spreading factor (SF). The challenge of finding the best transmission parameters for LoRa radios was already discussed by Bor and Roedig in [7]. There are over 6720 possible parameter settings and a bad choice may result in a 100 times shorter node lifetime due to higher current draw. For this evaluation the following settings were used: $SF = 12$ and $CR = (4/8)$. The bandwidth was set to 500 kHz for both radios.



(a) StorageLogger node with LoRa radio

(b) StorageLogger node with FSK radio

Fig. 3. Current draw during the transmission of ten radio frames with (a) the LoRa radio and (b) the FSK radio

Figure 3 shows the overall current draw of a sensor node equipped with the LoRa radio and a node equipped with the FSK radio both operating at 3.3 V. In both cases the radios were transmitting ten frames with a size of 64 B each and a 1 s period between the transmissions. The transmission of all frames was completed in less than 15 s by the FSK radio and required nearly 20 s on the LoRa radio due to the slightly lower transmission speed of the LoRa radio. The procedure of sending a radio frame is the same for both radios. It starts with setting the radio from RX mode to standby to write the frame to the FIFO of the radio. In RX mode the current draw of the LoRa node is slightly lower than the draw of the FSK node with a value of around 20 mA. The value drops further down for both nodes in standby mode. After the frame is written to the FIFO the radio is set to TX mode, which triggers the transmission. While in TX mode the current draw of the LoRa node is around 120 mA which is significantly higher than the draw of the FSK node with about 60 mA.

The benefit of using the LoRa version despite the higher current draw and lower transmission speed is an increased transmission range. The maximum transmission range of LoRa radios has already been discussed in great detail by other authors and is generally around 10 km depending on the surroundings of the sensor nodes. To compare the package loss of the used radios we applied a similar setup like Petäjäjärvi et al. used in [8]. A base station containing a node with LoRa radio and a node with FSK radio was mounted on top of a building (height: 59 m) in Braunschweig[2]. Each node of the base station periodically sends a beacon with a size of 64 B, which was captured with a mobile version of the base station.

The mobile node was moved along a track, moving away from the base station, with a maximum distance of 3.85 km between them. The track was then divided into different sections and the frame loss was calculated for each section

[2]Latitude: 52.272921 Longitude: 10.525355

TABLE I
FRAME LOSS OF THE RFM96 LORA RADIO AND THE RFM69 FSK RADIO FOR DIFFERENT TRANSMISSION RANGES

Section	LoRa	FSK
0 m - 500 m	12.13%	28.96%
500 m - 1000 m	17.07%	66.50%
1000 m - 1500 m	41.18%	93.72%
1500 m - 2000 m	41.62%	88.31%
2000 m - 2500 m	30.37%	89.35%
2500 m - 3000 m	41.01%	90.58%
3000 m +	67.74%	98.95%
Overall	**36.23%**	**76.48%**

with over 1300 beacons send in total per node. The results are shown in Table I. It becomes clear that the LoRa radio has a lower frame loss in every single section of the track. After 1000 m the frame loss of the FSK radio goes up rapidly and drops by a few points in the 1500 m - 2000 m section. This is due to the surroundings of the track, namely a large building, which blocked the line of sight between the base station and the mobile node, while traveling through the 1000 m - 1500 m section. The drop is also visible in the data for the LoRa radio, even though it is not nearly as substantial as with the FSK radio. Overall the frame loss of the LoRa radio is less than the loss of the FSK radio. Especially at the 3000 m + section it is impossible to get a reliable connection with the FSK radio.

When comparing this result to other experiments like the one of Petäjäjärvi et al. [8] it is important to consider the different environmental factors. The experiment in this paper was carried out in a city with potential interferences and large buildings partly blocking the line of side. This results in higher frame loss rates than in less crowded areas.

B. Real-World Evaluation

Both versions of the sensor node were deployed in a research storage of the VSD, for comparison under real-world conditions. The storage is shown in Figure 4 and consists of

Fig. 4. Potato storage of the VSD

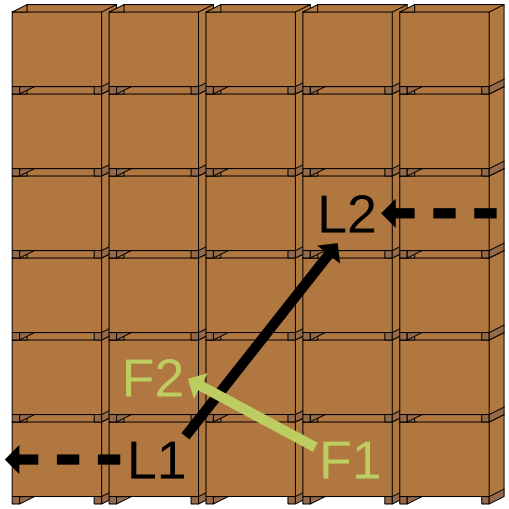


Fig. 5. Longest achived single hop communication path

four rows and six columns of potato boxes. The dimensions of the boxes are 1.2 m x 1 m x 0.85 m (WxDxH), with 20 cm between the rows. As seen in the picture, there are gaps between the stored boxes and the walls of the storage facility to all sides, enabling the potential reflection of radio waves inside the storage facility.

Two experiments were conducted, one for each version of the sensor node. For the first experiment ten sensor nodes with the FSK radio were deployed into one row of the storage in such a way that there is at least one box on each side of the box with the sensor node. The sensor node with the LoRa radio was deployed for the second experiment in a similar way.

Figure 5 shows the longest archived single hop communication path for both experiments. For the FSK nodes the maximum distance that could be covered was between nodes F1 and F2 at around 220 cm.

In comparison the longest distance between two nodes covered by LoRa is represented by the nodes L1 and L2, with a distance of approximately 320 cm (pictured by the solid black arrow) between each other. The radio waves do not necessarily spread on the direct path between the nodes, but could also spread to the left from node L1 and would then be reflected from the wall of the storage. But even if the communication from node L1 to L2 does happen through reflections outside of the boxes the minimum distance traveled through potatoes would still be 300 cm (pictured by the dashed black arrows). Overall this shows an increase of communication range by approximately 36% compared to the FSK nodes.

With regard to a cost efficient deployment strategy, which aims to reduce the number of nodes needed to monitor the storage conditions, while still receiving all data through multihop communication, the usage of LoRa results in less required nodes.

V. Conclusion

In this paper the *StorageLogger* was introduced, a wireless sensor node capable of monitoring the storage conditions of potatoes inside potato boxes. The node features a modular design, so it can be used with different sensors or radios.

An evaluation of using a LoRa radio for the discussed use case was performed and compared to the results of a FSK radio. The results show that the usage of LoRa increases the communication range through potatoes by at least 80 cm, with a maximum range of 300 cm. The downside of using LoRa is a significant increase in power consumption and a small decrease in transmission speed. To retain the lifetime of the battery powered nodes other measures are needed like the usage of a specially adjusted network protocol.

The authors would like to thank the VSD for the cooperation and provision of the potato storage.

References

[1] G. Magdalena and M. Dariusz, "Losses during storage of potato varieties in relation to weather conditions during the vegetation period and temperatures during long-term storage," *American Journal of Potato Research*, vol. 95, no. 2, pp. 130–138, Apr 2018.

[2] M. F. Rutolo, J. P. Clarkson, G. Harper, and J. A. Covington, "The use of gas phase detection and monitoring of potato soft rot infection in store," *Postharvest Biology and Technology*, vol. 145, pp. 15–19, 2018.

[3] B. Gernert, F. Schwartau, S. Raabe, J. Schoebel, K. Schubert, R. Stephan, and L. C. Wolf, "Evaluation of suitable radio frequencies for data transmission in potato warehouses," in *15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2018, pp. 220–227.

[4] J. Tervonena, "Experiment of the quality control of vegetable storage based on the internet-of-things," *Procedia Computer Science*, vol. 130, no. C, pp. 440–447, 2018.

[5] S. Heble, A. Kumar, K. V. D. Prasad, S. Samirana, P. Rajalakshmi, and U. B. Desai, "A low power iot network for smart agriculture," in *4th World Forum on Internet of Things (WF-IoT)*. IEEE, 2018, pp. 609–614.

[6] F. Büsching, U. Kulau, and L. Wolf, "Demo: INGA - An Inexpensive Node for General Applications," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2011, pp. 435–436.

[7] M. Bor and U. Roedig, "LoRa transmission parameter selection," in *13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2017, pp. 27–34.

[8] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology," in *14th International Conference on ITS Telecommunications (ITST)*. IEEE, 2015, pp. 55–59.

Ballistocardiography on Planes - Development Challenges for a Research Measurement System

Ulf Kulau[‡], Nico Jähne-Raden[§] , Thiemo Clausen[*] and Tobias Jura[†]
[‡]DSI Aerospace Technologie GmbH, [§]Hannover Medical School, [*†]Technische Universität Braunschweig
[‡]ulf.kulau@dsi-as.de, [§]nico.jaehne-raden@plri.de,[*]clausen@ibr.cs.tu-bs.de, [†]t.jura@tu-bs.de

***Abstract*—For years, the amount of medical incidents on passenger flights is increasing. Besides the personal stress and strains for concerned passenger, every incident leads to huge costs for the specific airline. Therefore, we face the challenge of using Ballistocardiography (BCG) in passenger planes and noisy environments respectively.**

To start with an extensive evaluation, we designed a precise, parallel and scalable measurement system for measuring BCG signals within planes or similar environments. We briefly describe the different challenges while designing the first prototype implementation and show a few first results.

I. Introduction

Sensor systems have been an established part of medical diagnostics for a long time. In addition to the conventional systems, accelerometers have increasingly entered the medical research. However, the use of accelerometers is usually reduced to activity determination. Due to technical advances, digital accelerometers have become attractive for medical diagnostics. Especially for the investigation of changes in body acceleration, as such for the Ballistocardiography (BCG).

The BCG is a method to gain detailed information of body movements imparted by the ballistic forces associated with cardiac contraction and ejection of blood and with the deceleration of blood flow through the large blood vessels. These heart related movements are translated by a sensor device into an electrical potential, which is suitably amplified and recorded [1]. Within our project, we are pursuing the utilization of BCG as a medical diagnostic tool for the discrete and long-term monitoring of progressive, function limiting heart diseases. Contrary to Electrocardiography (ECG), no skin contact is needed to conduct BCG measurements. Thus, BCG is a promising method to establish a non-invasive, non-disruptive health monitoring system, as sensor must not be attached to the body directly. This offers an opportunity for real world applications like the monitoring of passengers' health during a flight. Such a health monitoring system for passenger planes is highly beneficial for both, the passengers well-being, as well as for airlines to avoid medical accidents during a flight, which can lead to a flight abort.

Unfortunately, an extensive measurement of accelerations inside a cabin together with BCG measurements have never been carried out before. Therefore, we have to design a comprehensive measurement system for extensive evaluations within this environment beforehand. However, even the development of such a system goes along with several **challenges**, which will be described in this paper.

II. Related Work

The usability of BCG for medical applications, the analysis of BCG data and consecutive extraction of cardiovascular information is a current international research topic. Early research with digital accelerometers were driven by space agencies. Experiments were conducted during parabolic flights and on the International Space Station (ISS). There, sensor technology could be investigated independently of earth's gravitational influences and compared to ECG [2]. Various accelerometer sensors have already been used by other international research groups and have also been designed in some cases. These systems include immobile systems, such as weighing scales, as well as portable devices [3], [4], [5], [6], [7]. These devices are either physically unsuitable by beeing too large or the implementation lacks on data quality, especially temporal precision.

Prior to the creation of a BCG board as a diagnostic tool, various trials and measurements have been done. This includes a cooperation with the Physikalisch-Technische Bundesanstalt (PTB), to determine what features such a sensor system should have. At first, various measurements and investigations were carried out to determine the appropriate sensor technology. Furthermore, the selected acceleration sensors were examined for their precision. Also, the suitability for BCG measurement was examined. This was done with a series of test subjects, using measurements setups inferred from previous examinations [8]. We are currently preparing a project that will bring BCG into real world application, in particular the aforementioned health monitoring for passenger planes [9]. The project is still in an early stage but we gathered first results and derived several challenges towards such a system.

III. BCG in Planes

As a result of the ever-growing air traffic and passenger volume, the number of medical emergencies during flights is growing accordingly [10][11]. These incidents can range from uneasiness up to life threatening situations. For example, when a passenger is already suffering from cardiology diseases, the stress and the changed pressure or the anxiety can lead to a deterioration of the health condition. Monitoring the passengers health status during the flight, or even better, before departure (e.g. during boarding), enables flight attendants to initiate early counter procedures, e.g. serving water or sugar. Those minor actions might lead to an improvement of the status and could prevent serious consequences. The passenger's safety

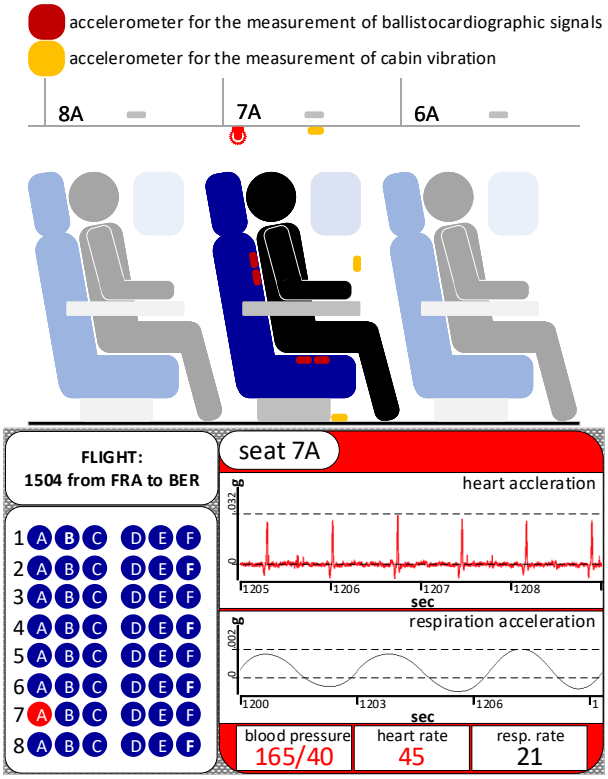


Figure 1. Sketch of the concept system in an aircraft including the flight attendant view

and the avoidance of additional costs due to unscheduled flight abortions is the motivation for this project. By utilizing accelerometer based BCG, we develop a comprehensive, non-invasive, autonomous and scalable on-board health-monitoring system. Early results from the project support an BCG based system design, even for noisy environments. Therefor, other applications might become possible (e.g. cars, busses, trains).

IV. Method

Using digital Micro-Electro-Mechanical systems (MEMS) sensors, the BCG health monitoring system can be extremely lightweight and cost efficient, which makes it particularly suitable for the deployment on an aircraft. It seems likely that the sensors are going to be mounted into the backrest (dorsal medio-frontal) and into the seat (dorsal medio-femoral), as depict in Figure 1. The sensors will be mounted redundant and inverse to each other, which will minimize the internal noise or occurring artifacts by the utilization of differential signaling. To allow a scalable system, an effective signal (pre-)processing at the seats is inevitable. But as wired power supply is not always present, a high energy efficiency and wireless data transmission is needed eventually. For convenient data representation, a back-end could be connected and integrated into the already existing flight attendant panel. However, before planing the actual integration of BCG in planes, several studies have to be performed by using a comprehensive measurement system to gather ground truth data.

V. Challenges for the Measurement System

This section provides challenges and research questions that resulted from our requirements analysis.

A. Measurement Platform

The biggest challenge, that is not solely limited to the exemplary application area of planes, is the noisy environment. The BCG signal constantly superimposes with other accelerations, like vibration of engines or flight movement. Furthermore, couplings throughout seats could lead to interference that have to be filtered out. Initially we will perform extensive studies that reveal which accelerations (frequency spectrum and amplitude) occur during a normal flight and at different flight manoeuvres. Based on this data we will be able to derive both, a generic model of the acceleration of an aircraft environment for evaluation purposes as well as suitable filtering techniques. The usage of reference nodes (e.g. at the cabin wall/floor) for real time noise canceling will be evaluated. To enable an adequate acquisition and signal processing/filtering of the data directly at the seat, a powerful but highly efficient hardware platform is needed. Hitherto, not every requirement for a proper hardware can be estimated. As a basic requirement, the simultaneous readout of the sensors has to be guaranteed, e.g., to allow the measurement of the Pulse Transit Time (PTT) and by extension the estimation of the passengers blood pressure [12]. For these reasons, the initial hardware-platform for evaluations will be based on an Multi-Processor System on Chip (MPSoC), combining the processing power of a multi-core CPU with the flexibility of a Field Programmable Gate Array (FPGA). While the FPGA allows an adaptive hardware design for, e.g., an effective filtering, the processing cores can be used for proper data processing in software. In particular we are using a Xilinx Zynq-7020 MPSoC that combines a dual core ARM processor with a Virtex 7 FPGA. At the current stage we rely on the Zedboard evaluation platform as it already offers several useful peripherals, for example Ethernet. Thus, the data will be gathered under ideal conditions. The current system will be used to obtain reference data for further modelling. The generation of a cabin vibration model is planed, which will allow us to emulate flight conditions in the cabin simulator of the Institute of Flight Guidance at TU Braunschweig.

B. Sensor Interfaces

For interfacing the sensors, we implemented custom hardware modules in the FPGA, which allow the utilization of parallel Serial Peripheral Interface Bus (SPI) controllers. All SPI controllers use a common clock, resulting in the absolutely synchronous readout of sensor data. As the parallel SPI controllers are implemented in hardware, a high tri-axial sampling rate can be achieved (up to 17kHz in preliminary tests). Each sample is additionally time-stamped in hardware to compensate delays that occur within the data chain. This is an important feature, as we want to apply differential signaling and other filtering techniques, which require a high temporal precision. All data is forwarded to the chips processing cores

via a Direct Memory Access (DMA) stream, packaged and further forwarded to a processing/storage server.

C. Sample Rate

The system is designed to fulfill specific timing constraints related to physical parameter of the human body. A top down approach is pursued, as the maximum relevant signal velocities are taken as references. More specifically, the fastest heart muscle related process is the rapid opening or closing of the aortic valve. The top speed measured by Leyh et al. was $13.5ms$ [13]. But to implement a true top down approach, the fastest muscle related process overall is taken into account. The electrical muscle potential necessary for muscle contraction is measured at $10kHz$ [14]. For this reason the target sample capture rate is set to be $10kHz$, which is achievable with the components described above (cf. Section V-A).

D. Sensor Selection

Prior to the design of the BCG sensor board, we performed various trials and measurements in cooperation with the PTB. Initially, the goal was to show the general feasibility of using commercially available digital accelerometers for BCG. We performed a series of tests with our subjects. By comparing the results of different accelerometers against reference values (ECG, Laser-Vibrometer) we showed that BCG is generally possible with digital devices but the data quality differs[8]. A follow-up study was performed to select the digital accelerometers with the best quality characteristics needed by BCG applications[15]. As a result, we selected the Kionix KX122 sensor for further investigations.

E. Scalability

With one measurement board we can equip one seat for evaluation purposes. However, the structure of an aircraft has a huge impact on the acceleration and thus have to be taken into account for potential filtering techniques. For this reason we have to scale the entire measurement system throughout the plane, e.g. place measurement boards at different rows. In doing so we ensure that all data streams share the same time reference, which renders them comparable on a sample by sample basis. We decided to use an Ethernet connection between the measurement boards. To ensure the common time base, we utilize a hardware-supported Precision Time Protocol (PTP) for synchronization of the boards. In first test we were able to show that the synchronization precision between the boards can be characterized by a median less than $1.5\mu s$. Ongoing research focuses on different approaches to further increase the board to board precision.

The reason why we selected Ethernet, is its easy integration into existing infrastructure. When performing first test during flights, we are only allowed to mount the measurement system in the cabin temporary (loose-equipment). However, considering Shannon's law, the synchronization error is far away from disturbing our goal of $10kHz$ sample rate.

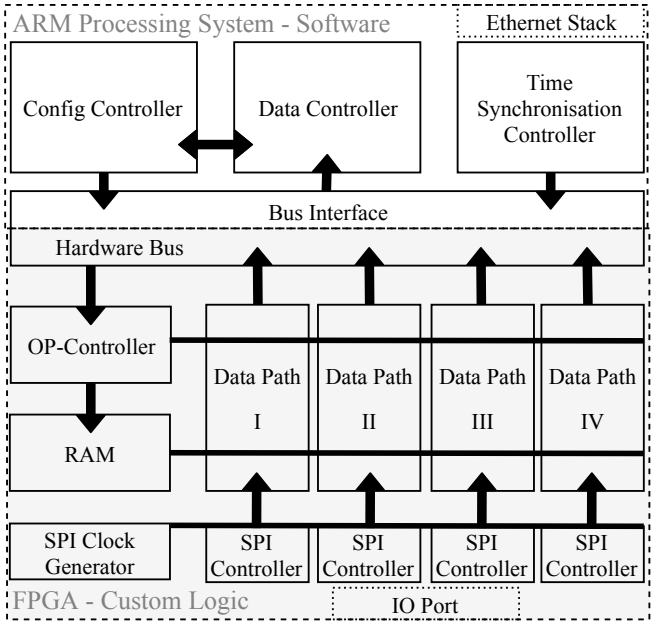


Figure 2. Board Block Diagram: Hardware and Software Components

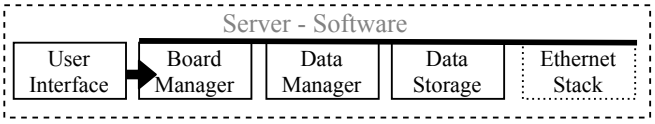


Figure 3. Server Block Diagram: Software Components

F. ECG Reference

For the first test, the measurement of an ECG reference signal is inevitable. Therefore we have selected a simple ECG shield (OLIMEX ECG shield [16])with 3 electrodes for the derivation of the electrical cardiac signals according to Einthoven and Goldberger (6-channel derivation). This 6-channel ECG is an appropriate method to obtain cardiac signal references to the actual heart contraction that will be measured across the BCG trials. The OLIMEX-Shield offers an analog output, which is converted into a digital signal by a SPI-ADC. Thus, the ECG signal can be recorded simultaneously to the accelerometers by utilizing one of the parallel SPI interfaces. The data resolution of the ECG board is at 10 bit for each channel, which is sufficient as a reference to the BCG signal.

VI. Prototype Implementation

Considering the described challenges, we implemented a first prototype for our initial field tests. As mentioned above, we rely on the Zedboard as the measurement platform. The general architecture of the board can be seen in Figure 2, the server is illustrated in Figure 3. The figures show the hard- as well as the software modules implemented on the Zedboard and on the server. The server itself is responsible for the board management, the initialization of the time synchronization and the data collection.

VII. Results

The project is still in an early stage, but we already made several evaluations to test the measurement system and gather BCG data.

A. BCG measurement campaign

A prototype of the presented system was deployed during a 50 day BCG study. During this time data from more than 30 subjects were acquired. The system was set up in a single board configuration, utilizing 3 channels for acceleration measurements. Channel 4 was used to gather ECG reference data. Triaxial acceleration data was acquired with a sample rate of c. 17 kHz, while ECG data was acquired with c. 13 kHz. In total, 1.35 - 1.55GB of data were generated per measurement and up to 6GB measurement of one subject. The analysis of the data is still in progress. For more information about this study we like to refer to [17].

B. BCG signals in planes

When presenting the general idea of the project, people have several doubts if BCG measurements in planes are possible in general. Therefore we performed a short measurement during a two hours flight. The result is shown in Figure 4.

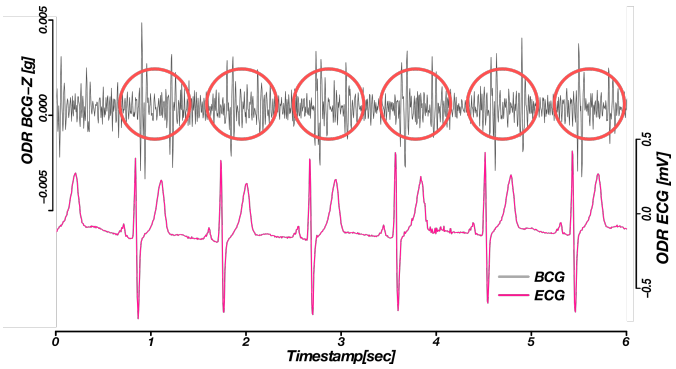


Figure 4. First results of BCG measurements during a flight.

Even without the ECG reference signal, the BCG signals can be seen clearly. In this case it should be mentioned, that the data were not pre-processed or filtered. Thus, with an appropriate signal processing the quality of the BCG signals can be improved further. In addition, a feature extraction could be applied to filter out unwanted noise or compress the data by providing only relevant data. However, this is part of our future work.

VIII. Conclusion

In this paper we introduced the utilization of BCG for a comprehensive health monitoring in passenger planes. For first evaluations a highly specialized measurement system is needed. The paper at hand presented the various design challenges for such a system and the architecture of its prototype implementation.

It should be mentioned, that several other challenges arise, when thinking about an actual implementation of a BCG-based health monitoring in plane seats. Hundreds of seats within a plane will form a very dense sensor network, where a reliable data transmission with low latency has to be guaranteed.

However, first measurements within a plane showed the general feasibility of our approach and we are motivated to face the upcoming challenges as well.

References

[1] L. Giovangrandi, O. Inan, R. Wiard, M. Etemadi, and G. T. A. Kovacs, "Ballistocardiography–a method worth revisiting," *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 2011, pp. 4279–4282, 2011.

[2] Q. Delière, P.-F. Migeotte, X. Neyt, I. Funtova, R. M. Baevsky, J. Tank, and N. Pattyn, "Cardiovascular changes in parabolic flights assessed by ballistocardiography," *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 2013, pp. 3801–3804, 2013.

[3] M. Di Rienzo, E. Vaini, and P. Lombardi, "Wearable monitoring: A project for the unobtrusive investigation of sleep physiology aboard the international space station," in *Computing in Cardiology 2015*, A. Murray and C. i. Cardiology, Eds. [Piscataway, NJ]: IEEE, 2015, pp. 125–128.

[4] A. M. Carek and O. T. Inan, "Robust sensing of distal pulse waveforms on a modified weighing scale for ubiquitous pulse transit time measurement," *IEEE transactions on biomedical circuits and systems*, vol. 11, no. 4, pp. 765–772, 2017.

[5] A. D. Wiens, M. Etemadi, S. Roy, L. Klein, and O. T. Inan, "Toward continuous, noninvasive assessment of ventricular function and hemodynamics: wearable ballistocardiography," *IEEE journal of biomedical and health informatics*, vol. 19, no. 4, pp. 1435–1442, 2015.

[6] A. Q. Javaid, H. Ashouri, and O. T. Inan, "Estimating systolic time intervals during walking using wearable ballistocardiography," in *3rd IEEE EMBS International Conference on Biomedical and Health Informatics*. Piscataway, NJ: IEEE, 2016, pp. 549–552.

[7] M. Di Rienzo, P. Meriggi, E. Vaini, P. Castiglioni, and F. Rizzo, "24h seismocardiogram monitoring in ambulant subjects," in *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2012, pp. 5050–5053.

[8] N. Jähne-Raden, T. Märtin, M. Marschollek, K. Heusser, and J. Tank, "Bcg-mapping of the thorax using different sensors: First experiences and signal quality," in *2016 IEEE SENSORS*. IEEE, 2016, pp. 1–3.

[9] N. Jähne-Raden, H. Gütschleg, M. Kallenbach, T. Feuerle, and U. Kulau, "Poster: Scarab^2 - scalable, robust and adaptive on board ballistocardiography," *2018 14th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 111–112, 2018.

[10] D. Silverman and M. Gendreau, "Medical issues associated with commercial flights," *The Lancet*, vol. 373, 2009.

[11] J. Hinkelbein, O. Spelten, W. Wetsch, R. Schier, and C. Neuhaus, "Emergencies in the sky: In-flight medical emergencies during commercial air transport," *Trends in Anaesthesia and Critical Care*, vol. 3, 2013.

[12] C.-S. Kim, A. M. Carek, R. Mukkamala, O. T. Inan, and J.-O. Hahn, "Ballistocardiogram as proximal timing reference for pulse transit time measurement: Potential for cuffless blood pressure monitoring," *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 11, pp. 2657–2664, 2015.

[13] R. Paulis, G. Maria De Matteis, P. Nardi, R. Scaffa, M. Michaela Buratta, and L. Chiariello, "Opening and closing characteristics of the aortic valve after valve-sparing procedures using a new aortic root conduit," *The Annals of thoracic surgery*, vol. 72, pp. 487–94, 09 2001.

[14] H. H. Yiu-Ming WONG, Wei-Hwa LIAW, "Technical Considerations for Measurement of Median Nerve Conduction Velocity at Wrist," *Journal of UOEH*, vol. 34, no. 3, pp. 217–224, 2012.

[15] N. Jähne-Raden, K.-H. Wolf, and M. Marschollek, "Signal detection accuracy of digital accelerometers for ballistocardiographic propose," in *2017 Computing in Cardiology (CinC)*. IEEE, 2017, pp. 1–4.

[16] OLIMEX, *Users Manual: SHIELD-EKG-EMG*, 2011, rev. E, Revised June 2014.

[17] N. Jähne-Raden, M. C. Wolf, U. Kulau, S. Sigg, and M. Marschollek, "Development of a novel ballistocardographic database," in *International Conference on Informatics, Management, and Technology in Healthcare (ICIMTH)*, 2019, accepted for publication.

Resilience against Shipping Noise and Interference of the AHOI Acoustic Underwater Modem

Fabian Steinmetz and Christian Renner
Research Group smartPORT, Hamburg University of Technology
Email: {fabian.steinmetz, christian.renner}@tuhh.de

***Abstract*—Underwater Wireless Sensor Networks (UWSNs) and micro Autonomous Underwater Vehicles (μAUVs) enable diverse underwater monitoring and service applications; e. g., observation of water quality or identification of pollution. Reliable underwater communication for data transmission between sensors, μAUVs and base stations is required. The smartPORT acoustic underwater modem AHOI is a small, low-power and low-cost modem, which was developed for these applications. This paper evaluates the modem's resilience against shipping noise and packet interference in UWSNs. At first, noise and interference sources are presented, followed by a short description of the modems's countermeasures. At last, simulated noise of ships and Autonomous Underwater Vehicles (AUVs) with different distances to the noise source were added to the communication signals and evaluated. And in addition, packet interference was simulated and evaluated in a real-world scenario.**

I. Introduction

Exploration and monitoring of underwater sceneries is drawing considerable attention [1]. Recent examples are UWSNs such as HydroNode [2], SUNRISE [3] or services for example Robotic Vessels as-a-Service (RoboVaaS) [4]. In all cases, reliable underwater communication is a major requirement. Due to the strong attenuation of the electro-magnetic wave in the water, most of the communication interfaces use an acoustic communication (e.g. [5], [6]). Many applications are located in ports and rivers and include several devices. Ships and AUVs produce acoustic noise, which could disturb the acoustic communication. In addition, in a network of acoustic modems packet collisions can occur when several modems transmit simultaneously.

In the following sections, we evaluate the AHOI modem's resilience against shipping noise and packet interference in a network. A preliminary study was presented in [7]. The resilience tests were used to simulate the modem behavior in DESERT [8], a simulator for underwater networks based on ns2. This paper extends the existing simulations with shorter distances to the noise sources (higher noise level at the receiver), an AUV noise simulation and additional interference combinations. Moreover, interference is tested in a real-world scenario. The interference evaluation is useful for prospective decision on a Medium Access Control (MAC) protocol.

II. AHOI - Acoustic Underwater Modem

The AHOI modem is a small, low-power and low-cost acoustic underwater modem (see Fig. 1 and [9], [10]), developed to be integrated into UWSNs or μAUVs (for example the HippoCampus [11]). The power consumption in idle and receive mode is around $300\,\mathrm{mW}$ and $2.1\,\mathrm{W}$ during data transmission with highest amplification. For acoustic signal reception and transmission, the AHOI modem uses an Aquarian Audio AS-1 hydrophone [12]. In case of the highest amplifier level, the transmission source level is between $150\text{-}160\,\mathrm{dB\,re\,\mu Pa^2\,@1\,m}$.

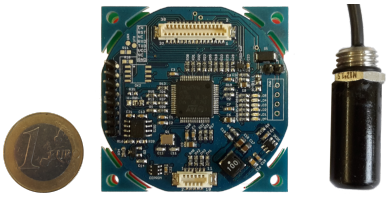


Fig. 1: AHOI acoustic underwater modem with hydrophone.

Signal processing is realized in software on the microcontroller, which allows a fast reconfiguration of frequency and coding setups. In the default setup, the modem uses an orthogonal Binary Frequency Shift Keying (BFSK) with $2.56\,\mathrm{ms}$ symbol duration and $781.25\,\mathrm{kHz}$ frequency spacing. Each symbol consists of four superimposed sinusoidal waveforms. To counter frequency cancellations caused by multipath propagation and to enhance the reliability against noise, each bit is repeated on three different carriers, and Frequency Hopping Spread Spectrum (FHSS) is applied to avoid inter-symbol interference. The modem has $25\,\mathrm{kHz}$ bandwidth around a center frequency of $62.5\,\mathrm{kHz}$. The default setup in combination with Hamming coding leads to a net data rate of $260\,\mathrm{bit/s}$ (up to $4.7\,\mathrm{kbit/s}$ are feasible with the current setup).

A. Receiver Design

Before the digitization of the received signal, the signal passes through an analog processing chain. At first, the signal is pre-amplified to have a higher signal level. Afterwards a highpass filter with cut-off frequency $f_c = 50\,\mathrm{kHz}$ reduces signal components with lower frequencies and a lowpass filter with cut-off frequency $f_c = 75\,\mathrm{kHz}$ reduces the higher parts. At last, the signal is amplified again. The amplification gain is controllable in the range from $60\,\mathrm{dB}$ to $96\,\mathrm{dB}$. Figure 2 shows the receiving characteristic for selected gain steps.

B. Hydrophone Characteristic

The AHOI modem uses a single transducer to receive and to transmit (see Sect. II). In Fig. 3 the Free-Field Voltage Sensitivity (FFVS) and Transmit Voltage Response (TVR) of the hydrophone are depicted. The FFVS in the range from

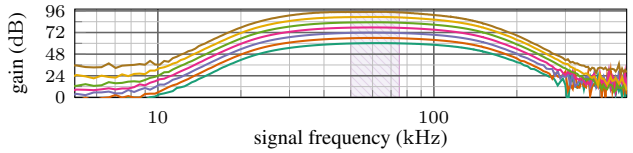
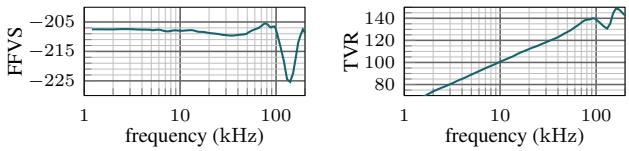


Fig. 2: Measured transfer function of the analog receiving signal chain of an AHOI modem in steps of 6 dB.



(a) AS-1 as receiver (b) AS-1 as transmitter

Fig. 3: FFVS in $[\mathrm{dB\,re\,1V/\mu Pa}]$ and TVR in $[\mathrm{dB\,re\,1\mu Pa, 1V@1\,m}]$ of an Aquarian Audio AS-1 hydrophone [12].

1 kHz to 100 kHz is almost linear (± 2 dB) and has a sensitivity of $-208\,\mathrm{dBV\,re\,1\mu Pa}$. Opposed to the FFVS, the TVR is highly frequency dependent. During a transmission, the modem compensates the frequency-dependent characteristic.

III. Fundamentals

This section presents the attenuation of acoustic signals in underwater scenarios and different ship and AUV noise profiles. Interference in underwater networks is discussed.

