



WASP Project Course - Final presentation

Examiner: Daniel Axehill, LiU

Main speakers: WASP Project Course Attendees



Course background

- WASP Project Course
 - Organized as 17 independent projects with 3-6 students.
 - 6 hp.
 - The last course in the WASP AS track.
 - Mandatory for AS students, optional for AI students.
 - The project work has been carried through during entire fall 2019.
- Course goals
 - Develop a prototype in the area of autonomous systems and software.
 - Get experience from working in a project in this area requiring different competences.
 - Learn the possibilities available in the WASP research arenas (WARA).
 - Get the opportunity to develop contacts with Swedish industry in the area of autonomous systems and software.
- About half of the projects have a connection or clear relevance to a WARA

People involved

- Course taken mainly by batch-2 AS students, with some exceptions
- Current course status
 - 59 students have passed.
 - 16 projects have been finalized, 1 postponed due to parental leave.
- Each project has had both an industrial supervisor and an academic supervisor
 - The academic supervisor has examined the project and recommended a grade.
- Special thanks to Gunnar Bark, Jesper Tordenlid, and Carl Lindberg for general support and arranging projects connected to the WARAs.
- Now, it's time for the main point!

Project pitch presentations

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

Project members: Joakim Brorsson, Pegah Nikbakht Bideh, Alexander Nilsson (Lund University)

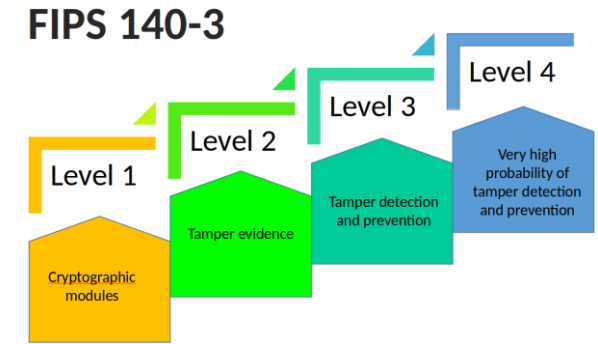
Project supervisors: Martin Hell (Lund University), Senadin Alisic (Combitech AB)

Background

- Security of systems depends on safeguarding cryptographic keys.
- Hardware Security modules (HSMs) are often used for this purpose.
- HSMs used today are not adapted for the cloud.
- Combitech uses HSMs in many projects today. Cloud based infrastructure could potentially benefit these projects.
- Intel Software Guard Extensions (SGX) could potentially fill the same purpose in a cloud adapted way.


Result

- Using FIPS 140-3, the industry standard for evaluating HSMs:
 - SGX can only achieve level 2
- We prototype a new security model with
 - More granularity
 - Better adoption to Cloud scenario
- This provides a measure of security for cloud native secure key storage solutions



| | Honest | Curious | Malicious |
|------------------|--------|---------|-----------|
| Remote User | R+H | R+C | R+M |
| Co-Hosted VM | V+H | V+C | V+M |
| Local Admin | L+H | L+C | L+M |
| Hypervisor Admin | H+H | H+C | H+M |
| Physical Owner | P+H | P+C | P+M |

| | R+C | R+M | V+C | V+M | L+C | L+M | H+C | H+M | P+C | P+M |
|--------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Application Design | ✓ | ✓ | ✓ | | | | | | | |
| Virtual Machines | ✓ | ✓ | ✓ | ✓ | | | | | | |
| Intel SGX | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| HSMs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |



Autonomous Calibration of 3D Computer Vision System

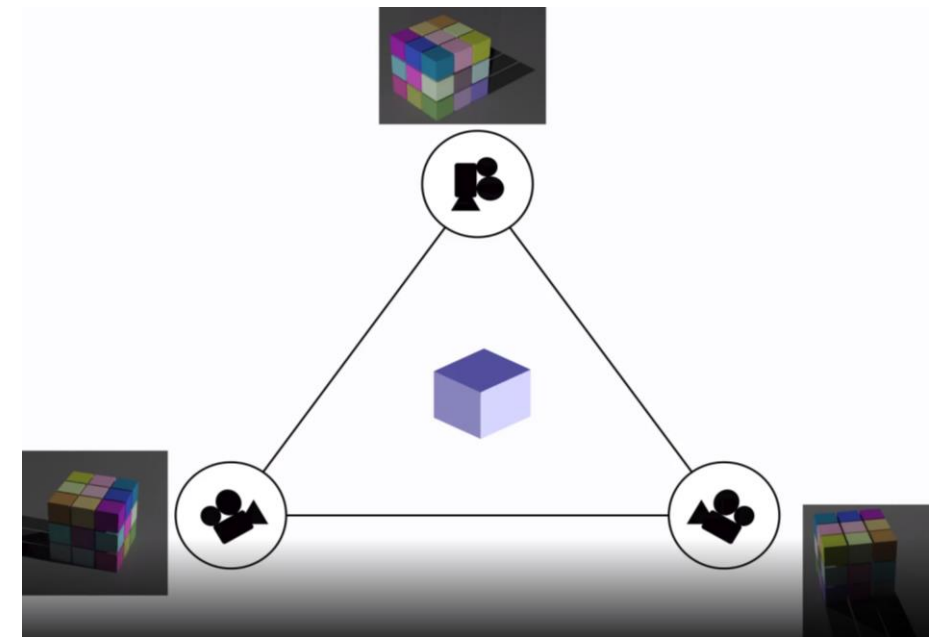
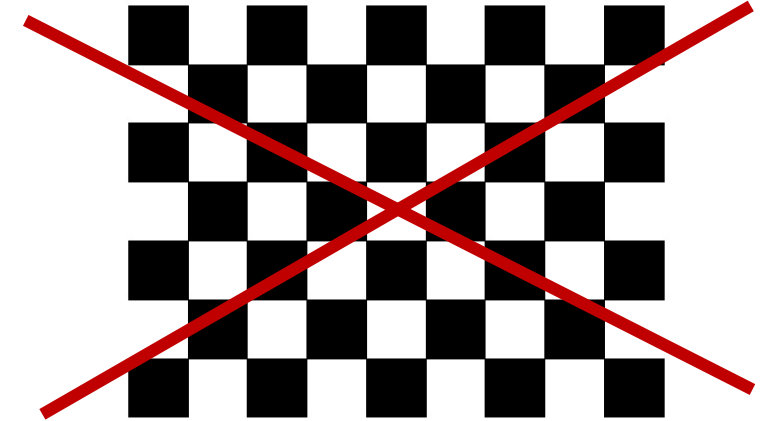
Project members: Håkan Carlsson (KTH), Martin Larsson (LTH/Combain), Mina Ferizbegovic (KTH), Olivier Moliner (Sony), Lissy Pellaco (KTH), Gustaf Waldemarson (ARM), Xuechun Xu (KTH)

Project supervisors: Mikael Lindberg (Axis), Karl Åström (LTH)

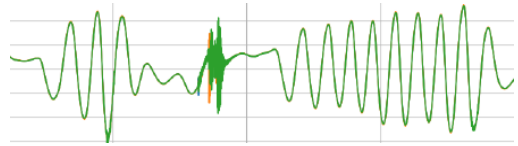
Background



- Cameras are very important for autonomous systems
- Camera calibration is necessary prior to camera use
- It usually requires manual intervention and the use of objects with known geometries
- Our goal is to limit the user intervention and achieve **autonomous calibration** by using multiple cameras and IMUs
- *This project is in collaboration with **Axis** and **WARA Public Safety arena***



