PROJECT PRESENTATIONS
WASP Winter Conference 2020

Title of project	Participants
Active Learning on video data for DNNs *	Abdelrahman Eldesokey
	Gustav Häger
	Joakim Johnander
Autonomous Calibration of 3D Computer Vision System	Mina Ferizbegovic
	Martin Larsson
	Olivier Moliner
	Lissy Pellaco
	Gustaf Waldemarson
	Xuechun Xu
Detection of colon cancer metastases in lymph nodes through deep learning	Martin Lindvall
	Karin Stacke
	Apostolia Tsirikoglou
Enabling Design And Execution of Large Scale Experiments on Maven Central	Nicolas Harrand
	Joel Scheuner
	Cesar Soto Valéro
Federated Kubernetes Sandbox *	Haorui Peng
	Johan Ruuskanen
	Alfred Åkesson
On the Suitability of Using SGX for Secure Key Storage in the Cloud	Joakim Brorsson
	Pegah Nikbakht Bideh
	Alexander Nilsson
Privacy Preserving Image De-identification	Md Sakib Nizam Khan
	Minh Ha Le
	Georgia Tsaloli
Time series generation for automotive software-in-the-loop testing	Karl Bäckström
	Sólrún Halla Einarsdóttir
	Jens Henriksson
	Dhasarathy Parthasarathy

*] Abstract not available in this catalogue

WASP | WALLENBERG AI,
AUTONOMOUS SYSTEMS
AND SOFTWARE PROGRAM

PROJECT PRESENTATIONS
WASP Winter Conference 2020

Session 2: Tuesday 14 January 16.00-17.00

Title of project	Participants
Detecting Anomalies in SS7 Network Traffic:Towards a Holistic Approach	Christopher Blöcker Timotheus Kampik
Human road users' (HRU) behavior learning and prediction based on mobile networks	Lucas Brynte Sarit Khirirat Joris van Rooij
Multimodal User Interfaces for Decision Support	Nikita Korzhitskii Johan Källström Martin Pallin Fredrik Präntare
Secure Federated Learning in 5G Mobile Networks *	Martin Isaksson Karl Norrman
Shared automation between a traffic tower operator and an automated vehicle	Goncalo Pedro Collares Pereira Mohammad Ali Nazari Amber Zelvelder
Simulation on WARA-PS Demo Arena and Evaluation of Quadracopter Trajectory Planners	Johan Karlsson Christian Rosdahl John Törnblom Peter Varnai
Static Program Analysis for the GObject Type System	Noric Couderc Alexandru Dura Claudio Mandrioli
Tuning filter parameters in an Unscented Kalman Filter Mine Edition	Kristin Nielsen Héctor Rodríguez Déniz

*) Abstract not available in this catalogue

WASP | WALLENBERG AI,
AUTONOMOUS SYSTEMS
AND SOFTWARE PROGRAM

Autonomous Calibration of 3D Computer Vision System

Project members:
Håkan Carlsson
Mina Ferizbegovic
Martin Larsson
Olivier Moliner
Lissy Pellaco
Gustaf Waldemarson
Xuechun Xu

Academic supervisor:
Kalle Åström

Industrial supervisor:
Mikael Lindberg

Abstract:
This project investigates various methods for autonomous calibration of computer vision systems, such as using traditional feature matching techniques, applying motion models to the features and incorporating measurements from IMUs. Current methods for calibration include several manual steps and removing them could make vision systems easier to deploy in the industry.

Detecting Anomalies in SS7 Network Traffic: Towards a Holistic Approach

Project Team:
Tobias Sundqvist, Christopher Blöcker, Timotheus Kampik

Academic Supervisor:
Monowar H. Bhuyan

Industry Supervisor:
Peter Olofsson

Participating Organizations:
Umeå University, Tieto

Abstract:
We implement different traffic data generation approaches for SS7 anomaly detection: a multi-agentgrid world-based approach, and a graph-based approach. Then, we use the data generated by these approaches to evaluate two anomaly detection methods: a Bayesian filter-based algorithm and a community detection-based algorithm. The two methods complement each other: the community detection algorithm identifies suspicious zones, to which the Bayesian filter can then be applied to single out specific devices. In addition, we propose a holistic human-in-the-loop architecture for integrating the proposed methods into realworld environments.