A. Acoustic Signal Attenuation

When the acoustic wave travels through the water, the signal is attenuated. The path loss depends on the frequency f and the distance d between sender and receiver. The attenuation is

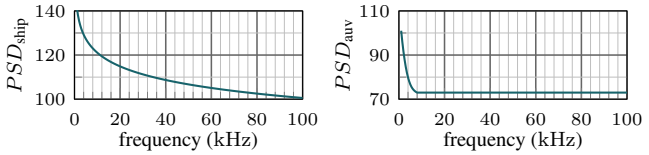
$$L(d,f) = L_{\mathrm{spr}}(d) + L_{\mathrm{abs}}(d,f) \quad (1)$$
$$= 20 \cdot n \cdot \log_{10}(d) + d \cdot \alpha(f)\ \mathrm{dB} \quad (2)$$

with spread loss L_{spr} and absorption loss L_{abs}. The path loss exponent n depends on the situation and environment. For a spherical spreading and a free-field assumption, the exponent is $n = 1$. In contrast to spread loss, absorption loss is frequency-dependent. The function $\alpha(f)$ models attenuation in relation to the frequency. Different models are discussed in [13], e.g. the Schulkin and Marsh formula. Assuming test conditions from Sect. V, typical absorption losses are less than $3\,\mathrm{dB/km}$ for frequencies up to 100 kHz. Based on that, absorption loss is negligible in small communication distances compared to spread loss; e. g., $L_{\mathrm{spr}}(100\,\mathrm{m}) = 40\,\mathrm{dB}$. Attenuation for short distances can be approximated with

$$L(d) = 20 \log_{10}(d)\,. \quad (3)$$

B. AUV and Shipping Noise

Ships and AUVs produce acoustic noise. The intensity and frequency depends, e. g., on speed and ship length. For acoustic noise modeling, the authors in [14] presented a detailed analysis of different noise sources, different ships and AUVs. In addition, an equation is derived to calculate noise Power Spectral Densities (PSDs). To evaluate the AHOI modem resilience against shipping noise, these noise PSDs are used. Two models are depicted in Fig. 4. At first a noise model for



(a) 180 m cargo ship, 15 knots (b) Bluefin Robotics AUV

Fig. 4: Noise PSD in $\left[\mathrm{dB\,re\,\mu Pa^2/Hz}\right]$ produced by a ship and an AUV. The PSDs are derived with the equations presented in [14].

a 180 m cargo ship, traveling with a velocity of 15 knots, and the second one for an AUV from Bluefin Robotics [15]. In both cases, the acoustic noise emitted by ship and AUVs have highest PSDs below 10 kHz.

C. Signal Interference

In UWSNs, multiple nodes transmit and receive data. The simplest way is to start a data transmission, when the data was recorded. This concept can lead to packet interference if several nodes need to use the transmission channel at the same time and packets overlap at the receiver. A more coordinated transmission medium access (Carrier Sense Multiple Access, CSMA), is to listen to the channel before the transmission. If the channel is unused, the sender starts the transmission. Opposed to the speed of light in a wireless over-water transmission (using electro-magnetic waves), the speed of sound in an underwater scenario is much lower. The speed of sound depends on temperature, salinity, depth and is approximately 1500 m/s. For short distances, propagation delays are in the millisecond range; e. g., for 150 m a propagation time of 100 ms (in contrast to propagation times less than 1 ns for wireless over-water communication). Based on that, CSMA is difficult to apply compared to wireless over-water communication. Additionally, in a network with μAUVs, protocols with time synchronization and a fixed communication time slot for each node, e. g., Time Division Multiple Access (TDMA), are impractical due to the high variation of the propagation time (due to mobility). In sum, media access is a critical point in UWSN and there is a risk of packet interference. An extensive discussion on UWSN media access can be found in [1].

IV. Experimentation Setup

The resilience against shipping noise and packet interference was evaluated via simulation and a real-world scenario.

A. Simulation

A simulation was performed to assess the resilience against ship and AUV noise. The noise was generated offline and added to different recorded packets. A single AHOI modem was used to receive the signal, which was generated with an arbitrary signal generator (TiePie Handyscope HS5, 200 kHz sampling). The signal generator simulated the hydrophone voltage response (see FFVS in Sect. II-B) for different PSDs and the signal strength was calculated with Eq. (3). Figure 5 shows the PSDs of received packets at the receiver side (neglecting all propagation paths besides Line-of-Sight (LOS)) for distances to transmitter

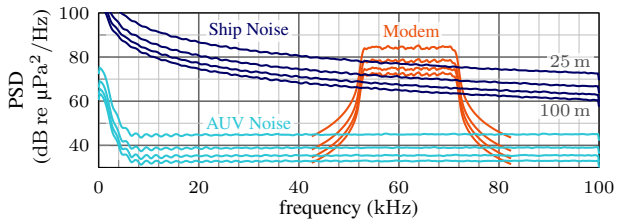


Fig. 5: PSDs of the simulated modem signals and additional shipping noise. The PSDs correspond to received signals (packets or noise) with $d_{\mathrm{M}}, d_{\mathrm{ship}}, d_{\mathrm{AUV}} \in \{25\,\mathrm{m}, 50\,\mathrm{m}, 75\,\mathrm{m}, 100\,\mathrm{m}\}$ distance to the transmitter or noise source.

$d_{\mathrm{M}} \in \{25\,\mathrm{m}, 50\,\mathrm{m}, 75\,\mathrm{m}, 100\,\mathrm{m}\}$ and distances to the noise source $d_{\mathrm{ship}}, d_{\mathrm{AUV}} \in \{25\,\mathrm{m}, 50\,\mathrm{m}, 75\,\mathrm{m}, 100\,\mathrm{m}\}$. During the simulations, different noise profiles were added to the packets. The noise profiles were generated in according to Sect. III-B and also shown in Fig. 5. For each combination of ship or AUV noise level and communication signal strength, 100 transmissions were simulated (with 32 B payload per packet).

In addition to ship and AUV noise, other underwater modems in a network could disturb the transmission (see Sect. III-C). To evaluate the effect of packet interference and the resulting Packet Reception Rate (PRR), the same simulation setup was used. Instead of additional simulated noise, a second recorded packet was added to the generator samples. All packets carried 32 B payload and had a signal duration of $T_{\mathrm{pkt}} = 1.3\,\mathrm{s}$, including the synchronization symbols. During the simulation two modems ($\mathcal{M}_1$ and $\mathcal{M}_2$) transmitted packets with different delays $\Delta t \in \{-1.25 \cdot T_{\mathrm{pkt}}, -1 \cdot T_{\mathrm{pkt}}, ..., 1.25 \cdot T_{\mathrm{pkt}}\}$. The time Δt is the reception time difference between $\mathcal{M}_1$ and $\mathcal{M}_2$ at the receiver side w. r. t. the reception of the packet from $\mathcal{M}_1$. For example, $\Delta t < 0$ means the packet from $\mathcal{M}_2$ arrives before the packet sent by $\mathcal{M}_1$. $|\Delta t| > T_{\mathrm{pkt}}$ is a reception without interference. The signal strengths of the received packets are similar to the noise test (see Fig. 5).

B. Real-World Evaluation

The real-world evaluation took place at the Port of Harburg, a small marina in Hamburg (see Fig. 6). It was a warm and windless day in June 2019 with 19.5 °C water temperature. In all cases, the hydrophones were placed 1.5 m under the water surface. During the evaluation three AHOI modems were used. The receiver was placed at a fixed position and two transmitters at the setups (1) $d_{\mathrm{M1}} = 25\,\mathrm{m}$, $d_{\mathrm{M2}} = 25\,\mathrm{m}$ (2) $d_{\mathrm{M1}} = 25\,\mathrm{m}$, $d_{\mathrm{M2}} = 40\,\mathrm{m}$. Each combination of setup and delay $\Delta t \in \{-1.5 \cdot T_{\mathrm{pkt}}, -0.5 \cdot T_{\mathrm{pkt}}, 0, 0.5 \cdot T_{\mathrm{pkt}}, 1.5 \cdot T_{\mathrm{pkt}}\}$, 100 packets with 32 B payload were transmitted. Due to serial connection and internal packet handling of the modems, the exact transmission time was not controllable (a few milliseconds difference). Both modems were connected to a laptop and we waited Δt between the transmission initialization and neglected the underwater propagation time. Compared to the packet overlap in the seconds range, these limitations are small (in the millisecond range). For $\Delta t = 0$ the transmission from $\mathcal{M}_1$ is initialized first.

Fig. 6: Test area of our real-world evaluation at a port in Hamburg.

V. Results

A. Simulation

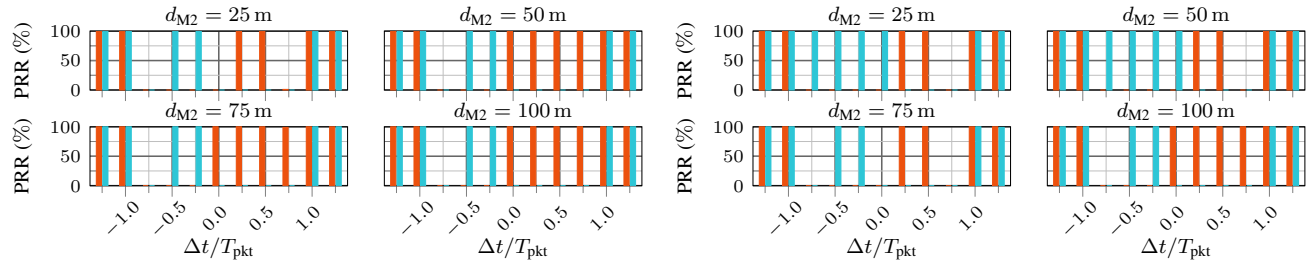
At first, the resilience against ship and AUV noise was evaluated. The ship noise affected packet reception in two cases and in the other cases all transmitted packets were received. The combination $d_{\mathrm{ship}} = 25\,\mathrm{m}$, $d_{\mathrm{M}} = 75\,\mathrm{m}$ resulted in 97 % and $d_{\mathrm{ship}} = 25\,\mathrm{m}$, $d_{\mathrm{M}} = 100\,\mathrm{m}$ in 26 % received packets. In both cases, the noise PSD is higher than the communication signal PSD. As a simplification during the simulations, the noise source was assumed as a point source and d_{ship} was smaller than the ship length (180 m). In general, the ship noise sources are distributed over the ship hull and the received signal level lower. The noise emitted by an AUV has a lower PSD. As expected, in all simulations with AUV noise profiles all packets were received. In sum, the modem is resilient against ship and AUV noise.

The second evaluation simulated packet interference between two modems and different communication distances. Due to space limitations, Fig. 7 depicts only the results for $d_{\mathrm{M1}} \in \{25\,\mathrm{m}, 75\,\mathrm{m}\}$ in combination with $d_{\mathrm{M2}} \in \{25\,\mathrm{m}, 50\,\mathrm{m}, 75\,\mathrm{m}, 100\,\mathrm{m}\}$. The results of the evaluation are: (1) Without interference ($|\Delta t| \geq T_{\mathrm{pkt}}$) all packets from $\mathcal{M}_1$ and $\mathcal{M}_2$ were received. (2) The first packet (w. r. t. the arrival at the receiver) is received, also for the case that the second transmitter is nearer. (3) For the case $\Delta t = 0$ and $d_{\mathrm{M1}} \neq d_{\mathrm{M2}}$ the packet from transmitter with a shorter distance is received. (4) For $\Delta t = 0$ and $d_{\mathrm{M1}} = d_{\mathrm{M2}}$ the PRR goes to zero. An exception are the cases: (a) $\Delta t = -0.75 \cdot T_{\mathrm{pkt}}$ and $d_{\mathrm{M1}} \leq d_{\mathrm{M2}}$ (b) $\Delta t = 0.75 \cdot T_{\mathrm{pkt}}$ and $d_{\mathrm{M1}} \geq d_{\mathrm{M2}}$ The generated simulation signals in Fig. 8 gives an explanation for the exception. For the case $\Delta t = 0.75 \cdot T_{\mathrm{pkt}}$ is a signal cancellation, which distorts the packet reception.

Based on the simulation, the modem is resilient against interference in the most cases. The resilience is independent of the packet overlap and dependents on frequency cancellations between the overlapping packets. Currently, other modulation schemes are under development to avoid cancellations [16].

B. Real-World Evaluation

Figure 9 depicts the results of the real-world evaluation. Opposed to the simulation, which simulates the LOS path only, a real-world scenario consists of multiple propagation paths and additional noise. Multipath propagation leads to symbol interference and lowers the PRR. The results of the evaluation are: (compared to the four points in Sect. V-A): (1) Without interference ($|\Delta t| \geq T_{\mathrm{pkt}}$) the PRR was between 87 − 100 %. (2) The first received packet wins with an average PRR of 68 % (in the case $\Delta t = 0$, $\mathcal{M}_1$ transmits



(a) Distance to $\mathcal{M}_1$: $d_{M1} = 25\,m$ (b) Distance to $\mathcal{M}_1$: $d_{M1} = 75\,m$

Fig. 7: Packet interference simulation between $\mathcal{M}_1$ and $\mathcal{M}_2$. The time Δt is the difference between the reception of the packet from $\mathcal{M}_1$ and $\mathcal{M}_2$ at the receiver side (w. r. t. the reception of the packet from $\mathcal{M}_1$). The received signal strength was calculated w. r. t. the transmission distances $d_{M1} \in \{25\,m, 75\,m\}$ and $d_{M2} \in \{25\,m, 50\,m, 75\,m, 100\,m\}$. Red bars show the PRRs from $\mathcal{M}_1$ and blue bars from $\mathcal{M}_2$.

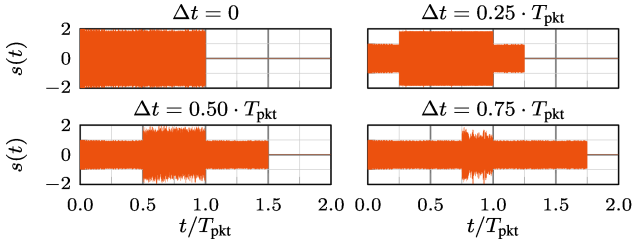


Fig. 8: Offline generated simulation signals $s(t)$ with packet interference. The amplitudes of both packages are normalized to 1.

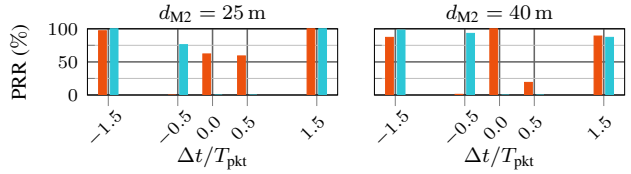


Fig. 9: Results of the packet interference real-world evaluation. Receiver and $\mathcal{M}_1$ were fixed with distance $d_{M1} = 25\,m$. Red bars show the PRRs from $\mathcal{M}_1$ and blue bars from $\mathcal{M}_2$.

a few milliseconds before $\mathcal{M}_2$). The points (3) and (4) were not included in the evaluation. Similar to signal cancellation during the simulation, at $d_{M2} = 40\,m$ and $\Delta t = 0.5 \cdot T_{pkt}$ the PRR decreased to 19 %. Also in a repetition of the experiment ($d_{M1} = 25\,m$, $d_{M2} = 40\,m$, $\Delta t = 0.5 \cdot T_{pkt}$) the PRR reduced to 7 %. In both cases, 99 % and 86 % of the packet headers were received. This leads to the assumption, that the second packet cancels the signals from the first during the payload reception.

In sum, the real-world evaluation supports the general finding from the simulation with the LOS signal. Due to multipath propagation and addition noise, the PRR decreased in the case of packet interference.

VI. Conclusion

We showed with a simulation that the modem is resilient against ship and AUV noise. In addition, we analyzed packet interference with simulations and a real-world tests. In many cases, the modem is resilient against packet interference. Based on our findings, it will be possible to choose a MAC protocol for UWSNs or swarms of μAUVs equipped with our AHOI modem.

Acknowledgment

This work was supported by the German Federal Ministry for Economic Affairs and Energy (BMWi, FKZ 03SX463C), and ERA-NET Cofund MarTERA (contract 728053).

References

[1] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater Sensor Networks: Applications, Advances, and Challenges," *Philosophical Transactions of the Royal Society–A*, vol. 370, no. 1958, 2012.

[2] D. Pinto, S. S. Viana, J. A. M. Nacif, L. F. M. Vieira, M. A. M. Vieira, A. B. Vieira, and A. O. Fernandes, "HydroNode: A Low Cost, Energy Efficient, Multi Purpose Node for Underwater Sensor Networks," in *37th IEEE Conf. on Local Computer Networks*, Clearwater, FL, USA, 2012.

[3] "SUNRISE FP7 research project," http://fp7-sunrise.eu, ac.: 2019/06/03.

[4] A. Signori, F. Steinmetz, F. Campagnaro, D. Zordan, M. Zorzi, and C. Renner, "Poster: Underwater Communications for the Robotic Vessels as-a-Servic Project," in *13th ACM Int. Conf. on Underwater Networks & Systems (WUWNet)*, Shenzhen, China, 2018.

[5] E. Gallimore, J. Partan, I. Vaughn, S. Singh, J. Shusta, and L. Freitag, "The WHOI Micromodem-2: A Scalable System for Acoustic Communcations and Networking," in *MTS/IEEE Oceans Conf. & Expo. (OCEANS)*, 2010.

[6] Evologics GmbH, "Underwater Acoustic Modems," http://www.evologics.de/en/products/acoustics/, ac.: 2019/06/03.

[7] F. Campagnaro, F. Steinmetz, A. Signori, D. Zordan, C. Renner, and M. Zorzi, "Data Collection in Shallow Fresh Water Scenarios with low-cost Underwater Acoutic Modems," in *5th Int. Conf. & Exhibition on Underwater Acoustics (UACE)*, Crete, Greece, 2019.

[8] F. Campagnaro, R. Francescon, F. Guerra, F. Favaro, P. Casari, R. Diamant, and M. Zorzi, "The DESERT underwater framework v2: Improved capabilities and extension tools," in *3th IEEE Underwater Communications & Networking Conf. (UComms)*, Lerici, Italy, 2016.

[9] C. Renner and A. J. Golkowski, "Acoustic Modem for Micro AUVs: Design and Practical Evaluation," in *11th ACM Int. Conf. on Underwater Networks & Systems (WUWNet)*, Shanghai, China, 2016.

[10] J. Heitmann, L. Bublitz, T. Kortbrae, and C. Renner, "Evolution of an Acoustic Modem for Micro AUVs," in *16th GI/ITG KuVS Fachgespräch "Sensornetze" (FGSN)*, Hamburg, Germany, 2017.

[11] A. Hackbarth, E. Kreuzer, and E. Solowjow, "HippoCampus: A Micro Underwater Vehicle for Swarm Applications," in *IEEE Int. Conf. on Intelligent Robots & Systems (IROS)*, Hamburg, Germany, 2015.

[12] Aquarian Audio & Scientific, "AS-1 Hydrophone," http://www.aquarianaudio.com/as-1-hydrophone.html, ac.:2019/05/27.

[13] R. J. Urick, *Principles of Underwater Sound 3rd Ed.* Peninsula, 1996.

[14] E. Coccolo, F. Campagnaro, A. Signori, F. Favaro, and M. Zorzi, "Implementation of AUV and Ship Noise for Link Quality Evaluation in the DESERT Underwater Framework," in *13th ACM Int. Conf. on Underwater Networks & Systems (WUWNet)*, Shenzhen, China, 2018.

[15] General Dynamics, "Bluefin SandShark UUV," https://gdmissionsystems.com/products/underwater-vehicles/bluefin-sandshark-autonomous-underwater-vehicle, ac.: 2019/05/27.

[16] F. Steinmetz, J. Heitmann, and C. Renner, "A Practical Guide to Chirp Spread Spectrum for Acoustic Underwater Communication in Shallow Waters," in *13th ACM Int. Conf. on Underwater Networks & Systems (WUWNet)*, Shenzhen, China, 2018.

Wireless sensor network for retrofitting production systems

1st Gordon Lemme
Cyber-physical production systems
Fraunhofer IWU
Dresden, Deutschland
gordon.lemme@iwu.fraunhofer.de

2nd Kilian Armin Nölscher
Cyber-physical production systems
Fraunhofer IWU
Dresden, Deutschland
kilian.noelscher@iwu.fraunhofer.de

***Abstract*—Under the premise of the retrofit idea of machine tools, this paper discusses a self-sufficient, wireless sensor network for the acquisition of machine-related process data as well as environmental information for context enrichment. Based on the requirements of the production environment, a solution consisting of sensor technology and embedded system will be designed and an implementation possibility will be presented.**

***Index Terms*—WLAN, production, retrofit, temperature, single board computer, WSN, ESP32**

I. Introduction

The accuracies of machine tools and the individuality of products have been gaining in importance for years [1] and, with regard to the market situation [2], form a know-how advantage at the production location Germany. This knowledge lead in the field of mechanical engineering can only be secured by continuous further development and mirroring application-driven challenges. This is not least achieved by the support programmes initiated by the Federal Government with reference to digitization and industry 4.0, especially for small and medium-sized enterprises. A recurring core topic of these initiatives is the growing automation and individualization of production [3] in order to secure Germany as a production location. In addition to communication and control, the basis for industry 4.0 is process digitization for the generation of a "digital shadow" or a "digital twin". This requires the use of existing standards in communication in order to avoid further diversity, as with existing machine controls. At the same time, it must be possible to integrate retrofit variants into existing infrastructures with little effort and to use them for future software ecosystems as well as their services in the field of mechanical engineering.

II. Motivation

For a comprehensive process analysis, continuous data acquisition under real-time conditions in the sense of the application as well as continuous subsequent condition monitoring to record the machine and ambient conditions is indispensable. In addition, context-related data fusion offers a holistic machine or process image, but requires data pre-processing close to the machine in order to minimize various latency and data transfer effects on possible computing power cloud systems. With the help of autonomous sensor networks, such context-related data acquisition can be carried out close to the machine and in particular with existing machines (retrofit), whereby, for example, signs of wear are minimized, downtimes are optimized and the total costs of the machine during its life cycle are reduced [4]. In addition, the context reference generated in this way contributes to the monitoring of safety violations and machine damage by recording suitable data via a sensor network [5]. Due to the extensive data situation associated in this way, additional functions can be developed for existing machines in addition to pure condition monitoring. This includes, for example, predictive maintenance, where predictions of necessary maintenance measures are made with the help of this data volume, either by means of regular control or by machine learning procedures [6]. The necessary data fusion from different sources (e.g. machine data, room climate data) helps to generate a holistic, context-related system image with the goal of increased system availability. The comprehensive recording of process parameters is essential and is only supported in its entirety to a limited extent by current machine tools or their controls. Rather, it is the integration of existing building sensors, function-integrated tool parameters and additional sensors remote from the machine. Not only the quantity of the data is decisive, but also its quality, which has a considerable effect on the results to be achieved with regard to downstream data processing.

The high demands placed on machine tools in terms of dimensional accuracy and repeatability of production steps for the realization of high-quality products also represent an enormous challenge (parameter correction) with regard to the interference influences acting on the process and the machine. An example of a significant disturbance factor is the thermal material expansion effect, which manifests itself as position deviation in the space between the Tool Center Point (TCP) and the workpiece [7]. Different assemblies or components of the machine have different proportions of the total deviation, depending on their respective characteristics (material, size, construction design). Although the heat input to machine parts can be reduced by constructive solutions in the design of a machine tool, an inhomogeneous temperature field will occur during operation, which has a negative influence on process stability. By means of appropriate data analysis and an

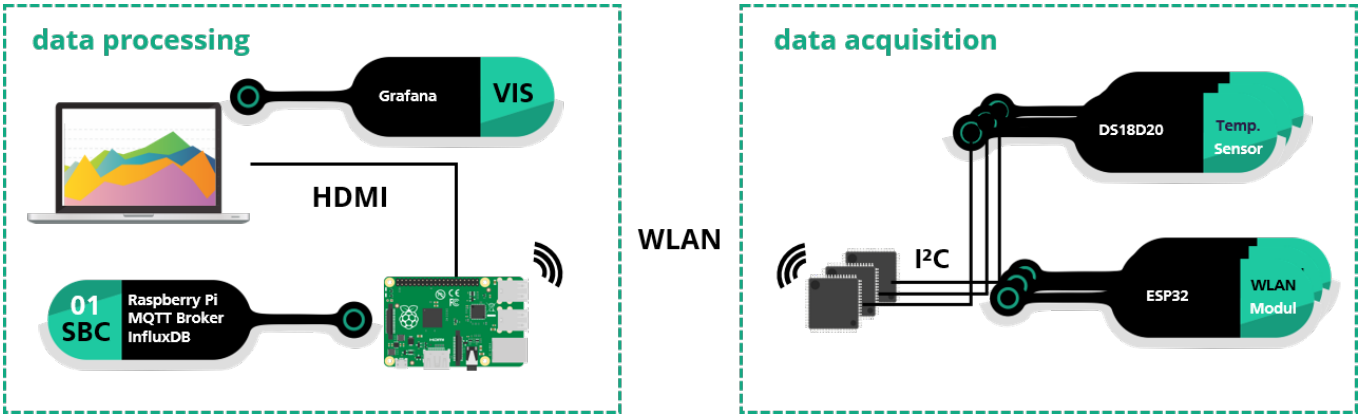


Fig. 1. Separation of the network into sensor nodes and collector including visualization, own representation.

existing understanding of the process model, it is possible to counteract the disturbing influences through targeted process control and thus achieve adequate temperature compensation. The so-called indirect compensation method is supported with the aid of process-accompanying data acquisition, in which the process parameters, that ultimately have an influence on the temperature, are collected, evaluated and the expected temperature-related machine displacements are determined. At the control level, an axis path correction is performed as misalignment compensation by returning the temperature changes as a controlled variable to the numerical control (NC) [8].

In addition to these listed aspects of process monitoring and optimization, the production history of a product can be recorded by such an extensive data acquisition by sensor nodes and stored with suitable methods (e.g. Distributed Ledger [9]) forgery-proof and yet verifiable for third parties. This type of unchangeable storage and traceability will become more and more important in the future, especially with regard to the more frequent value creation networks. At the same time, future software ecosystems and associated services will play an increasingly important role in the provision of services.

Single Board Computers (SBC) have become increasingly popular in recent years, not least in the industrial environment. Initiated by the Raspberry Pi Foundation [10] and the rapidly growing community around the single board computer of the same name, digitization projects could be implemented cost-effectively. The individual models differ greatly in form factor, equipment, acquisition costs as well as installed hardware and thus also in computing power. HAT modules (hardware on top) are used for the expansion of such SBCs in order to compensate for deficits in the basic equipment compared to fully-fledged computer or control systems. As a result, interfaces can usually be added, which reduces development costs and increases flexibility through the use and creation of self-sufficient, modular hardware and application adaptation. Condition monitoring requires small and cost-effective computer systems that can be easily integrated into production systems and machines. Single board computers meet these requirements by existing interfaces for wireless as well as wired communication and sensor interfaces via so-called GPIO pins, which is why they are predestined for such tasks from an economic point of view and due to their simple system adaptation [11].

For tasks in which even a single-board computer appears to be oversized in every respect (more capacity than necessary), small microprocessor units (MCUs) such as the ESP32 have established themselves in the IoT area. This MCU has various communication interfaces such as Wifi 2.4 GHz, Bluetooth, SPI, I²C and can be programmed for certain tasks via a scaffolding system such as MicroPython [12].

III. Requirements

The need to collect process parameters from production systems in a timely and comprehensive manner demonstrates the need for an open and extensible wireless system that can be used self-sufficiently in harsh production environments. In the field of machine tools, the essential functions of temperature and vibration measurement offer a decisive added value in order to supplement existing or parallel machine parameters and thus obtain a context-related machine image. This makes it possible to derive detailed information about the machine status and to carry out a holistic, context-related process analysis within the framework of subsequent data evaluations. The aim is an open source, low vibration, modular embedded system as well as corresponding development components in order to offer end users of existing production plants retrofitting possibilities for context formation. At the same time, it must be possible to embed the sensor network into an existing IT infrastructure and, for security reasons, do without a direct internet connection. A further challenge is to implement different sampling rates for the various sensors with regard to their application in the production environment. In the field of vibration measurement, the real-time requirements in terms of application are much higher than for temperature measurement. In addition, the sensor network must record data reliably and at runtime in high quantity and quality as well transmit them via radio transmission.

The sensor network in its entirety can be separated into two parts (see Figure 1): sensor node (data acquisition) and collector (data processing). The former exclusively collect and provide data, the latter clustering a group of subordinate sensor node instances, collects the data and sends it to the next instance either unchanged or preprocessed. The exchange of measurement data and control instructions takes place via Message Queuing Telemetry Transport (MQTT), Python is the ideal programming language for the required scripts. Each sensor node has its own software identification number and publishes its data on its own channel(topic), but all sensor nodes listen on the /instruction channel(-topic), so that central machine-supported control as well as task distribution and adaptation of the individual sensor nodes is possible.

In order to be able to scale the sensor network globally to the required extent, the approach is pursued that 1 to n sensors are combined locally and represented by a collector. Thus, for example, such a collector represents a machine and thus the digital temperature twin of this machine. Individual machines can be combined in any number to form so-called systems, which in turn represent a finite number of production halls. Such a subdivision in the form of a directed tree can be scaled freely and individually for different production systems, since there is no dependency between the individual groups but only a certain local determinacy within a branch. This means that individual objects in a group are self-sufficient in relation to others, which results in a high degree of flexibility.

IV. Realization

Derived from the requirements, the implementation of the sensor node concept with ESP modules (ESP32) in combination with the respective sensor (e.g. temperature sensor DS18D20) results ipso facto from the point of view of energy and resource efficiency. The data collector in the form of a single-board computer (Raspberry Pi) is used for the first data acquisition or data preprocessing. The sensor network thus consists of two basic components (see Figure 1), whereby the sensor maintains a wired connection to the battery-operated ESP module and becomes a sensor node. Thus it represents that part of the continuous data acquisition that can be freely placed at selected points of a machine tool. In order to maintain flexibility with regard to the sensors to be integrated, various protocols (One-Wire, I^2C, SPI, etc.) are supported by the designed structure. This allows the system modularity to be individually adapted to the respective examination case or machine retrofit. Through a corresponding configuration, the ESP module can be integrated into an existing WLAN network or connected via a WLAN network initiated by the single-board computer. Using the first in, first out approach, the measured sensor data is continuously sent to a server address according to the configured time interval. This can be a server on the Internet, which would make the data available worldwide, or a local server solution on the single-board computer or a downstream system. Due to this architectural basic structure, the sensor node is self-sufficient, can be positioned on moving parts of the machine tool to be examined, can be freely scaled in number and enables comprehensive data access. If required, the SBC provides an independent, machine-oriented and local WLAN into which the sensor nodes can integrate themselves in order to preprocess (filter, persist, etc.) or directly process (visualize, calculate, etc.) the recorded sensor values (temperatures). Due to the data persistence in a time series-based database (influxDB) on the single board computer, the data is available near the machine, but can also be transferred to more computationally efficient systems for data analysis purposes (condition monitoring, predictive maintenance, etc.).
To increase robustness, the sensor node has a housing with various signal LEDs and an on/off switch to provide system feedback in a harsh production environment without a display. Various node housings have been designed to protect the electronics from external influences such as moisture, dust and chips. To attach the sensor nodes protected by the housing to the machine parts, magnets are embedded. These are designed in such a way that no dislocation of the sensor nodes takes place even during strong machine movement or vibration. For some applications (e.g. predictive maintenance), a data fusion from the sensor nodes and, for example, the machine control is necessary close to the machine (see Motivation). For this purpose, the data collector is qualified to offer corresponding interfaces (e.g. OPC UA) and to carry out direct data preprocessing and assistance.

V. Summary

The high quality data generated in the production environment represent an important resource in the course of industry 4.0, which must be made more usable in the foreseeable future. For this purpose, a stand-alone solution for the problem of the currently not or only insufficiently sensory recorded parameters of a production system, as for example on hardly accessible parts of a machine tool. The requirements for the retrofit system such as robustness, free scalability and positioning were successfully implemented in this work. The selected hardware components ensure energy efficiency and simple interchangeability while simultaneously integrating into existing wireless networks. Furthermore, the design offers operators of production systems the possibility of cost-effective retrofitting of existing systems, whereby, for example, they can also be retrofitted with predictive maintenance. This sensor network has thus created a solid basis for using data-intensive methods for machine analysis, such as machine learning, condition monitoring and predictive maintenance.

VI. Further Work

As further work, the sensor network must be tested and evaluated in a test field, and a target-oriented solution for the permanent storage of the data must be found. In addition, it would be useful to find out to what extent decentralized storage methods such as blockchains are suitable across the various levels. In order to underline the self-sufficiency of the system and thus its encapsulation, edge computing via the collectors and uniform distribution of the workload over them would be a clever way of performing data processing

and machine analysis and monitoring, while at the same time maintaining a high level of resource efficiency. Furthermore, a change to, or the combination with, other radio technologies such as LoRaWAN or 5G as well as the integration of AR functionalities is worth considering, in order to create a holistic system in the sense of industry 4.0, which continues to transport the strong retrofit idea. In addition, software ecosystems for machine tools must be designed in which sensor nodes, existing controls and future machines can be easyly integrated. This is the only way to offer appropriate microservices that provide manufacturer-independent services to cope with the increasing complexity in mechanical engineering and process automation.

REFERENCES

[1] A. Lotz, Losgröße Eins auf der Werkzeugmaschine, Der Konstukteur 9/2017, Vereinigte Fachverlage GmbH, S. 58, 2017.

[2] R. Neugebauer, Werkzeugmaschine,n S. 6, Springer-Verlag Berlin Heidelberg 2012.

[3] Perspektivenpapier der Forschungsunion: "Wohlstand durch Forschung – Vor welchen Aufgaben steht Deutschland?", S. 54, 2013.

[4] J. Kraus, "Condition Monitoring" in Maschinenmarkt 9/2005, Vogel Communications Group, Feb. 2005.

[5] F. Jung, "Gefreit vor bösen Überraschungen" in Am Puls der Maschine: Condition Monitoring S. 14 - 16, VDMA Verlag 2015.

[6] S. Luber (2019, Jun.), Was ist Predictive Maintenance?, [Online], Available: www.bigdata-insider.de.

[7] A. Hirsch, Werkzeugmaschinen, S. 55 f, Springer Fachmedien Wiesbaden 2016.

[8] Weck, Brecher, Werkzeugmaschinen 4, S. 334 ff, Springer-Verlag Berlin Heidelberg 2006.

[9] P. Frey, M. Lechner, T. Bauer, T. Shubina, A. Yassin, S. Wituschek, M. Virkus, M. Merklein, Blockchain for forming technology – tamper-proof exchange of production data, in press, 2019.

[10] M. Strohmayer. Fruit Pi: Raspberry Pi versus Banana Pi versus Orange Pi. 2017.

[11] K. Berns, B. Schürmann, M. Trapp, Eingebettete Systeme: Systemgrundlagen und Entwicklung eingebetteter Software, S. 147, Vieweg+Teubner Verlag — Springer Fachmedien Wiesbaden GmbH 2010.

[12] Espressif Systems, ESP32 Series Datasheet Version 3.0, S. 1 ff, 2019.

Towards Structural Health Monitoring using Vibro-Acoustic Modulation in the Real World

Peter Oppermann*, Lennart Dorendorf†, Benjamin Boll‡, Abedin Gagani‡, Nikolay Lalkovski†,
Christian Renner*, Marcus Rutner†, Robert Meißner‡§, Bodo Fiedler‡
* *Institute smartPort, Hamburg University of Technology*
† *Institute for Metal and Composite Structures, Hamburg University of Technology*
‡ *Institute of Polymer and Composites, Hamburg University of Technology*
§ *MagIC - Magnesium Innovation Centre, Institute of Materials Research, Helmholtz Centre for Materials and Coastal Research*

***Abstract*—In this paper we explore the opportunities and challenges of deploying a Wireless Sensor Network to monitor the structural health of civil infrastructure using Vibro-Acoustic Modulation. The fundamentals of the method are explained and the challenges for a sensor network in a practical implementation are investigated. Ideas and requirements for the sensor nodes are analyzed and presented.**

***Index Terms*—energy harvesting, vibration sensing, wireless sensor networks**

I. Introduction

Vibro-Acoustic Modulation (VAM) is a non-linear non-destructive testing (NNDT) technique to evaluate the structural integrity of solid materials. It has first been introduced in 1998 in [3]. Since then several research groups have successfully detected fatigue damage in a material using VAM, even before a defect is visible to the bare eye [4].