Results



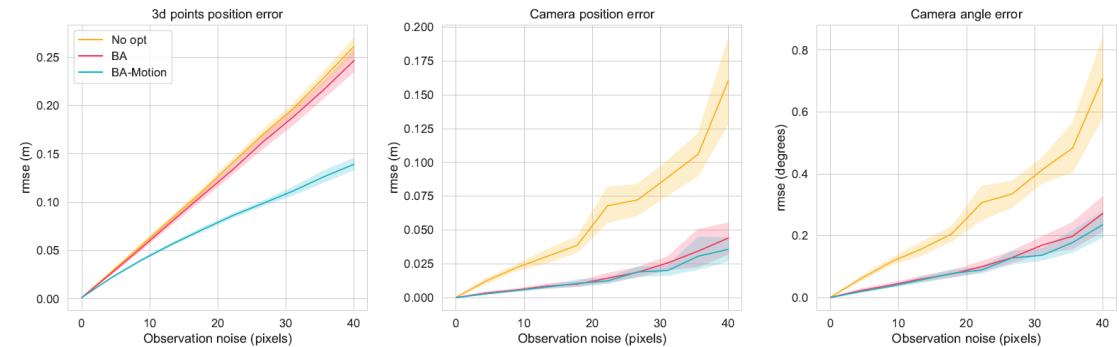
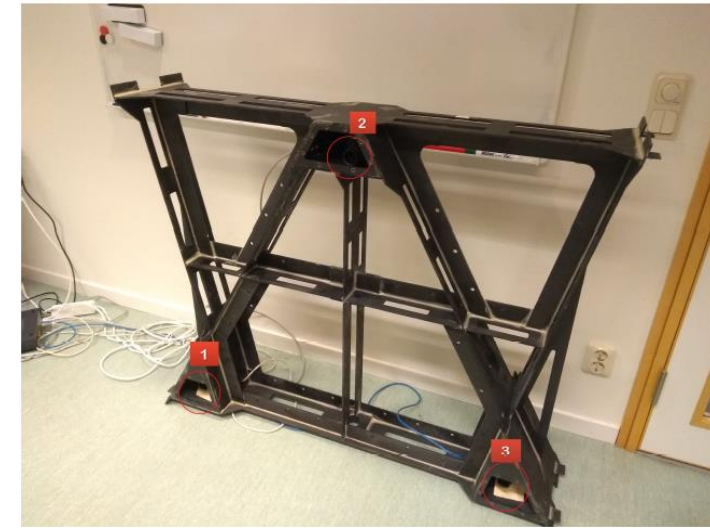
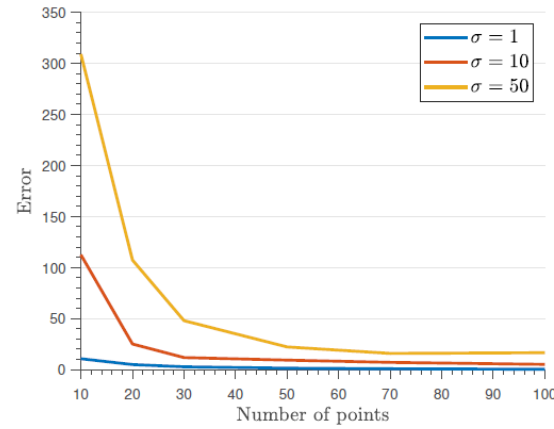
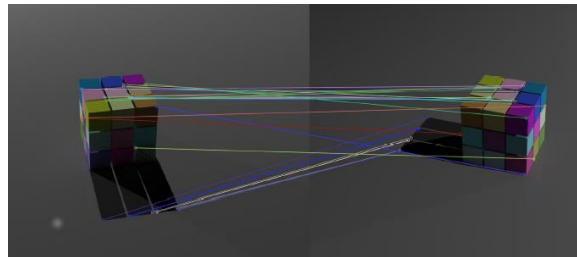
IMU data

Estimate cameras
relative
position and
orientation

Images

Feature detection
and matching

Estimate internal
cameras
parameters



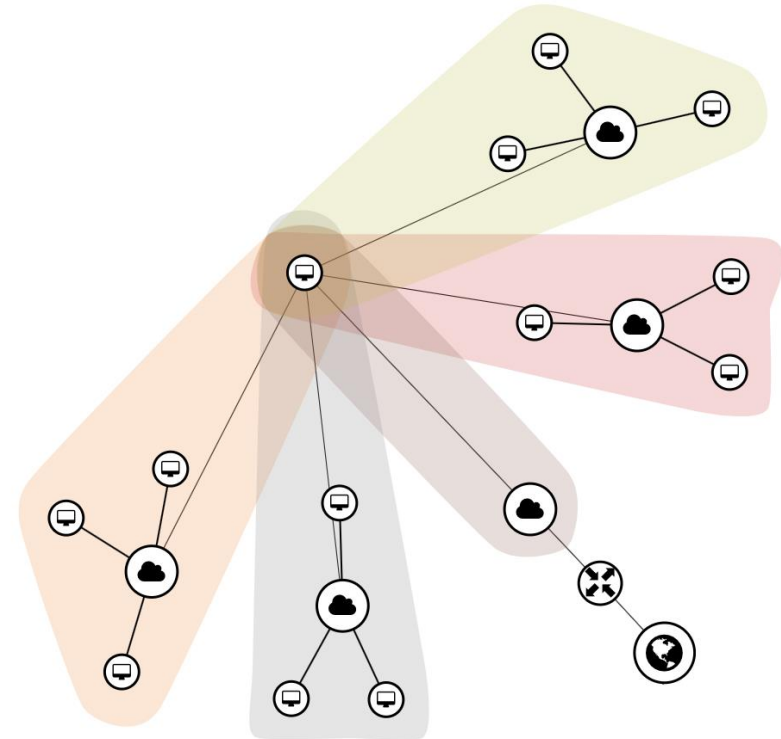
Federated Kubernetes Sandbox

Project members: Haorui Peng, Johan Ruuskanen, Alfred Åkesson (Lund)

Project supervisors: Lars Larsson (Umeå), Johan Eker (Ericsson)

Background

- Kubernetes is a software for deploying and managing applications in a datacenter
- A Kubernetes federation handles the interactions between different Kubernetes clusters
- It is hard to test things in a federated environment
- We created K8sFedSandbox to provide a tool to deploy a Kubernetes federation experimental environment
- Why is this relevant?
 - WARA PS: critical infrastructure resilient to data center outage
 - Edge computing: testbed for arbitrary amount of small-scale clusters



Result

- The sandbox
 - Allocating VM/networks on ERDC (Ericsson Research Data Center)
 - Set up network emulation
 - Deploying Kubernetes
 - Deploying monitoring using Grafana/Prometheus
 - Deploying Istio to allow interconnections between Kubernetes deployments
- The application
 - As a demonstration, we used the sandbox to deploy a multi-cluster face-detection application that is resilient to cluster outage
- Future work?
 - Github release
 - Tool paper

Static Program Analysis for the GObject Type System

Noric Couderc (Lund University)

Alexandru Dura (Lund University)

Claudio Mandrioli (Lund University)

Project supervisors:

Christoph Reichenbach (Lund University)

Baldvin Gislason Bern (Axis Communications AB)

Background

- Software running on the Axis cameras uses the **GStreamer** library, which in turn relies on the **GObject** library
- The **GObject** library implements a **dynamic type system**, which delays the detection of **type errors** to the running time of the software
- Our goal is to **statically** detect these **type errors**, before the software is deployed



Result

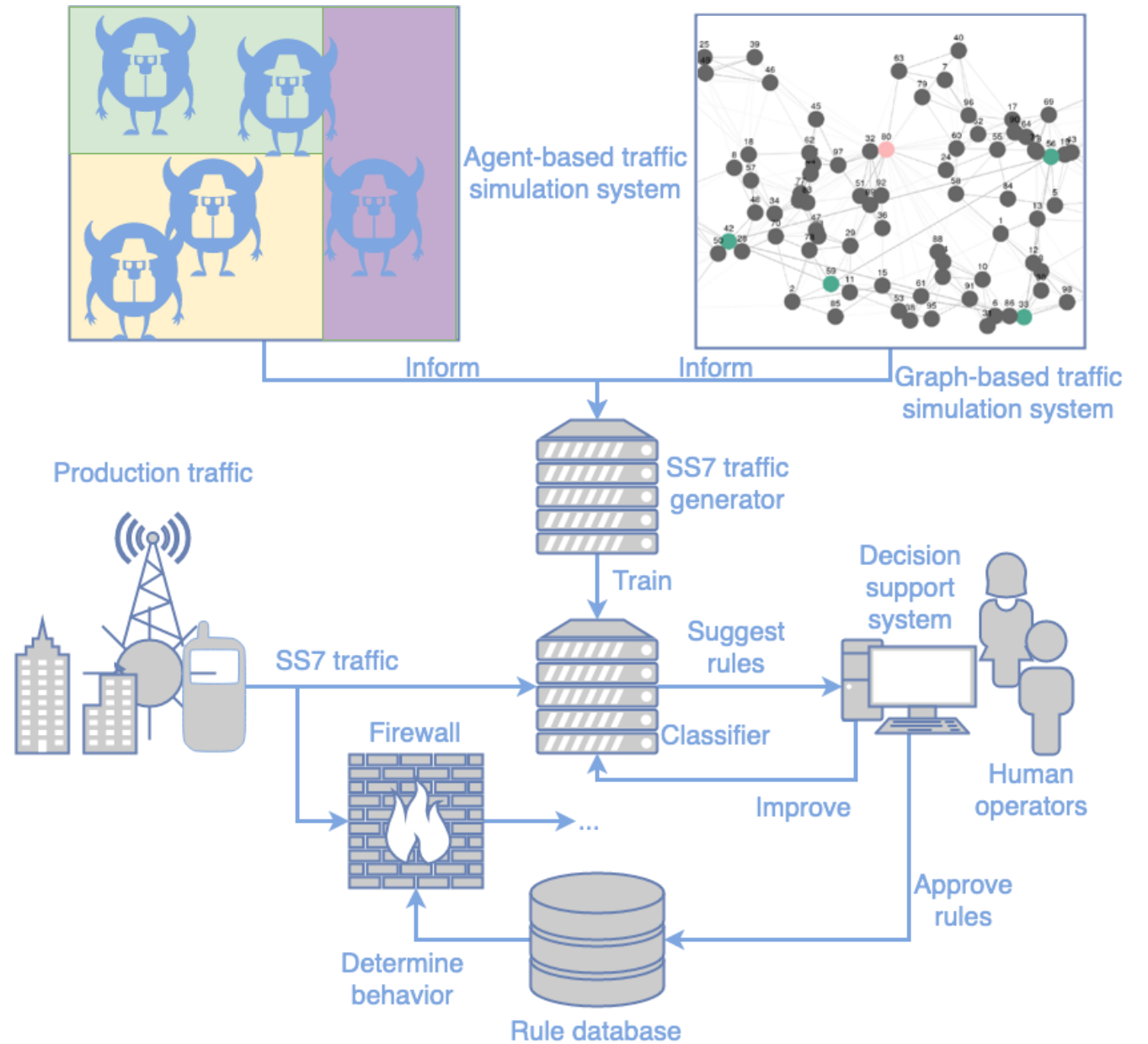
- A **whole-program analysis** implemented using the Phasar static program analysis framework
- Our static analysis computes all the possible object types a pointer may refer to and **reports incompatible type casts** that may result in runtime errors
- Open question: how **precise** is the analysis?