Detection of colon cancer metastases in lymph nodes through deep learning

Project members:
Martin Lindvall, Karin Stacke, Apostolia Tsirikoglou

Supervisors:
Gabriel Eilertsen (academic), Claes Lundström (industry)

Abstract:
This course project aims to support detection of tumor cells in lymph nodes of colon cancer patients, touching upon all stages of a running application pipeline, from designing a baseline model architecture, exploring transfer learning and synthetic data generation as augmentation strategies when limited data are available, to a final user interface product prototype.

Enabling Design and Execution of Large Scale Experiments on Maven Central

Participants:
César Soto Valero (KTH), He Ye (KTH), Joel Scheuner, (Chalmers) Long Zhang (KTH) and Nicolas Harrand (KTH)

Industrial supervisor:
Torsten Ek, Combient

Academic supervisor:
Benoit Baudry, KTH

Abstract:
In order to develop the software transformations involved in automatic software engineering, large datasets of software artifact containing at the same time artifacts, their sources, as well as build instructions and test are extremely valuable. This work provides data and tooling enabling large scale experiment on 4.2M of Maven Central artifacts.

Human road users' (HRU) behavior learning and prediction based on mobile networks

Project members:

Lucas Brynte, Joris van Rooij, Sarit Khirirat

Supervisors:

Paolo Falcone, Henrik Sahlin

Abstract:

5G will make high precision location data available for all 5G devices. We propose a CNN-based model to use this data for short-term trajectory prediction of Human Road Users in different traffic scenarios. Our model is evaluated on the Stanford Drone Dataset and shows promising results.

Multimodal User Interfaces for Decision Support

Authors:
Veronika Domova (ABB/LiU), Erik Gärtner (LU), Nikita Korzhitskii (LiU), Johan
Källström (Saab/LiU), Martin Pallin (Saab/KTH), Fredrik Präntare (LiU)

Industrial supervisor:
Jesper Tordenlid and Pontus Nilsson (Combitech)

Academic supervisor:
Patric Ljung (LiU)

Examinator:
Daniel Axehill (LiU)

Project Description:
We investigate three improvements to the user interface of the WARA-PS simulator in the
form of AI-assisted decision support, 3d visualization and improved UX design. To obtain
domain knowledge and evaluate our improvements we interviewed search and rescue
professionals.

On the Suitability of Using SGX for Secure Key Storage in the Cloud

Members:

Joakim Brorsson, Pegah Nikbakht Bideh, Alexander Nilsson

Academic supervisor:

Martin Hell, Lund University, Sweden

Industrial supervisor:

Senadin Alisic, Combitech, Sweden

Short summary:

This project evaluates the security of Intel SGX as an alternative to HSMs for securing sensitive data in the cloud. Our analysis proceeds from the FIPS 140-3 standard which is commonly used to assess the security properties of HSMs. Since FIPS 140-3 does not allow for considering threats from different actors present in a cloud environment separately, we develop a supplementary threat model addressing this. Using FIPS 140-3 in combination with the threat model, we find that SGX provides sufficient protection against a large part of the potential actors in the cloud.

Privacy Preserving Image De-identification

Members:
Georgia Tsaloli, Le Minh Ha, & Md Sakib Nizam Khan

Supervisors:
Sonja Buchegger & Katerina Mitrokotsa

Abstract:
k-anonymity based image de-identification techniques cluster input images based on similarities and then replace all the k images in a cluster with the same fake image that provides a formal privacy guarantee. The level of privacy provided by these techniques depend on the right value of k, however, to the best of our knowledge, there is no existing technique for choosing the right value of k for a given dataset. In this project, our goal is to evaluate techniques to cluster images based on similarities considering the entire image similarity distribution and based on it select the right value of k for specific requirements of privacy and utility.