One potential application for VAM is preventive maintenance of civil infrastructure such as bridges or wind turbines. Not only can continuous monitoring help to prevent collapses and save lives, it can also reduce maintenance cost drastically. Manual inspection is carried out rarely and is costly, time-consuming and error-prone. Further, the early detection of small defects usually allows for simpler and smaller repairs.

A self-powered Wireless Sensor Network (WSN) leverages the potential of VAM-implementations on real-world structures. Because of the complexity of many structures, several sensors in different places are needed for checking all fundamental structural elements, which calls for low-cost hardware. Both sensors and actuators need to synchronize themselves and measurements need to be transmitted to a central place for evaluation. Cable-bound communication and power would drastically increase the cost of deployment. Therefore, an energy harvesting solution is preferable.

In context of the I^3-Lab program at the Hamburg University of Technology we, an interdisciplinary team of researchers from structural engineering, material science and computer science aim to further improve the method's reliability to eventually enable applicability on a real physical structure. During this four-year project, we want to gain new insights in the early process of crack formation through VAM and try to improve the method's prediction capabilities using artificial intelligence. To finally develope a prototype of a WSN on a real structure, we will also work on applying and improving methods from the fields of energy harvesting and transient computing.

In the remainder of the paper, we briefly introduce the VAM method and the underlying principles in Section II. Section III will explain the research questions related to WSNs that need to be addressed during the project. Further, we will give an overview of our first steps in Section IV and lay out planned work for the future in Section V.

This work has been supported by the agency for science, research and gender equality of the city of Hamburg (BWFG, Behörde für Wissenschaft, Forschung und Gleichstellung).

II. Vibro-Acoustic Modulation

The VAM-method uses two sinusoidal signals which are applied to a solid specimen under test (SUT) simultaneously and continuously. The first signal, which we refer to as the modulating signal X_Ω, has a low frequency Ω, and a high amplitude A_Ω. The other signal, which we refer to as the carrier signal X_ω has a much higher frequency ω and a much lower amplitude A_ω.

In a specimen with perfectly linear material behavior, we would only observe a superposition of the two signals and the power spectrum of the resulting signal Y will consist of two bars only (see Fig. 1, left). However, in the presence of defects with nonlinear stiffness properties, e.g. cracks (whose contact area, and thus stiffness, will be varied by the modulating signal), additional sidebands will evolve in the power spectrum at frequencies $\omega \pm \Omega$ (see Fig. 1, right). In other words, a modulation of the carrier signal will be observed.

The modulation of the carrier correlates with the presence and growth of fatigue damage [3]. Figure 2 shows a power spectrum observed in an aluminum specimen after 4000 load cycles. The sidebands at $\omega \pm \Omega$ can clearly be seen and the modulation index is visualized. The exact setup of the experiment is described in Section IV-A.

To measure the intensity of modulation, the Modulation Index (MI) [2] can be calculated from the power spectrum. MI gives the ratio of the Carrier-Amplitude and the Sidebands-Amplitude in dB (see Fig. 2).

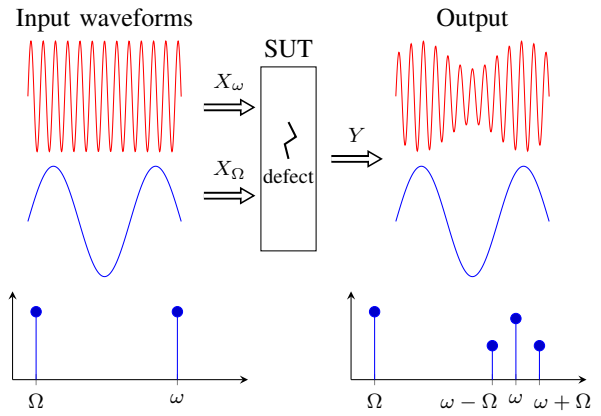


Fig. 1. The carrier signal X_ω is modulated due to nonlinear properties of a crack in the SUT (top). This leads to sidebands emerging in the spectrum of Y (bottom). X_Ω travels through the SUT unchanged

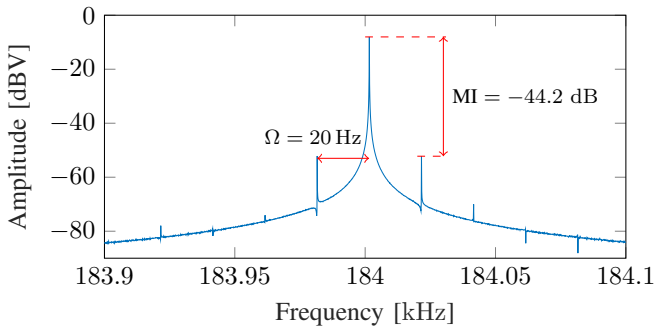


Fig. 2. Power spectrum of a signal recorded with a specimen after 4000 load cycles. Sidebands emerge next to the peak at ω.

Recent research in [2] suggests analyzing the modulation of the carrier in the time domain instead of the frequency domain. This approach might allow the separation of different modulation types, such as amplitude modulation (AM) and frequency modulation (FM), leading to superior evaluation techniques for VAM that are yet to investigate.

III. Research Challenges

To take VAM from the laboratory to a structure in the real world, several limitations still have to be overcome: Knowledge about the influence of specimen geometry, boundary conditions, sensor positioning and structural (not defect-related) nonlinearities on the methods reliability is still largely lacking. A further major challenge is the current lack of an efficient sensor network. It is the latter challenge that will be primarily addressed in this article.

In general we assume to have many nodes that record the modulated signal Y in different locations on the structure, while one of the nodes will be generating X_ω. Because of the advantages mentioned in Section I, we aim to build self-sustained nodes and use wireless transmission of results to a base station.

A. Signal Creation and Sensing

Both the generation of X_ω as well as the sensing of Y happen in the same frequency range since $\omega \gg \Omega$. In [3] ω is in the order of 100 kHz. The exact frequency is chosen by performing a sweep over a range of frequencies and choosing the one that yields the biggest amplitude in Y, which is one resonance frequency of the SUT. Piezoceramic discs can be used both for exciting the material as for sensing in this frequency range. We have conducted first experiments with aluminum specimen, where we observed a strong response Y when applying X_ω with a resonant ω. However, it is still an open question how this scales with bigger dimensions and more complex geometry of the SUT.

Generating the vibration X_Ω in the structure is more challenging. In previous studies in [3] and [2] it has been chosen to be as low as 10 Hz. Moreover the amplitude of the vibration A_Ω effects the intensity of the modulation that we wish to measure [4]. Hence, a high A_Ω is preferable to produce a strong modulation. Unfortunately, this demands an amount of energy that is hard to supply with a self-powered embedded system. Therefore, we plan to use the vibrations that are already present in the structure. Recent studies in [9] and [5] report vibrations introduced into bridges by passing traffic peaking in the range of 3 Hz to 20 Hz and persisting for several seconds. However, these vibrations are significantly different from the laboratory conditions since they are not a sinusoidal wave at a single frequency. They vary in frequency and amplitude depending on the traffic. The exact effect of a varying X_Ω on Y has to be investigated to reach comparable modulation indexes over multiple measurements.

B. Low-Frequency Detection and Synchronization

As discussed in Section III-A we rely on naturally occurring vibrations in the structure as X_Ω. To avoid performing unusable measurements and wasting energy, we hence need to reliably detect a vibration that is strong enough to produce significant modulation on X_ω in the presence of defects. Only then it makes sense for a sensor node to generate X_ω. Since these vibration events only last for a short time and are clearly irregular and potentially rare, an energy conserving mechanism has to be employed to detect the presence of a sufficiently strong vibration without actively and constantly checking. Further, due to the dependence of the modulation on the vibrations amplitude, A_Ω has to be measured or estimated.

In the same way the sensors recording Y need to know when to start their recording of the signal. Therefore, also an energy conserving way needs to be developed for the generating node to trigger the recording at the receiving nodes.

C. Computation and Networking

Requirements for communication between nodes and between nodes and a base station strongly depend on the features that are chosen to assess structural integrity. Ideally, features, e.g. the modulation index can be extracted already on the node, which would drastically reduce the amount of data that has to be transferred from the nodes to the base station. If, however,

more complex algorithms prove to be superior in assessing structural integrity, transfer of the whole time series to the base station might be necessary. This requires higher data rates and increases the energy demand of the nodes compared to single features.

In any case, the recording nodes need to transmit their results to a base station, where they can be processed and finally inspected by maintenance personnel. This base station does not need to be permanently available, but could also be just a maintenance car, that drives by the structure in irregular intervals and checks the current state of the structure.

D. Energy Harvesting

Since the sensor nodes will be distributed across the structure, they may be on hard to reach places. Therefore, self-powered nodes are beneficial to lower maintenance cost. In general, the application is well suited to energy harvesting, since the defects in the structure are expected to arise slowly over long periods of time. Therefore, duty cycling with long charging periods is tolerable.

The described method is relying on naturally occurring vibrations, which makes vibrational energy harvesting an appealing possibility. In case of highway bridges, [7] and [5] have reported average power of vibrational energy harvesting between $300\,\mu\mathrm{W}$ and $660\,\mu\mathrm{W}$ in high traffic times, and [9] even reports peak power of $12.5\,\mathrm{mW}$. Unfortunately the real energy requirement of the application will only become clear during the project runtime as we answer the open research question. Thus, we cannot say yet if vibrational energy harvesting alone will be sufficient. In any case, also solar or wind can be taken into account as energy sources; however, this would either limit the places where the sensors can be deployed on the structure or require more cabling to mount the solar cells or wind harvesters in more appropriate locations.

IV. Preliminaries

A. Reproduce VAM Method

To reliably reproduce the results from [3], we set up an experiment with an aluminum specimen in a tensile testing machine sketched in Fig. 3. The specimen has a notch in the middle to predetermine the cross-section of fatigue failure. Two piezoceramic discs were attached to the probe using an epoxy adhesive. A signal generator and an amplifier are used to produce X_ω with amplitude $A_\omega = 50\,\mathrm{V_{pp}}$ and frequency $\omega = 184\,\mathrm{kHz}$. At the same time, the tensile testing machine generates X_Ω by applying a periodical tensile force between max. $1.25\,\mathrm{kN}$ and min. $0\,\mathrm{kN}$ with $\Omega = 20\,\mathrm{Hz}$ to the specimen. Finally, an oscilloscope is used to record the voltage Y produced by the other piezoceramic disc.

Using this setup, we conducted experiments applying a number of load cycles with the tensile testing machine and performing a measurement every 2000 load cycles. Then we calculated MI from the measurement as described in Section II. Figure 4 shows MI vs the number of load cycles. A strong increase can clearly be seen in the last 8000 load cycles before the specimen finally broke after $39\,000$ cycles.

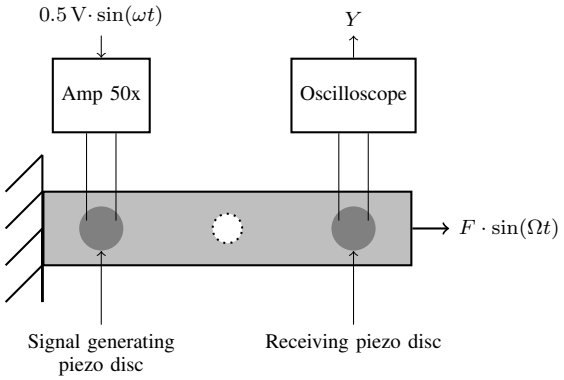


Fig. 3. The experiment setup. Two piezo discs are applied onto an aluminum specimen with a predetermined breaking point. One to generate the carrier signal X_ω and one to measure the modulated signal Y in the specimen.

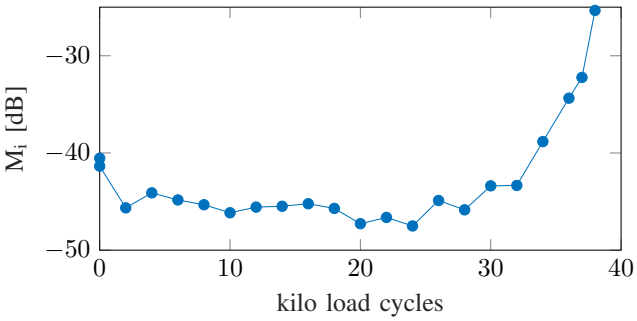


Fig. 4. The modulation index MI in our experiment increased strongly during the last 8000 load cycles. The specimen broke after $39\,000$ cycles.

B. Low-Frequency Detection

To monitor the structure under test for low-frequency vibrations, we have constructed a low-power sensor, that can wake up a microcontroller from sleep mode in the presence of a sufficiently strong vibration X_Ω. It basically consists of a small vibrational energy harvester with a circuit to detect an increasing charge on a capacitor.

As voltage source, we have used a cantilevered piezo stripe. This resembles a spring-mass-damper system, which can be tuned for certain resonance frequencies [6] by varying weight and lever length. However, as [1] shows, the efficiency of vibrational energy harvesting in resonance is inversely proportional to the cube of the resonance frequency ω_0. Therefore, even if the structure under test has a resonance frequency under $10\,\mathrm{Hz}$, the power yield of our system is bigger, if tuned to higher frequencies. Also, to harvest enough energy despite the lower frequencies, bigger amplitudes of the cantilever and a greater weight have to be employed, which results in bigger dimensions. Our prototype is shown in Fig. 5. By manual optimization we settled with a weight and lever length tuning the system to approximately $27\,\mathrm{Hz}$.

Figure 6 shows the circuit used for harvesting inspired by [8]. A bridge rectifier is used to load the capacitor C_1. Since the piezo only produces small voltages in the range of

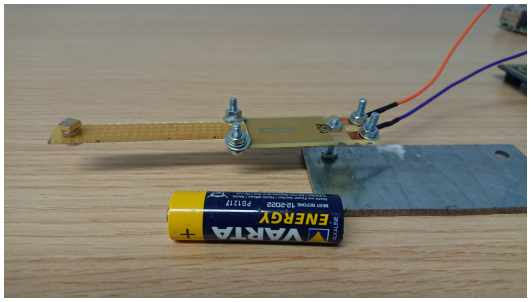


Fig. 5. The cantilevered vibrational energy harvester. For size comparison, a standard AA battery is placed next to the harvester.

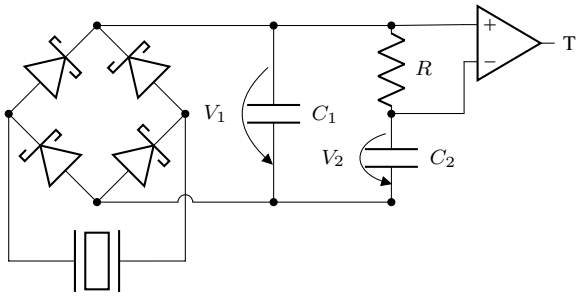


Fig. 6. The trigger circuit has a bridge rectifier. The rectifier's output directly charges C_1. The voltage V_2 on C_2 is low-pass filtered. Therefore, $V_1 > V_2$ on an increase of rectifier output and $V_1 < V_2$ on a decrease of rectifier output.

a few hundred mV, we use Shottky-diodes, which are best suited for this application due to their low forward voltage drop [11]. When vibration increases and the voltage V_1 rises, C_2 is charged over R. A comparator is used to detect the voltage drop across R and produces a logic one while current is flowing into C_2. Whenever vibration decreases, V_1 will drop. This happens due to the reverse leakage current of the diodes in the rectifier. In this case, the current will flow inversely from C_2 to C_1 and the voltage drop over R will also be inverted and the comparator will output a logic zero. This circuit has the advantage that it adapts to constant low vibration level and only triggers when the vibration rises over the usual level. The comparator output T can then be used to wake up the sensor node from a low-power mode, once vibration is sufficient.

The comparator is an active element that constantly draws current. However, using an ultra-low power device such as the TS882 [10], the typical active current is only $220\,\mathrm{nA}$. For comparison, a low-power microcontroller already draws currents in the range of several microampere in sleep mode. Therefore, this detection mechanism is much more energy-conserving than actively measuring the vibrations, even when duty cycling.

The sensitivity and rise time of the trigger can be tuned by the parameters C_1, R and C_2. The only hard constraint to the sensitivity is the hysteresis of the comparator, which has a maximum specified value of $4.2\,\mathrm{mV}$.

V. Future Work

Starting from our experimental setup, in which we reproduced the VAM method, we are currently exploring ways to limit the energy demand of the method. First tests with an oscilloscope suggest that such high signal strengths are not necessary. With a $1.6\,\mathrm{V_{pp}}$ excitation on the transmitting piezo, we could record a clear signal on the receiving piezo. It is still an open question, how well this scales with bigger and more complex specimen under test. Also, we will investigate, how long the bursts of the signal need to be in order to produce reliable results.

As discussed in Section III-B, a way of synchronization is needed for the sensor nodes to notify each other about the start of an acoustic emission. Instead of using a low-power radio one can reuse the piezos for notification. Once a node is ready to start an emission, it can just generate a small burst of a high-frequency acoustic signal. In the same manner as the low-frequency detection in Section IV-B, the receiving nodes can employ a small harvester to produce an interrupt using their piezo discs. It has to be examined, however, how much energy this method demands and how this compares to traditional low-power radio.

Furthermore, tests must be conducted using the vibration detector on real structures like railway and highway bridges to evaluate how the parameters must be tuned in different scenarios to achieve the robustness and sensitivity needed.

References

[1] K. Ashraf, M. H. M. Khir, and J. O. Dennis. Energy harvesting in a low frequency environment. In *2011 National Postgraduate Conference*, 2011.

[2] Dimitri M. Donskoy and Majid Ramezani. Separation of amplitude and frequency modulations in Vibro-Acoustic Modulation Nondestructive Testing Method. *Proceedings of Meetings on Acoustics*, 34(1), 2018.

[3] Dimitri M. Donskoy and Alexander M. Sutin. Vibro-Acoustic Modulation Nondestructive Evaluation Technique. *Journal of Intelligent Material Systems and Structures*, 9(9), 1998.

[4] Philippe Duffour, Marco Morbidini, and Peter Cawley. A study of the vibro-acoustic modulation technique for the detection of cracks in metals. *The Journal of the Acoustical Society of America*, 119(3), 2006.

[5] Andrea Gaglione, David Rodenas-Herraiz, Yu Jia, Sarfraz Nawaz, Emmanuelle Arroyo, Cecilia Mascolo, Kenichi Soga, and Ashwin A. Seshia. Energy neutral operation of vibration energy-harvesting sensor networks for bridge applications. *Proceedings of the 2018 International Conference on Embedded Wireless Systems and Networks*, 2018.

[6] Lei Gu and Carol Livermore. Impact-driven, frequency up-converting coupled vibration energy harvesting device for low frequency operation. *Smart Materials and Structures*, 20(4), 2011.

[7] Yu Jia, Jize Yan, Sijun Du, Tao Feng, Paul Fidler, Campbell Middleton, Kenichi Soga, and Ashwin A Seshia. Real world assessment of an auto-parametric electromagnetic vibration energy harvester. *Journal of Intelligent Material Systems and Structures*, 29(7), 2018.

[8] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. Ambient backscatter: Wireless communication out of thin air. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, pages 39–50. ACM, 2013.

[9] E. Sazonov, H. Li, D. Curry, and P. Pillay. Self-Powered Sensors for Monitoring of Highway Bridges. *IEEE Sensors Journal*, 9(11), 2009.

[10] STMicroelectronics. TS882, TS884. https://www.st.com/resource/en/datasheet/ts882.pdf. Accessed: 2019/06/11.

[11] Ming Yuan, Ziping Cao, and Jun Luo. Characterization the influences of diodes to piezoelectric energy harvester. *International Journal of Smart and Nano Materials*, 9(3), 2018.

A DTLS Abstraction Layer for the Recursive Networking Architecture in RIOT

M. Aiman Ismail, Thomas C. Schmidt
Internet Technologies Group, Dept. Informatik, HAW Hamburg, Germany
{muhammadaimanbin.ismail, t.schmidt}@haw-hamburg.de

***Abstract*—On the Internet of Things (IoT), devices continuously communicate with each other, with a gateway, or other Internet nodes. Often the nodes are constrained and use insecure channels for their communication, which exposes them to a selection of attacks that may extract sensitive pieces of information or manipulate dialogues for the purpose of sabotaging.**

This paper presents a new layer in the RIOT networking architecture to integrate secure communication between applications using DTLS seamlessly. The layer acts as a modular abstraction layer of the different DTLS implementations, enabling swapping of the underlying implementation with just a few lines of code. This paper also introduces credman, a new module to manage credentials used for (D)TLS connections.

I. Introduction

Security is an important part when communicating through the Internet. Although knowing that without proper security practices, bad actors could break into our network infrastructures and cause severe damage to parties involved, there are still numerous devices, IoT appliances in particular, that expose themselves to the Internet without having any proper security measures in place.

Datagram Transport Layer Security (DTLS) [1] is a protocol for traffic encryption on top of UDP [2]. It is based on the concepts of TLS [3] and provides equivalent security guarantees. DTLS guarantees reliable transport during the handshake process but maintains UDP transport properties during application data transfer. The protocol is deliberately designed to be as similar to TLS as possible, both to minimize new security inventions and to maximize the amount of code and infrastructure reuse.

RIOT [4] is an open-source real-time OS, based on a modular architecture built around a lightweight micro-kernel, and developed by a worldwide community of developers. The modular approach enables easy prototyping and development to test new ideas and deploy applications. Its default network stack GNRC follows a cleanly layered, recursive design that easily allows for stacking and exchanging protocol layers or implementations.

In this paper, we describe how we built the DTLS abstraction layer on top of existing components in the RIOT networking architecture. This layer provides an API that can be implemented using third-party DTLS libraries. It is designed to be independent of the underlying DTLS implementation, therefore allows the DTLS stack to be exchanged without altering the applications that use it. We also introduce a new RIOT module *credman* to manage the credentials used for the handshake.

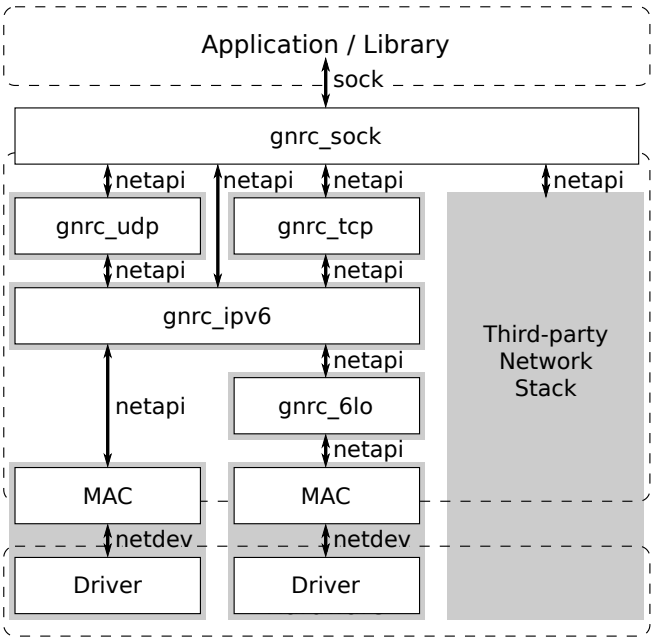


Fig. 1. RIOT networking stack

The remainder of this paper is structured as follows. In Section II, we introduce the existing networking stack of RIOT. In Sections III, we describe the new secure network stack, and Section IV presents experiments that assess its performance. In Section V, we conclude with an outlook on future work.

II. RIOT networking subsystem

The RIOT networking subsystem is designed to follow a modular architecture with clean interfaces for abstracting all layers [5]. This facilitates the creation and integration of new protocols, different implementations, or additional layers such as a new encryption layer to the existing stack. It consists of two external APIs *netdev, sock*, and a single internal API for communication between layers, *netapi*. It is noteworthy that the RIOT networking subsystem simultaneously supports multiple interfaces with different protocol stacks, which makes it capable of running gateway services. An architectural overview is visualized in Figure 1.

The Device Driver API: netdev. Individual network devices in RIOT are abstracted via *netdev*, which allows networking stacks access to the devices via a common, portable interface. *netdev* remains neutral in that it does not enforce implementation details regarding memory allocation, data flattening, and threading. These decisions are delegated to the users of the interface.

The Internal Protocol Interface: netapi. Internal protocol layers in the RIOT networking subsystem can be recursively composed via the *netapi*. The interface is kept simple so that even an exotic networking protocol could be implemented against it. Messages passed between layers are typed as following: two asynchronous message types (`MSG_TYPE_SND, MSG_TYPE_RCV`) and two synchronous message types (`MSG_TYPE_GET, MSG_TYPE_SET`) that expect a reply with the type `MSG_TYPE_ACK`. No further semantic is built into the messages of *netapi*, but certain preconditions on packets or option values handed to *netapi* can be set as requirements to implement more complex behavior that goes beyond these plain specifications.

The User Programming API: sock. This module provides a network API for applications and libraries in RIOT. It provides a set of functions to establish connections or send and receive datagrams using different types of protocols. In comparison to POSIX sockets, *sock* does not require complex and memory expensive implementation and therefore more suited for use in constrained hardware. Only common types and definitions from either *libc* or POSIX are used. This ensures that *sock* is easy to port to other target OS.

GNRC is the native IPv6 networking stack for RIOT. It takes full advantage of the multi-threading model supported by RIOT to foster a clean protocol separation via well-defined interfaces and IPC. Each network protocol is encapsulated in its own thread and uses RIOT thread-targeted IPC with a message queue in each thread to communicate between layers. Other stacks that introduce different networking protocols such as ICN also integrate via the same interfaces. Various experimental evaluations and benchmarks [5], [6] have proven the feasibility and efficiency of this flexible approach to networking in RIOT.

III. Introducing the secure network stack

The modular nature of the existing GNRC stack allows for an easy extension by adding DTLS at the top while maintaining its modularity. We introduced two new modules *credman* and DTLS sock (see Figure 2).

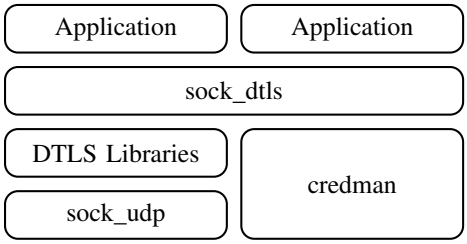


Fig. 2. Architecture of sock_dtls

credman is a module to manage credentials used in (D)TLS encryption protocols. Credentials registered with the system are identified by using the tuple of the int-based tag *credman_type_t* and the credential type *credman_tag_t*. This in combination with the DTLS sock API allows users to register multiple credentials of the same type, which can be the case if the nodes are communicating with multiple other nodes simultaneously and each node uses different credentials for authentication. *credman* does not copy the credentials into the system memory. It only has information about the credentials and points to the location of the credential itself, which can be stored in protected regions of the memory. Users have to ensure that a credential is available at the location given to credman during the lifetime of their application.

We defined a new *sock* type — *sock_dtls*. It is designed to mimic the behavior of UDP sock as closely as possible so that integrating it into existing applications can be done with little changes. By adding a line in the Makefile, users can choose which underlying DTLS implementation to use. Swapping to a new DTLS implementation is done by specifying the corresponding implementation in the Makefile. Through this mechanism, testing and evaluation of DTLS implementations can be performed without altering the application.

Figure 2 summarizes the integration of the DTLS abstraction layer with the existing network stack in RIOT. Currently, RIOT only has support for tinyDTLS[1], but there is ongoing work[2] to add support for wolfSSL[3].

The procedure to set up a DTLS server can be summarised as follows:

1) Register credentials available for use
2) Create the UDP sock for the transport layer
3) Create the DTLS sock
4) Start listening for incoming datagram packets

The steps are similar for a DTLS client, except for the latter part:

4) Establish session with a DTLS server
5) Start sending and receiving datagram packets

Listing 1 and Listing 2 shows a simplified code for a secure echo client using DTLS sock and tinyDTLS respectively.

```
int main(void) {
    credman_credential_t credential = {...};
    credman_add();
    sock_udp_create();
    sock_dtls_create();
    sock_dtls_session_create();
    int res = sock_dtls_send();
    if (res > 0) {
        sock_dtls_recv();
    }
}
```

Listing 1. DTLS sock code example

[1]https://projects.eclipse.org/projects/iot.tinydtls
[2]https://github.com/RIOT-OS/RIOT/pull/10308
[3]https://www.wolfssl.com

```
static int _write() {...}
static int _read() {...}
static int _psk() {...}
static dtls_handler_t cb = {
    .write = _write,
    .read = _read,
    .get_psk_info = _psk,
};

int main(void) {
    dtls_context = dtls_new_context();
    if (new_context)
        dtls_set_handler(new_context, &cb);
    sock_udp_create();
    dtls_connect();
    int res = dtls_write();
    if (res > 0) {
        sock_udp_recv();
        dtls_handle_message();
    }
}
```

Listing 2. TinyDTLS code example

IV. Experiments and Evaluation

We are now ready to validate our concept and assess the performance of our implementation. We compared DTLS sock with tinyDTLS and UDP sock and examine the metrics CPU overhead and goodput during the transmission of payloads, memory consumption as well as lines of code (LOC) needed. All measurements were performed on *samr21-xpro* boards positioned side-by-side over the 802.15.4 wireless radio network [7] with 6LoWPAN encapsulation and header compression [8].

We wrote three versions of a client and a server program that sends packets of increasing payload sizes from the client to the server while recording the time taken to transmit the packets. The first version uses tinyDTLS directly while the second version uses our new DTLS abstraction layer DTLS sock with tinyDTLS. The third version employs no encryption layer but uses RIOT UDP sock API *sock_udp* to transmit the packets and acts as a controlling baseline.

The test was set up as follows unless stated otherwise. The server is instantiated to listen for new connections and receives packets from clients. For each received packet, the payload size is logged into a file. On the client, two metrics are measured: the time taken to process a packet for the full network stack, that is (1) DTLS, UDP, IP, 6LoWPAN, MAC, and auxiliary components, and (2) the time taken to process only the DTLS part of the transmission, which starts from accepting the packet from the user and encrypting it using specified keying materials to just before passing it to the UDP layer for further processing. The test is run with payload size ranging between 25 Bytes and 300 Bytes in 25 Bytes intervals. Each configuration is repeated 5000 times with averages and standard deviations recorded in the following diagrams.

CPU Overhead. Figure 3 depicts the CPU overhead during packet transmission. The test program using DTLS sock and tinyDTLS need approximately the same average processing time per packet with DTLS sock being slightly higher. The extra overhead when adding an abstraction layer is expected as a tradeoff for faster prototyping time and ease of use, which in this case is virtually negligible. The steps-shaped line for the full-stack processing can be attributed to the fragmentation of packets by the underlying 6LoWPAN layer when certain size limits are reached. Comparison of the times taken to process only the DTLS layer shows an almost linear line of the processing time with increasing payload size, and again, there is only a little difference between the values. This indicates that our DTLS sock abstraction layer comes at negligible processing overhead.

Goodput. The average goodput is shown in Figure 4. It follows the same trend with the DTLS sock version admitting approximately the same performance values as the tinyDTLS version. These results not only indicate a picture consistent with processing but also confirm the robustness of our interface layer.

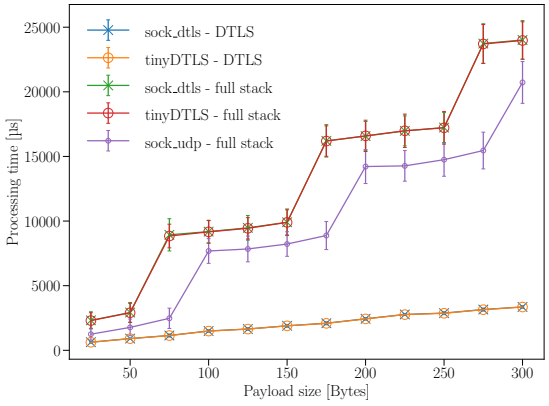


Fig. 3. CPU Overhead

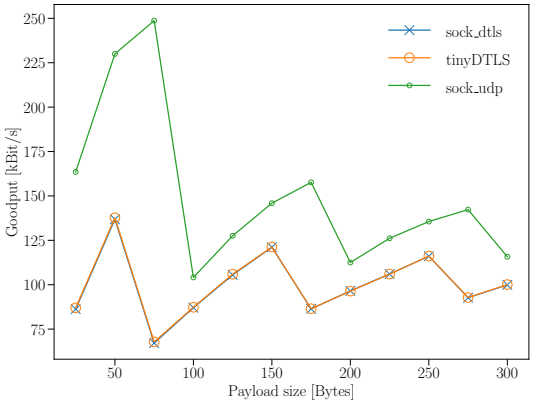


Fig. 4. Average Goodput

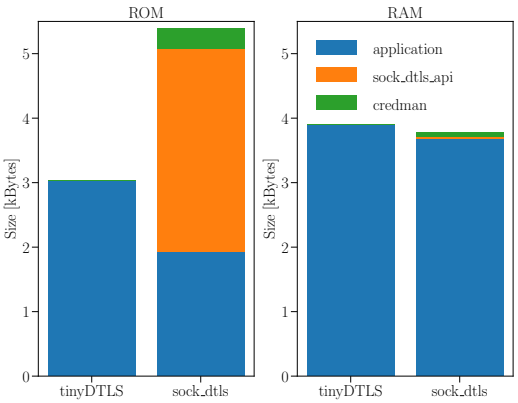


Fig. 5. Memory Usage

Memory. Figure 5 compares the memory consumptions of the different DTLS code versions. Here we measured the memory usage of a simple echo client and server application implemented using DTLS sock and tinyDTLS instead of our test application to mirror a standard DTLS application compared to the test application. The hardware setup is the same.

The RAM usage of both programs is similar to DTLS sock saving around 120 Bytes compared to tinyDTLS. This saving is mainly contributed by the compiler, which can optimize away some of the variables used for the sending and receiving functions in user application but not in tinyDTLS. As a result, even though we need about 80 Bytes more in DTLS sock for *credman* and the API, we still end up using less RAM. Nevertheless, because the saving is only around 100 Bytes and is mainly caused by compiler optimization, we could say that the RAM usage is approximately the same in both versions and the exact value is determined by the quality of implementation in user application.

In contrast, the ROM usage in DTLS sock is about two kilobytes larger than in tinyDTLS. The larger ROM size is due to the code size of DTLS sock. This value is implementation specific as each implementation needs to be implemented against the DTLS sock interface first before used as the underlying implementation of DTLS sock. When using tinyDTLS specifically, we could delegate the bulk of credential management to *credman*. For tinyDTLS, this must be implemented as callbacks by the users. This simplifies the user application and achieves around the same performance using less code.

Lines of Code. This metric serves as a rough guideline to compare the ease of use of the interface. When writing a DTLS application using tinyDTLS directly, users are required to implement the callback functions for sending and receiving the packets as well as the credential loading and comparison as seen in Listing 2. DTLS sock handles this for the user, taking over the task of writing boilerplate code and reducing the total LOC of the user application by about **150** lines. Due to the stack-agnostic nature of the DTLS sock, the user can focus on their applications instead of learning how to use a particular DTLS stack each time they want to test a new stack.