Detecting Anomalies in SS7 Network Traffic

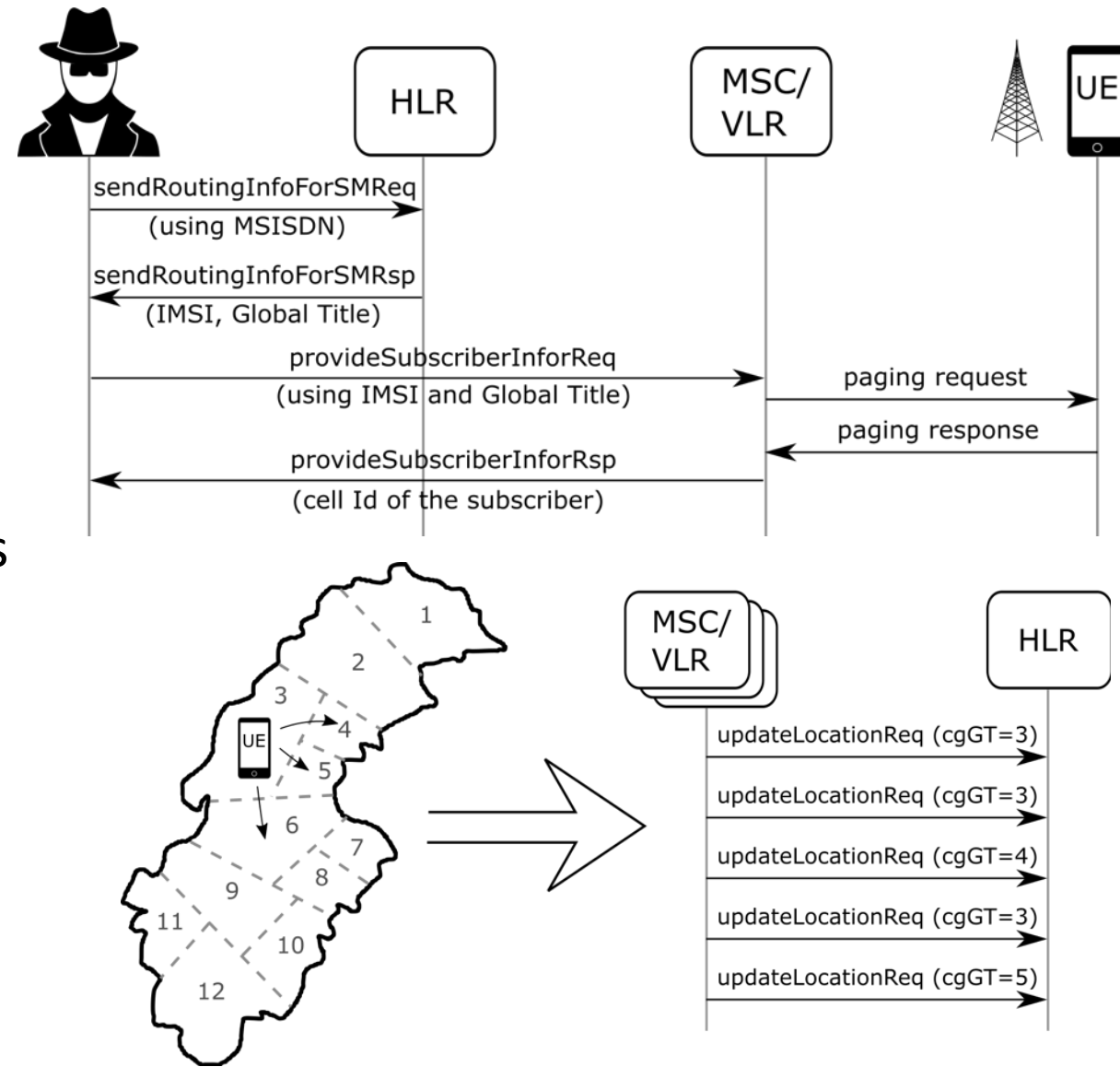
Project members: Tobias Sundqvist^{1,2},
Christopher Blöcker¹, Timotheus Kampik¹
Project supervisors: Monowar H. Bhuyan¹,
Peter Olofsson²

1: Umeå University
2: Tieto



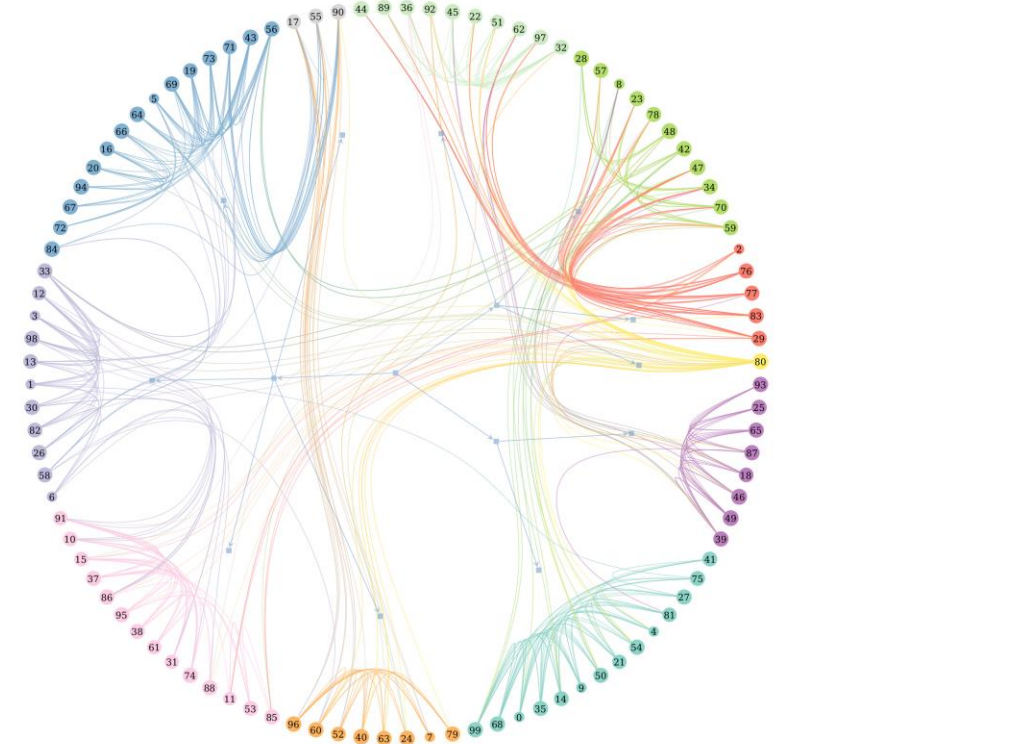
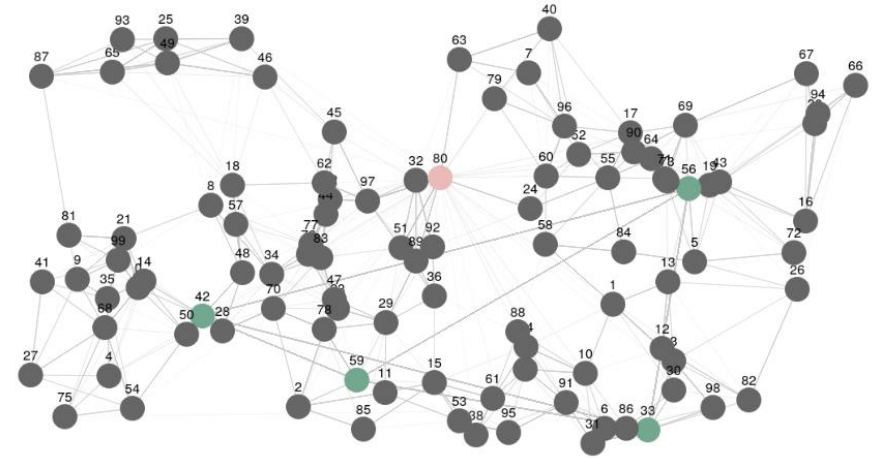
Background

- SS7 key component of mobile networks
 - SS7 networks have become more open in recent years
 - Consequence: security crucial concern
 - Typical attack: attacker remotely assumes identity of victim
 - However, requests are localized at MSC (zone) level
 - "Unlikely" location transitions are likely attacks
- ⇒ Localization problem



Result

- Two traffic simulators:
 - Network-based on macro-level
 - Agent-based on micro-level
- Two anomaly detection approaches:
 - Community detection on macro-level
 - Bayesian filter-based detection on micro-level
- Human-in-the-loop architecture proposal
 - For integration into production systems