Secure Federated Learning in 5G Mobile Networks

Participants:

Martin Isaksson and Karl Norrman, Ericsson Research, KTH Royal Institute of Technology

Industrial supervisor:

Rickard Cöster, Ericsson

Academic supervisor:

Mads Dam, KTH Royal Institute of Technology

Abstract:

In this project we constructed a privacy enhancing scheme for machine learning in 5G mobile networks. The scheme is based around federated learning and multiparty computation. We integrate the scheme in 3GPP 5G Network Analytics Framework.

Shared automation between a traffic tower operator and an automated vehicle

Team:
Gonçalo Pedro Arrais Ivens Collares Pereira, Amber Zelvelder, Masoud Bahraini, Mohammad Nazari

Supervisors:
Jonas Mårtensson (KTH) and Linda Meiby (SCANIA)

Abstract:
This project sets out a framework in the form of a prototype that allows an autonomous vehicle (AV) to share autonomy with a remote control tower to assist in situations that the AV cannot solve at all, or not without breaking a traffic or safety regulations. This shows that shared automation is a possibility for the future and warrants further research.

Simulation of WARA-PS Demo Area and Evaluation of Quadcopter Trajectory Planners

Project members:
Christian Rosdahl (LTH), Damianos Tranos (KTH), Johan Karlsson (Chalmers), John Törnblom (LiU), Péter Várnai (KTH)

Project supervisors:
Olov Andersson (LiU), Jonas Kvarnström (LiU)

Abstract:
The goal of this project is to simplify research on obstacle avoidance for drones within the WARA-PS research arena. We compare two different trajectory planners implemented in the Robot Operating System (ROS): Fast-Planner from Hongkong University and MAV Voxblox planner from ETH Zürich. In addition to this, we try to integrate a simulation of part of the WARA-PS research arena at Gränsö with ROS and the trajectory planners.

Static Program Analysis for the GObject Type System

Project Members:
Noric Couderc (Lund University), Alexandru Dura (Lund University), Claudio Mandrioli (Lund University)

Supervisors:
Christoph Reichenbach (Lund University), Baldvin Gislason Bern (Axis Communications AB)

Abstract:
The speed and precision of static analysis of programs that make use of external libraries can be significantly improved when the analysis models the respective libraries. The GObject library is widely used for emulating object oriented programming in the C language. The programs implemented using this library are less reliable compared to their equivalent implementation in a statically typed object-oriented language, like Java or C++.
To address this problem, we present a static program analysis using the interprocedural distributive environment (IDE) framework. We evaluate the analysis on GStreamer, a large open-source project, and briefly discuss its running time and precision.

Time series generation for automotive software-in-the-loop testing

Project members:
Dhasarathy Parthasarathy (Chalmers/Volvo Group), Karl Bäckström
(Chalmers), Jens Henriksson (Chalmers/Semcon), Sólrún Einarsdóttir (Chalmers)

Project supervisors:
Henrik Lönn (Volvo Group), Christian Berger (Chalmers)

Project Summary:
Testing automotive mechatronic systems partly uses the software-in-the-loop approach,
where systematically covering inputs of the system-under-test remains a major challenge.
This work applies the well-known unsupervised learning framework of Generative
Adversarial Networks (GAN) to learn an unlabeled dataset of recorded in-vehicle signals and
uses it for generation of synthetic input stimuli. Additionally, a metric-based linear
interpolation algorithm is demonstrated, which guarantees that generated stimuli follow a
customizable similarity relationship with specified references. This combination of techniques
enables controlled generation of a rich range of meaningful and realistic input patterns,
improving virtual test coverage and reducing the need for expensive field tests.

Tuning filter parameters in an Unscented Kalman Filter Mine Edition

Project members:
Kristin Nielsen[1,2], Hector Rodriguez-Deniz[1] and Caroline Svahn[1,3]

Supervisors:
Gustaf Hendeby[1], Fredrik Gunnarsson[1,3]

Affiliations:
[1] Linköping University
[2] Epiroc Rock Drills AB
[3] Ericsson AB

Abstract:
We present a static optimisation strategy to obtain suitable values for the unscented parameters in the Unscented Kalman Filter. While in our underground mining scenario the filter fails to converge with the standard settings, our approach substantially improve the estimation in terms of the normalized estimation error squares (NEES).