V. Conclusion and Future Works

In this paper, we introduced and analyzed the new DTLS abstraction layer designed to be modular and easy for integrating into existing applications. We demonstrated that the tradeoff between performance and ease of use is well acceptable for typical use cases. Leveraging a clean and implementation-independent interface, we increased the portability of applications and also the maintainability of upper layer protocol implementations such as CoAP [9] over time.

In the future, we will work on implementing a DTLS profile for authentication and authorization for the constrained environment, such as [10] to provide a framework for a secure network infrastructure. The integration of DTLS sock in upper-layer protocols such as the RIOT *gcoap*[4]is also on our schedule.

References

[1] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," IETF, RFC 6347, January 2012.
[2] J. Postel, "User Datagram Protocol," IETF, RFC 768, August 1980.
[3] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF, RFC 8446, August 2018.
[4] E. Baccelli, C. Gündogan, O. Hahm, P. Kietzmann, M. Lenders, H. Petersen, K. Schleiser, T. C. Schmidt, and M. Wählisch, "RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4428–4440, December 2018. [Online]. Available: http://dx.doi.org/10.1109/JIOT.2018.2815038
[5] M. Lenders, P. Kietzmann, O. Hahm, H. Petersen, C. Gündogan, E. Baccelli, K. Schleiser, T. C. Schmidt, and M. Wählisch, "Connecting the World of Embedded Mobiles: The RIOT Approach to Ubiquitous Networking for the Internet of Things," Open Archive: arXiv.org, Technical Report arXiv:1801.02833, January 2018. [Online]. Available: https://arxiv.org/abs/1801.02833
[6] C. Gündogan, P. Kietzmann, M. Lenders, H. Petersen, T. C. Schmidt, and M. Wählisch, "NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT," in *Proc. of 5th ACM Conference on Information-Centric Networking (ICN)*. New York, NY, USA: ACM, September 2018, pp. 159–171. [Online]. Available: https://conferences.sigcomm.org/acm-icn/2018/proceedings/icn18-final46.pdf
[7] IEEE 802.15 Working Group, "IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE, New York, NY, USA, Tech. Rep. IEEE Std 802.15.4™–2011, Sep 2011.
[8] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF, RFC 4944, September 2007.
[9] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, RFC 7252, June 2014.
[10] S. Gerdes, O. Bergmann, C. Bormann, G. Selander, and L. Seitz, "Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)," IETF, Internet-Draft – work in progress 01, March 2017.

[4]https://riot-os.org/api/group__net__gcoap.html

A Test Bench to Collect Electrical Appliance Load Signatures and Ambient Conditions

Daniel Serbu, Andreas Reinhardt
Technische Universität Clausthal
Clausthal-Zellerfeld, Germany
dani.serbu@gmail.com, reinhardt@ieee.org

***Abstract*—Most electrical appliances exhibit characteristic power consumption patterns, so called *load signatures*, during their operation. Through the application of signal processing and machine learning, these characteristics can be extracted and subsequently leveraged to identify appliance activities, their modes of operation, and even the impending need for maintenance. A research domain that has not yet experienced extensive activity, however, is to what extent a correlation between appliance activity and ambient conditions exists. In other words: Do appliances exhibit *characteristic* features in non-electrical domains (e.g., temperature, vibration, sound, magnetic field, etc) during their operation and/or when state changes happen? In order to accelerate the research activities in this field, we present a data collection setup to investigate these dependencies in detail. Our test bench facilitates the collection of electrical voltage and power samples while enabling a variable amount of ambient features to be captured using wireless sensing devices. By enabling the analysis of dependencies between electrical and ambient sensor data, we foster the creation of improved energy data analysis methods. We show that our data acquisition test bench is capable of creating a time-synchronized data set, comprised of ambient data and energy measurements at high sampling rates.**

I. Introduction

Since the publication of George Hart's seminal work on non-intrusive load monitoring (NILM) in 1985 [1], research activities to extract and utilize the information content in electricity consumption data have seen an almost exponential increase. Data sets to train and test such algorithms have been collected by research teams around the globe. A commonality of virtually all data sets in this domain (e.g., [2]–[4]) is their exclusive focus on purely electrical features, mostly voltage and current readings, or electrical power as the product of both. Only a few data sets provide additional annotations, e.g., occupancy information [5], user-generated events [6], or user activities [7]. This emphasizes the prevailing assumption that electrical features are the primary phenomena to capture when trying to infer more details about appliances. In fact, only very few works have determined to what extent appliance activity can be sensed without relying on electrical data, e.g., through appliances' acoustic signatures [8], [9]. This is surprising, given that the great potential of data set annotations was determined in [10], [11], and the practical cases in [12]–[16] confirm how appliances' ambient information can be further exploited. Still, no existing data set features comprehensive annotations by ambient conditions and metadata, in order to facilitate such research activities.

This has motivated us to create a versatile test bench for the simultaneous collection of electrical consumption data and ambient conditions. It combines the accurate collection of energy-related features (through the use of dedicated measurement hardware) with an extensible sensor network to capture ambient information in the required detail. The test bench facilitates the collection of comprehensive data sets, which in turn allow for the development of improved NILM approaches. For example, a better disambiguation can be achieved between a kitchen light and a ceiling light fixture with similar power consumption by correlating their operation with measurements of light intensity, light temperature, or the user's currently pursued activity. Our practical implementation of the test bench is shown in Fig. 1.

Our test bench allows researchers to capture both short-term appliance operation data (like in PLAID [17], where only appliance start-up transients of a few seconds length have been captured) as well as long-time traces (like in AMPds [18], which spans several months). It is easy to replicate due to its reliance on commercially available devices, and represents a valuable tool to accelerate research in NILM and other energy-centric research fields. We discuss its architecture and the hard- and software design decisions in Sec. II. Subsequently, we demonstrate the system's practical use in Sec. III. We conclude our paper in Sec. IV.

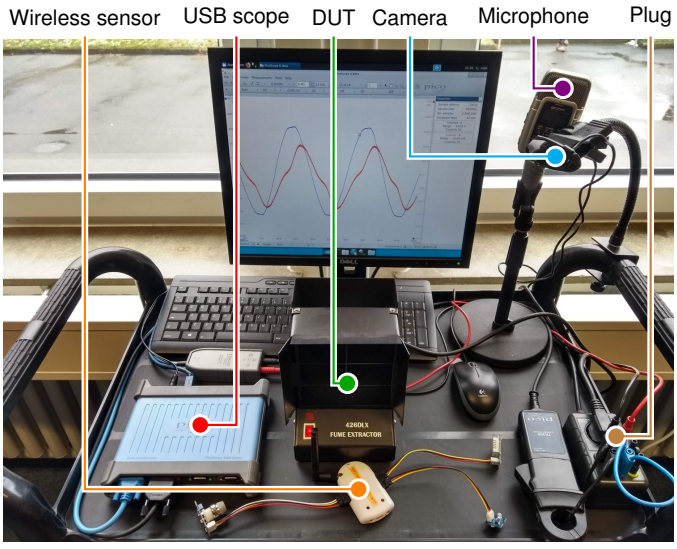


Fig. 1. Practical setup of the data collection test bench.

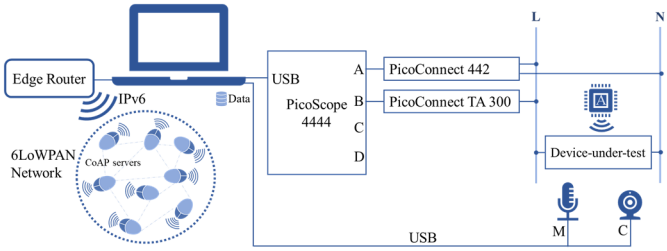


Fig. 2. Schematic setup of the data acquisition architecture.

II. System Overview

In order to enable accurate energy data analysis, both the mains voltage and the current flowing into an electrical appliance must be sampled at a high temporal and amplitude resolutions. Moreover, in order to enable the investigation of dependencies between ambient conditions and energy consumption, corresponding contextual data must be recorded. Thus, the following three design decisions need to be made:

1) Suitable transducers to capture voltage and current signals need to be carefully selected,
2) Sensors for the ambient conditions must be chosen and their integration must be catered for, and
3) Collected data must be consolidated and stored in a scalable and time-synchronized manner.

We discuss our design considerations and the practical realizations of each of these aspects as follows.

A. Sensing Electrical Quantities

In order to collect an electrical appliance's load signature, the voltage across an its terminals as well as the current it consumes must be synchronously captured. Through their multiplication, the appliance's demand for real, reactive, and apparent electrical power over time can be extracted. To support a wide range of sampling frequencies and ensure accurate readings, we have have relied on a USB oscilloscope to collect electrical load signatures. Since the scientific community has not yet converged to an optimum sampling rate for appliance detection, we have decided to use a default sampling rate of 40 kHz, which was already highlighted as a meaningful design choice by Armel et al. in [19] and is in-line with approaches presented recently [20]. The system has been developed to allow for later changes of this setting. Our data acquisition unit for electrical quantities is comprised of the following components:

- PicoScope 4444[1] with a maximum sampling rate of 256 MS/s, a bandwidth of 20 MHz and an amplitude resolution of 14 bit.
- PicoConnect 442 voltage probe with a measurement range up to 1000 V and a signal bandwidth of 100 MHz.
- PicoConnect TA300 current probe with a measuring range of up to 40 A AC/DC and a signal bandwidth of 100 kHz.

[1] www.picotech.com/download/datasheets/picoscope-4444-data-sheet.pdf

The electrical data acquisition setup is schematically shown in Fig. 2, where voltage and current probes are directly connected to the power inlet of the device-under-test (DUT). The diagram also highlights the presence of a PC that controls the USB oscilloscope and stores its readings using the CSV file format.

B. Ambient Context Sensing

To enhance the collected electrical consumption data by the ambient conditions at the time of collection, we use a modular sensing system setup. Only two sensor types are hard-wired into the system in order to collect *ground truth* information from the electrical appliance: A USB microphone and a USB camera. The stereophonic two-way (front and rear) microphone is being used to capture all acoustic emissions appliances exhibit during their operation. The USB webcam is mounted on a movable arm in order to allow for its free positioning to capture all user interactions with the DUT. Streams of both sensor modalities are recorded in their native formats (WAV and MPEG4, respectively).

Besides the wired sensor devices, a wireless sensor network gateway is attached to the computer to allow for the modular extension of the sensing setup by additional modalities. We have specifically chosen to use wireless devices in order to enable their free placement on and around the DUT, e.g., to monitor the temperature inside a refrigerator or capture button presses. Our wireless sensors are based on the Zolertia RE-Mote platform [21] and rely on 6LoWPAN to communicate over the IEEE 802.15.4 standard in the 2.4 GHz ISM band. The actual interfacing to the data provided by physical sensors is implemented based on the CoAP protocol [22], as part of the Contiki operating system. This choice of service abstraction makes a later addition and removal of sensor services easily possible, and caters to the long-term operability of our system.

Each wireless node implements a CoAP server which offers resources (through URIs) for all attached physical sensor devices. Through CoAP's auto-discovery feature, available resources are identified by the controlling system before a data collection process is started. CoAP allows two different methods (`GET` and `OBSERVE`) to be used to obtain sensor data from wireless devices. Currently, the `OBSERVE` method is being used to obtain data from all connected sensors, at a polling rate of 1 Hz. The actual data exchange is performed via a 6LoWPAN edge router, which forwards wireless sensor data to the computer, shown in the left-hand part of Fig. 2.

C. Data Storage and Postprocessing

A set of scripts has been developed to concurrently capture all data streams and write their data to the PC's disk storage. By annotating all recorded data streams with the computer's local timestamp, their tight time synchronization is guaranteed. Delays of up to 1 s are, however, experienced for events from the wireless sensor network, which are only polled periodically from all wireless sensors. While the wireless nature of the communication channel does not provide real-time guarantees, practical testing (cf. Sec. III-C) has still shown events to be recorded in a timely manner.

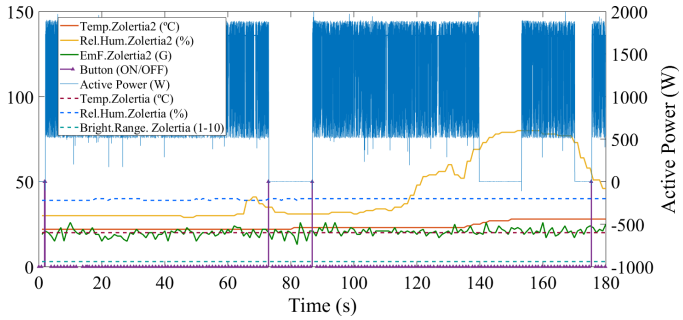


Fig. 3. Overlay visualization of the water kettle's multimodal sensor streams.

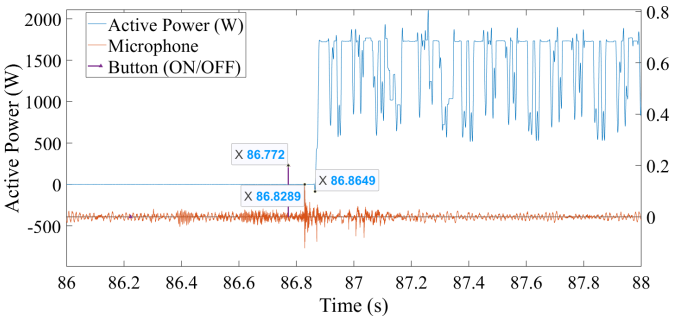


Fig. 4. Temporal displacement between button, electrical, and acoustic data.

All data are stored without any further postprocessing applied to preserve their characteristics in full. We thus leave it up to the individual researcher to define the postprocessing needs, e.g., the application of different mathematical operations [23], [24] or the extraction of features for their use in conjunction with machine learning algorithms. We would also like to note that the video recording is only supposed to be a reference for the easier interpretation of the other captured values. This way, events collected from electrical, acoustic, and ambient parameters can be correlated more easily with the actual appliance operation and possible user interaction.

III. Practical Use of the Test Bench

After having introduced the design rationale of our data collection test bench, we share some insights from its practical operation next. We use an electric water kettle as the DUT.

A. Step-by-Step Operation Sequence

The following steps are needed to record traces for the DUT.

1) Sensor Choice and Installation: Considerations need to be made regarding the potential sensor data streams of interest. In our case, by way of example, we consider temperature and humidity changes above and on the side of the kettle, as well as changes to the electromagnetic field and the luminosity surrounding the kettle. Thus, two wireless sensors are deployed: One that is mounted above the kettle to monitor temperature and humidity, and a second one that logs the electromagnetic field, brightness, temperature, humidity, as well as when users press the activation button. Corresponding CoAP resources have been implemented in Contiki, such that their automatic identification is facilitated.

2) Connect the Device-under-Test: Once all sensors have been configured, the DUT is placed on the test bench and the wireless sensors are brought into position. Flexible mounting options (such as visible on the right of Fig. 1) help to keep the wireless devices in place. Besides the wireless sensors, both camera and microphone are positioned to capture signals accurately. Lastly, the power plug of the DUT is attached to mains power via the oscilloscope.

3) Conduct the Measurement: Our sensing setup allows the sampling rate and resolution of the oscilloscope to be defined (if they deviate from the default rate of 40 kHz). Once all configuration settings have been defined, the actual data collection process is initiated. The measurement scripts on the computer contain an initial waiting time that is required to initialize and stabilize the readings of all sensors; in practice, this takes up to 10 s. Once this time has elapsed, the user can interact with the DUT like during regular operation (i.e., start its operation and provide further input as relevant) in order to collect its load signature.

4) Stop the recording: Many appliances operate according to an internal state machine [1]. Thus, their operational sequence terminates after all relevant operational phases have completed. Once the appliance's operation has terminated and no further data shall be recorded, the user can stop the recording. This triggers all data file streams to be closed, such that the data are available for further processing.

B. Sample Measurements

We show results from a run of the water kettle in Figs. 3 and 4. To unify the view of all different measured entities (including temperature, relative humidity, environmental brightness, and others), we present a graphical representation of the data in Fig. 3. Note that video content is not shown in the figure, since the camera is only meant to provide a visual ground truth for manual annotation. The left y-axis represents the range of the values of the environmental sensors (uncalibrated), whereas the right y-axis relates to the electrical power data (visible in the top of the graph). The total duration of the experiment was 180 s.

The impact of the operated electrical appliance on the ambient parameters becomes visible from the graph in several aspects: First, presses on the kettle's power button (happening at time offsets 2, 73, 87, and 175 of the recording) indicate the user interaction with the device. It also becomes apparent that one event was missed (at time offset 154) due to unknown reasons. Second, the electrical power consumption, visible in the top of the diagram, varies between fully active operation (500 W to 2000 W) and inactivity (0 W), depending on the user interaction with the water kettle. Third, the humidity level rises towards the end of a water boiling process because of the steam evaporating from the opening. Fourth, a higher temperature can also be observed above the kettle as the water heating process evolves. Lastly, the remaining environmental sensors maintain stable values given their unrelatedness to the kettle's operation.

C. Event synchronization

An accurate synchronization between events is crucial to correctly interpret the collected multi-modal sensor data streams. To confirm the degree of synchronization of logged events, we zoom in on the sensor streams for the time frame between 85–87 seconds after the recording has been started. The results are illustrated in Fig. 4 and show the corresponding data except during which the button of the kettle is pushed and the corresponding change to active power is observed. Besides the electrical power intake, the user button's action and the amplitude of the signal recorded from the microphone is shown. Although the three elements do not match exactly in the time step where the kettle is turned on, the time difference between events is below $100\,\mathrm{ms}$, which can be considered close enough for many aspects of energy data analysis. It needs to be noted, however, that the periodic polling of CoAP services may introduce delays of up to $1\,\mathrm{s}$.

IV. Conclusions

Most data sets that have been released to be used in conjunction with NILM feature only measurements of electrical voltage and current, or appliance power consumption. However, many ambient conditions are directly influenced by appliance operation. Such dependencies cannot be resolved using currently available data sets because ambient information is generally not provided alongside the electrical data. We have therefore presented a system that has the capability to record both electrical and non-electrical sensor data with a high sampling rate. Through the use of an extensible wireless sensor network based on the CoAP protocol, the integration of sensors for various modalities is simplified. Data collected using our test bench can be used to improve disaggregation algorithms to detect appliances from the overall usage and thus foster future developments. An open question that remains to be resolved in future work is the further processing of collected data. Software to automatically extract relevant features from the multi-modal sensor streams is required to simplify and unify the data analysis process, and reduce the need for human interaction to a minimum.

Acknowledgments

This research was supported by Deutsche Forschungsgemeinschaft (DFG) grant no. RE 3857/2-1.

References

[1] G. W. Hart, "Prototype Nonintrusive Appliance Load Monitor," MIT Energy Laboratory and Electric Power Research Institute, Tech. Rep., 1985.

[2] J. Z. Kolter and M. J. Johnson, "REDD: A Public Data Set for Energy Disaggregation Research," in *Proceedings of the Workshop on Data Mining Applications in Sustainability (SustKDD)*, 2011.

[3] A. Reinhardt, P. Baumann, D. Burgstahler, M. Hollick, H. Chonov, M. Werner, and R. Steinmetz, "On the Accuracy of Appliance Identification Based on Distributed Load Metering Data," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet and ICT for Sustainability (SustainIT)*, 2012, pp. 1–9.

[4] N. Batra, M. Gulati, A. Singh, and M. B. Srivastava, "It's Different: Insights into Home Energy Consumption in India," in *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings (BuildSys)*, 2013.

[5] C. Beckel, W. Kleiminger, R. Cicchetti, T. Staake, and S. Santini, "The ECO Data Set and the Performance of Non-intrusive Load Monitoring Algorithms," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings (BuildSys)*, 2014.

[6] K. Anderson, A. Ocneanu, D. Benitez, D. Carlson, A. Rowe, and M. Berges, "BLUED: A Fully Labeled Public Dataset for Event-Based Non-Intrusive Load Monitoring Research," in *Proceedings of the 2nd KDD Workshop on Data Mining Applications in Sustainability (SustKDD)*, 2012.

[7] A. Alhamoud, F. Ruettiger, A. Reinhardt, F. Englert, D. Burgstahler, D. Boehnstedt, C. Gottron, and R. Steinmetz, "SMARTENERGY.KOM: An Intelligent System for Energy Saving in Smart Home," in *Proceedings of the 3rd Workshop on GlObal Trends in Smart Cities (goSMART)*, 2014.

[8] F. Englert, I. Diaconita, A. Reinhardt, A. Alahamoud, and R. Steinmetz, "Reduce the Number of Sensors: Sensing Acoustic Emissions to Estimate Energy Wastage," in *Proceedings of the 5th ACM Workshop On Embedded Systems For Energy-Efficient Buildings (BuildSys)*, 2013.

[9] M. A. Guvensan, Z. C. Taysi, and T. Melodia, "Energy Monitoring in Residential Spaces with Audio Sensor Nodes: TinyEARS," *Ad Hoc Networks*, vol. 11, no. 5, 2013.

[10] A. Schoofs, A. Guerrieri, D. T. Delaney, G. M. O'Hare, and A. G. Ruzzelli, "ANNOT: Automated Electricity Data Annotation using Wireless Sensor Networks," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2010.

[11] H. Cao, T. K. Wijaya, K. Aberer, and N. Nunes, "A Collaborative Framework for Annotating Energy Datasets," in *Proceedings of the 2015 IEEE International Conference on Big Data (Big Data)*, 2015.

[12] A. Rowe, M. Berges, and R. Rajkumar, "Contactless Sensing of Appliance State Transitions through Variations in Electromagnetic Fields," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys)*, 2010.

[13] A. G. Ruzzelli, C. Nicolas, A. Schoofs, and G. M. O'Hare, "Real-time Recognition and Profiling of Appliances Through a Single Electricity Sensor," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2010.

[14] J. Yoo, B. Park, and K. Hur, "Context Awareness-based Disaggregation of Residential Load Consumption," *IFAC Proceedings Volumes*, vol. 44, no. 1, 2011.

[15] M. Uddin and T. Nadeem, "EnergySniffer: Home Energy Monitoring System using Smart Phones," in *Proceedings of the 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2012.

[16] M. Bergés, L. Soibelman, and H. S. Matthews, "Leveraging Data from Environmental Sensors to Enhance Electrical Load Disaggregation Algorithms," in *Proceedings of the 13th International Conference on Computing in Civil and Building Engineering (ICCCBE)*, 2010.

[17] J. Gao, S. Giri, E. C. Kara, and M. Bergés, "PLAID: A Public Dataset of High-resolution Electrical Appliance Measurements for Load Identification Research," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings (BuildSys)*, 2014.

[18] S. Makonin, F. Popowich, L. Bartram, B. Gill, and I. V. Bajic, "AMPds: A Public Dataset for Load Disaggregation and Eco-Feedback Research," in *Proceedings of the Electrical Power and Energy Conference (EPEC)*, 2013.

[19] K. C. Armel, A. Gupta, G. Shrimali, and A. Albert, "Is Disaggregation the Holy Grail of Energy Efficiency? The Case of Electricity," *Energy Policy*, vol. 52, 2013.

[20] B. Völker, P. M. Scholl, and B. Becker, "Semi-automatic generation and labeling of training data for non-intrusive load monitoring," in *Proceedings of the Tenth ACM International Conference on Future Energy Systems (e-Energy)*, 2019.

[21] Zolertia S.L., "Re-Mote Data Sheet," 2019. [Online]. Available: https://zolertia.io/product/re-mote-suite/

[22] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," RFC 7252, 2014.

[23] J. Liang, S. K. K. Ng, G. Kendall, and J. W. M. Cheng, "Load Signature Study – Part I: Basic Concept, Structure, and Methodology," *IEEE Transactions on Power Delivery*, vol. 25, no. 2, 2009.

[24] ——, "Load Signature Study – Part II: Disaggregation Framework, Simulation, and Applications," *IEEE Transactions on Power Delivery*, vol. 25, no. 2, 2009.

Haptic Communication Latency in Large-Scale Wireless Mesh Networks

Frank Engelhardt, Mesut Güneş
Communication and Networked Systems (ComSys)
Faculty of Computer Science
Otto-von-Guericke University Magdeburg
Universitätsplatz 2, 39106 Magdeburg, Germany
{fengelha,guenes}@ovgu.de

***Abstract*—Haptic Communication will be an integral part of the future Tactile Internet. While IEEE 802.11 (WiFi) networks achieved an outstanding market penetration to the day, their readiness to stand the upcoming requirements for Haptic Communication services are yet to be proven. We discuss the major problems that arise in IEEE 802.11 networks for Haptic Communication and propose a linear modeling approach that is capable of median latency prediction, which is one of the key Quality of Service (QoS) properties.**

***Index Terms*—Haptic Communication, Wireless Multi-Hop Networks, Carrier Sense Multiple Access, Tactile Internet**

I. Introduction

The idea of the Tactile Internet [1] is to enable low-latency, high-resolution and highly available services for human-to-machine and machine-to-machine interaction. Through the availability of a respective core network infrastructure, applications can exchange data at the high rates necessary for tactile sensors and actuators. Packet rates of $1\,\mathrm{kHz}$ at a maximum latency of $1\,\mathrm{ms}$ are required to support those applications, for example Networked Control Systems (NCSs), teleoperation, telepresence, and Haptic Communication. Tactile Internet Applications currently evolve around the upcoming mobile communication standard 5G, which is a promising candidate to fulfill these requirements. Since 5G will support Device To Device (D2D) functionality, it will introduce a multi-hop characteristic in addition to its otherwise cellular nature. However, this fact is rarely covered in literature.

Although 5G may revolutionize many aspects of mobile communication, and it also offers many different services for various applications, it may not replace all present communication standards. IEEE 802.11, for example, mainly succeeded in consumer-grade as well as non-real-time business use cases because of its simplicity, low hardware cost, utilization of freely available radio spectrum and excellent configurability. It also has a significant market penetration. As of 2019, the WiFi-Alliance estimates 13 billion WiFi devices worldwide, with 4 billion shipping in 2019 alone [2]. For Haptic Communication one therefore has to take into account potential IEEE 802.11-based multi-hop networks on the network path, which make it hard to predict latency behavior.

In this paper, we discuss problems regarding Haptic Communication in Wireless Multi-Hop Networks (WMHNs) and propose a solution through probabilistic modeling, rather than calculating with absolute worst-case timing guarantees. We find that the latter approach is not suitable for IEEE 802.11 ISM-band technology as the rather unpredictable Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CSMA/CA) Medium Access Control (MAC) scheme is dominant on these frequencies. We propose a linear modeling approach that we evaluate on a large-scale simulated IEEE 802.11 network. The model is able to predict median latencies at a network utilization of about $29.4\,\%$ in our simulation experiment. Although it is not suitable for hard real-time applications, this preliminary idea may be suitable for consumer-grade applications like haptic teleoperation or telepresence.

The rest of this paper is structured as follows. Section II gives an overview of related work on modeling approaches. Section III exposes the problems that arise in prediction of certain network parameters. Section IV proposes a simple linearized model. In Section V, we show experimental evaluation on this model, and Section VI concludes the paper.

II. Related Work

There is some scientific work regarding throughput prediction in WMHN. Stojanova et al. [3] proposed a model for throughput of CSMA-based infrastructure networks derived from the network's conflict graph, which can be determined at run-time. Frohn et al. [4] propose another throughput model by taking multi-hop communication and frame aggregation into account. Throughput models are suitable, for example, for load-based assessment of network capabilities. However, latency predictions can be made only indirectly. Zocca et al. [5] propose a delay model for infrastructure networks that is derived from the stochastical hard-core model. None of the aforementioned models focus on Haptic Communication specifically. In our previous work [6], we showed that IEEE 802.11n networks are already capable of transmitting haptic flows within three hops while maintaining mean delay constraints. To achieve this, we proposed an extension to the Enhanced Distributed Channel Access (EDCA) mechanism in order to reduce delay.

III. Background and Problem Exposition

IEEE 802.11 networks are based on the CSMA medium access scheme which is originally based on works of Kleinrock and Tobagi from the 1970s [7]. It is a decentralized scheme as nodes do not need to register at a central coordinator such

as the Access Point (AP), which strongly supports scalability, robustness against node failure, mobility and provides some intrinsic self-X properties as self-configuration and self-optimization. A big advantage, which falls into the latter category, is its ability to exploit spatial reuse [8]. Spatial reuse describes the capability of nodes that are far enough apart from each other to actually be able to send at the same time. It is an ability that is otherwise only achievable in mobile communication standards involving a high amount of configuration and management overhead. CSMA is based on random access, where a collision is detected by the receiving node by means of a checksum. Failed transmissions are repeated following a persistence scheme which is either 1-persistent, non-persistent or p-persistent.

The simplicity also comes with drawbacks. The QoS requirements of Haptic Communication demands high availability, low latency communication services, which IEEE 802.11 cannot provide, as mentioned earlier. However, there have been some amendments issued to address these issues. 802.11e (2004) includes the EDCA and Hybrid Control Function Controlled Channel Access (HCCA) channel access modes that introduce differential services for prioritization of QoS classes like voice, video, or background. Further notable extensions include Fast Handover (802.11r, 2008), Single-User Beamforming (802.11ah, 2016), Sub-GHz Communication (IEEE 802.11ah, 2017), Fast Initial Link Setup (802.11ai, 2017), as well as several throughput extensions (802.11n, 2009; 802.11ac, 2013; 802.11ad, 2016; 802.11ax and IEEE 802.11ay, both expected 2019). We will further go into detail which problems still remain, also in these future IEEE 802.11 networks, regarding Haptic Communication.

A. Timing Guarantees

Because of the random-access nature, with CSMA one cannot provide any worst-case timing guarantees. It is therefore not suitable for hard real-time applications, like, for example, industrial- or medical-grade NCS. Timing guarantees can only be provided in form of a statistical distribution model, for example by specifying a mean and a standard deviation. Extensions to improve real-time capabilities exist; most prominently is the HCCA access function specified with IEEE 802.11e. However, it did not get much acceptance to the day, being a non-mandatory feature to implement. The applicability of the point coordination approach in HCCA is also not clear for mesh networks.

B. Throughput Dependence on Load

For CSMA networks, the relationship between network throughput and network load is generally non-linear [7] for unsaturated states. The higher the load, the more contention will happen, which may potentially even decrease network throughput in high load circumstances. Latency, of course, is also related to load, since the transmission delay computes from packet size divided by throughput. This behavior stems from the lack of reservation and also from the random backoff procedure that occurs after collisions. In case of a collision, not only the need for retransmissions will delay the packet, but also the idle time of the random backoff period that is necessary in order to avoid a future collision. In other words, in order to meet low timing constraints, the network utilization needs to be as low as possible. Network designers may therefore wish to increase the capacity (i.e., the node density) to support a higher number of applications. Our experiment setup, however, shows that there are limits for the node density, as the interference range of nodes cannot be reduced in order to maintain high throughput.

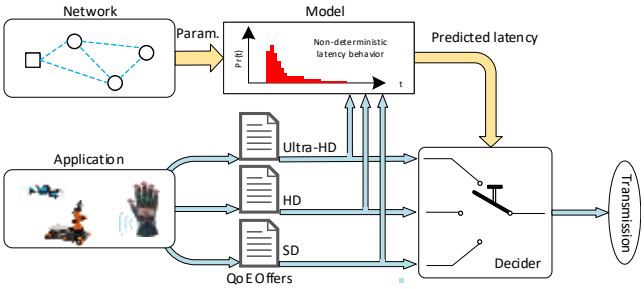


Figure 1: With a probabilistic model, applications are able to decide based directly on the predicted latency. If a required level of Quality of Experience (QoE) cannot be supported, the application might choose a lower level prior to cease functioning at all.

C. Load Dependence on Hop Count

The network's load is not only determined by the number of applications and their individual net throughput requirements, but also by the number of hops. Each hop includes an additional transmission process from one node to another, requiring medium capacity. In other words, the load depends also on distance between source and sink.

D. Carrier Sensing Range and Interference Range

There are several models for determining which nodes in a network interfere with each other [9]. The carrier sensing range of a node is commonly defined as twice the communication range, and the interference range as twice the carrier sensing range. This circumstance suggests a low node density, in order to minimize nodes interfering each other. This common picture in real world networks, however, is very different. Since the physical data rates of IEEE 802.11 networks are much higher for short-distance communication, the node density has to be kept very high, as many of the high-throughput coding schemes work merely within distances of several few meters.

IV. Probabilistic Linear Modeling Approach

We propose a probabilistic model for latency estimation (see Figure 1) which includes the current network load as well as the applications QoS requirements. It is suitable to compare requirements with the predicted load that admittance of the application would induce to the network. An application might choose between different QoE setups, which all have different specifications and result in different requirements in load. The prediction model should be able to interpret the current network load state and calculate a predicted mean latency derived from the requirements.

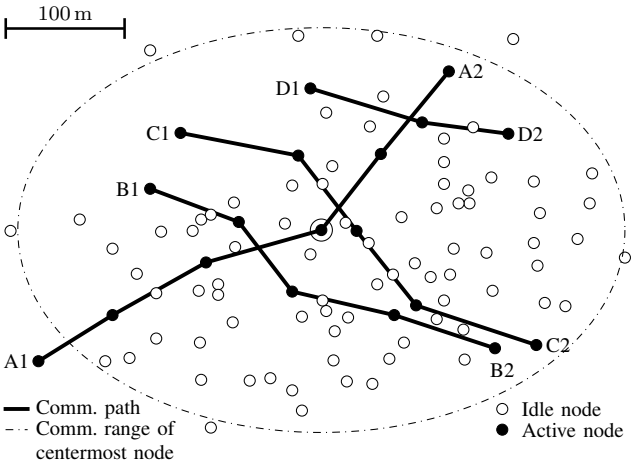


Figure 2: The Network used in our simulation with the path's of the four flows shown. The centermost node is indicated by a small solid circle and its communication range drawn with a dash-dotted line.

Table I: Simulation parameters

Parameter	Value
Number of nodes	100
Coverage area	500×500 m
Radio Model	INET `Ieee80211ScalarRadioMedium`
Node model	INET `StandardHost`
NIC Model	INET `Ieee80211Interface`
Routing	Static, with pre-initialized ARP caches
NIC properties	IEEE 802.11ac, 4×4 MIMO
TX power	2 mW
Channel	20 MHz bandwidth @2.4 GHz, free space path loss
Flow message length	100 B
Flow send interval	5 ms
Number of flows	1 to 4 (A1↔A2 to D1↔D2)

We choose a simple linear model for the end-to-end latency d_{e2e} of the form

$$d_{\text{e2e}} = k_1 n + k_2 h, \tag{1}$$

where h denotes the hop count and n denotes the number of haptic flows present in the network and currently interfering with each other. The two model parameters $k_1, k_2 \in \mathbb{R}$ need to be estimated. The model does not consider the limited capacity of the network, and thus only holds if the load of the network is much lower than the channel capacity. However, this simple approach has two advantages. First, it only considers two easy to determine variables. Second, linearity offers calculation with only local information which eliminates the necessity of a reservation protocol. n can be, for example, determined by each node individually by listening to the local network traffic, h will be determined by the routing mechanism.

Our approach assumes that haptic flows are of higher priority than other data transmitted within the network. In our previous work, we showed that such a prioritization is possible using the EDCA mechanism [6].

V. Simulation Results

We have conduced simulation experiments to assess feasibility of our model. The large-scale network we constructed in OMNet++ (Version 5.5.1) / INET (Version 4.1.1) is depicted in Figure 2. It comprises of 100 nodes that operate in IEEE 802.11ac mode. We start with one application (i.e. one haptic flow) on our network and measure the achieved latency, and then consecutively add more haptic flows to a total number of four flows, named A to D. The first flow, A, will have no competitors in our first experiment. The following flows B-D are settled to interfere with A (and each other). This way, we enforce competition between nodes and stress the CSMA scheme. The network routes are chosen to optimize the throughput, which means that shorter hops and thus longer routes are preferred over routes with low hop count, as described earlier. In Figure 2 this is seen as the maximum transmission distance, as depicted with a dashed line for the centermost node, is much bigger than the length of the chosen individual hops. Table I shows the simulation settings.