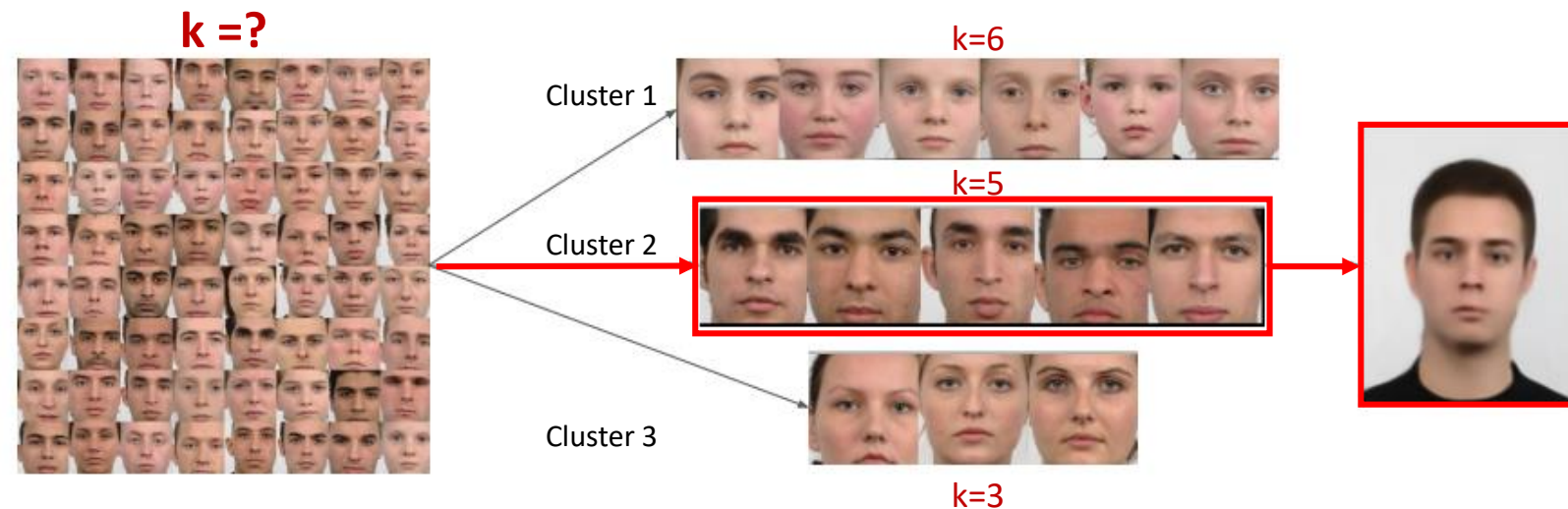
Privacy-Preserving Image De-identification

Project members: Md Sakib Nizam Khan (KTH), Minh-Ha Le (LiU), Georgia Tsaloli (Chalmers)

Project supervisors: Sonja Buchegger (KTH), Katerina Mitrokotsa (Chalmers)

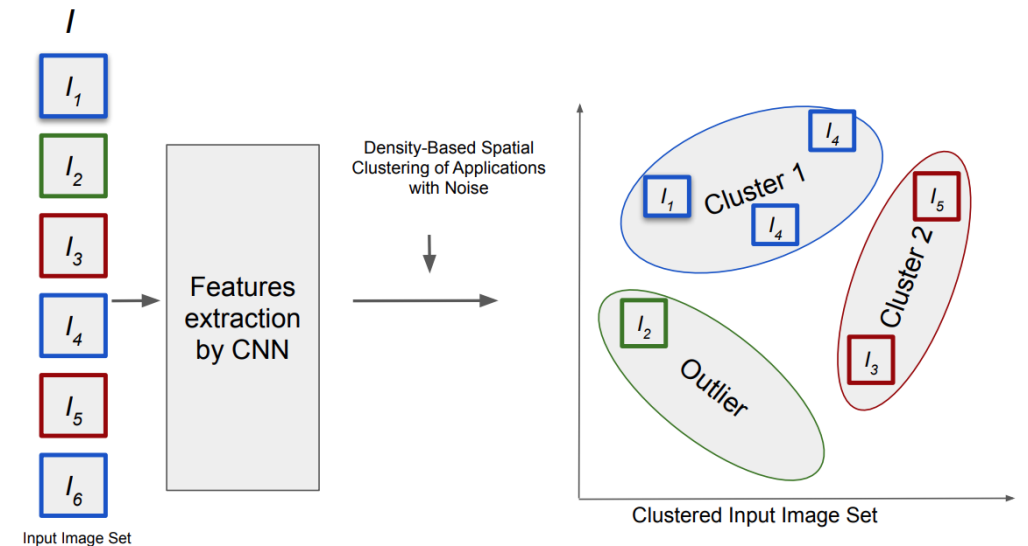
Background

- Analysis and sharing of image and video data poses a **privacy risk**.
- Image de-identification is a popular countermeasure, **replacing directly identifiable** information with **fake** information.
- E.g. k-Same-Net combines Generative Neural Networks (GNNs) with **k-anonymity** for privacy guarantees. Images are **clustered** based on similarities, then **all k images** in a cluster are replaced with the **same fake image**.
- Problem: not known how to choose k and its effects on the **utility** of the **de-identified data**.
- Research question: How to **quantify** and improve the **privacy-utility trade-off**?
- Importance: Better **quality** of analysis and **safer sharing** under privacy guarantees
- Relevance: cameras in cars, public transport, CCTV.



Result

- Our approach: Consider the **entire distribution** of image population for better clustering
 - Use **CNN based feature extraction** with **density-based spatial clustering**
 - Then use **GNN** like k-same-Net to generate the fake images.
- Result: **increased utility** at constant k , i.e., better utility for the same privacy or better privacy at same utility compared to k-Same-Net
- Future work:
 - Replicate experiments on **different types of datasets**
 - Investigate **non-linear trade-offs** between k (privacy) and similarity of de-identified to original images (utility)
 - Abstract **recommendations for tailoring k** to specific privacy or utility constraints



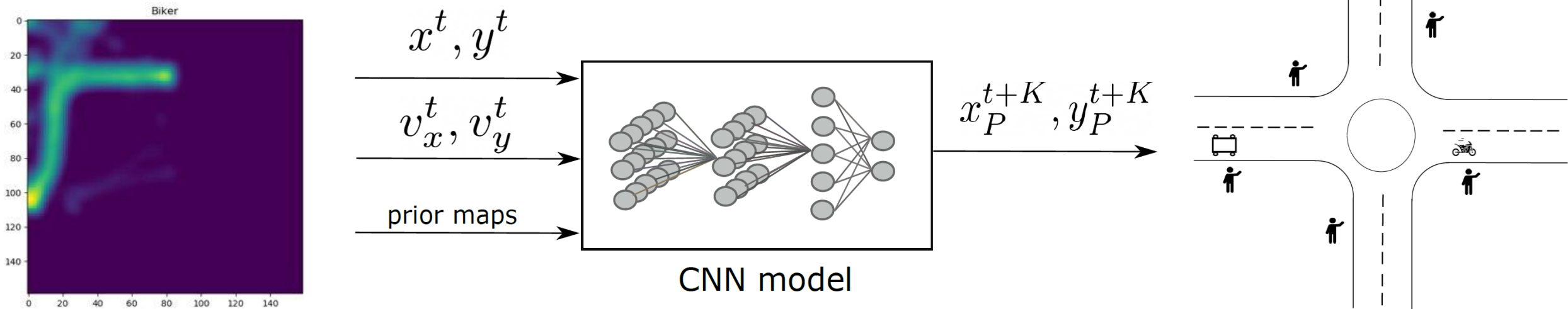
Human road users' behavior learning and prediction based on mobile networks

Project members: Lucas Brynte (Chalmers), Joris Van Rooij (Chalmers), Sarit Khirirat (KTH)

Project supervisors: Paolo Falcone (Chalmers), Henrik Sahlin (Ericsson)

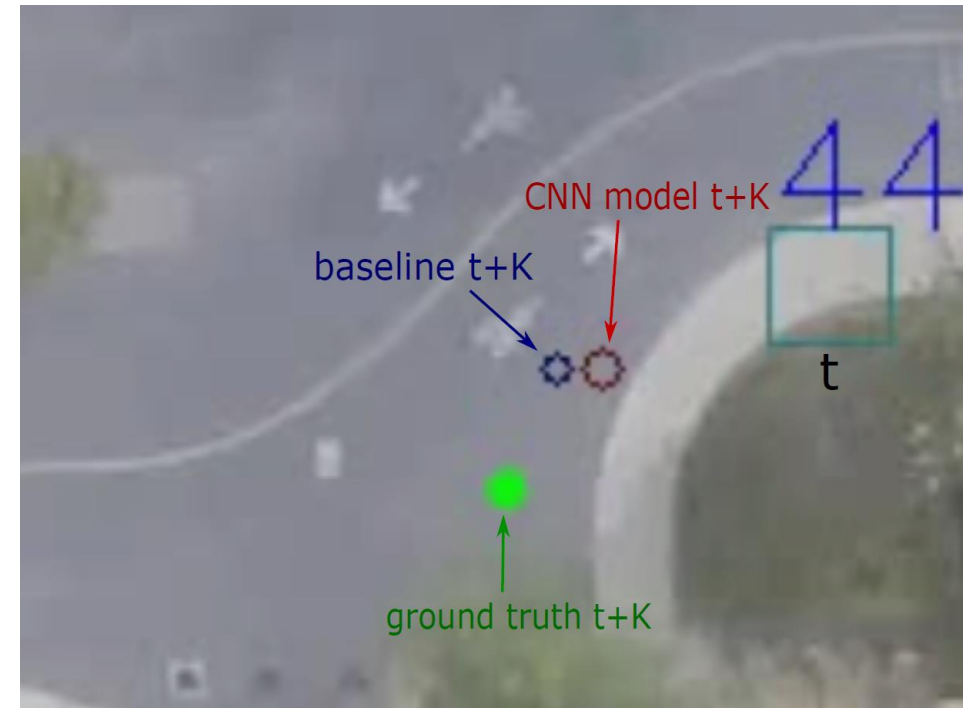
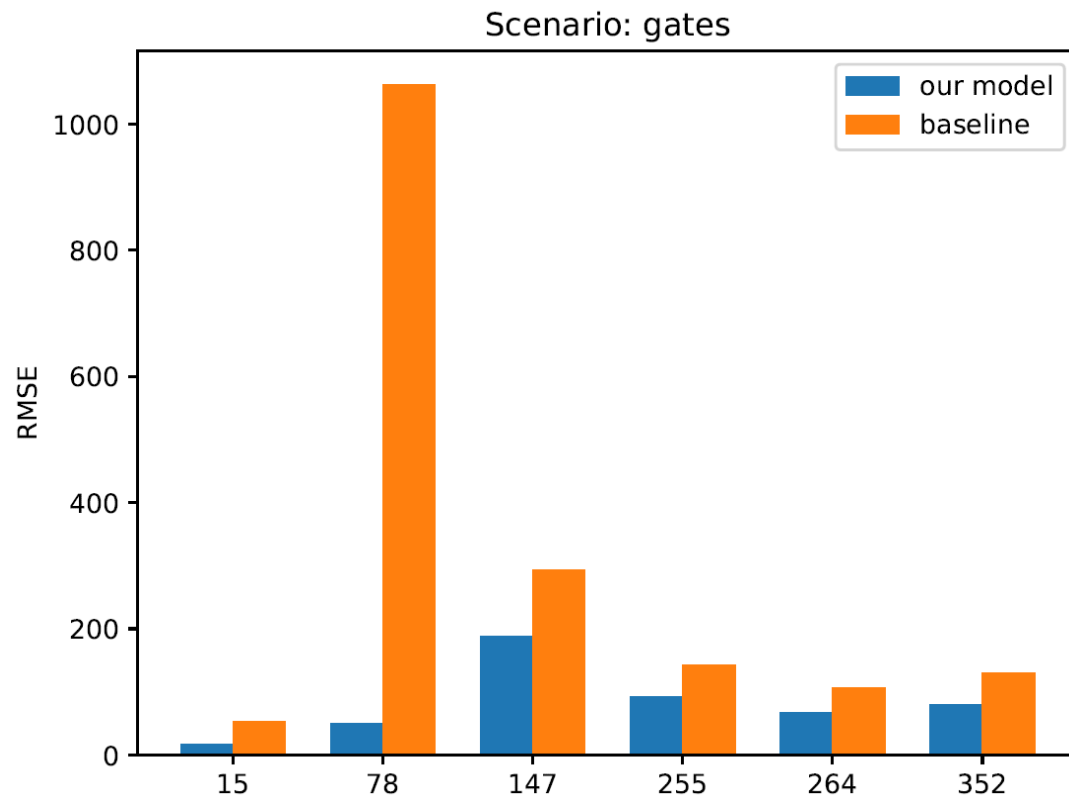
Background

- 5G networks enable fast and accurate tracking of vehicles and positions.
- Autonomous vehicles need accurate human future trajectories in traffic.
- We proposed a **CNN-based architecture** to predict human trajectory.
 - Given past trajectories of objects (e.g. pedestrians) up to time t , predict **future position** of each pedestrian at time $t+K$.
 - Utilize positions and velocities, and prior maps (distributions) as features.

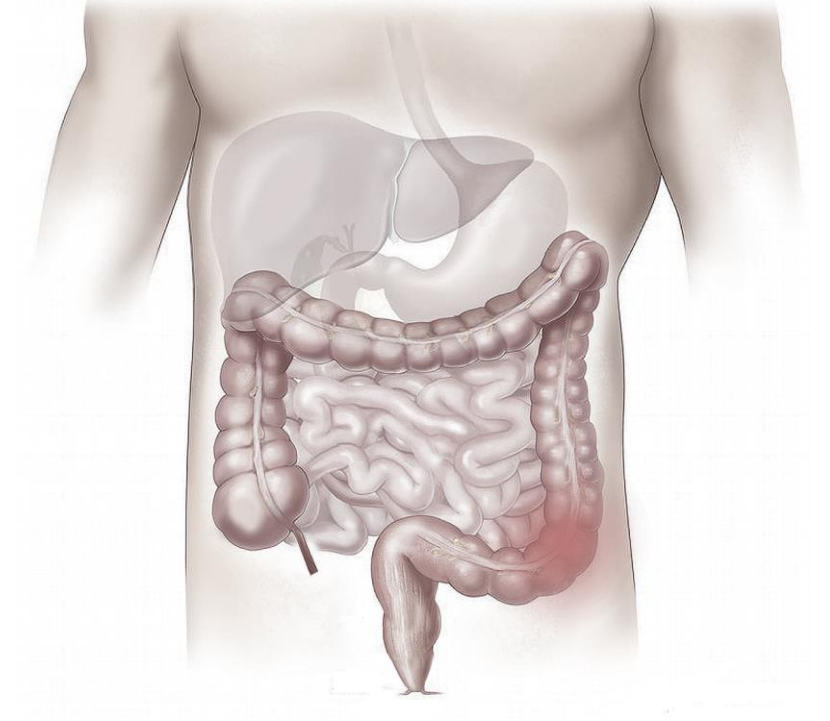


Results on the Stanford Drone Dataset

- 8 scenes, 60 videos, and $K = 4.8$ seconds.
- Compared the performance of CNN against the baseline prediction.

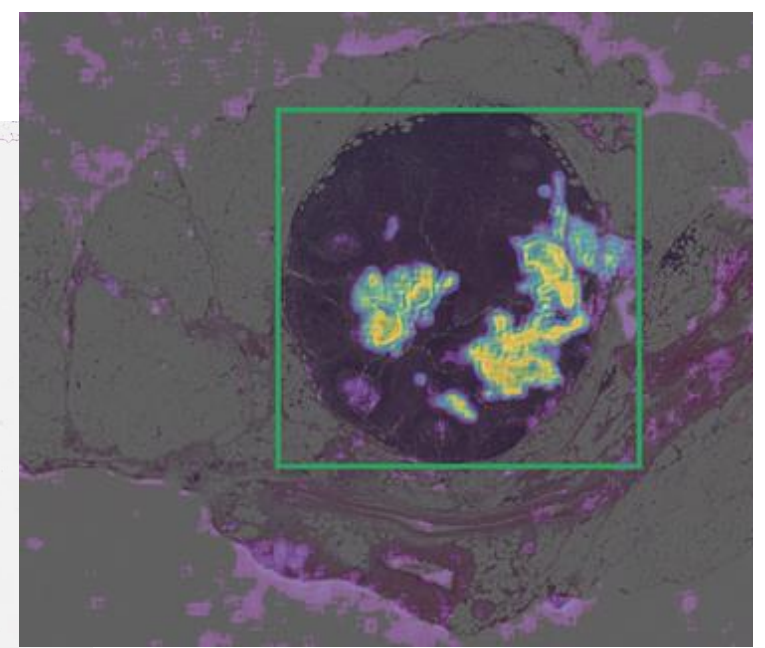
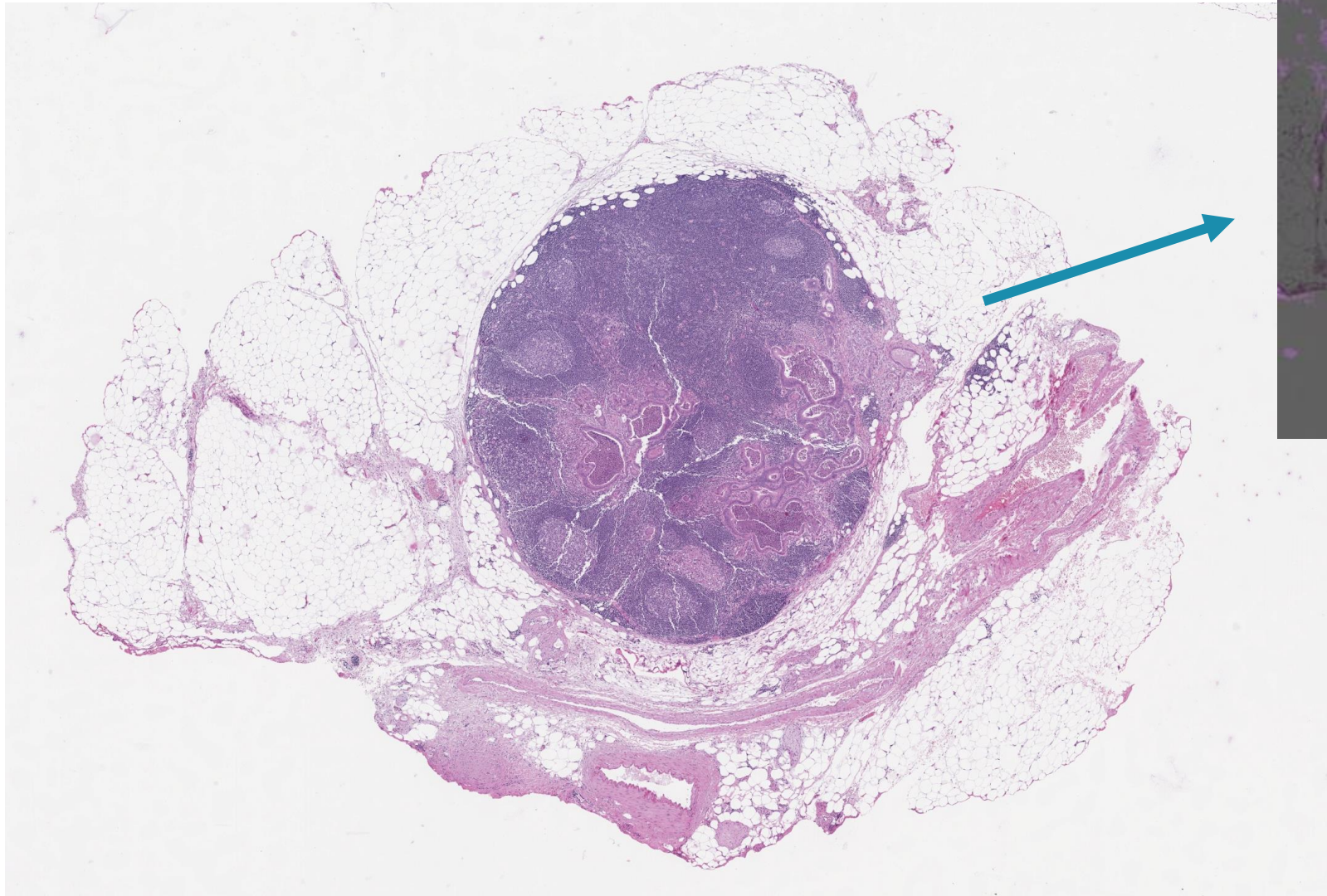