As the number of applications increases, we expect the latency behavior of the individual haptic flows to drop in performance. Each of the flows requires isochronous transmission of a 100 B packet every 5 ms, resulting in a net throughput requirement of 20 KB/s. The gross requirement in transmission time for this flow is much higher, though. The h-hop flow needs to acquire the medium h times, which is costly as the communication range of the nodes is much higher than the actual hop distance. Every single transmission thus forces large portions of the network to silence and defer transmission of other packets.

Figure 4 shows the observed latency distributions (we define the jitter hereby as the interquartile distance Q3-Q1). It is clearly observable how the interference between each of the applications affects the network performance. As, for example, application A has low mean latency and jitter of 0.948 ms and 0.108 ms, as long as it is the only application running in the network, the network's performance gracefully degrades as more applications come together. With all four applications active, the mean latency and jitter that the network provides for application A degrades to 2.324 ms and 2.257 ms, respectively.

We calculated the model parameters k_1, k_2 from Equation 1 for application A from the observations at $n = 1$ and $n =$

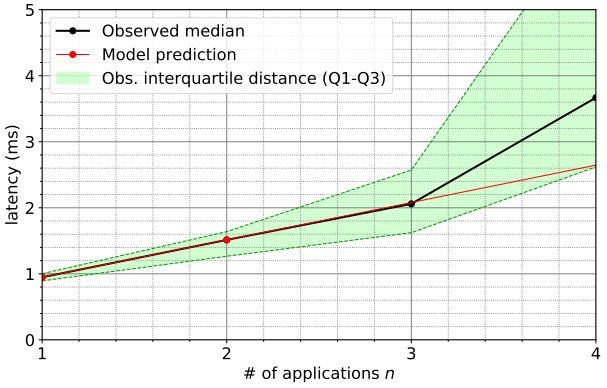


Figure 3: Observed and predicted latency of application A. The prediction is based on the two reference points $n = 1$ and $n = 2$.

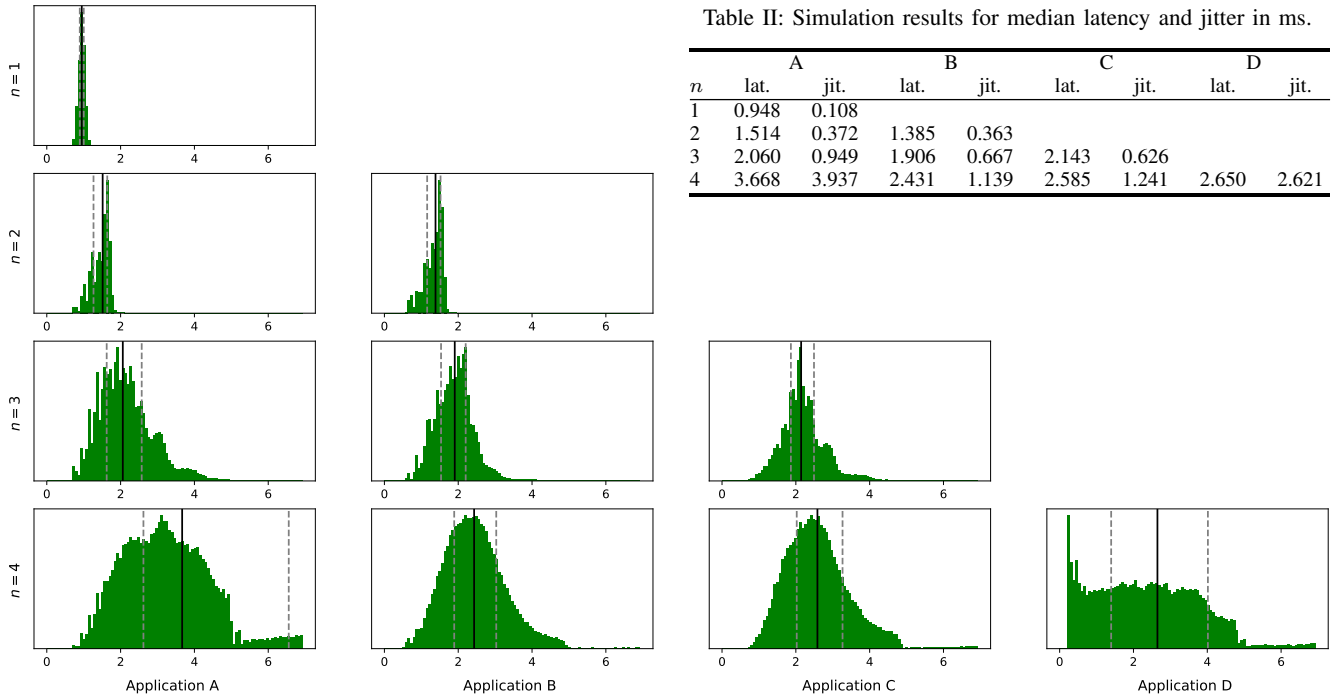


Figure 4: Latency histograms (in milliseconds) observed during in the experiment. Black solid lines indicate the median values. Dashed grey lines indicate quartiles Q1 and Q3, respectively.

Table II: Simulation results for median latency and jitter in ms.

	A		B		C		D	
n	lat.	jit.	lat.	jit.	lat.	jit.	lat.	jit.
1	0.948	0.108						
2	1.514	0.372	1.385	0.363				
3	2.060	0.949	1.906	0.667	2.143	0.626		
4	3.668	3.937	2.431	1.139	2.585	1.241	2.650	2.621

2. Since A's hop count $h = 5$ is known, these two points suffice for obtaining the model parameters. Observations and model predictions are depicted in Figure 3. The parameters calculate as $k_1 \approx 0.566$ and $k_2 \approx 0.076$, respectively. The prediction error for $n = 3$ is approx. $0.020\,\mathrm{ms}$ and for $n = 4$ approx. $1.021\,\mathrm{ms}$. During the experiment, we also measured the medium utilization at the centermost node of the network. At $n = 4$, the utilization reached about 29.4 %. Adding more applications resulted in an exponential growth and significant packet loss, so we assume the network to be saturated at $n = 4$.

VI. Concluding Remarks

In this paper, we have discussed a linear modeling approach for mean latency prediction of Haptic Communication in large-scale WMHN. The model depends on the hop count and the number of flows in the network. Simulation results show a good prediction quality for the median latency, although the model is rather simple.

In our future work, we will provide analytical models to derive probabilistic latency predictions. However, linearization might be a promising way, since Haptic Communication is less demanding in terms of throughput as other traffic like video or audio communication. In this sense, as it is most likely to receive top priority through differential services, Haptic Communication will cover only a small part of the entire network load and therefore might behave nearly linear in real networks.

We plan to evaluate applications in our own testbed for the Internet of Things, the Magdeburg IoT-Lab[1], that consists of 60 nodes with IEEE 802.11, IEEE 802.15.04 and sub-GHz technology. The testbed will be extended to other technologies and bigger size in future, enabling a diverse analysis of Tactile Internet applications and Haptic Communication.

[1] http://www.comsys.ovgu.de/MIOT_Lab.html

References

[1] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis. 5G-enabled Tactile Internet. *IEEE Journal on Selected Areas in Communications*, 34(3):460–473, 2016.

[2] WiFI Alliance. Wi-Fi Alliance® celebrates 20 years of Wi-Fi®. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-celebrates-20-years-of-wi-fi, 2019.

[3] M. Stojanova, T. Begin, and A. Busson. Conflict graph-based model for IEEE 802.11 networks: A Divide-and-Conquer approach. *Performance Evaluation*, 130:64 – 85, 2019.

[4] S. Frohn, S. Gübner, and C. Lindemann. Analyzing the effective throughput in multi-hop IEEE 802.11n networks. *Computer Communications*, 34(16):1912 – 1921, 2011.

[5] A. Zocca, S. C. Borst, J. S. H. van Leeuwaarden, and F.R. Nardi. Delay performance in random-access grid networks. *Performance Evaluation*, 70(10):900 – 915, 2013.

[6] F. Engelhardt, C. Rong, and M. Güneş. Towards Tactile Wireless Multi-Hop Networks - The Tactile Coordination Function as EDCA Supplement. In *Proceedings of the Wireless Telecommunications Symposium*, New York City, USA, April 2019.

[7] Leonard Kleinrock and Fouad Tobagi. Packet switching in radio channels: Part I-carrier sense multiple-access modes and their throughput-delay characteristics. *IEEE transactions on Communications*, 23(12):1400–1416, 1975.

[8] Khaldoun Al Agha and Laurent Viennot. *Spatial Reuse in Wireless LAN Networks*, pages 209–219. Springer US, Boston, MA, 2002.

[9] J. Padhye, S. Agarwal, V. N. Padmanabhan, L. Qiu, A. Rao, and B. Zill. Estimation of link interference in static multi-hop wireless networks. In *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*. USENIX Association, 2005.

Privacy-enhanced Authentication for the Internet of Things

Sara Stadler
University of Bremen, TZI
Bremen, Germany
stadlers@tzi.de

Stefanie Gerdes
University of Bremen, TZI
Bremen, Germany
gerdes@tzi.de

Olaf Bergmann
University of Bremen, TZI
Bremen, Germany
bergmann@tzi.org

***Abstract*—The Internet of Things (IoT) emerges as an ubiquitous network of smart objects and sensors collecting sensitive data and performing vital tasks. To avoid unauthorized data access and control of the devices, authentication and authorization for the IoT have become a particular interest of security research. The Delegated CoAP Authentication and Authorization Framework (DCAF) is a promising approach to address this problem for constrained devices. Authentication is often based on identity proofs, thereby sacrificing certain privacy aspects such as data minimization and unlinkability. In IoT scenarios, where devices accompany their users in every aspects of their private lives, this facilitates extensive tracking and profiling. In this paper, we present an extension to DCAF, intended to address the problem of authentication and authorization for constrained devices, while at the same time protecting the users' privacy.**

***Index Terms*—IoT, Authentication, DCAF, Attribute-based credentials, Privacy-enhancing technologies**

I. Introduction

The Internet of Things (IoT) interconnects smart objects that often come with limited computing power and small amounts of ROM and RAM, over the internet infrastructure. Missing authentication and authorization not only threaten this infrastructure, but also the (often sensitive) data collected by the devices, or even their users' lives (e.g., maliciously accessed medical devices). Therefore, authentication and authorization for constrained devices in the IoT have become a particular interest of security research.

While authentication and authorization provide important security features, they often come with privacy drawbacks such as introducing the linkability of transactions and the possibility to relate transactions to actual persons. In this paper we address the importance of privacy and emphasize the users' right to data minimization and control. Storing every transaction is very cheap nowadays and with the evolving IoT the number of digital transactions related to personal every day activities grows rapidly. As Ziegelsdorf et al. [1] point out, the threat of tracking and profiling has aggravated, while users become less aware of it. We illustrate the privacy threats by the means of a fictional but realistic scenario. We designed this scenario to give a concrete impression of tracking and profiling possibilities. Afterwards, we present an extension to the Delegated CoAP Authentication and Authorization Framework (DCAF) [2] that is intended to address authentication and authorization for constrained devices, while at the same time protecting the users' privacy. In particular, we address the problem that a client wants to authenticate itself towards a server in an IoT setting, where the server must not gain any insight besides the information the client wants to share. Our solution makes use of attribute-based credentials (ABCs) [3].

This paper is structured as follows: In Section II we describe our scenario and point out the related privacy threats and challenges. Afterwards, we discuss related work covering privacy-preserving authentication in Section III. In Section IV we recall DCAF and give an overview over ABCs. Based on this background we present our extension to DCAF in Section V. Section VI contains concluding remarks and an outlook on future work.

II. Privacy in the IoT

Imagine a scenario where an enthusiastic user integrates IoT devices in her daily life.

A. Motivating example

Today Alice uses her car because her day is quite busy. As she lives in a big city, where parking spots are rare, she is registered with *ExamplePark*, where the payment of a membership fee grants entrance to all facilities run by this company. Her car is equipped with a smart parking module taped to its front window, which is able to authenticate Alice towards the constrained parking barriers of all parking facilities. All locations she visits today are close to a particular facility of *ExamplePark*.

Before work, Alice has an appointment with her doctor. As Alice has a heart condition she is wearing a device called *HeartGuard* (cf. [4]). The device collects data on her heart rate that the doctor checks in regular terms to assess her heart condition.

As her heart appears to be fine, Alice treats herself to a coffee when she arrives at her office. The company she works for has a contract with COFFEE Inc. that allows all employees to get free coffee from all COFFEE Inc. vending machines (cf. [5]). Therefore, her smart coffee mug authenticates her towards the vending machine she uses.

During her break she uses the car to visit her psychologist. The psychological group practice has a car park run by *ExamplePark*. On her way back she treats herself to another coffee.

After work Alice visits the fitness studio. In the studio she puts on her sports clothes that are equipped with sensors that measure humidity, heart rate, blood pressure and body temperature and her jogging shoes that embed humidity, pressure and activity sensors (cf. [6]). Her clothes and shoes connect to the fitness equipment she uses. This way the equipment can give her personal advice and also warn her if her heat rate goes high.

After a rough workout Alice treats herself with another coffee before she drives home.

B. Privacy threats and challenges

During the day Alice's devices have authenticated towards different remote services or towards other devices in different locations she entered. Even if none of the often very sensitive data the devices communicated is disclosed, the scenario bears various privacy risks that are well known to be exacerbated by the IoT (see e.g., [1], [7]).

1) Tracking and Profiling: When the authenticating devices can be linked to Alice, Alice's movement can be tracked, and further information (such as hobbies or illnesses) can be derived, based on different instances of authentication. If this information is linked, principals with various interests may be able to build profiles on Alice's behavior. For example, her health insurance might be interested in correlating Alice's activities related to her health (e.g., how much coffee she drinks and how much she exercises) and in the fact that she uses a *HeartGuard* (and therefore probably has a heart condition).
2) (Re-)Identification: Even if authentication and authorization are performed using pseudonyms, Alice can potentially be identified by linking different usages: information concerning the devices she owns and the places she visits frequently can yield a unique *fingerprint*. If only one of the services Alice uses knows her identity, the *fingerprint* can definitely be linked to her identity and she can potentially be re-identified by services or in contexts where she assumes to be anonymous, if the services collaborate and share information about their users.

To avoid these threats, authentication and authorization must be performed in a way that is unlinkable and compliant with the principle of data minimization. ABCs are a promising approach to achieve this and, therefore will be introduced in IV-B. Authentication and authorization themselves are challenging in an IoT setting due to the constraints of the involved devices. These challenges are addressed by DCAF, see IV-A .

III. Related Work

A broad variety of concepts exists that allow for the users' authentication without presenting identifying information, and provide the unlinkability of different transactions. Approaches that we consider most appropriate for our use-case scenario are based on so-called *credential mechanisms* first proposed in 1985 by Chaum [8]. Currently two main credential systems exist: U-Prove [9] and Identity Mixer (Idemix) [3]. As both systems enable the users to disclose only certain attributes (e.g., a membership or age) signed by a (or a group of) trust issuer(s) towards a system, they are referred to as *attribute-based credential systems*. Both schemes have been implemented on smart cards (e.g., [10], [11]) and integrated into light weight infrastructures (e.g., [12]–[14]). They also have been mentioned as suitable solutions addressing privacy issues by the European Research Cluster on the Internet of Things in 2015 [15, p. 72f].

The first concrete proposition to adopt ABC technologies within the IoT was published in 2016 by Alpár et al. [7]. Afterwards, this idea has been followed up, e.g., by de Fuentes et al. [16], [17], Bernabé et al. [18] and Sanchez et al. [19]. To the best of our knowledge, there is no proposal which combines ABCs with DCAF and thus enables both client and server to delegate computational or memory expensive operations to less constrained devices.

IV. Background

In this section we introduce the basic components of our solution: DCAF and ABCs.

A. The Delegated CoAP Authentication and Authorization Framework

DCAF is designed to provide constrained clients and servers with the necessary authentication and authorization information that they require to securely communicate with each other. In DCAF, each constrained device is coupled with an own less-constrained authorization manager that helps with difficult security tasks; on the client side, the client (C) is coupled with the client authorization manager (CAM), while on the server side, the server (S) has a security association with its server authorization manager (SAM). The authorization managers act as mediators between the constrained devices and the human beings that are in charge of them, the client overseeing principal (COP) and the server overseeing principal (SOP), respectively. To establish a secure communication with S, C requires an access ticket from SAM. To obtain it, C contacts its own CAM, which then establishes a secure channel with SAM. With COP's and SOP's approval, C is provided with an access ticket that contains the necessary authentication and authorization information for C and S to establish a secure channel.

Constrained devices only need a security association with their own manager and are not required to authenticate authorization managers from other security domains. The authorization managers vouch for the attributes of their own constrained devices. DCAF does not require the use of unique identifiers as attributes. Therefore, DCAF can be used in a privacy-preserving way. But DCAF does not specify how CAM and SAM authenticate each other. If the used authentication mechanism does not prevent it, distinct instances may still be linked. A solution for this problem are attribute-based credentials, which we describe in the next section.

B. Attribute-based credentials

Our proposal is based on the Idemix ABC system. An Idemix ABC is a set of attributes signed by an issuer via a Camenisch–Lysyanskaya signature [20] that not only allows for blind signing, but is also randomizable. One of the credential's attributes is always a master secret key that binds the credential to a particular user. This key is always signed blindly. All attributes in an ABC can be shown individually by so-called *selective disclosure proofs* [21] to provide only the necessary information (such as a membership). As the signature on the credential is randomized prior to each proof, different instances of attribute disclosure cannot be linked. By using ABCs for authentication and authorization we can avoid the issues of (re-)identification as well as of tracking and profiling by data minimization and unlinkable transactions. Of course, these properties only hold if no identifying attributes are revealed. Also, showing non-identifying attributes always leaks some information that reduces the users' anonymity to a certain degree. Therefore, it is desirable to reveal as little attributes as possible, e.g., only the mere possession of the credential signed by a certain issuer [7].

In addition to their privacy features, ABCs comply with standard security requirements as the issuer's signature on the credential is verifiable and unforgeable. Existing work already indicates how they can be used for the setup of a mutually authenticated secure channel. Alpár et al. [13], [22] propose two different protocols for this purpose, where the first facilitates the anonymous authentication of a client towards a server and the second enables both parties to mutually authenticate anonymously.

V. Combining DCAF and ABCs

In this section, we describe how the authentication between CAM and SAM in DCAF can be performed with ABCs to protect Alice's privacy. Integrating ABCs into DCAF implies the following extensions/modifications:

1) Issuing a credential over multiple attributes from an issuer (I) to CAM (and COP, respectively).
2) Setup of a mutually authenticated TLS channel between CAM and SAM by means of ABCs.
3) Transfer of authorization information from CAM to SAM via a selective disclosure proof.

The issuing of credentials requires a pre-existing issuing infrastructure and the registration of COP with a particular issuer. It is then carried out as specified by the Idemix specification [21]. The TLS channel setup can be performed using a variant of the protocols introduced by Alpár et al. [13], [22]. The following proposal uses the variant that facilitates only the client's anonymity. This is suitable for scenarios where Alice's devices communicate with servers, whose anonymity is not required, such as external services or devices associated with large service providers. The authorization is carried out within the secure channel by means of ABCs. Fig. 1 sketches how our extensions are integrated into DCAF.

The figure is divided into two parts: on the left the credential issuing is sketched. This step is only carried out once and is not

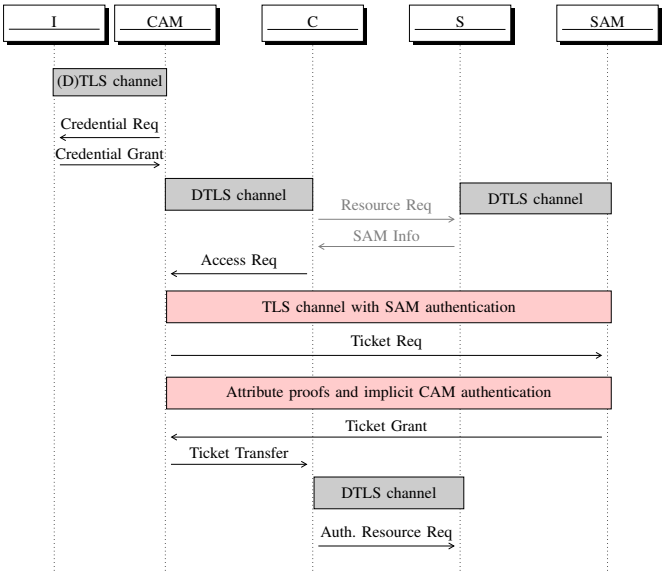


Fig. 1. Schematic overview of the extended DCAF protocol.

a part of the DCAF protocol run itself. Note that in Fig. 1 the three-way issuing protocol is simplified. The right half shows a schematic view of a DCAF protocol run where our extensions are highlighted in red. The original DCAF requests have not been modified, instead only the authentication of CAM and SAM has been specified in a privacy-preserving way. SAM authenticates during the TLS handshake by means of an X.509 certificate. CAM authenticates either by an empty proof showing the mere possession of a valid credential issued by I or by a selective disclosure proof showing some attributes *and* the possession of the credential. Selective disclosure proofs additionally can provide authorization information for resources on S. On this basis, the access ticket can be issued from CAM to SAM and transferred to C. But access tickets should not be used more than once to guarantee the unlinkability. Our extensions allow CAM and SAM to mutually authenticate each other in a way that is verifiable and unforgeable, and potentially to provide authorization information. Furthermore, our extensions add important privacy features to DCAF that are associated with ABCs (see e.g., [22]). We transfer these features to our scenario where Alice acts as COP.

1) Issuer unlinkability: Credential issuers might be aware of Alice's identity or of some identifying attributes (depending on the way Alice registered). They will, however, not learn anything about instances where the issued credential is used. E.g., *ExamplePark* will not know when (or if ever) Alice uses its facilities. This is due to the fact that in a blind signature scheme the signer never learns the resulting signature. The signer is therefore not able to link a signature to an instance of signing (where the receiver's identity is known).
2) Minimal information: The user can potentially stay anonymous. E.g., when Alice parks her car in a particular garage, she does not need to reveal more information

than being registered with *ExamplePark* (credential issuer) and having paid the membership fee for a certain period (disclosed attributes). Of course, additional metadata (such as network addresses) can be disclosed if this is not prevented by the use of further privacy-enhancing technologies such as network traffic anonymization.

3) Multi-show unlinkability: As the signature on the credential can be randomized prior to every selective disclosure proof, different instances of disclosing attributes cannot be linked (unless the disclosed attributes make them linkable).

In summary, Alice's devices can potentially be authenticated and authorized by revealing only non-identifying information. Additionally, multiple instances of revealing the same or different information remain unlinkable.

We implemented our proposal [23] using the gabi cryptographic library [24] underlying the IRMA implementation of the Idemix attribute-based credential system [25], [26].

VI. Conclusion

In this paper we focus on the privacy implications of authentication and authorization in the evolving IoT. We study a fictional but realistic use-case scenario to illustrate the threat of tracking, profiling and (re-)identification resulting from the linkability of different instances of authentication. We also make a concrete proposal how to protect IoT users from these threats by combining DCAF with ABCs. In particular, we design the establishment of a trust relation between CAM and SAM such that the authentication and authorization are privacy-preserving for CAM.

In the future the presented results will be extended to address cases where both communicating devices (CAM and SAM) are associated with individuals that want to reveal as little information as possible towards each other. Additionally, we will further evaluate the applicability of our approach in real-world scenarios and provide a detailed analysis of its security and privacy properties.

References

[1] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[2] S. Gerdes, O. Bergmann, and C. Bormann, "Delegated Authenticated Authorization for Constrained Environments," in *IEEE 22nd International Conference on Network Protocols (ICNP) 2014*, Oct 2014, pp. 654–659.

[3] J. Camenisch and E. V. Herreweghen, "Design and implementation of the Idemix anonymous credentialsystem," in *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, 2002*, V. Atluri, Ed. ACM, 2002, pp. 21–30.

[4] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, "Use Cases for Authentication and Authorization in Constrained Environments," RFC 7744, Jan. 2016. [Online]. Available: https://rfc-editor.org/rfc/rfc7744.txt

[5] C. Bormann and A. Keränen, "Chair slides," Jul. 2017, Thing-to-Thing (t2trg) RG, IETF 99. [Online]. Available: https://datatracker.ietf.org/doc/slides-99-t2trg-chair-slides/

[6] OrganiCity, "Scenarios: Personal trainer." [Online]. Available: https://scenarios.organicity.eu/scenarios/6663fa94-de7c-47f8-a04f-e02790ba3981

[7] G. Alpár, L. Batina, L. M. Batten, V. Moonsamy, A. Krasnova, A. Guellier, and I. Natgunanathan, "New Directions in IoT Privacy Using Attribute-Based Authentication," in *Proceedings of the ACM International Conference on Computing Frontiers, CF'16*, G. Palermo and J. Feo, Eds. ACM, 2016, pp. 461–466.

[8] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[9] C. Paquin, "U-Prove Technology Overview V1.1. (rev 2)," Microsoft Research, Tech. Rep., 2013.

[10] W. Mostowski and P. Vullers, "Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards," in *Security and Privacy in Communication Networks - 7th International ICST Conference, SecureComm 2011*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, M. Rajarajan, F. Piper, H. Wang, and G. Kesidis, Eds., vol. 96. Springer, 2011, pp. 243–260.

[11] P. Vullers and G. Alpár, "Efficient Selective Disclosure on Smart Cards Using Idemix," in *Policies and Research in Identity Management - Third IFIP WG 11.6 Working Conference, IDMAN 2013*, ser. IFIP Advances in Information and Communication Technology, S. Fischer-Hübner, E. de Leeuw, and C. J. Mitchell, Eds., vol. 396. Springer, 2013, pp. 53–67.

[12] G. Alpár, L. Batina, and W. Lueks, "Designated Attribute-Based Proofs for RFID Applications," in *Radio Frequency Identification. Security and Privacy Issues - 8th International Workshop, RFIDSec 2012*, ser. Lecture Notes in Computer Science, J. Hoepman and I. Verbauwhede, Eds., vol. 7739. Springer, 2012, pp. 59–75.

[13] G. Alpár and J. Hoepman, "A Secure Channel for Attribute-Based Credentials: [short paper]," in *DIM'13, Proceedings of the 2013 ACM Workshop on Digital Identity Management*, T. Groß and M. Hansen, Eds. ACM, 2013, pp. 13–18.

[14] K. Rannenberg, J. Camenisch, and A. Sabouri, Eds., *Attribute-based Credentials for Trust: Identity in the Information Society*. Springer, 2015.

[15] G. Baldini, T. Peirce, and M. Botterman, "IoT Governance, Privacy and Security Issues," European Research Cluster on the Internet of Things, Tech. Rep., 2015.

[16] J. M. de Fuentes, L. González-Manzano, A. Solanas, and F. Veseli, "Attribute-Based Credentials for Privacy-Aware Smart Health Services in IoT-Based Smart Cities," *IEEE Computer*, vol. 51, no. 7, pp. 44–53, 2018.

[17] J. M. de Fuentes, L. González-Manzano, J. Serna-Olvera, and F. Veseli, "Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 869–891, 2017.

[18] J. B. Bernabé, J. L. H. Ramos, and A. F. Gómez-Skarmeta, "Holistic Privacy-Preserving Identity Management System for the Internet of Things," *Mobile Information Systems*, vol. 2017, pp. 6 384 186:1–6 384 186:20, 2017.

[19] J. L. C. Sanchez, J. B. Bernabé, and A. F. Skarmeta, "Integration of Anonymous Credential Systems in IoT Constrained Environments," *IEEE Access*, vol. 6, pp. 4767–4778, 2018.

[20] J. Camenisch and A. Lysyanskaya, "A Signature Scheme with Efficient Protocols," in *Security in Communication Networks, Third International Conference, SCN 2002*, ser. Lecture Notes in Computer Science, S. Cimato, C. Galdi, and G. Persiano, Eds., vol. 2576. Springer, 2002, pp. 268–289.

[21] I. R. Security Team, Computer Science Department, "Specification of the Identity Mixer Cryptographic Library ," Resaerch Report, 04 2010, revised version 2.3.0 of RZ Report.

[22] G. Alpár, "Attribute-Based Identity Management: Bridging the Cryptographic Design of ABCs with the Real World," Ph.D. dissertation, Radboud Universiteit Nijmegen, 2015.

[23] DCAF, "DCAF," GitLab. [Online]. Available: https://gitlab.informatik.uni-bremen.de/DCAF/dcaf/tree/abc

[24] M. Everts, "Gabi," GitHub. [Online]. Available: https://github.com/mhe/gabi

[25] Privacy by Design Foundation, "About IRMA," Homepage. [Online]. Available: https://privacybydesign.foundation/irma-en/

[26] ——, "IRMA Authentication," GitHub. [Online]. Available: https://github.com/privacybydesign

Technical Report: Designing a Testbed for Wireless Communication Research on Embedded Devices

Kai Kientopf, Marian Buschsieweke, Mesut Güneş
Communication and Networked Systems (ComSys)
Faculty of Computer Science
Otto-von-Guericke University Magdeburg
Universitätsplatz 2, 39106 Magdeburg, Germany
{kai.kientopf, marian.buschsieweke, mesut.guenes}@ovgu.de

***Abstract*—Real world experiments are worthwhile tools to evaluate new approaches in the area of Wireless Multi Hop Networks (WMHNs) or Wireless Sensor Networks (WSNs). However, individual experimental setups come with drawbacks such as high hardware costs, long setup time, and low reproducibility. Testbeds are developed to addresses these issues. In this paper we report about our ongoing work to construct a new testbed, the Magdeburg Internet of Things Lab (MIoT-Lab), with the focus on realistic environment, long term persistence, and reproducibility.**

***Index Terms*—Testbed, WMHN, WSN**

I. Introduction

Research on wireless communication is often based on simulations and not validated in reality. While simulations are cost efficient and make replicating a test setup and reproducing results trivial, it is difficult to consider all relevant environment variables. This leads to simulation results differing often significantly from real world performance. Therefore, it is necessary to test and study protocols additionally with experiments on physical hardware setups.

Individual hardware setups for real world tests are cost intensive, time consuming to set up, and difficult to reproduce. These problems can be addressed by permanent testbed builds. The price per experiment is reduced, because the major part of costs, the acquisition of the hardware, is only spend once. The reproducibility is increased by fixed positions, identical hardware, and a relatively stable environment. It is clear that due to the various factors affecting the wireless medium, each experiment may differ from one to another. However, the fixed position of the nodes in the same environment reduces the difference in the experimental results.

We are constructing the Magdeburg Internet of Things Lab (MIoT-Lab) with 200 nodes as a successor of the DES-Testbed [1]. The nodes will be distributed in the Faculty of Computer Science (FIN) of the Otto-von-Guericke University Magdeburg (OVGU) and some surrounding buildings. To achieve a realistic experiment environment the nodes will be placed in regular offices, laboratories, and seminar rooms.

The remainder of this paper is structured as follows: In Section II we cover a selection of other testbeds. The hardware for the testbed nodes is specified in Section III. In Section IV we describe the associated software. This report concludes with a summary in Section V.

II. Related Work

There are current active and historical testbeds for wireless research [2]. In the following we shortly present a selection of them and their focus.

The DES-Testbed was developed and deployed at Freie Universität Berlin. In the context of the DES-Testbed an experiment description language named DES-Cript [3] was designed, that will be further described later. In 2010 and 2011 the DES-Testbed was used for more than 1000 experiments, which contributed to 32 theses and 25 publications [4]. The DES-Testbed was part of the WISEBED federation [5]. Later on, SmartSantander was developed and based on the WISEBED API [6]. Our planned MIoT-Lab is based on the design, software, and experience of the DES-Testbed.

The FIT IoT-Lab is a distributed testbed located at six different locations in France [7]. It offers 2728 nodes based on three boards of custom design and various commercial boards. A power monitoring solution is provided that allows to track the total power consumption of the boards. Access to all nodes regardless of their location is available through a single web portal and consistent REST APIs. Furthermore, 117 robots are integrated in the testbed.

The TWIST testbed is located at the Technical University Berlin [8] and distributed over 3 floors. It consists of TmoteSky and eyesIFXv2 nodes, TP-Link WDR4300 and Intel NUC PCs for WiFi communication, as well as some robotic platforms [9].

The Indriya2 testbed is located at the National University of Singapore [10] and distributed over 3 floors. It is the successor of the Indriya testbed. The current hardware setup consists of 74 TelosB boards and 28 CC2650 sensortags.

All presented testbeds provides only a limited number of boards with multiple connectivity in more than one frequency domain. Hence, large scale experiments with multiple connectivity are currently impossible with these testbeds. Additionally, power monitoring features are often missing or only allow to monitor the total power consumption of the node.

III. Testbed Nodes

Since we are interested in wireless communication and networked systems, the testbed is assumed to provide the infrastructure for our experiments. Thus, the testbed nodes (TBNs)

Table I: Hardware parts of the planned testbed nodes (TBNs).

Attribution	Function	Model Name / Material
x86 Node	Mainboard	PC Engines APU.3C4
	Int. WiFi Module	Compex WLE900VX
	Ext. WiFi Modules	2 × Asus USB-N14 N300
Embedded Node	Base Board	STM32 NUCLEO-F767ZI
	Adapter Board	Custom PCB
	802.15.4 Transceiver	Atmel AT86RF232
	LoRa Transceiver	RFM95W (Semtech SX1276)
	Sub-Gigahertz ISM Transceiver	TI CC1101
	802.11n (2.4 GHz) & BLE	Espressif ESP32 (via UART)
	Low-Cost 2.4 GHz Transceiver	Nordic nRF24L01+
	Current & Power Monitor	2× TI INA3221
	Calibration & Config. Data Storage	Atmel AT24C256
	Environmental Data Sensor	Bosh BME680
	Temperature & Humidity Sensor	Sensirion SHT30
Reset Solution	WiFi-enabled reset controller	ESP32 Node MCU
Case	Custom	Laser Cutted Acrylic

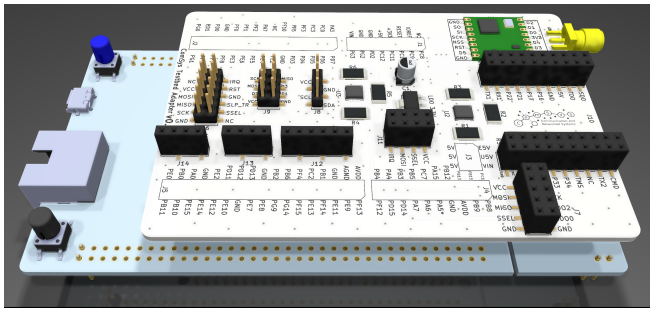


Figure 1: A 3D model of the adapter board plugged into the Nucleo-F767ZI (includes 3D models by SnapEDA (CC-BY-SA)).

need to cover the most important technologies. Therefore, one TBN is composed out of different hardware parts (see Table I) that are combined to cover many scenarios. In our design we focused on commercial available parts, in contrast to earlier testbeds nodes composed of custom hardware. Only a housing and an adapter board was designed, that basically replaces jumper wires. This should save development time and enable interested users to build their own node (or only the necessary parts) for development and debugging.

A. x86 Node

The x86 Node (XN) uses an APU.3C4 mainboard equipped with a x86_64 CPU and 4 GiB of RAM. The CPU is capable (4 cores clocked at 1 GHz) and most software can be executed without additional effort, as the x86 architecture is common for desktop PC's. Furthermore, it flashes the firmware images to the Embedded Nodes (ENs) that are described in the following subsections.

1) Connectivity

The XN is connected via IEEE 802.3 (Ethernet) to the Testbed Management System (TBMS) for loading the software and settings, controlling experiments, and collecting the results. For experiments with WiFi, the XN is equipped with one internal and two external WiFi interfaces. The WiFi devices are chosen according the availability of mainline Linux drivers. A Compex WLE900VX interface is supported by the ath10k driver and is used as an internal WiFi card supporting IEEE 802.11ac/a/b/g/n standards with 3 antennas. Two Asus USB-N14 N300 are supported by the rt2800usb driver and are used as external WiFi devices supporting IEEE 802.11b/g/n standards with 2 antennas for each device.