Detection of colon cancer metastases in lymph nodes through deep learning



Martin Lindvall, Karin Stacke, Apostolia Tsirikoglou (Linköping University)

Project supervisors: *Claes Lundström (Sectra AB), Gabriel Eilertsen (Linköping University)*



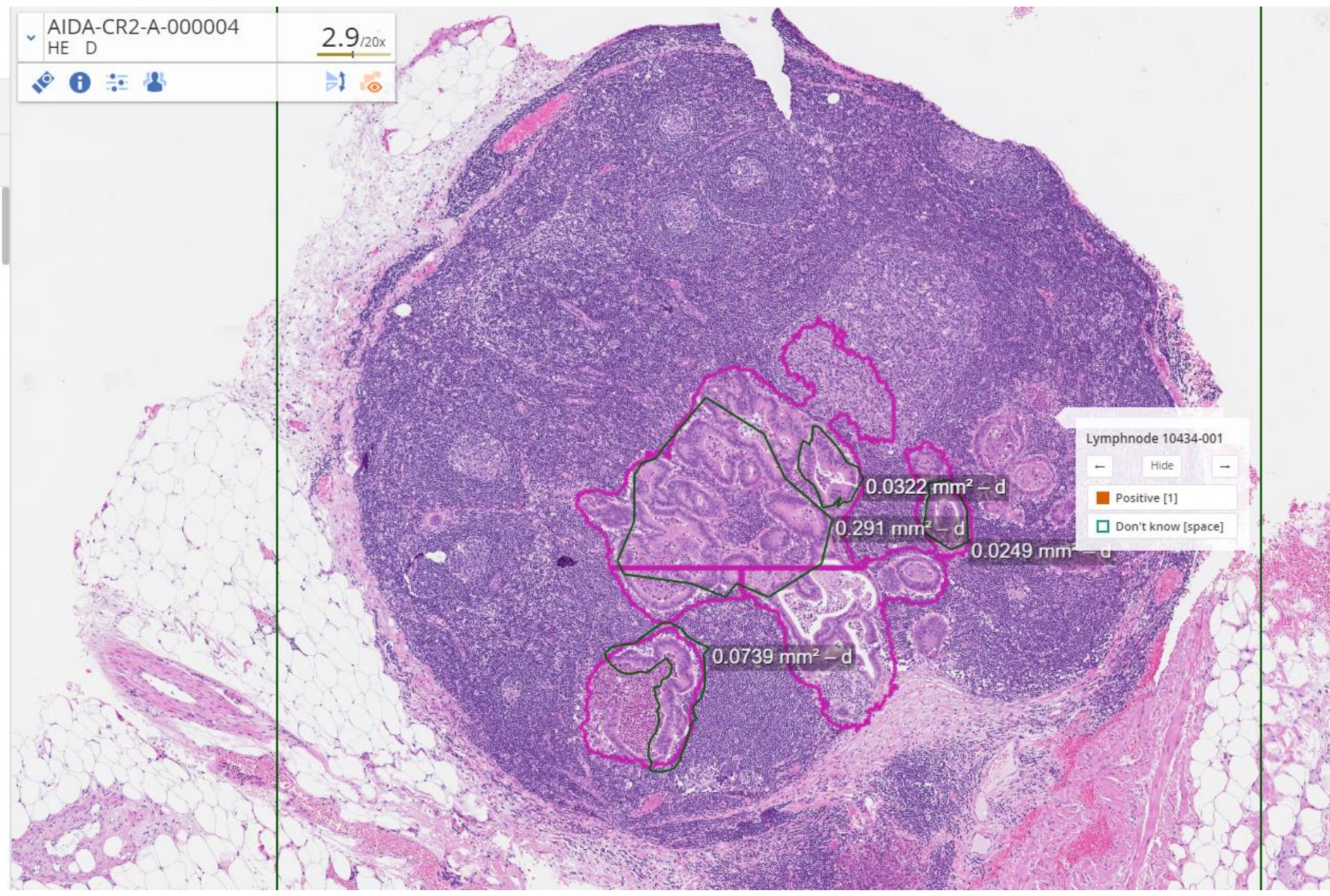
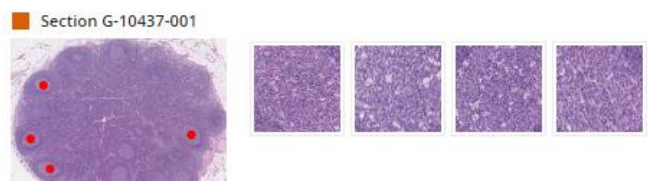
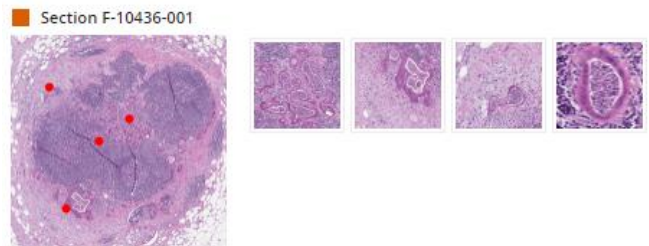
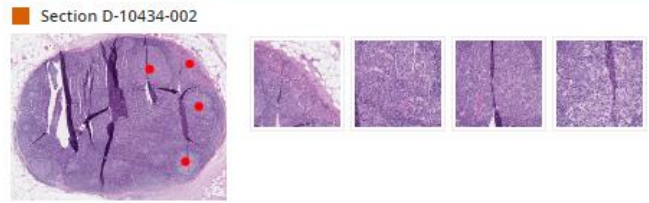
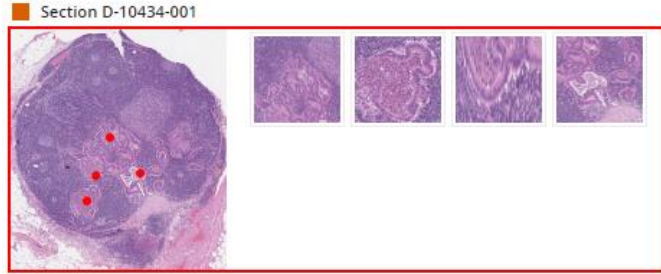
 Region
Gävleborg

 LINKÖPING
UNIVERSITY

SECTRA

0 positive, 62 unverified (out of 62 lymph nodes)

sensitivity



Lymphnode 10434-001

Hide

Positive [1]

Don't know [space]

Online Tuning of Filter Parameters: Mine Edition

Project members: Kristin Nielsen (LiU/Epiroc Rock Drills AB), Hector Rodriguez-Deniz (LiU), Caroline Svahn (LiU/Ericsson AB)

Project supervisors: Gustaf Hendeby (LiU), Fredrik Gunnarsson (Ericsson AB)

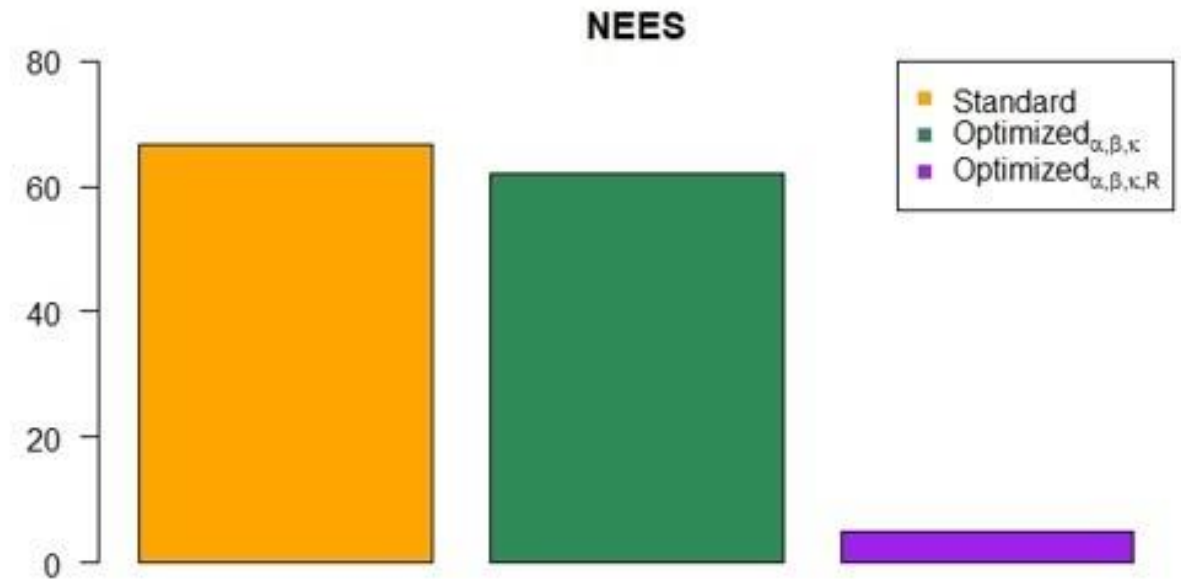
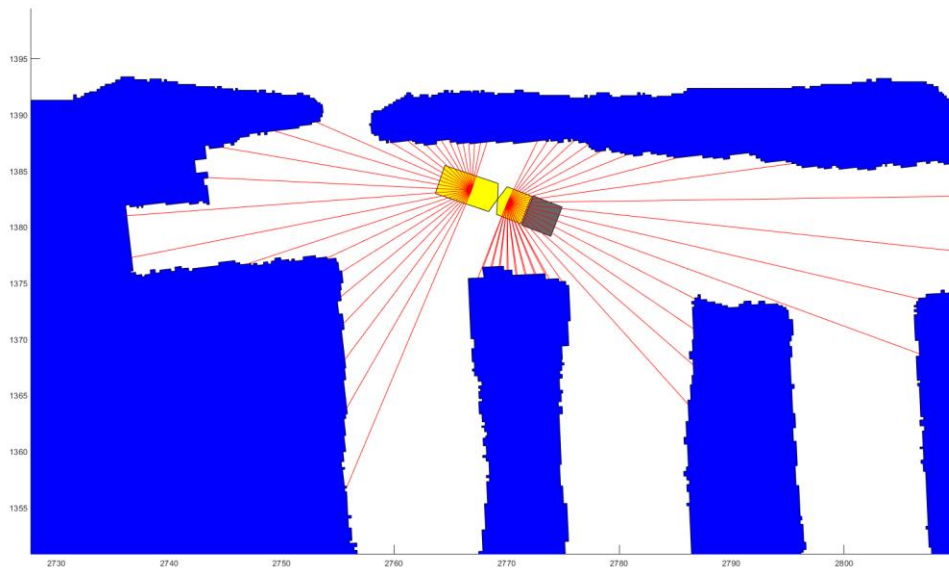
Background

- Highly-accurate positioning is crucial for automated operations in underground mining
- Commercial products currently use Bayesian filtering
- Industry lacks strategies to automatically tune filtering parameters
- We find optimal parameters for a UKF



Result

- We present an optimisation strategy to obtain suitable values for the parameters in the UKF
- Our approach substantially improve the estimation in the normalized estimation error squares (NEES)



Active Learning on video data for DNN

Project members: Joakim Johnander (LiU), Gustav Häger (LiU), Abelrahman Eldesokey (LiU)

Project supervisors: Erik Werner (Zenuity), Per-Erik Forssén (LiU)

Background

- We consider 2D Object Detection for Autonomous Driving
- What data points should we annotate?
 - Active Learning: Annotate points on which the model is uncertain
 - In this project: Use temporal smoothness as proxy for certainty
- Connection to Zenuity and WARA-DAT/PS:
 - Aim to find scenarios where our models perform poorly, in order to train on those scenarios

Algorithm 1: The active learning loop.

```
1 Annotate  $A_0$  examples from potential training set  $\mathcal{D}^{\text{train}}$  to form
  training set  $\mathcal{A}$ 
2 Train detector for  $N_0$  epochs
3 for  $i = 1, \dots, p$  do
4   | Run detector on potential training set  $\mathcal{D}^{\text{train}}$ 
5   | Select  $A_i$  new examples from  $\mathcal{D}^{\text{train}}$  to annotate, add to  $\mathcal{A}$ 
6   | if Reset detector between episodes then
7   |   | Reinitialize all weights of the detector
8   |   end
9   |   train detector on  $\mathcal{A}$  for  $N_i$  epochs
10 end
```

Result

- Experiment with a large dataset, compare different selection criteria
 - Oracle: Utilize ground truth, select data points on which model performs poorly
 - Uniform: Randomly select data points
 - Temporal: Utilize temporal consistency
- Results were insignificant as
 - Annotations were too noisy
 - There was an extreme class imbalance
- Future work:
 - Try another dataset

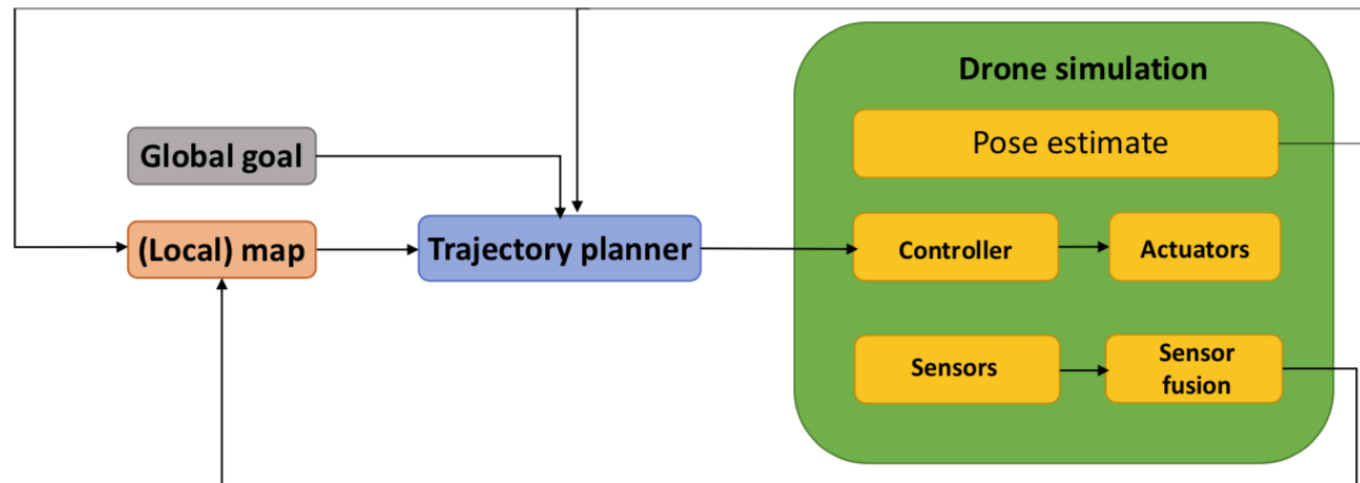
Simulation of WARA-PS Demo Area and Evaluation of Quadcopter Trajectory Planners

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)