B. Embedded Node

In order to allow running experiments with IoT nodes of class C2 (using RFC7228 [11] terminology) and below, an EN is integrated into every TBN. The EN is programmed from the XN using an JTAG/SWD programmer connected via USB. This programmer includes an UART adapter connected to the EN, which allows to control the nodes individually and gather data from the node.

1) Base Board

An STM32 NUCLEO-F767ZI evaluation board is used as base of the EN, which features an ARM Cortex® M7 CPU equipped with 512 KiB SRAM and 2 MiB Flash. According to classification in RFC7228 [11], the EN exceeds the highest class C2. However, stricter memory constraints can easily be enforced at link time and by inserting hooks to the dynamic memory management functions such as `malloc()`. In the same way the CPU frequency, which can be up to 216 MHz, can be reduced in software. As a result, the capability of each individual EN in terms of computational performance and memory capacity can be scaled down to meet the requirements of particular experiments.

2) Adapter Board

In order to improve the maintainability and reduce the development time and costs, the EN is build upon off-the-shelf hardware. The base board is extended by using breakout boards for the individual transceivers, which already include all components required by the transceiver IC for optimal operation. To avoid connecting these components with dozens of jumper wires, a dedicated adapter board (see Figure 1) has been developed. This custom PCB is plugged on top of the NUCLEO-F767ZI and connected to its pin headers. The individual breakout boards are plugged into the pin sockets on top of the adapter board. With the exception of two components, every part of the EN can therefore be replaced within seconds, greatly simplifying maintenance and repairs. The two exceptions are the RFM95W breakout board for the Semtech SX1276 LoRa transceiver and the power monitoring solution, which are soldered directly onto the PCB.

3) Power Monitoring

The power monitoring solution employs two TI INA3221 power/current monitor ICs with a total of 6 power channels. In order to prevent any impact on power consumption by monitoring the power consumption, the power monitors are not connected to the NUCLDEO-F767ZI. Instead, the power monitors are connected to the ESP32 via Inter-Integrated Circuit (I^2C) and also connected to the power domain of the ESP32. This way neither the power consumption of the INA3221 ICs nor the increase in power consumption by reading and processing the power consumption data has any influence on the monitored power domains. The six power monitoring channels of the two INA3221 are used to monitor: 1) The NUCLEO-F767ZI 2) the AT86RF233 802.15.4 transceiver 3) the CC1101 Sub-Gigahertz transceiver 4) the nRF24L01+ ultra-low-cost transceiver 5) the SX1276

Table II: Wireless Connectivity of the testbed nodes (TBNs).

Technology	Frequency	Max. Data Rate	Hardware	MIMO
x86 Node				
802.11ac	2.4 / 5 GHz	1300 $\frac{\text{Gbit}}{\text{s}}$	Compex WLE900VX	3x3
802.11n	2.4 / 5 GHz	300 $\frac{\text{Mbit}}{\text{s}}$	Asus USB-N14 N300	2x2
Embedded Node				
802.11n	2.4 GHz	150 $\frac{\text{Mbit}}{\text{s}}$	Espressif ESP32[1]	–
BLE 4.2	2.4 GHz	4 $\frac{\text{Mbit}}{\text{s}}$	Espressif ESP32[1]	–
802.15.4	2.4 GHz	250 $\frac{\text{kbit}}{\text{s}}$	Atmel AT86RF233	–
LoRa	868 MHz	9380 $\frac{\text{bit}}{\text{s}}$	Semtech SX1276	–
Custom	433 MHz	600 $\frac{\text{kbit}}{\text{s}}$	TI CC1101	–
Custom	2.4 GHz	2 $\frac{\text{Mbit}}{\text{s}}$	Nordic NRF24L01+	–

1 Only one ESP32 is used to provide both Bluetooth v4.2 and 802.11n

LoRa transceiver, and 6) the sensors and EEPROM.

4) Connectivity

The EN has in addition to an Ethernet controller multiple options for wireless connectivity, as is detailed in Table II. Except for the Espressif ESP32, all transceivers are connected via SPI. The ESP32 is connected over UART using SLIP [12], which allows to forward IP packets via 802.11n or Bluetooth (BT) 4.2 BR/EDR and BLE. This rich support of connectivity covers various frequency bands (433 MHz, 868 MHz, 2.4 GHz), a huge range of different data rates, as well as different communication technologies. Therefore, wireless communication with characteristics ranging from short-range, high-energy, and high-data-rate connections to long-range, low-power, ultra-low-data-rate connections are available on the TBNs.

5) Storage of Calibration and Configuration Data

An Atmel AT24C256 is connected via I^2C to persistently store 256 KiB of sensor calibration and configuration data. Having a separate EEPROM storage is particularly useful to preserve data even after reprogramming a node. The CC1101 for example uses 8 bit layer 2 addresses. Due to the birthday paradox the generation of 20 random 8 bit layer 2 addresses already has a collision probability of over 50%. In order to prevent address conflicts, the layer 2 addresses of these transceivers have to be manually configured for the 200 TBN and cannot be derived e.g. from the CPU ID. The EEPROM allows storing an unique layer 2 address for every EN.

6) Sensors

The EN is equipped with an SHT30 temperature and humidity sensor, that will monitor the conditions inside the case of the TBN. Additionally an BME680 temperature, humidity, and air quality sensor is connected to the EN and placed next to air vents on the outside of the case, so that environmental conditions can be monitored.

C. Reset Solution

Experiences with the previous testbed hardware show one major problem: Once the nodes are deployed in different rooms, a failure rendering a TBN unreachable will require time-consuming manual intervention to restart the affected node. Therefore we plan to use a second ESP32 development board to restart the nodes by triggering the reset pin of the APU.3C4 board. To avoid a reflashing of the firmware by the user, the board is only connected to the XN as a power source and not via USB.

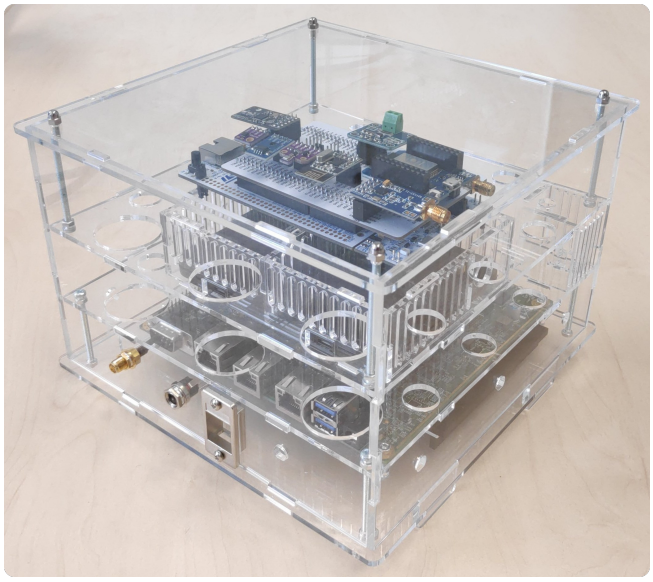


Figure 2: A prototype of the node housing with the x86 Node, the external WiFi devices, and an ESP32 development board for the reset solution, as well as the Embedded Node.

D. Housing

We designed an acrylic housing for the hardware that can be produced via a laser cutter (prototype is depicted in Figure 2).

It has 3 levels where the hardware is located: 0) The APU.3C4 Board, 1) the two external WiFi devices, the ESP32 board for the reset solution, and the air quality sensor, and 2) the EN with its adapter board and all components except the air quality sensor. Furthermore, a heat sink is integrated below the APU.3C4 board to provide the required cooling. A passive heat sink was chosen over a fan to avoid mechanical components suffering from a wear and failures on the one hand. On the other hand many nodes will be placed in offices and labs, so that the nodes have to emit as little noise as possible. The housing has an Ethernet and a DC socket to provide network and power for the hardware. In addition there are 10 antenna connectors: a) 3 × for Compex WLE900VX, b) 4 × for 2 × Asus USB-N14 N300, c) 1 × for LoRa, d) 1 × for C1101, and e) 1 × for nRF24L01+. The design was developed with OpenSCAD for 3 mm material.[1]

IV. Software

The software from the DES-Testbed is currently updated and extended. Its main component is the TBMS collection that can create experiments, schedule these, and collect the results. It is running on an server that is connected to the nodes over Ethernet. In the following we describe the most important features of the MIoT-Lab's software.

A. Experiment Creation

A web interface is provided to allow users to create experiments. Beside general information like a name, a description,

[1]For the development process and presentation we use transparent acrylic. The version that we want to distribute will get a non-transparent material.

and a earliest start time, also the number of repetitions for statistical relevance and a restart of the nodes for a clean system environment can be specified. The nodes for the experiment can be grouped. Each group can be assigned different actions for execution. These actions are command line commands that are executed by the XN. Every action can be evaluated by its output over a python script, for example filtering for the interesting information. The actions may depend on (binary) files or variables that can also be specified via the experiment creation.

B. Experiment Execution

The TBNs are booting a Linux image via PXE over the Ethernet connection. Each node gets its individual configuration via SSH from the TBMS. After the execution of the experiment, the results get uploaded and the node may reboot for a clean environment if specified.

C. DES-Cript

DES-Cript [3] defines a file format that includes the experiment settings as well as the results of an experiment. It is based on XML and is therefore readable by machines and humans. A DES-Cript file can be used to repeat an experiment to validate its reproducibility. Therefore, an import function is offered in the experiment creation web interface. All experiment results are provided via a DES-Cript file.

D. RIOT OS

RIOT [13] is an operating system for IoT devices that stands out from its high level of POSIX compatibility. The ESP32 used to monitor the power consumption of the EN and to provide the EN with 802.11n and Bluetooth connectivity is running on RIOT OS. While the software used in the EN can be chosen freely, RIOT has a feature allowing to efficiently deploy complex test setups easily: The RIOT shell is POSIX like command line interface available via UART, that can be controlled from the XN. The use of shell commands for configuring the EN or starting different parts of test runs allows deploying the same firmware on all ENs in a test. The desired behavior of each individual EN can be achieved by sending the right shell commands from the XN.

E. Reset Solution

As the reset solution should not depend on the XN being in a valid software state, a dedicated board with its own network connection is used. Due to infrastructure constraints an additional Ethernet connection is not possible. Therefore, the ESP32 used to reset the node is connected the WPA2 enterprise WiFi of the university. For possible updates an over the air solution will be integrated. As communication protocol we plan to use Constrained Application Protocol (CoAP) [14] to get more robustness against unstable WiFi connections.

V. Conclusion

We are building up a large scale testbed for wireless communication. Therefore, the testbed is developed with a focus on providing a realistic environment and offering a collection of different current state technologies. Furthermore, the six channel power monitoring solution can be used to simulate scenarios with battery powered nodes and to analyze the power consumption of the individual components of the node. With the reset solution we try to keep maintenance time low and thereby the uptime high.

On the software side we use a management system that cares for the substantial tasks in an experiment setup, like scheduling, repetitions, and a defined software environment. The DES-Cript file format ensures a human and machine readable representation as well as the base for reproducing the experiments.

At the time of writing this paper, the testbed is still in a prototype phase. Hence, it is possible that some details will change by further improving the setup.

References

[1] Bastian Blywis, Mesut Günes, Felix Juraschek, and Jochen Schiller. Trends, Advances, and Challenges in Testbed-based Wireless Mesh Network Research. *Mobile Networks and Applications*, 15:315–329, 2010. doi:10.1007/s11036-010-0227-9.

[2] Anne-Sophie Tonneau, Nathalie Mitton, and Julien Vandaele. How to choose an experimentation platform for wireless sensor networks? A survey on static and mobile wireless sensor network experimentation facilities. *Ad Hoc Networks*, 30:115–127, 2015. doi:10.1016/j.adhoc.2015.03.002.

[3] Mesut Günes, Felix Juraschek, and Bastian Blywis. An Experiment Description Language for Wireless Network Research. *Journal of Internet Technology (JIT), Special Issue for Mobile Internet*, 11(4):465–471, 7 2010. doi:10.6138/JIT.2010.11.4.04.

[4] Mesut Günes. On the scientific value of large-scale testbeds for wireless multi-hop networks, 2017. arXiv:1702.01052.

[5] Geoff Coulson, Markus Anwander, Gerald Wagenknecht, Sándor P. Fekete, Alexander Kröller, Tobias Baumgartner, Barry Porter, Ioannis Chatzigiannakis, Christos Koninis, Stefan Fischer, Dennis Pfisterer, Daniel Bimschas, Torsten Braun, and Philipp Hurni. Flexible Experimentation in Wireless Sensor Networks. *Communications of the ACM*, 55(1):82, January 2012. doi:10.1145/2063176.2063198.

[6] Michele Nati, Alexander Gluhak, Hamidreza Abangar, and William Headley. SmartCampus: A user-centric testbed for Internet of Things experimentation. In *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pages 1–6, June 2013.

[7] Cédric Adjih, Emmanuel Baccelli, Eric Fleury, Gaetan Harter, Nathalie Mitton, Thomas Noël, Roger Pissard-Gibollet, Frederic Saint-Marcel, Guillaume Schreiner, Julien Vandaele, and Thomas Watteyne. FIT IoT-LAB: A large scale open experimental IoT testbed. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 459–464, Dec 2015. doi:10.1109/WF-IoT.2015.7389098.

[8] Vlado Handziski, Andreas Köpke, Andreas Willig, and Adam Wolisz. TWIST: A Scalable and Reconfigurable Testbed for Wireless Indoor Experiments with Sensor Networks. In *Proceedings of the 2nd International Workshop on Multi-hop Ad Hoc Networks: From Theory to Reality*. ACM Press, 2006. doi:10.1145/1132983.1132995.

[9] Technische Universität Berlin. TKN WIreless NetworkS Testbed. www.twist.tu-berlin.de, 2016.

[10] Paramasiven Appavoo, Ebram Kamal William, Mun Choon Chan, and Mobashir Mohammad. Indriya2: A Heterogeneous Wireless Sensor Network (WSN) Testbed. In Honghao Gao, Yuyu Yin, Xiaoxian Yang, and Huaikou Miao, editors, *Testbeds and Research Infrastructures for the Development of Networks and Communities*, pages 3–19, Cham, 2019. Springer International Publishing. doi:10.1007/978-3-030-12971-2_1.

[11] Carsten Bormann, Mehmet Ersue, and Ari Keränen. Terminology for Constrained-Node Networks. RFC 7228, May 2014. doi:10.17487/RFC7228.

[12] J. Romkey. Nonstandard for transmission of IP datagrams over serial lines: SLIP. RFC 1055, June 1988. doi:10.17487/RFC1055.

[13] Emmanuel Baccelli, Oliver Hahm, Matthias Wählisch, Mesut Günes, and Thomas Schmidt. Riot: One os to rule them all in the IoT. Technical Report RR-8176, INRIA, 2012. URL: http://hal.inria.fr/hal-00768685.

[14] Z. Shelby, K. Hartke, and C. Bormann. The Constrained Application Protocol (CoAP). RFC 7252, June 2014. doi:10.17487/rfc7252.

Security for the Industrial IoT: The Case for Information-Centric Networking

Michael Frey*, Cenk Gündoğan†, Peter Kietzmann†, Martine Lenders‡, Hauke Petersen‡, Thomas C. Schmidt†, Felix Juraschek*, Matthias Wählisch‡
Safety IO* HAW Hamburg, Germany† Freie Universität Berlin, Germany‡
{first.last}@{safetyio.com, haw-hamburg.de, fu-berlin.de}, t.schmidt@haw-hamburg.de

***Abstract*—Industrial production plants traditionally include sensors for monitoring or documenting processes, and actuators for enabling corrective actions in cases of misconfigurations, failures, or dangerous events. With the advent of the Internet-of-Things (IoT), embedded controllers link these 'things' to local networks that often are of low power wireless kind, and are interconnected via gateways to some cloud from the global Internet. Inter-networked sensors and actuators in the industrial IoT form a critical subsystem while frequently operating under harsh conditions. It is currently under debate how to approach inter-networking of critical industrial components in a safe and secure manner. In this paper, we analyze the potentials of information-centric networking (ICN) for providing a secure and robust networking solution for constrained controllers in industrial safety systems.**

***Index Terms*—DoS resilience, unprotected channel, robust communication**

I. Introduction

Things in the Internet of Things (IoT) are often represented by small embedded controllers which possess orders of magnitude less resources than regular Internet nodes, but still need to communicate using protocols that interoperate in a common infrastructure. One predominant deployment area is industrial automation and surveillance, since embedded controllers are already prevalent in this industry, and adding a networking layer can generate immediate cost and performance benefits for its users. Initial deployments rely on legacy protocols such as MQTT—convergence on a future common networking standard for the industrial IoT is still under debate. Today's things are sensors or actuators that speak with a remote cloud or talk with each other locally. The prevalent communication for edge devices happens on wireless channels that are from low power lossy networks (LLNs) in the battery-powered world. Information Centric Networking (ICN) [1] was introduced as a networking paradigm for improved content access in a Future Internet. Ubiquitous caching is a core feature of ICN. Named Data Neworking (NDN) [2], one of its most popular flavors, was designed from a strong security perspective as a pure request-response scheme. It became apparent [3], [4] that ICN exhibits great potential for the IoT. The access of named content instead of distant nodes does not only allow for a much leaner and more robust implementation of a network layer, but in particular the request-response pattern of NDN prevents overloading the receiver with data. ICN deployment in the IoT has been studied with increasing intensity [3], [5], touching design aspects and practical use cases. Several implementations have become available in common IoT operating systems such as RIOT [6]. In this paper, we discuss central security aspects of NDN using the example of an industrial safety system. We introduce a real-world use case which we implemented in a recent prototype and identify key security requirements in Section II. The fundamental security contributions of the ICN networking layer are derived in Section III. Section IV is dedicated to comparative analyses of NDN versus traditional IP-based approaches. A summary and an outlook conclude this paper in Section V.

This article is a shortened version of previously published work: M. Frey, C. Gündoğan, P. Kietzmann, M. Lenders, H. Petersen, T. C. Schmidt, F. Juraschek, M. Wählisch. Security for the Industrial IoT: The Case for Information-Centric Networking. In *Proc. of IEEE WF-IoT*, IEEE, 2019.

II. Use Case: Security and Safety in Hazardous Industrial Environments

Industrial safety and control systems are increasingly interconnected to interchange operational conditions locally and to report their status updates to external observers. A typical deployment scenario consists of IoT stub networks that are often wireless and confined to the production plant, together with gateways that uplink to an Internet service provider. Current initial deployment scenarios further involve a (private) cloud which a dedicated group of trustees can access. Typical stakeholders are the operators of the systems. All parties rely on secure communication channels established between the network endpoints and the cloud. This scenario builds closed data silos for a preselected, confined group.

Already today it becomes apparent that the number of stakeholders in emerging scenarios will widen—plant operators, emergency teams, equipment vendors, and supervisory authorities may retrieve information about current safety conditions, intermediate operational statistics, as well as long-term reports. Furthermore, even a wider public may legitimately require civil participation in affairs of common impact, as is developing from open urban sensing initiatives [7], as well as participatory European laws. Following this demand, data silos need to break up in favour of a flexible, distributed data access that cannot easily rely on preconfigured trusted channels. Still, data might not be uniformly public, but continue to require protection. Protecting the data itself instead of the transmission

channels paves the way to transparent data replication and caching—an efficient method for eliding today's silos.

Industrial deployments often operate under harsh conditions. In our use case, we consider industrial environments with a threat of hazardous contaminant (e.g., explosive gas) that need continuous monitoring by stationary, as well as mobile sensors. In case of an emergency, immediate actions are required such as issuing local alarms, activating protective shut-downs , initiating a remote recording for first responders and forensic purposes, and eventually may need to trigger evacuations of the plant or even the region. Such complex settings obviously involve many parties and require a level of robustness which a single uplink to a remote cloud cannot guarantee. This use case specifically relies on a fast sensor-actuator network including embedded IoT nodes. The harsh industrial environment raises the challenges of mobile, intermittently connected end nodes, network partitioning, and enhanced reliability from safety requirements. Devices often need to connect spontaneously, and a corresponding IoT system cannot reliably establish end-to-end channels in many situations. Varying connectivity challenges and mobility, as well as external hazardous impacts are much easier mitigated in a replicative environment, where data diffuses hop-wise in an asynchronous fashion. It is easy to build such a compliant networking layer based on NDN primitives [8]. Taken from real-world deployment, this study makes the case for a distributed, multi-stakeholder environment and identifies three major objectives for the networking layer: i) allow for ubiquitous multiparty data access without pre-established secure data channels or VPNs in the constrained IoT, ii) provide a robustly secure networking infrastructure that is resilient to varying link conditions and mobility with the ability to recover locally from intermittent impairments, and iii) raise the barriers for distributed denial-of-service (DDoS) attacks of constrained devices and confine the attack surface of unwanted traffic to local links. We will show in the following, how the NDN approaches to Information Centric Networking can significantly contribute to these goals. We will also assess the shortcomings of current IoT solutions such as MQTT [9] and the Constrained Application Protocol (CoAP) [10].

III. Security Contributions of NDN

According to our use case, an industrial IoT deployment enhances requirements in the security and safety domain, but on the other hand narrows the utilization of ICN functions down to rather specific settings. In this section, we will discuss the three security aspects derived from our use case and identify certain benefits for NDN from its specific deployment in an industrial setting.

a) Ubiquitous data access in the constrained IoT: Sensor data need to be accessible both in the local constrained IoT, and in the remote for stakeholders. Safety and security of the industrial monitoring system indeed largely depend on its availability even under the harsh conditions of local or regional incidents with intermittent connectivity. As critical industrial facilities are always also susceptible to malicious threats, utmost resilience against (networked) attacks is strongly desirable. A centralized cloud-based approach falls short as tampering the cloud has proven to be a pronounced attack vector (cf. the Cloudflare attack 2013). Ubiquitous caching is the most striking contribution ICN makes to the security and safety of the distributed information system. Configuring the constrained nodes as well as the gateway to replicate and store IoT data for (most of) its lifetime will maximize redundancy and minimize unavailability of critical information. It is noteworthy that common IoT data is small and of limited lifetime—archives being a well-localized exception. Furthermore, flash storage in constrained nodes is the least scarce resource and typically can accommodate an 'infinite' amount of IoT data. Local mass storage facilitates the delay-tolerant network nature of ICN for the IoT. The hop-by-hop transmission of sensor readings and actuator commands increases resilience in the presence of caching. When links re-establish after mobility handovers or failures, the NDN network layer can easily resume the content propagation and will thus provide an efficient self-healing mechanism.

b) Robustly secure networking infrastructure: Sensors and actuators of the constrained IoT are typically challenged by maintaining an authenticated or even encrypted data channel to some remote data repository. In addition, unstable and lossy links in IoT edge networks make it hard to persist a stateful communication relation. Also for these reasons, IoT nodes are commonly deployed behind gateways that execute protocol translations and thereby intercept secured channels. This sacrifices end-to-end transport security and exposes a significant attack surface at the gateway. By authenticating or encrypting content instead of channels NDN circumvents these operational challenges of the IoT. As each content chunk can be hopwise replicated throughout the network without impairing its security measures, data integrity and confidentiality remain independent of transport or paths. Moreover, there is no requirement of performing synchronous actions between specific endpoints on the Internet which makes the security layer robust against link failures and network disconnects.

c) DDoS resistance: Constrained nodes are easy victims of resource exhaustion when receiving too many IP packets. A gateway may shield the IoT nodes from the global Internet and may even perform some rate limiting, but it cannot reasonably track individual resources of nodes nor hinder the communication needs of the application use case. In addition, a malicious member of the IoT stub domain may not only jam radio channels, but utilize IP multihop forwarding to overload remote nodes. Conversely, as has been recently reported from the MIRAI incident, huge multiplicities make IoT nodes an interesting amplification tool for attackers. A key design objective of ICN had been the reduction of this IP attack surface with respect to DDoS attacks. In NDN this led to designing a request-response communication scheme without node addresses that hinders the plain transmission of unwanted content to a receiver. For a few years, it was the believe that NDN can be DDoS resistant by design, until Interest- and state-based attacks were discovered [11]. Subsequent work [12], [13] elaborated the threats of Interest

flooding and overloading FIB and pending interests table (PIT) structures by user-generated names and content requests. This has proven difficult to mitigate in general [14]. However, in a specific industrial setting of pure machine-to-machine communication with well known traffic patterns, buffers and PIT tables can be pre-configured according to well-formed communication flows. Hence, Interest flooding can be detected at the first hop and eliminated by the receiving stack. State-based attacks can thus be restricted to the local link which can never be protected by a network layer.

IV. Comparative Assessment

We provide a qualitative security comparison of our ICN solution with the common IP-based protocols MQTT and CoAP. We also evaluate the complexity of content object security that is inherent to ICN, but for a quantitative performance analysis we refer to [15].

MQTT: MQTT is a message-based publish subscribe protocol, with a special focus on low bandwidth environments. A typical MQTT network involves a client that publishes data on a specific *topic*. Each topic is managed by a server (or *broker*) which distributes data about the topic to subscribers. By default, a message that has been published and distributed to the consumers by the broker is deleted after delivery. Different Quality-of-Service (QoS) levels allow for storing messages on the broker or advanced reliability on top of the transport protocol. Low-end IoT devices are challenged by basic MQTT, as MQTT communicates over TCP. A lightweight version of MQTT is provided by *MQTT for Sensor Networks* (MQTT-SN) [16]. It is tailored to wireless domains and optimized for devices that are constrained in energy, processing, or storage. MQTT-SN is implemented on top of UDP and replaces topic strings by topic IDs to shorten messages. Security features depend on the broker implementation. Using username and password, or alternatively a client certificate, the broker may authenticate the client it connects to. If transport layer security (TLS) or datagram transport layer security (DTLS) is used, the client may also authenticate the server. However, there is no end-to-end security support between publisher and subscriber. This threatens message integrity when the broker changes content, because subscribers do not have an out of the box mechanism to verify the content. To protect the payload, additional encryption efforts of application data are required on top of MQTT. In general, MQTT assumes a trust relationship between broker, publishers, and subscribers. Usually, authentication and authorization is ignored, to simplify device management. This trust assumption reflects current deployment models, in which either brokers and clients are under the same administrative control, or where service contracts between end devices and a cloud network with broker service exist.

CoAP: CoAP is standardized in the IETF with the aim for replacing HTTP in constrained deployment scenarios. It operates on top of UDP and defines a compact protocol header. It specifies three communication schemes: (i) polling, (ii) push, and (iii) observe. Using push and observe, CoAP implements publish subscribe scenarios. In contrast to push, observe does not require explicit subscription in advance but delivers data to clients based on pre-configuration at the server side. To enable machine-to-machine communication, CoAP implementations usually provide both client and server capabilities. Thus, without an explicit intermediary node such as a broker in MQTT, CoAP nodes may interact directly with each other. The security support in CoAP is more advanced compared to MQTT, even though specifications are still under discussion in the IETF. CoAP is secured on the transport layer using DTLS or alternatively on the application layer using specific extensions such as OSCoAP, which allows for object security in CoAP. However, it is worth noting that DTLS might conflict with constrained environments as packet sizes increase. On the other hand, current approaches for object security may conflict with privacy as not all CoAP headers are encrypted and, for example, may reveal content names.

A. Comparing MQTT, CoAP, and ICN

Caching: Caching does not only improve performance in terms of faster data delivery but also increases data availability and robustness. A common malicious scenario includes a denial of service attack. With proper replication, the origin data source can go offline without loosing data in the global network. MQTT is easily threatened by this kind of attack because of the dedicated broker service. CoAP inherently supports caching on intermediary nodes. However, this mitigation is only implemented on the application layer. In common single stakeholder scenarios, where CoAP servers are managed by a single administrative domain, this usually does not help, in particular when network providers are under attack. ICN provides ubiquitous in-network caching that is independent of individual stakeholders. Thus, attacking a specific content source is intricate.

Reliability: IoT nodes connected via low-power wireless networks suffer severely from lossy communication channels. Even the transmission of small data chunks to the gateway is frequently impaired by unstable links, and transport protocols are challenged to cope with the unstable environment in a reliable fashion. We compare NDN, confirmable and non-confirmable CoAP (c/n), and MQTT (Q0/Q1) in Figure 1. The success rate of packet delivery was measured in two large experiments of 50 nodes from the FIT IoT testbed at different publishing intervals. Low power lossy radios of the IEEE 802.15.4 standard were deployed with link-layer retransmissions set to four. Results demonstrate the superior

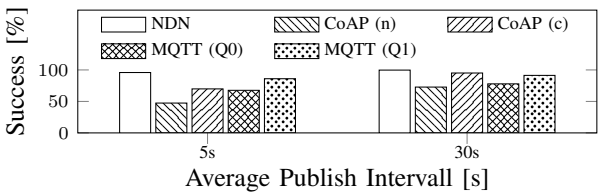


Fig. 1: Resilience of NDN vs. CoAP vs. MQTT.

reliability of the hop-by-hop approach of NDN, while even the reliable variants of CoAP (c) and MQTT (Q1) fail significantly by 30 % resp. 15 % in the tighter scenario of publishing every 5 s. NDN always delivers more than 95 % of the packets, the success rate approaching 99.9 % in the more relaxed publishing at 30 s.

Object security: Security of content objects is crucial in inter-domain scenarios, in particular in the industrial Internet where sensors communicate sensitive information or actuators interact with critical infrastructure components based on data. Ideally, content can be forwarded by any node in the network without sacrificing security. MQTT and CoAP need additional efforts to achieve this objective. ICN, on the other hand, has been designed with democratized content distribution in mind. In-network caching is not limited to specific service nodes but envisioned to run on any network node that is willing to share resources for caching. Consequently, content security is a first principle in ICN, allowing multi-stakeholder scenarios with respect to scalable and secure content distribution. In ICN, trust is not based on contracts but technically provided by design.

Infrastructure protection: CoAP runs on top of UDP. As UDP is a connection-less protocol without congestion control, it can easily operate IP packet bursts and spoofing. Having IP spoofing in place, an attacker can initiate a reflective amplification attack, in which the attacker sends a small request towards the CoAP server that replies with a significantly larger packet to the victim (i.e., the spoofed IP address). Amplification attacks are common in the current Internet and a major threat for operators. With increased deployment of CoAP, we will experience more of such attacks in the future. MQTT makes spoofing attacks much more challenging because of TCP. However, in MQTT-SN, TCP is replaced by UDP to reduce overhead on low-end IoT devices and thus opens up the identical attack surface. On the contrary, ICN abandons the end-to-end paradigm and provides de-localized services off the shelf.

End node protection: End nodes are not protected in MQTT and CoAP but may receive arbitrary amounts of unwanted data. Security extensions may enable authentication and authorization but protection against unsolicited traffic requires firewall extensions, either as infrastructure middleboxes, or as dedicated local software component running on the end node. The latter conflicts with constrained resources of low-end IoT devices. An industrial Internet benefits from ICN as ICN does not support end-to-end communication. It thus protects end devices against malicious traffic without additional overhead.

Name privacy: To comply with privacy requirements, obfuscating the requested content name in the content delivery infrastructure is important. Implementing this with low overhead and strong privacy protection is one of the most challenging tasks in content delivery scenarios, yet. Neither MQTT, nor CoAP, nor ICN provide a solution out of the box until now. The hope here is that the ICN community will introduce a sufficient solution in the long-term because naming is a key component, which affects all applications on top of an ICN network layer.

V. Conclusion and Outlook

The industrial IoT connects safety critical environments to the Internet, requiring a high level of reliability and security for data, infrastructure, and end devices. Multiple stakeholders in this inter-domain communication challenge security, but current protocols in the IoT are weak in meeting these demands. In future work, real-world deployment and experimentation is needed to evaluate and harden the contributions ICN can make towards a safe and secure industrial Internet of Things.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, July 2012.

[2] V. Jacobson, D. K. Smetters, J. D. Thornton, and M. F. Plass, "Networking Named Content," in *5th Int. Conf. on emerging Networking Experiments and Technologies (ACM CoNEXT'09)*. New York, NY, USA: ACM, Dec. 2009, pp. 1–12.

[3] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild," in *Proc. of 1st ACM Conf. on Information-Centric Networking (ICN-2014)*. New York: ACM, September 2014, pp. 77–86. [Online].

[4] E. M. Schooler, D. Zage, J. Sedayao, H. Moustafa, A. Brown, and M. Ambrosin, "An Architectural Vision for a Data-Centric IoT: Rethinking Things, Trust and Clouds," in *IEEE 37th Intern. Conference on Distributed Computing Systems (ICDCS)*. Piscataway, NJ, USA: IEEE, June 2017, pp. 1717–1728.

[5] G. C. Polyzos and N. Fotiou, "Building a reliable Internet of Things using Information-Centric Networking," *Journal of Reliable Intelligent Environments*, vol. 1, no. 1, pp. 47–58, 2015.

[6] E. Baccelli, C. Gündogan, O. Hahm, P. Kietzmann, M. Lenders, H. Petersen, K. Schleiser, T. C. Schmidt, and M. Wählisch, "RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4428–4440, December 2018. [Online].

[7] H. Bornholdt, D. Jost, P. Kisters, M. Rottleuthner, D. Bade, W. H. Lamersdorf, T. C. Schmidt, and M. Fischer, "SANE: Smart Networks for Urban Citizen Participation," in *2019 26th International Conference on Telecommunications (ICT) (ICT 2019)*. Piscataway, NJ, USA: IEEE Press, April 2019.

[8] C. Gündogan, P. Kietzmann, T. C. Schmidt, and M. Wählisch, "HoPP: Robust and Resilient Publish-Subscribe for an Information-Centric Internet of Things," in *Proc. of the 43rd IEEE Conference on Local Computer Networks (LCN)*. Piscataway, NJ, USA: IEEE Press, Oct. 2018, pp. 331–334. [Online].

[9] A. Banks and R. G. (Eds.), "MQTT Version 3.1.1," OASIS, OASIS Standard, October 2014. [Online].

[10] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, RFC 7252, June 2014.

[11] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Bulk of Interest: Performance Measurement of Content-Centric Routing," in *Proc. of ACM SIGCOMM, Poster Session*. New York: ACM, August 2012, pp. 99–100. [Online].

[12] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in Named Data Networking," in *Proc. of ICCCN*. IEEE, 2013, pp. 1–7.

[13] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Network Infrastructure," *Computer Networks*, vol. 57, no. 16, pp. 3192–3206, Nov. 2013. [Online].

[14] S. Al-Sheikh, M. Wählisch, and T. C. Schmidt, "Revisiting Countermeasures Against NDN Interest Flooding," in *2nd ACM Conference on Information-Centric Networking, Poster Session*, ser. ICN 2015. New York: ACM, Oct. 2015, pp. 195–196.

[15] C. Gündogan, P. Kietzmann, M. Lenders, H. Petersen, T. C. Schmidt, and M. Wählisch, "NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT," in *Proc. of 5th ACM Conference on Information-Centric Networking (ICN)*. New York, NY, USA: ACM, September 2018, pp. 159–171. [Online].

[16] A. Stanford-Clark and H. L. Truong, "MQTT For Sensor Networks (MQTT-SN) Version 1.2," IBM, Protocol Specification, November 2013. [Online].

Inline process analysis with wireless powered sensors

Ulrike Steinmann
Otto-von-Guericke-University Magdeburg
Chair Measurement Technology
Magdeburg, Germany
ulrike.steinmann@ovgu.de

Axel Hoppe
Institut für Automation und Kommunikation e.V.
Department Measurement Technology and Power Electronics
Magdeburg, Germany
axel.hoppe@ifak.eu

Jörg Auge
Magdeburg-Stendal University of Applied Sciences
Institute of Electrical Engineering
Magdeburg, Germany
joerg.auge@hs-magdeburg.de

Large scaling industrial processes, e.g. charging or mixing, often are attended by inhomogeneities in the material composition. One vision of monitoring these processes involves autonomously moving sensors in the process volume which obtain and transmit spatially resolved data. The paper illustrates first approaches for those requests. An experimental platform is described which drives an optic, an acoustic and a dielectric sensor module via a rotating unit in the (liquid) medium. The work is focused on the realization of wireless power and data transfer and presents the conceptual design of sensor modules. First experimental results are discussed.

Keywords—mobile sensors, process analysis, wireless transfer data energy

I. INTRODUCTION

Nowadays, tomographic monitoring of analytic information (inline, online) is of increasing importance. A possible scenario is the following: instead of monitoring a process by using spatially fixed measurement equipment the sensors are directly inserted in the process. By this, information is permanently obtained from the inside of the process [1]. Based on the measured data process monitoring and control in real time is possible and tomographic reconstruction algorithms become abdicable [2], [3]. Though, such a monitoring requires the solution of manifold detailed problems. These include e.g. a robust, miniaturized and process-adapted acquisition of multiple parameters, a reliable and wireless data transmission, the navigation and localization of sensors, and a concept for the energy supply. To solve these problems an intense and multidisciplinary research work is required. In this context the contribution is focused on the technology of wireless energy and data transmission to process-adapted sensor modules.

II. SENSOR SYSTEM

A. General information

A future scenario in process industry, as it is outlined also in the roadmap "Prozess-Sensoren 2015+"([1]), does not exclusively use stationary installed sensors but introduces them directly into the process where a continuous acquisition of data occurs. During the time that the sensor stays in and is carried by the process medium location- and time-resolved process information are to be obtained and communicated to the outside. After passing the process chain the sensor will be discharged from the final product or the process vessel. Based on the measurement data monitoring and control of the process can be realized in real-time without using complex tomographic algorithms.

Those mobile sensors need a power supply which works reliable also under extreme conditions. In principle the use of batteries, energy harvesting or contactless power transfer solutions are imaginable. However, batteries and energy harvesting solutions have significant disadvantages. Whereas batteries have to be changed from time to time and they are subject to an aging process, energy harvesting solutions are only suitable for low power applications. Because of these restrictions the power supply should be realized with an inductive power transfer system which is able to transmit up to 10 W.

Furthermore, a bidirectional data transfer should be available. Thereby, the measured data can be read out from the sensor and control commands can be sent to it and vice versa. For this task contactless systems represent a promising approach since data rates up to 115 kbit/s can be realized.

On sensor side, robust, mobile, multi-parameter transducers for the inline measurement of process data have been developed. The sensors contain acoustic, optical and dielectric measurement modules which can be fixed each to a moving element, e.g. a stirrer, in a first technical approach. During its continuous rotation the local distribution of the interesting process data can be recorded within the concentric near field of the stirrer (areal scan). Due to a controlled motion of the stirrer the sensor positions are known instantaneously (Fig. 1).

Power supply and data transfer of the prototype system in Fig. 1 occurs through the medium at the bottom of the container (distance about 30 mm). In a constructional improvement the inductive transfer system interacts with the sensor system along the container's circumference, which increases the system flexibility. A prerequisite for an autonomous sensor system is also that suitable, size-optimized components for navigation and motion can be integrated to replace the previous obligatory (e.g. rotary) guidance. In another prototype solution the acousto-optic concept is expanded by a dielectric measurement method in order to

Fig. 1. Experimental platform comprising optical and acoustic sensor modules and components for energy and data transmission (right, center), illustration of the spatial resolved data in real-time (left).

form a multi-sensor platform for the characterization of a (liquid) substance under test. The realized principles are presented in the following.

B. *Ultrasonic sensor module*

This probe allows measurements in transmission mode as well as in the reflection mode (Fig. 2). Both transducers, for transmitting and receiving signals, are piezoceramics of 2 MHz resonance frequency. The time of flight of the acoustic impulse is captured using a time-digital-converter. The obtained resolution is in the range of several picoseconds. Due to short runtimes of the acoustic waves, a data acquisition rate of several hundred Hz is achieved.

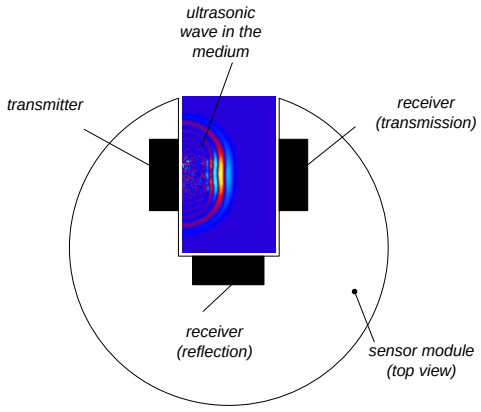


Fig. 2. Setup of ultrasonic sensor module.

C. *Dielectric sensor module*

This sensor module measures the permittivity of the medium (Fig. 3). The electrodes of the sensor are electrically insulated from the medium. The electronics of the sensor works as an impedance analyzer. With a sweep generator, sinusoidal signals with constant amplitude are created and are automatically swept through the frequency range. A low pass *RC*-element consisting of capacitor *C* (interacting with the medium) and a reference resistor *R* is used to obtain the amplitude and phase of the voltage across the capacitance. This voltage is digitized by an analog-digital converter.

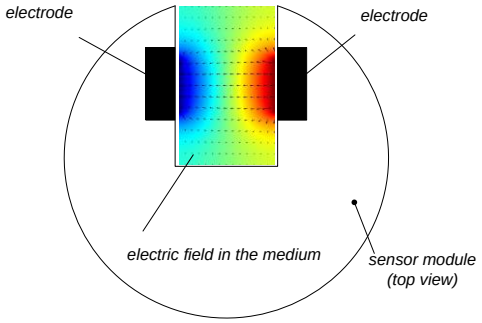


Fig. 3. Setup of dielectric sensor module.

D. *Optical sensor module*

In analogy to the acoustic module, the optical module allows transmission and reflection measurements as well (Fig. 4). Thus, important information is available about substances like suspensions or emulsions. This probe works in the non-visible frequency range (λ = 880 nm) using transmitting and receiving units that are adjusted to each other. A main module containing a micro controller (ATmega 664P) administrates the coupling of all sensor modules, the capturing and processing of raw data, the sequential control, and the interface between the energy and data transmission.

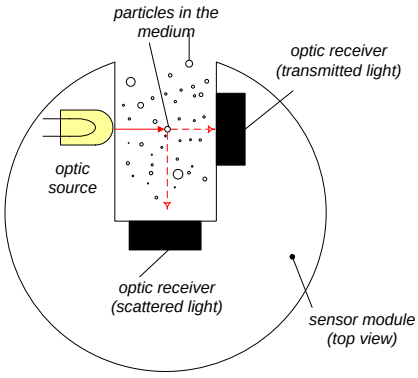


Fig. 4. Setup of optical sensor module.

III. WIRELESS ENERGY AND DATA TRANSMISSION

An inductive transmission system with air gap is based on the principle of a transformer. Whereby a transformer is guiding the magnetic flow through an iron core in order to get a high efficiency. In our application, the transmission system consists of separate windings for energy and data transfer without an iron core. Working at higher frequencies with optimized coiling geometry and using resonance effects the transmission system can reach comparable efficiencies. The power transmission system was designed unidirectional. The system for data transmission is bidirectional in order to introduce the control signals from the outside into the sensor system and to read out the measured data from the sensor system. The experimental setup is shown in Fig. 5 and represents the inner components of the coil system as shown in Fig. 1 (bottom right). The air gap to be bridged between the primary and secondary side is 30 mm. The contactless energy transmission operates at an operating frequency of 100 kHz and conveys 1..10W. Data transmission enables a data rate of 115 kBit/s at an operating frequency of 2 MHz allowing also underwater communication.

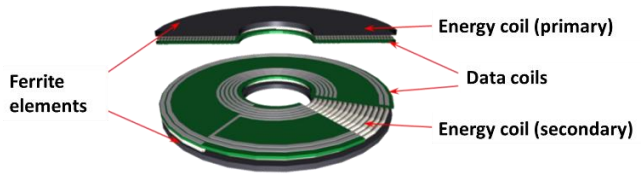


Fig. 5. Coil system for combined energy and data transmission.

As shown in Fig. 1 (left), with this optical-acoustic demonstrator the real-time-capable combination of location information of the rotary drive system and media information (detection of air entrapment, acoustic emission) can be demonstrated. Both the temporal course of the sensor data and the location-related 360° representation can provide useful information on the process to the plant operator.

IV. MOBILE SENSORS

A. General information

Future scenarios envisage introducing sensors directly and freely into liquids instead of permanently installing them. In this way, information on temperature, pressure or concentration can be obtained from the "inside of the process". But the sensors need energy and must be able to transmit their data. The transmission of energy and data to an object that can move freely in three-dimensional space places completely new demands on the transmission system, in contrast to classic point-to-point couplings or force-guided consumers. A concept for the realization of contactless energy and data transmission for freely movable sensor modules was developed and implemented in a further experimental setup.

The coil system developed for the supply of mobile sensors is shown in Fig. 6. The primary side is formed by a winding located on the outer surface of a cylindrical container. The individual windings are distributed in such a way that an almost homogeneous field distribution is formed inside. The field homogeneity can be recognized by the uniform color distribution in the section plane in Fig. 6 center. This ensures a relatively constant coupling to the freely movable elements in the container. A voltage is induced there which is independent of the radial and axial position. The receiving elements are spherical (a few centimeters in diameter) and have 3 coils arranged orthogonally to each other on the surface. In contrast to the rotary experimental platform, data and energy transmission is realized on one common coil system, only. The determined parameters for this concept are: frequency: 625 kHz, primary voltage 12 V, primary current 5 A (peak value), secondary output power 400 mW per sensor, efficiency of energy transmission approx. 5%.

The efficiency of the energy transfer of the system is very low. This is caused by the very weak coupling between relatively large primary side with small secondary side and small number of turns of the coils. The maximum power to be delivered is therefore limited to less than 1 W. The energy transmission is operated at 625 kHz in order to achieve an acceptable efficiency of approx. 5 % in this case. In an optimized design the efficiency of the inductive transmission system can be increased beyond this shown experimental case.

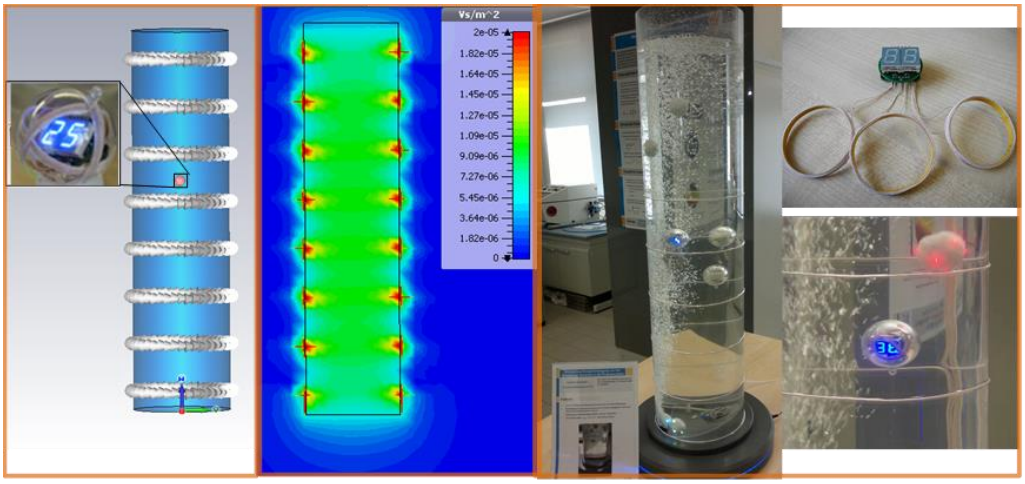


Fig. 6. Simulation model of an acrylic glass cylinder with primary and secondary coil system (left); simulation of the magnetic flux density over the cylinder cross-section (center left); experimental setup (center right) with mobile sensors (bottom right)

B. *Identification*

Unique identification is possible through communication between the sensor module and the primary system. The sensor module transmits a specific data signal, which is recognized on the primary side and assigned to the sensor. The data signal is modulated onto the energy coil system. A voltage containing the frequency of the data signal is induced in the primary system via the inductively coupled coils. The carrier frequency of the data signal is many times higher than the energy transmission frequency. This results in a sufficiently high signal-to-noise ratio between the energy level and the data level. If several sensors are used, an undisturbed and collision-free data transmission must be guaranteed. A separate carrier frequency can be used for each sensor.

C. *Position recognition*

Due to the transmission principle presented above with freely moving sensors, position determination is not possible when using one primary data coil that is equivalent to the energy coil system. Several data windings must be applied on the outside, which make it possible to communicate with each sensor integrated in the system. The primary data windings could be designed similar to the primary energy coil system. This means that a separately controlled data winding is installed next to each primary coil ring. The position is then determined along the axis. The coils of this data winding must be supplied separately (parallel connection). By evaluating the coupling of the individual primary data windings to the sensors, it is possible to determine the position along the axis. If the positions of several sensors in the container are to be determined simultaneously, this is possible by tuning the coupling between data windings and sensors to different frequencies.

An alternative to the above concept is to supply the sensor system via the outer surface of the cylindrical vessel (Fig. 7). A sector-shaped subdivision of the coils for energy and data makes it possible to determine the circular position (along the circumference) of the sensor module in the vessel by evaluating the primary coil connected in each case. The following parameters have been theoretically determined for this concept: frequency: 200 kHz, secondary voltage 12 V, secondary current 800 mA for a module which is supplied with battery charging electronics, output power 9.6 W in charging mode, energy transmission efficiency approx. 80 %.

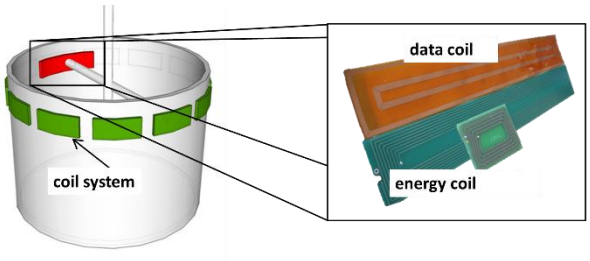


Fig. 7. Energy and data transmission via the outer surface of a cylinder: structure (left); energy and data coils (right)

A combination of the above concepts allows the determination of the position of sensors in a cylindrical vessel (see Fig. 8). For this concept, the couplings between each detection coil attached to the shell surface and each sensor are to be evaluated. For this purpose, the coil system and sensor must be tuned to a resonant frequency. If several sensors are detected, the number of resonances to be tuned increases with the number of sensors.

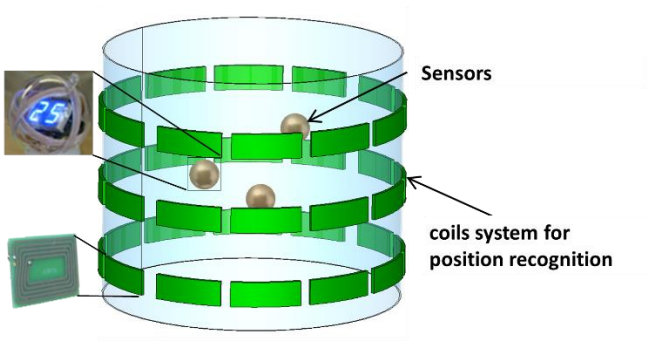


Fig. 8. Acrylic glass cylinder with detection coils distributed over the surface of a cylinder for position recognition of sensor modules.

V. SUMMARY

The paper illustrated first approaches for monitoring industrial processes via autonomously moving sensors. An experimental platform has been realized which drives an optic, acoustic and dielectric sensor module in an aqueous solution of varying conductivity.

With regard to contactless energy and data management, several conceptual approaches were developed and evaluated in initial experimental and/or theoretical investigations. Thus, a solution has been demonstrated which allows the assurance of real-time, uninterrupted operation of and communication with self-sufficient, freely movable sensor modules, even under process-related environmental conditions. A perspective application scenario addresses the use of many sensor systems moving autonomously in a process volume.

REFERENCES

[1] Roadmap „Prozess-Sensoren 2015+“, NAMUR und VDI/VDE-GMA

[2] S. Woeckel, U. Hempel, J. Auge, Phase boundary characterization in liquids by acoustic waves, Special Issue Meas. Sci. Technol. 20 (2009) 124013 (6pp), IOP Publishing

[3] S. Woeckel, U. Hempel, J. Auge, Acousto-capacitive tomography of liquid multiphase systems, Sens.& Act. A: Physical, Vol. 172, Issue 1 (Dec.2011), pages 322-329

[4] C. Rathge, S. Thamm, A. Hoppe, Systematically Design and Optimisation of Inductive Power Transmission Systems, Proceedings Electric Drives Production Conference 2013, pages 339-342, ISBN: 978-1-4799-1102-8

[5] D. Kuerschner, C. Rathge, U. Jumar, Design methodology for high efficient inductive power transfer systems with high coil positioning flexibility. IEEE Transactions On Industrial Electronics 2011, ISSN: 0278-0046, DOI: 10.1109/TIE.2011.2181134

[6] D. Kuerschner: Methodischer Entwurf kontaktlos induktiver Energieübertragungssysteme. Shaker Verlag Aachen, 2010, ISBN: 978-3-8322-8897-6

[7] C. Rathge, A. Hoppe, Wireless Inductive Power and Data Transfer – Design, Opportunities, Chances and Limitations, E|TEV 2012, Nürnberg, 17.10.2012, Proceedings on CD ROM

A Survey of Selected Evaluation Tools and Metrics for Low-power and Lossy Networks: A Simulation Approach

Saleem Raza, Ali Nikoukar, and Mesut Güneş
Communication and Networked Systems (ComSys), Faculty of Computer Science,
Otto-von-Guericke University Magdeburg, Germany
{saleem.raza, ali.nikoukar, mesut.guenes}@ovgu.de

***Abstract*—Performance evaluation is crucial to understand the key performance indicators of any network, protocol, or algorithm. This paper explores methodologies and metrics that are used in performance analysis of low-power Internet of Things networks with particular focus on medium access control layer. Our target is computer simulation, which is a low-cost and less laborious method compared to real hardware experiments or measurements. This paper provides a survey on selected simulation tools that are used to study and analyze low-power wireless networks. Wireless low-power and lossy networks are different from wired computer networks, therefore we consider performance metrics that are commonly used in medium access control performance analysis.**

***Index Terms*—Evaluation methods, Medium Access Control, Simulation**

I. Introduction

Verification and validation of any proposed protocol or algorithm is necessary so as to examine its performance under certain constraints for which the protocol is developed. This leads to the area of performance evaluation, which is fundamental to developing and analyzing new communication protocols. Performance evaluation has been applied to computer networks and protocols since decades which involves testing them prior to their deployment in real world applications. Thus, it ensures that the protocol serves at its best through the life-cycle of its operation. It equally applies to the domain of Low-power and Lossy Networks (LLNs) which involves constrained sensor nodes. Consequently, saving resources and meeting Quality of Service (QoS) criteria are not only imperative but also challenging aspects of protocol performance.

The core foundation of Internet of Things (IoT) [1] and LLNs [2] depends on software, network, and embedded engineering. Although, these fields are well developed but they need to adapt certain practices and methodologies according to the specifications of wireless LLNs [3]. Over the years, most of the solutions tailoring to the IoT are based on the modular protocol stack as depicted in Figure 1. Thus, as per the application requirements, appropriate protocols and standards may be selected prior to actual deployment. In this way, deployment cost and efforts can be reduced by allowing several applications to operate on top of the same wireless infrastructure [5]. In particular, agile methodologies are suitable in the development of IoT research solutions as they involve a repetitive development life-cycle, which has the advantage of quickly rectifying errors during the conception or in the assumptions. Generally, research pertaining to LLNs follows certain steps similar to ones mentioned in [3] as given in Figure 2. These steps are needed to conduct performance evaluation of a protocol, an algorithm, or an entire networking stack. Often, neglecting certain steps, for example, making quick transition from protocol idea to hardware experiment evaluation may lead to inappropriate results.

In this paper, we discuss about performance evaluation of Medium Access Control (MAC) protocols in low-power and lossy networks and survey existing methods of performance evaluation. This survey focuses on simulation approach which is extensively used to analyze protocol performance as compared to hardware experiment. Several simulation platforms are described that are commonly used for protocol assessment in low-power networks. We explain important performance metrics commonly used in the validation of MAC protocols.

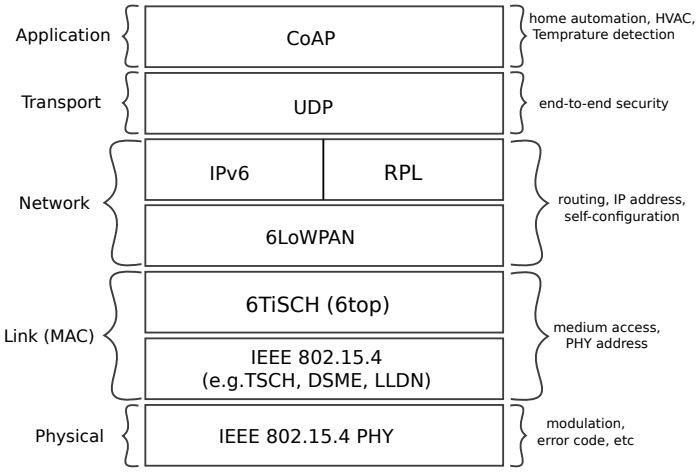


Figure 1. A modular protocol stack of IoT defined by IETF [4].

The remainder of the paper is organized as follows. Section II gives a general overview on performance evaluation and validation methods, it talks about theoretical, measurements, and simulation methods. Section III describes performance metrics, that are crucial to determine MAC performance. Finally, we provide a conclusion in Section IV.

II. Performance Evaluation Methods

Generally there are three common approaches to conduct performance evaluation of a protocol: theoretical analysis, measurements, and simulation as depicted in Figure 2. All these approaches come up with their own strengths and limitations, which approach is appropriate, when and how to apply it, is widely discussed in literature [6]. We focus on MAC layer because it controls radio related activities which can impact network performance. Associated with MAC are performance metrics that determine how reliably a MAC functions as per the requirements of application.

A. Theoretical Analysis

Often the first step is to evaluate the proposed protocol by examining it theoretically. Although, it is considered preliminary step, yet it helps prove convergence of the protocol or algorithm which ensures that the design is correct. Typically, certain properties are respected such as approximation, lower and upper bounds, complexity [3]. This approach deals with mathematical abstractions, deriving formulas that best describe performance of a system or protocol. Theoretical analysis is performed when real measurement is not available, but it requires rigorous

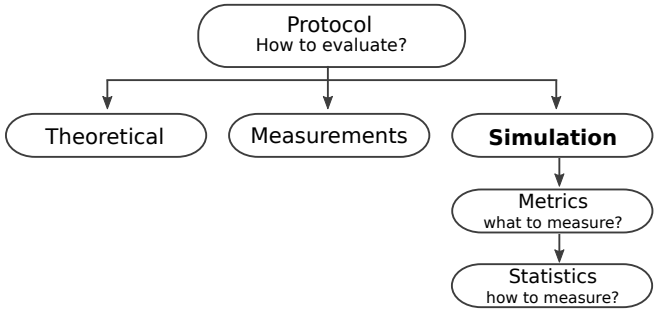


Figure 2. Different approaches of protocol performance evaluation.

mathematical background. In terms of efforts and cost, this is the most convenient approach, however it offers limited insights followed by certain assumptions [7]. This is the first step which is later validated by either simulation or experimental work [6]. Theoretical analysis does not have to be complex, often an available probability distribution function can help do job of model fitting on it. We have seen examples of deriving simple models of traffic generators from the user behavior.

B. Measurements Analysis

This approach undertakes existing instance of the actual system to conduct performance measurements or experiments. This approach produces highly reliable results because the measurements are taken on the system itself, however it is very expensive and takes more time because it requires costs associated with hardware, installation, maintenance, and staff. This method is not always possible, because it may be the case that the system may not yet exist.

C. Simulation Analysis

Simulation has been widely used for protocol validation over the decades. It involves developing computer programs that are used to implement a system or protocol and perform experiments by running those computer programs [7]. This approach is less expensive and reliable alternative when analytical models or experimental measurement approaches are not directly suitable. It is often the case in protocol development that once it is simulated, it can be later tested through real world experiment or measurement. However, dealing with experiment is costly and laborious as it requires precise calculation and sometimes controlled environment to accomplish reliable results. The decision to perform simulations only or both the simulation and hardware experiment largely depends on the nature of protocol requirements and its underlying complexities. Various simulation platforms have been developed such as OMNeT++, Cooja, OpenWSN, MATLAB, NS-2, and NS-3.

There are different types of computer simulations such as discrete-event, Monte Carlo, continuous, trace-driven, and spreadsheets. Discrete event simulation is widely used technique in low-power networks. Discrete-event simulations follows certain sequence of events that take place in a chronological order. It is called discrete event owing to the fact that the occurrence of events or change of states in simulation takes place at distinct points in time. Thus, it offers modularity in the evaluation process and protocol can be studied under different conditions. Reproducibility is another strong aspect offered by simulation which allows to re-produce same results given the same seed, simulator version, and the code. Simulation also allows repeatability which permits different protocols to be evaluated under precisely the same (random) environment [7]. Commonly, a pseudo-random number generator is used in simulation which can mimic uncertainty when probabilities are to be respected [3].

Particularly, the simulation of LLNs, involves the use of Physical (PHY) models which includes various radio propagations, however, it is too complex to capture the radio characteristics as it shows dynamic behavior in different environments like indoor, outdoor, urban, and rural. Moreover, most of the simulators do not take into account all the characteristics of specific hardware, and often lack fine grained modeling behavior. For example, clock drift is often not taken into account in simulations which significantly impacts behavior of a protocol [8].

Compared to simulation, emulation takes into account a fine grained model which is hardware specific. It offers more realism than simulation and provides greater reusability, which means the same implementation can be used not only on emulated nodes but also on real hardware [3]. Most of the development efforts in LLN utilize two frequently used emulators: Cooja and OpenWSN. These tools have been widely used to perform simulation experiments to test MAC protocols in different scenarios with different parameters. In the following text, we describe widely used simulation tools pertaining to LLNs.

1) OMNeT++

OMNeT++ [9] is not a simulator itself, rather it is an open source discrete event simulation library and framework, which is component-based and extensible. It is widely used for building simulators for modeling and evaluating queuing and distributed wired and wireless communication networks [9]. It is implemented in C++ and has a rich integrated development and graphical interface, which helps design, run, evaluate, and trace simulations. The structure of the OMNeT++ model is based on modules, that can be reused in different ways same as LEGO blocks which makes it more modular. It allows unlimited modules nesting, with which several simple modules can be combined to create compound modules. A simple module is written in C++ together with simulation class library provided by the OMNeT++. Communication between the modules takes places via message passing and these messages may contain arbitrary data structures. Depending on the model under consideration, these messages serve as jobs, events, packets, or commands. Modules have input and output interfaces called gates. A link between input and output gates is called connection. In this ways, connections can be assigned different parameters such as propagation delay, bit error rate, and data rate [9]. Similarly, modules can be assigned different parameters that help configure module behavior and customize model topology. An OMNeT++ model is described in NEtwork Description (NED) language, which is a Domain Specific Language (DSL) [7]. It provides extensive random number generating distributions and the ability to perform parallel simulations. OMNeT++ provides support for collecting, analysis, and visualization of simulation results contained in scalar and vector files. Python programming support is also underway for results processing and analysis, in this way several python-based packages can be used for easy result plotting and visualization.

OMNeT++ supports various ways to run simulations such as graphical and command line interfaces, the former is useful for demonstration and debugging whereas the latter is preferred for batch execution [9]. Based on OMeNT++, several independent simulations models and frameworks have been developed such as INET, INETMANET, Castalia, OverSim, and MiXiM. These frameworks and models are now commonly used to test different types of protocols and networks.

INET

INET [9] is a widely used simulation package as it contains several Internet protocols and other models to perform simulation particularly in communication and networking. In this

way, it helps evaluate and validate new protocols in different scenarios [10]. Often the latest frameworks and models take INET as a base and build on it to simulate more complex networks and protocols.

MiXiM

MiXiM [11] is a simulation package based on OMNeT++, which was primarily used for simulation of wireless and mobile networks. It is a merger of several frameworks such as ChSim, MAC simulator, Mobility framework, Positif framework. Several other projects have been integrated into MiXiM such as EnergyFramework, CSMA module, IEEE 802.15.4 and IEEE 802.15.4 modules, B-MAC layer, L-MAC layer, MoBAN - Mobility Model for Body Area Networks, Flooding network layer, WiseRoute network layer, ProbabilityBroadcast network layer modules, and Analogue Models: BreakpointPathlossModel and PERModel. Therefore, it features detailed wireless channel models, mobility models, obstacles models, and numerous protocols, particularly, it has a great support for MAC layer. MiXiM is now deprecated and all its contents have now been merged with INET since INET-3.x version [12].

INETMANET

INETMANET [13] framework offers similar features as the INET framework but extends INET by providing increased support for simulating Mobile Ad Hoc NETworks (MANETs). It was initially a fork of the INET. It supports several protocols such as AODV, OSLR, DSR, and others. INET's first version had limitations for link layer and routing protocols for simulation of MANETs. INETMANET overcame those limitations by including support of IEEE 802.11a/g/e and 802.15.4 (now they are also part of INET) [10]. In this way, it supports low-power IoT networks in more realistic scenarios. As MiXiM is no longer maintained, so several propagation models developed for MiXiM are now part of INETMANET. The initial version of INET did not have energy producer and consumer model. INETMANET uses MiXiM models and adapted them to facilitate energy consumption simulation of wireless networks. Several link layer models have been included in INETMANET which cannot be found in INET. Certain simulation models and implementation codes which were originally written for INETMANET, they have been included in INET as well. INETMANET is being actively maintained and developed with major difference to INET with respect to routing protocols, mobility models, application models, interference models. [10].

2) Cooja

Cooja is part of the Contiki-OS which is an operating system [14] that provides hardware and software support for LLNs platforms. Contiki-OS is open source and it enables low-power IoT devices to connect to the Internet. It offers fully standard network stacks such as Micro (u)IP with the support of standard protocols like IEEE 802.15.4, 6LoWPAN, TSCH, 6TiSCH, RPL and COAP. Contiki provides easy and fast development of applications which are written in C. After Contiki version 3.0, it is no longer maintained, rather a new Contiki-ng called next generation OS for IoT, has been developed which is a fork of Contiki-OS.

Cooja is a network simulator within Contiki-ng, that has capability to emulate real hardware platforms. It is extensively used to simulate small and relatively large wireless networks of low-power and low-cost embedded sensors and actuators called motes. It helps develop, validate, run, and debug protocols and applications. Researchers and developers build and test networks with Cooja emulated motes before actually running them on real hardware. Cooja is based on Java and has a graphical interface. It supports various widely used hardware platforms such as CC2420, CC2650, Zolertia Zoul, openmote, native Cooja motes, nrf52dk, NXP jn516x, Tmote Sky/TelosB, and several others. It includes various propagation models such as Unit Disk Graph Medium (UDGM), distance loss UDGM, Directed Graph Radio Medium (DGRM), multipath Ray-tracer Medium (MRM). It also has support for the integration of external tools and plug-ins to provide additional features for networks, protocols, and applications. Two such plug-ins are mobility plug-in and interference plug-in, which help emulate behavior close to reality. Cooja is currently the most dominant tool used by researchers and developers for simulation and emulation of LLN networks as can be seen in Figure 3 which is adopted from [15]. Figure 3 depicts that 62.9% simulation studies related to Contiki-rpl were conducted using Cooja. This is based on results of 97 research publications between 2010 to 2016 found in IEEE Xplorer, Google Scholar, ACM Digital Library, and IETF RFCs [15]. Cooja/Contiki is actively maintained and supported by the community, this is the reason that most of the latest IETF standard drafts are often available for them.

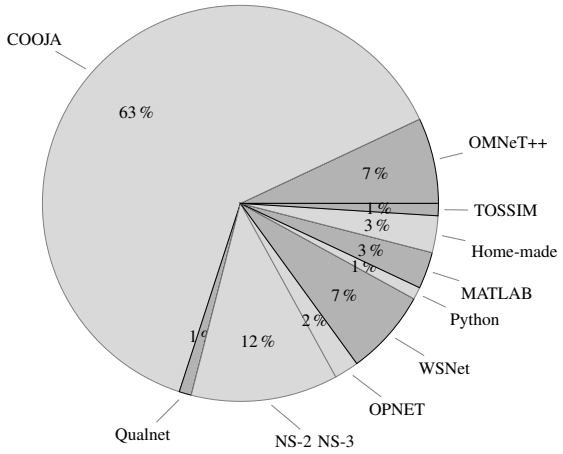


Figure 3. Usage of different simulators in RPL-based low-power and lossy network implementations.

Table I
COMPARISON OF DIFFERENT SIMULATION TOOLS BASED ON DIFFERENT FEATURES.

Simulator	Simulation type	Language	License	GUI
Cooja	Discrete event	C	Open Source	Yes
OMNeT++	Discrete event	C++	Open/Commercial	Yes
TOSSIM	Discrete event	nesC	Open source	No
NS-2	Discrete event	C++/OTcl	Open source	Limited
NS-3	Discrete event	C++	Open source	Yes
MATLAB	Event driven	C/Java	Commercial	Yes
Qualnet	Discrete event	C++/Parsec	Commercial	Yes
WSNet	Event driven	C++	Open source	Yes
OPNET	Discrete event	C/C++	Commercial	Yes

D. Comparison of Simulation Tools

Table I depicts comparison among aforementioned simulation tools based on different features.

III. METRICS

The performance evaluation of MAC protocol undertakes certain performance metrics or factors which define a criteria that should be measured to analyze their performance. Thus, determining performance metrics is inherent and imperative part of MAC protocol development, however, the choice of metrics depends on application. Below we detail, widely used

metrics that are used during the performance evaluation of MAC protocols. It should be noted that these metrics are commonly used in link-layer studies for LLNs.

A. Packet Delivery Ratio

In various communication networks and protocols, reliability is mostly tied with Packet Delivery Ratio (PDR). As link unreliability, packet collision, or packet loss due to interference and fading is common in low-power networks, thus accurate measure of packet delivery is mandatory. PDR is the ratio of sum of the packets received by the destination node to the total number of packets generated by a source node and is given as $PDR = \frac{\sum Pkt_{received}}{\sum Pkt_{generated}}$

Reliability can be as overall or end-to-end, end-to-end PDR undertakes the calculation of PDR at every receiver and transmitted by every source. PDR is a good measure of MAC performance and it gives a good picture of overall packet loss in the network which reflects reliability and robustness of a protocol.

B. Delay

Delay is a crucial metric that is used to assess network performance and application QoS. Packets in LLN are usually timestamped so that source and destination nodes can keep track of timing information and measure delay. Often an end-to-end delay or node-to-node delay is measured. Depending on application, it is imperative to guarantee an upper bound for the data transfer between source and target nodes.

MAC protocols fall into contention-based, schedule-based, and hybrid schemes. Contention-based protocol cannot guarantee deterministic delay, because each network node competes to gain access to the shared wireless medium without knowing the status of its neighbor transmission. Thus, transmissions may collide and nodes have to wait random amount of waiting period before making another transmission attempt and this causes more delay. On the other hand, schedule-based protocols can offer deterministic delay because each node is pre-assigned a dedicated time slot for the transmission of data. Often superframe or slotframe is constructed which defines at which time a particular nodes to has transmit, receive, or sleep. In this way, it fully avoids the collisions and provides guaranteed delay. Hybrid scheme takes advantages of both contention-based and schedules-based approaches and tries to offer improved performance.

C. Energy Consumption

Energy consumption is undoubtedly one of the main metrics for resource constrained sensor nodes as they are mostly battery powered and battery replacement is often infeasible. Various problems can cause energy waste such as collisions, interference, packet overhearing, hidden node problem, control packet overhead, and idle listening. Thus, the radio transceiver should be turned-on precisely when a node transmits and receives a packet else it should be tuned-off, however, it is non-trivial to achieve this in practical scenarios. To overcome unnecessary radio wake-up, , duty cycling (DC) is widely used to save energy in which nodes sleep by turning-off their radio related circuity if they do not have packets to transmit or receive. Duty cycling is defined as the ratio of total listen interval to total sleep and listen interval and is given as $DC = \frac{T_{listen}}{T_{listen}+T_{sleep}}$

In reality, different states of the radio transceiver consume different amount of energy. In this way, duty cycling serves an important metric to represent the energy consumption of nodes. Energy consumption and network life time are closely related and are often interchangeable.

D. Scalability

Scalability can be defined from two perspective, one is related to scaling up network by adding more number of nodes, and another is related to changing topology or functionality of the existing network. Due to wide adoption of low-power networks, we witness large scale networks to be deployed such as smart city or industrial applications. Often thousands of small nodes are deployed for monitoring and control purpose. Managing large number of nodes is non-trivial task, for example, in case of contention-based schemes, increasing the number of nodes causes the medium access competition to grow which increases the delay and energy consumption. Scalability becomes a challenge for schedule-based protocols as they are less scalable, for example, adding new nodes in network requires the entire schedule of nodes to be updated which incurs additional overhead for energy and delay. Therefore, scalability is an important metric that should be put on priority during the development of MAC protocol.

IV. Conclusion

This paper discussed about performance evaluation and how it should be conducted. Various methodologies used in performance evaluation have been surveyed. In particular, we focused on simulation approach to analyze MAC protocol performance. Several simulation platforms along with their working mechanism were explained with reference to LLNs. Several MAC performance metrics such as PDR, delay, scalability, and energy consumption were elaborated.

References

[1] A. Nikoukar, S. Raza, A. Poole, M. Güneş, and B. Dezfouli. Low-power wireless for the internet of things: Standards and applications. *IEEE Access*, 6:67893–67926, 2018.

[2] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander. Rpl: Ipv6 routing protocol for low-power and lossy networks. Internet Requests for Comments, March 2012. http://www.rfc-editor.org/rfc/rfc6550.txt.

[3] K. Kritsis, G. Z. Papadopoulos, A. Gallais, P. Chatzimisios, and F. Théoleyre. A tutorial on performance evaluation and validation methodology for low-power and lossy networks. *IEEE Communications Surveys Tutorials*, 20(3):1799–1825, thirdquarter 2018.

[4] P Thubert, T Watteyne, R Struik, and M Richardson. An architecture for ipv6 over the tsch mode of ieee 802.15. 4. draft-ietf-6tisch-architecture-10. *IETF Draft, March*, 2015.

[5] G. Gaillard, D. Barthel, F. Theoleyre, and F. Valois. Service level agreements for wireless sensor networks: A wsn operator's point of view. In *IEEE Network Operations and Management Symposium (NOMS)*, pages 1–8, Krakow, Poland, May 2014.

[6] Stênio Fernandes. *Performance Evaluation for Network Services, Systems and Protocols*. Springer, 2017.

[7] K. Wehrle, M. Günes, and J. Gross. *Modeling and tools for network simulation*. Springer Science & Business Media, 2010.

[8] T. van der Lee, S. Raza, G. Exarchakos, and M. Günes. Towards co-located TSCH networks: An inter-network interference perspective. In *IEEE Global Communications Conference: Ad Hoc and Sensor Networks (Globecom AHSN)*, Abu Dhabi, United Arab Emirates, December 2018.

[9] OMNeT++ Discrete Event Simulator. https://omnetpp.org/doc/omnetpp/manual/. Version 5.2, Last visited: 30.03.2018.

[10] Antonio Virdis and Michael Kirsche. Recent advances in network simulation.

[11] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. T. Klein Haneveld, T. E. V. Parker, O. W. Visser, H. S. Lichte, and S. Valentin. Simulating wireless and mobile networks in omnet++ the mixim vision. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, pages 1–8, ICST, Brussels, Belgium, 2008.

[12] omnetpp-models/mixim. https://github.com/omnetpp-models/mixim. Last visited: 05.06.2019.

[13] INETMANET Framework. https://github.com/aarizaq/inetmanet-3.x. Last visited: 20.02.2018.

[14] A. Dunkels, B. Gronvall, and T. Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *29th Annual IEEE International Conference on Local Computer Networks*, pages 455–462, Nov 2004.

[15] H. Kim, J. Ko, D. E. Culler, and J. Paek. Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. *IEEE Communications Surveys Tutorials*, 19(4):2502–2525, Fourthquarter 2017.

Demo: Inline process analysis with wireless powered sensors

A. Hoppe, S. Wöckel, ifak – Institut für Automation und Kommunikation e.V., Magdeburg,
U. Steinmann - University Magdeburg, Chair Measurement Technology, Magdeburg

***Abstract*—The contribution introduces a compact system that demonstrates all necessary components of a modern sensor network (on small scale) and supports the simple understanding for the whole data chain. It includes two sealed sensor-actuator-heads an inductive (plug-free) power supply, a wireless communication module and a handheld processing unit with corresponding software.**

***Index Terms*—sensor network, process monitoring, wireless probes**

I. Introduction

The chemical and biological industry aims for an ongoing progress in optimizing manufacturing processes in complex fluid or liquid systems. The control of such processes requires the monitoring of different physical parameters like density, concentration or temperature gradients and thus the implementation of different sensor probes. In case of large reaction vessels, the main disadvantage occurs by the fixed implementation of the sensor probes, that only measure in a restricted region or spot within the vessel. The spatial distribution of a density or the temperature is not known exactly – mostly derived by a simulation model only. Thus, the process industry is in need of flexible (non-fixed) sensor-probes, that can be installed very quickly (without interrupting the process) and that are able to gather parameters all over the volume – all in conjunction with online measurements, long-term operation and wireless power supply. In this context the mayor aims of the research activities at the ifak where tomographic systems [1], combination of sensor principle and wireless probes for inline process analysis [2]. Such system is suitable to monitor different process values within larger vessels or even with non-invasive data and power support. The concepts for a compact and mobile sensor system used in liquid multiphase systems were developed. In order to achieve near real-time knowledge of an underlying process, the temporal and spatial analysis of (multi-phase) liquids is intended. Of main importance are firstly the utilisation and integration of different robust and process-suited measurement methods into a multisensor-module which can be placed directly in the process medium. Secondly, concepts for the contactless transfer of power and measurement data [3] were developed and realized in order to achieve an uninterruptible and long-term operation of the mobile sensor module within the process. Contactless inductive transmission systems offer the advantage of dispensing with electrical sliding contacts or plug connections and thus increase the safety and reliability of the power supply in many areas of application, such as underwater applications or under harsh environmental conditions. Typical coil systems are shown in Figure 1.

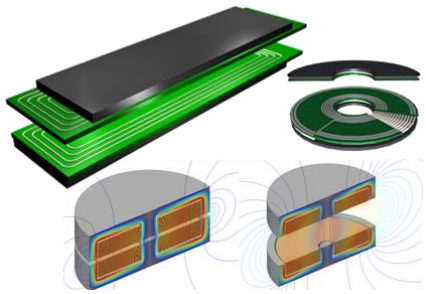


Fig. 1. Coil systems for contactless power and data transmission with galvanic isolation

II. Demonstrator

The WASABI demonstrator (Fig. 2) is suitable for demonstrating the advantages of digitizing process values and transferring them via networks to the use of information. The demonstrator shows the whole chain of a sensor network in a clear way.

Fig. 2. WASABI - Wireless underwAter Sensor Actor with Bidirectional data transfer and "plug-free" power transmission consisting of: water tank, two sensor-actor modules (switchable), inductive power supply and processing unit (tablet)

Using a sensor arrangement with integrated communication devices, the demonstrator will demonstrate the path from digital data from the application (data acquisition from sensors, actuators and controllers (PLCs) as well as other sources) to the processing and evaluation of the digitization/integration of process information into the information chain of the company.

The demonstrator consists of a water tank (the process vessel) with two sensor or actuator heads (distributed sensors) and a tablet as a visualization and control system (Fig. 2).

A. Functionalities:

- The sensors and actuators integrated in the WASABI demonstrator are supplied with wireless inductive energy.
- Besides a thermal an optical sensor is implemented and thus can be used to detect particles and concentrations under water. With the help of solutions from the field of softsensing (fusion of sensor data in the time and frequency domain), powerful solutions for physical, chemical or biological sensors can be developed further.
- "Plug-free" real time process monitoring: The sensor modules can be removed or even replaced during operation without interrupting the network. The sensors are detected automatically.
- The acquired data are transferred from the sensor head to the base station via contactless inductive communication (near field) and processed.
- Using a Bluetooth connection, the processed data can be transmitted to the tablet and visualized (Fig. 3). In addition, various control commands can be sent to the sensor heads via these communication links.

Fig. 3. Software for sensor control and data processing: the values of a LED-transfer

B. Addressed Applications:

In context of the variety of process parameters in chemical and biotechnological industry, the following underlying applications are addressed:

- Monitoring of concentration, density and sound velocity in liquids.
- Particle analysis (concerning size distribution and concentration) with photometric and acoustic sensors,
- Monitoring of streaming with distributed sensor-particles [2].
- Detection of thermal gradient and hotspots in large vessels.
- "Plug-free" power transfer and communication modules between an "autarkic" sensor system inside a vessel and a processing unit outside.

III. Conclusion

The demonstrator (Fig. 4) shows all aspects and necessary modules of wireless sensor networks in a simple way and illustrates the advantages and challenges of such a sensor network.

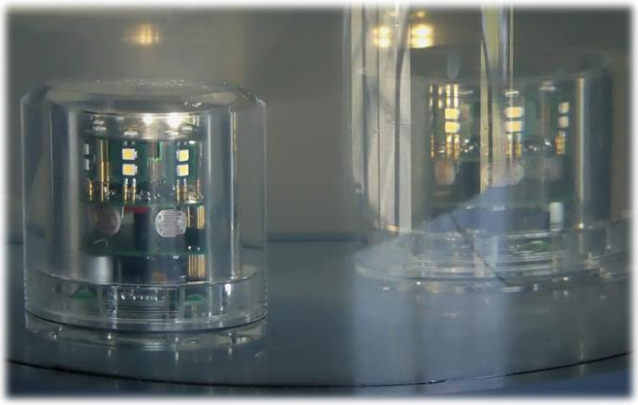


Fig. 4. Water proofed sensor-head including optical receiver and emitter, sensor electronic, communication module and inductive power converter for plug-free supply.

References

[1] TOPAS - Tomographische Prozesskontrolle von Mehrphasengemischen, BMWi, Vorlaufforschung, VF 071016, 09/07 - 08/10

[2] DIP - Drahtlos versorgter Multisensor zur Inline-Prozessanalyse, BMWi, Programm Vorlaufforschung, Förderkennzeichen: VF 100014, 2011-2014

[3] Hoppe, A.: Neue Einsatzmöglichkeiten und Entwicklungstendenzen in der kontaktlosen Energie- und Datenübertragung. 9. Fachveranstaltung Kontaktlose Energieübertragung Stand der Technik, 30.06. - 01.07.2014, Stuttgart, Universität Stuttgart, 2014

Demo: A Haptic Communication Testbed - Integrating The Control Systems Domain Into Communication Testbeds

Frank Engelhardt, Johannes Behrens, Mesut Güneş
Communication and Networked Systems (ComSys)
Faculty of Computer Science
Otto-von-Guericke University Magdeburg
Universitätsplatz 2, 39106 Magdeburg, Germany
{fengelha,johannes.behrens,guenes}@ovgu.de

***Abstract*—For wireless research of Haptic Communication an integrated testbed that covers both the networking and the control part is needed. With this demo, we show a Haptic Communication framework that is intended for experiment design that covers Networked Control System (NCS) in action, allowing for repeatable as well as empirical data collection. We demonstrate our Haptic Communication Testbed within in a small demo setup that shows a remotely controlled line following robot.**

***Index Terms*—Haptic Communication, Tactile Internet, Testbeds**

I. Introduction

Finding a solution for efficient Haptic Communication is an integral part of the Tactile Internet [1]. One of the key requirements to develop sound, applicable codecs for Haptic Communication is a testbed that will allow for large-scale evaluation, validation, and refinement of approaches and concepts. Testbeds mainly solve the problem of reproducibility of real-world measurements. By giving a structured and automatized approach to experiment design, execution and data gathering, they bridge the gap between reproducible simulations and empirical case studies. Haptic Coding imposes a special challenge to testbed design, as it lies in between two big scientific domains: The control domain, which is determined all by physical, real-world quantities, and the digital network-domain, which measures pure abstract information.

When combined setups have to be investigated, there is currently a lack of concepts and functionality. The standard way to overcome this problem is to translate a given control application's constraints into network constraints and then simulate the application's data flow within a communication testbed. For example, if a network-controlled robot has to work within certain metric tolerances, one might calculate the minimum packet rate, maximum omission degree, and maximum latency necessary. This approach, however, introduces many abstractions and is only applicable to evaluate small systems of low complexity. We therefore aim to develop a testbed for Haptic Communication, which offers a user specifiable network configuration combined with a configurable, state of the art robotics simulation. This approach enables an integrated evaluation of NCS in both the control as well as the network domain. The conceptual approach for a Haptic Communication Testbed will finally be integrated into our MIoT-Lab [2] and will therefore allow for distributed deployment, scheduled large-scale experimentation, and automated data collection.

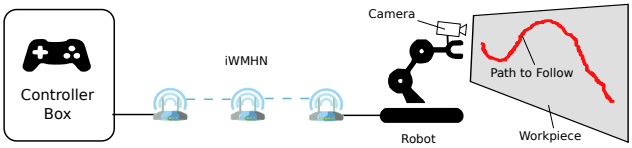


Figure 1: Application scenario: A line following robot as part of a NCS. The robot is controlled remotely utilizing industrial Wireless Multi-Hop Network (WMHN) infrastructure.

We present our approach using the demo scenario depicted in Figure 1. A robot that is controlled via a NCS has to fulfill a certain goal, which is in our case a simple line-following task. The system has to implement an efficient Haptic Coding technique that is able to maintain the data rate, packet loss, and latency constraints needed by the application. These network constraints arise completely from the physical domain, given the speed that the robot should follow the line and the maximum tolerable deviation. The intended framework, however, is generic and flexible and will support arbitrary scenarios.

There currently exist several testbeds for the network domain, like the MIoT-Lab [2] and the FIT IoT-Lab [3]. For the control domain, some specialized testbeds have been used over time that depend on the exact application, like for grasp planning in robotics [4] or Haptic Coding [5].

The rest of this paper is structured as follows. Section II briefly introduces our novel Haptic Communication testbed design. Section III describes the demonstration scenario. Section IV concludes the paper.

II. Haptic Communication Testbed

The testbed basically consists of two parts. On the one hand this is the framework that connects the robot simulation with a network and allows remote control of it. Another component is the MIoT-Lab, which takes over the network

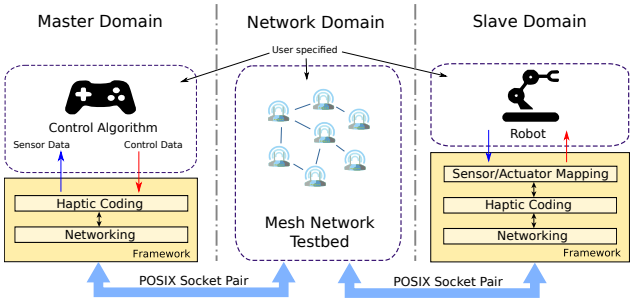


Figure 2: The scenario application as part of the MIoT-Lab [2] Haptic Testbed concept. Control algorithms, robots and the network configuration are freely specifyable, while the Framework ensures that application modules are interchangeable and re-usable.

role and the Testbed Management System (TBMS) [6] for the experiments. The setup and interplay of these parts is depicted in Figure 2. The TBMS controls the experiments and allows the experiments to be stored in DES-Cript [7] format and repeated on other testbeds that support this format. The DES-Cript file stores important information about the experiments, which includes, among other things, commands executed on the individual nodes as well as general configurations such as execution times, metadata and an initialization of the nodes. Thus the user does not have to worry about the control of the experiments and the experiments become repeatable and comparable under the same conditions. The framework in turn consists of a plugin for the simulation environment v-rep [8] and a stand-alone application that runs on a remote computer and controls the simulation. The plugin is a shared library and is loaded at the start of v-rep and allows access to the so-called regular API with over 500 functions. A plugin for v-rep must implement at least three procedures as entry points. One is called at the start, one at the end and a third at other events, like at every simulation step. Plugins, in general, do not allow asynchronous execution, but a fixed frequency is required for sending the sensor data, so we use threads for synchronization of both feedback and control streams. Threading is only possible when initiated from the main thread as a result of an event. Therefore, the plugin is structured so that it starts two threads at the beginning for communication with the controller. One thread is responsible for sending data and another thread is responsible for receiving data. They communicate with the main thread via mutex-protected data structures. The main thread converts the received control data via API calls in the simulation and updates the sensor data to be sent. The data is sent at a specified frequency, for example 1 kHz. A standalone software runs on the control side. It receives the sensor data, executes the algorithm and then sends the calculated control data to the plugin.

III. Scenario

In the demo scene depicted in Figure 1 a stationary robot follows a path using a camera attached to the robot arm. In the real world, this could be a robot inspecting a weld seam. The scene was chosen because it is a real world problem and it is easy to determine the quality of the control. It is possible to add the sum of the deviation in the vertical

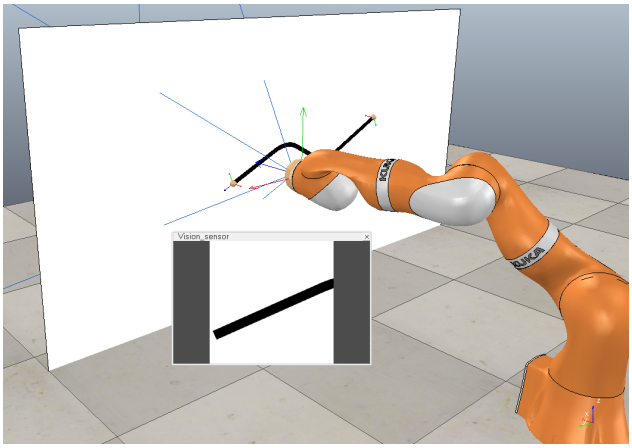


Figure 3: Screenshot shows the robot following the path. The camera image can be seen in the additional window.

direction from the path over each simulation step. In order to keep the control algorithm as simple as possible and still allow an endless simulation, the robot always moves back and forth in the horizontal direction. This position change is performed locally. The algorithm only has to make a correction in the vertical direction. It looks at the middle column of the image and determines the position of the path. The vertical correction of the position is proportional to the deviation from the center.

IV. Discussion

Testbeds, in general, bridge the gap between pure simulations and case-studies as a means of evaluation, testing, validation, or verification. The Haptic Communication Testbed is intended as an aid to improve the mapping between (non-functional) network constraints and physical application parameters in scenarios where Haptic Communication is involved. We aim to support the gain of insights in the slowly emerging field of Haptic Communication.

References

[1] A. Aijaz and M. Sooriyabandara. The Tactile Internet for Industries: A Review. *Proceedings of the IEEE*, 107(2):414–435, 2019.

[2] MIoT-Lab. http://comsys.ovgu.de/MIOT_Lab.

[3] FIT IoT-Lab. https://www.iot-lab.info/.

[4] S. Levine, P. Pastor, A. Krizhevsky, J. Ibarz, and D. Quillen. Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection. *The International Journal of Robotics Research*, 37(4-5):421–436, 2018.

[5] E. Steinbach, M. Strese, M. Eid, X. Liu, A. Bhardwaj, Q. Liu, M. Al-Ja'afreh, T. Mahmoodi, R. Hassen, A. El Saddik, and O. Holland. Haptic codecs for the tactile internet. *Proceedings of the IEEE*, 107(2):447–470, Feb 2019.

[6] M. Günes, B. Blywis, F. Juraschek, and O. Watteroth. Experimentation Made Easy. In ICST, editor, *Proceedings of the First International Conference on Ad Hoc Networks*, volume 28 of *28*, pages 493–505, Ontario, Canada, September 2009. Springer Berlin Heidelberg.

[7] M. Günes, F. Juraschek, B. Blywis, and O. Watteroth. DES-CRIPT - A Domain Specific Language for Network Experiment Descriptions. In *Inproceedings of the International Conference on Next Generation Wireless Systems (NGWS) 2009*, Melbourne, Australia, 12-14, October 2009.

[8] v-rep virtual robot experimentation platform. http://www.coppeliarobotics.com/.

Demo: Wireless sensor network for retrofitting production systems

1st Gordon Lemme
Cyber-physical production systems
Fraunhofer IWU
Dresden, Deutschland
gordon.lemme@iwu.fraunhofer.de

2nd Kilian Armin Nölscher
Cyber-physical production systems
Fraunhofer IWU
Dresden, Deutschland
kilian.noelscher@iwu.fraunhofer.de

***Abstract*—This paper describes the prototypical implementation for demonstration purposes of a wireless sensor network for recording production parameters like temperature and acceleration for machine monitoring on machine tools. The data collection is done with devices and components from the low-budget area, like a single board computer (SBC) and Adafruit Breakout Boards, as well as directly from the machine control via the communication protocol Open Platform Communications Unified Architecture (OPC UA). The message queuing telemetry transport (MQTT) broker is used for the transfer of the data packets. The collected data is collected by means of a time-series-based database (InfluxDB) and visualized via a Grafana server.**

***Index Terms*—IIoT, MQTT, OPC UA, Sensors, Retrofit**

I. Introduction

In the context of the Industry 4.0 Initiative and the associated technologies such as condition monitoring, predictive maintenance, context adaptive machine control and the change to flexible production systems, keyword ”lot size 1”, the collection of high quality data in the style of ”Smart Data” plays an important role. The necessary data fusion from different sources (e.g. machine data, room climate data) helps to generate a holistic, context-related system image with the goal of increased system availability. Rather, it is the integration of existing building sensors, function-integrated tool parameters and additional sensors remote from the machine. The necessity for a machine retrofit lies in the high acquisition costs for machine tools and the long lifecycle of machine tools, particularly special machines. Not only the quantity of the data is decisive, but also its quality, which has a considerable effect on the results to be achieved with regard to downstream data processing. In order to be able to offer a retrofit option for existing plants, a wireless sensor network has to be developed. With the help of such an additionally installed sensor network, existing machines can be qualified for current and future applications without generating high investment costs. This system can also be used as an additional system in combination with current machine tools to redundantly design sensors or to act independently of the machine control.

The designed architecture (Fig. 1) consists of sensors, sensor nodes, a message queuing telemetry transport (MQTT) broker and possible clients. The nodes themselves contain temperature and acceleration sensors, as well as an interface in the form of a RJ45 socket for connecting additional sensors via cable. All sensors are connected to the MQTT broker via the respective nodes and handle the communication. Connected clients can either write the output data or transfer parameters for measurements. The conditions set for the development of components for a prototype of such a network are simplicity and robustness as well as easy replaceability.

II. Demo Setup

The central instance of the sensor network is the MQTT broker in the form of a single board computer (SBC). This can be used for communication with instructions to the sensor nodes and from these to publish the sensor data. A clever separation of the parameters from each other is useful in order to clearly assign the values to their origin. The MQTT broker is wirelessly connected to the sensor network via 2.4 GHz. The basic framework for the sensor nodes is the MCU ESP32 from espressif in the form of the DevKitc V4 [1] with micropython. This low-power system-on-a-chip (SoC) with 4 MB memory, Wifi and Bluetooth module and a clock frequency of 240 MHz is an inexpensive component from the IoT range. The acquisition of temperature values takes place via OneWire Bus using the DS18B20 sensors from Maxim Integrated [2] and the acquisition of acceleration values takes place via I^2C Bus using the LIS3DH sensors from ST Microelectronics [3] as a breakout from Adafruit Industries. A lithium-ion accumulator serves as power supply. The sensor node can be operated either as an automatic system with standard values or with a desired configuration, which is transferred to the ESP32 via MQTT. The collected data packets are sent to the MQTT broker via 2.4 GHz Wifi.

So-called secondary drives are responsible for the realization of the necessary effective movement between tool and workpiece on machine tools. Spindle nut systems are widely used to convert rotary motion into translational motion. For this reason, a drive unit in the form of a ball screw with associated machine control is embedded in the demonstrator as a machine component (Fig. 2).

A Bosch - Rexroth Indra Control XM22 is used as control unit and a Bosch - Rexroth Indra Drive Cs as converter. The data acquisition with a sampling rate of up to 1000 Hz

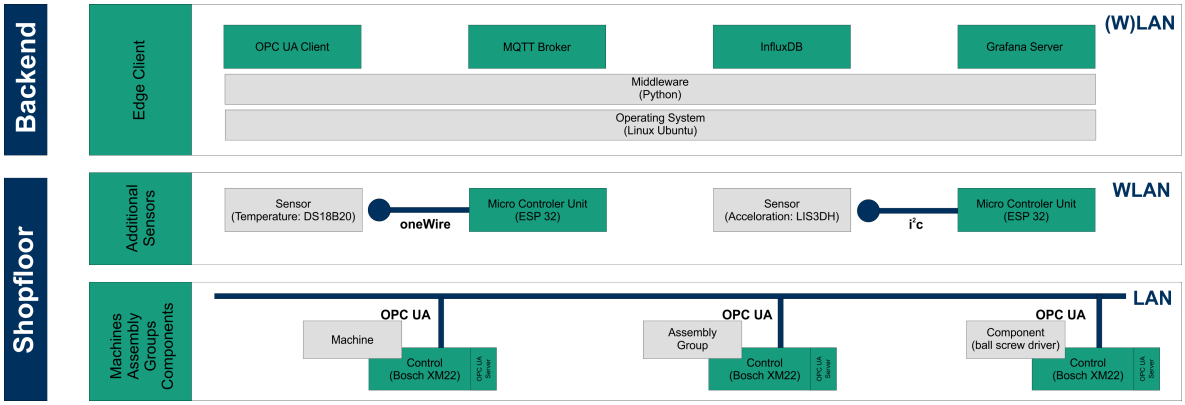


Fig. 1. Schematic representation of the system architecture

Fig. 2. Ball screw drive with Rexroth control as machine component

of the parameters acceleration, speed and position from the controller is done by a singe board computer and takes place via the Open Platform Communications Unified Architecture (OPC UA) interface with a corresponding Python script, which immediately publishes the data stream via 2.4 GHz Wifi to the MQTT broker.

The last part of the demonstrator is the time series based database InfluxDB and a visualization using Grafana. These two features run also on the single board computer with Intel Pentium CPU, 4 GB RAM and an active cooling due to higher demands on the computing power. The representation takes place via an Internet browser by calling the respective IP.

III. Results

The practical test shows that the designed system can cope with the demands placed on it. Process parameters can be collected from various sources and merged. In addition, a visualization in quasi real time was achieved. The system can therefore be used in industrial environments and is particularly suitable for retrofit measures, in order to generate Smart Data through data acquisition and to make existing plants industry 4.0 ready. The acceleration sensors of the sensor nodes are limited by the ESP32 in the presented test setup to approximatly 100 Hz, this is sufficient in the industrial environment for condition monitoring or predictive maintenance with respect to the application.

IV. Outlook

With this approach, further technical solutions can be developed through the consistent implementation of the system of systems concept. These individual technical solutions can result in a service ecosystem for machine tools. This enables the successive development of new services that facilitate the handling of increasingly complex machine tools. Software developments (e.g. apps) for the detailed evaluation of production processes or determination of the state of health / wear of the machine tool are conceivable here. In addition, services directly on the machine (e.g. maintenance, calibration tasks) can be better planned on the basis of existing context information, which can shorten machine downtimes and increase capacity utilization. New business models (pay-per-use, pay-on-demand) can be implemented on the basis of this now possible comprehensive data situation, enabling various service providers to offer their services on a customer-specific basis.

References

[1] https://docs.espressif.com/projects/esp-idf/en/latest/hw-reference/get-started-devkitc.html
[2] https://datasheets.maximintegrated.com/en/ds/DS18B20.pdf
[3] https://www.st.com/resource/en/datasheet/lis3dh.pdf

Demo: Interoperability of the RIOT CoAP Implementation

M. Aiman Ismail, Thomas C. Schmidt
Internet Technologies Group, Dept. Informatik, HAW Hamburg, Germany
{muhammadaimanbin.ismail, t.schmidt}@haw-hamburg.de

I. Introduction

There can be many different implementations of internet protocols. That means each implementation will come with its own ways of doing things. This can sometimes lead to failure when used against different implementation. Therefore. to make sure that they all can interoperate, plug-testing needs to be done regularly between all these implementations. This demo aims to show the interoperability of the RIOT CoAP implementation - gcoap - against other available CoAP implementations.

The Contrained Application Protocol (CoAP) [1] is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. By default, the packets are transported in plain UDP but in the specification it is described how the packet can be encrypted using DTLS [2].

The Datagram Transport Layer Security (DTLS) protocol provides communication privacy for datagram protocols. It is based on the Transport Layer Security (TLS) [3] protocol and provides equivalent security guarantees.

This demo shows the interoperability of the DTLS-secured CoAP implementation of *gcoap*[1] — the RIOT CoAP implementation, with other CoAP implementations.

II. DTLS-Secured CoAP

Section 9.1 of the CoAP RFC defines the binding to DTLS, along with the minimal mandatory-to-implement configurations appropriate for constrained environments. The binding is defined by a series of deltas to unicast CoAP. In practice, DTLS is TLS with added features to deal with the unreliable nature of the UDP transport.

III. Setup

There are many CoAP implementations to choose from. In this demo, gcoap is tested against the following CoAP libraries and the corresponding DTLS library used:

- libcoap + tinydtls (client and server)
- californium + scandium (client and server)
- aiocoap + tinydtls (client only)

On the RIOT side, gcoap example application is flashed onto a samr21-xpro board. As shown in Figure 1, DTLS integration in gcoap is done through DTLS sock [2]. This allows us to change the underlying DTLS library used without rewriting our application.

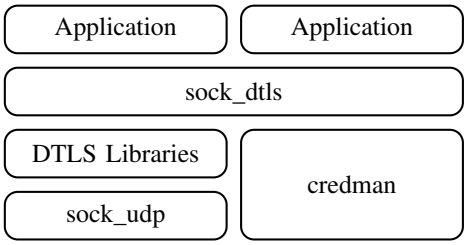


Fig. 1. Architecture of DTLS sock

Selected CoAP implementations are run on a raspberry pi equipped with a 802.15.4 radio. Currently, link-local IPv6 is not supported on aiocoap, so we will also need a global IPv6 address for the nodes in the demonstration. For that, we will use radvd to make the raspberry pi act as a router distributing global IPv6 address to other nodes.

For the test itself, the RIOT node will try to act as the CoAP client and send a packet to the server on the raspberry pi. As gcoap also supports CoAP server operations, the example client application of the selected CoAP implementations will be used to send a packet to the RIOT node.

IV. Conclusion

Through this demo, we hope to show the current state of the RIOT CoAP implementation and its ease of use. Through DTLS sock, changing of the underlying CoAP implementation can be done with minimal line of code, which is very useful when doing testing and prototyping.

References

[1] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, RFC 7252, June 2014.
[2] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," IETF, RFC 6347, January 2012.
[3] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF, RFC 8446, August 2018.

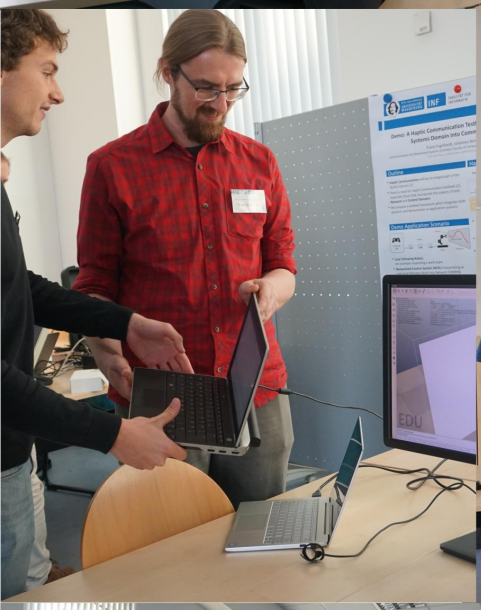
[1] https://riot-os.org/api/group__net__gcoap.html
[2] http://api.riot-os.org/group__net__sock__dtls.html

FGSN 2019 List of Authors

- Jan Schlichter, Institute of Operating Systems and Computer Networks, TU Braunschweig
- Björn Gernert, Institute of Operating Systems and Computer Networks, TU Braunschweig
- Lars C. Wolf, Institute of Operating Systems and Computer Networks, TU Braunschweig
- Ulf Kulau, DSI Aerospace Technology
- Nico Jähne-Raden, Peter L. Reichertz Institut für Medizinische Informatik
- Thiemo Clausen, Institute of Operating Systems and Computer Networks, TU Braunschweig
- Tobias Jura, TU Braunchweig
- Fabian Steinmetz, Hamburg University of Technology
- Christian Renner, Hamburg University of Technology
- Gordon Lemme, Fraunhofer-Institut für Werkzeugmaschinen und Umformtechnik IWU
- Kilian A. Nölscher, Fraunhofer-Institut für Werkzeugmaschinen und Umformtechnik IWU
- Peter Oppermann, Hamburg University of Technology
- Lennart Dorendorf, Hamburg University of Technology
- Benjamin Boll, Hamburg University of Technology
- Abedin Gagani, Hamburg University of Technology
- Nikolay Lalkovski, Hamburg University of Technology
- Marcus Rutner, Hamburg University of Technology
- Robert Meißner, Hamburg University of Technology
- Bodo Fiedler, Hamburg University of Technology
- M. Aiman Ismail, HAW Hamburg
- Thomas Schmidt, HAW Hamburg
- Daniel Șerbu, TU Clausthal
- Andreas Reinhardt, TU Clausthal
- Frank Engelhardt, Otto-von-Guericke University, Magdeburg
- Sara Stadler, University of Bremen, TZI
- Stefanie Gerdes, University of Bremen, TZI
- Olaf Bergmann, University of Bremen, TZI
- Kai Kientopf, Otto-von-Guericke University, Magdeburg
- Marian Buschsieweke, Otto-von-Guericke University, Magdeburg
- Mesut Günes, Otto-von-Guericke University, Magdeburg
- Michael Frey, Safety IO
- Cenk Gündogan, HAW Hamburg
- Peter Kietzmann, HAW Hamburg
- Martine Lenders, Freie Universität Berlin
- Hauke Petersen, Freie Universität Berlin
- Felix Shzu-Juraschek, Safety IO
- Matthias Wählisch, Freie Universität Berlin
- Ulrike Steinmann, Otto-von-Guericke University, Magdeburg
- Axel Hoppe, ifak – Institut für Automation und Kommunikation e.V., Magdeburg
- Jörg Auge, Magdeburg-Stendal University of Applied Sciences
- Saleem Raza, Otto-von-Guericke University, Magdeburg
- Ali Nikoukar, Otto-von-Guericke University, Magdeburg
- Sebastian Woeckel, ifak – Institut für Automation und Kommunikation e.V., Magdeburg
- Johannes Behrens, Otto-von-Guericke University, Magdeburg





Für was lässt sich Ballistokardiographie (BCG) verwenden?
Die „Pulse Transit Time" kann zur Bestimmung des Blutdrucks verwendet werden


18. GI/ITG KuVS Fachgespräch Sensornetze
19. - 20. September 2019, Otto-von-Guericke Universität Magdeburg
Welcome to Magdeburg