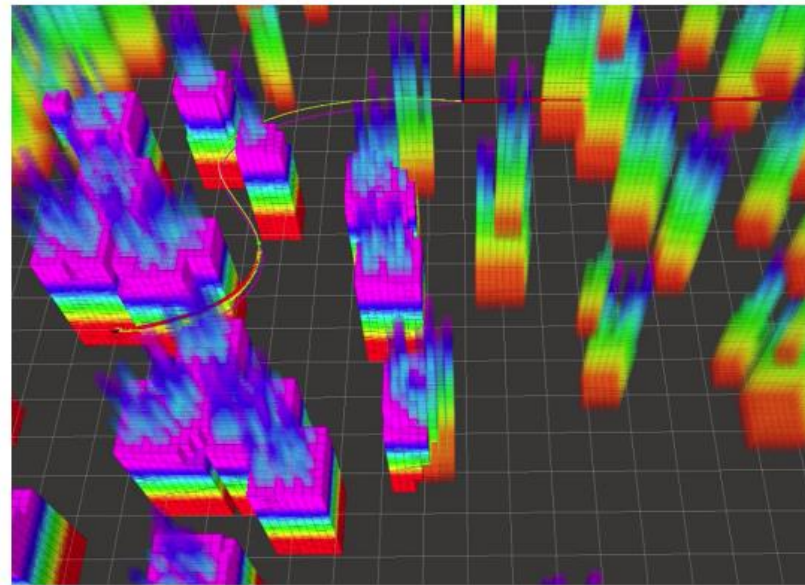
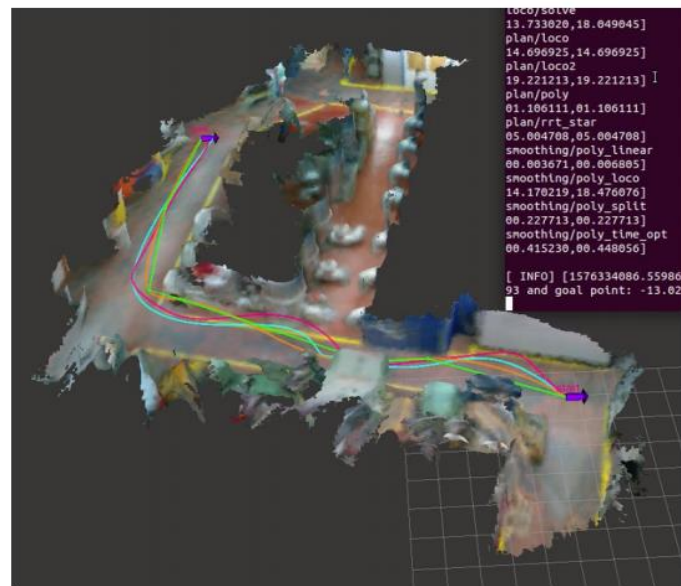
Background

- **Goal:** Research on **obstacle avoidance** for drones within the **WARA-PS** research arena.
- **Compare** two different **trajectory planners** implemented in the Robot Operating System (**ROS**): *Fast-Planner* from Hongkong University and *MAV Voxblox* planner from ETH Zürich.
- Try to **integrate** a **simulation** of part of the **WARA-PS** research arena at Gränsö with **ROS** and the trajectory planners.



Result

- *MAV Voxelox* planner: global RRT planner, tested on built-in map
 - **Case study:** initial planning: 190 s, minor replanning: 63 s, shorter trajectory: 41s
- *Fast-Planner:* tested on built-in box environment
 - **Case study:** planning time: 13 s, replanning time: 15 s
 - Faster, but suboptimal results



Enabling Design And Execution of Large Scale Experiments on Maven Central

César Soto Valero (KTH)

He Ye (KTH)

Joel Scheuner (Chalmers)

Long Zhang (KTH)

Nicolas Harrant (KTH)

Project supervisors:

Torsten Ek (Combient)

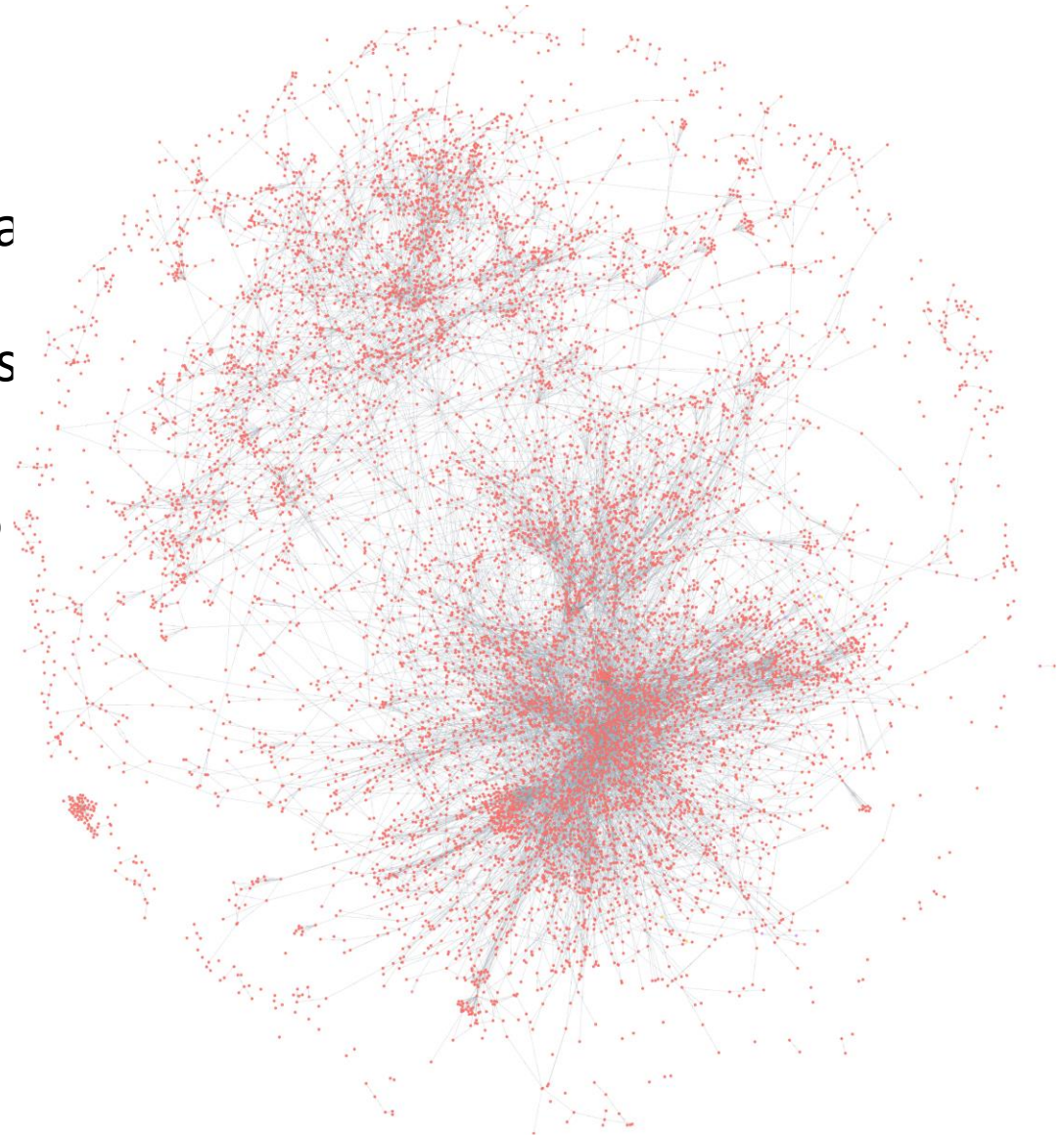
Benoit Baudry (KTH)

Background

- This project aim at enabling **Automated Software Engineering** experiment in the context of the **Software WARA**.
- Automated Software Engineering relies heavily on **transformations** applied to software artifacts
- To **assess the validity** of a transformation, a solution consist into gathering:
 - **large** datasets of artifacts
 - that contains sources, **build instructions and tests**
 - that are **representative** of their ecosystem, and **diverse**
- applying the transformation on each artifact and, then, checking that they still build and pass their tests.

Result

- We build a **graph database** of containing meta information on the 4M artifacts in **Maven Central** to help researchers designing datasets
- We provide **tooling** to mine the sources, builds instructions and tests corresponding to these artifacts,
- and **distribute** automated software engineering **experiments** to test their transformations.



Multimodal User Interfaces for Decision Support

Veronika Domova (Linköping University)

Erik Gärtner (Lund University)

Nikita Korzhitskii (Linköping University)

Johan Källström (Linköping University)

Martin Pallin (KTH Royal Institute of Technology)

Fredrik Präntare (Linköping University)

Project supervisors:

Jesper Tordenlid (Combitech)

Pontus Nilsson (Combitech)

Patric Ljung (Linköping University)

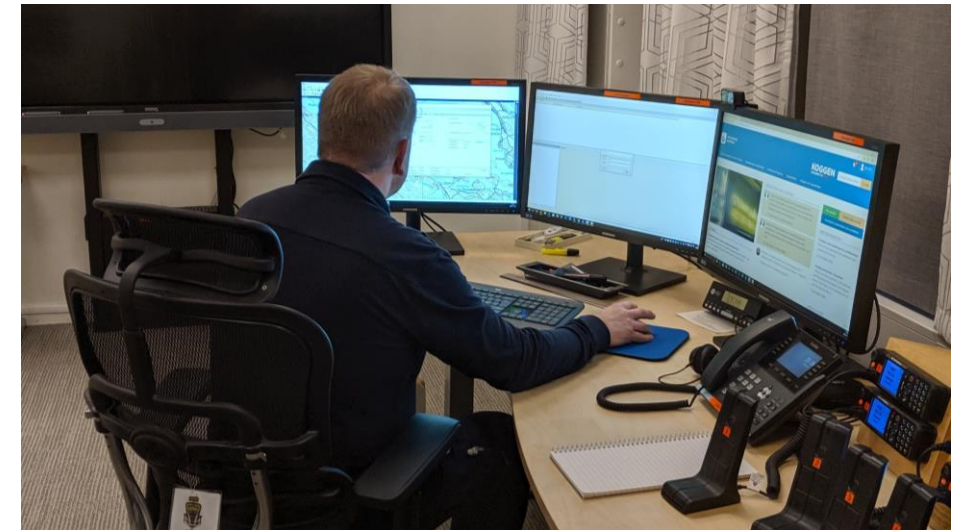
Background

- Autonomous **search and rescue systems are critical** for public safety
- Human involvement is still necessary



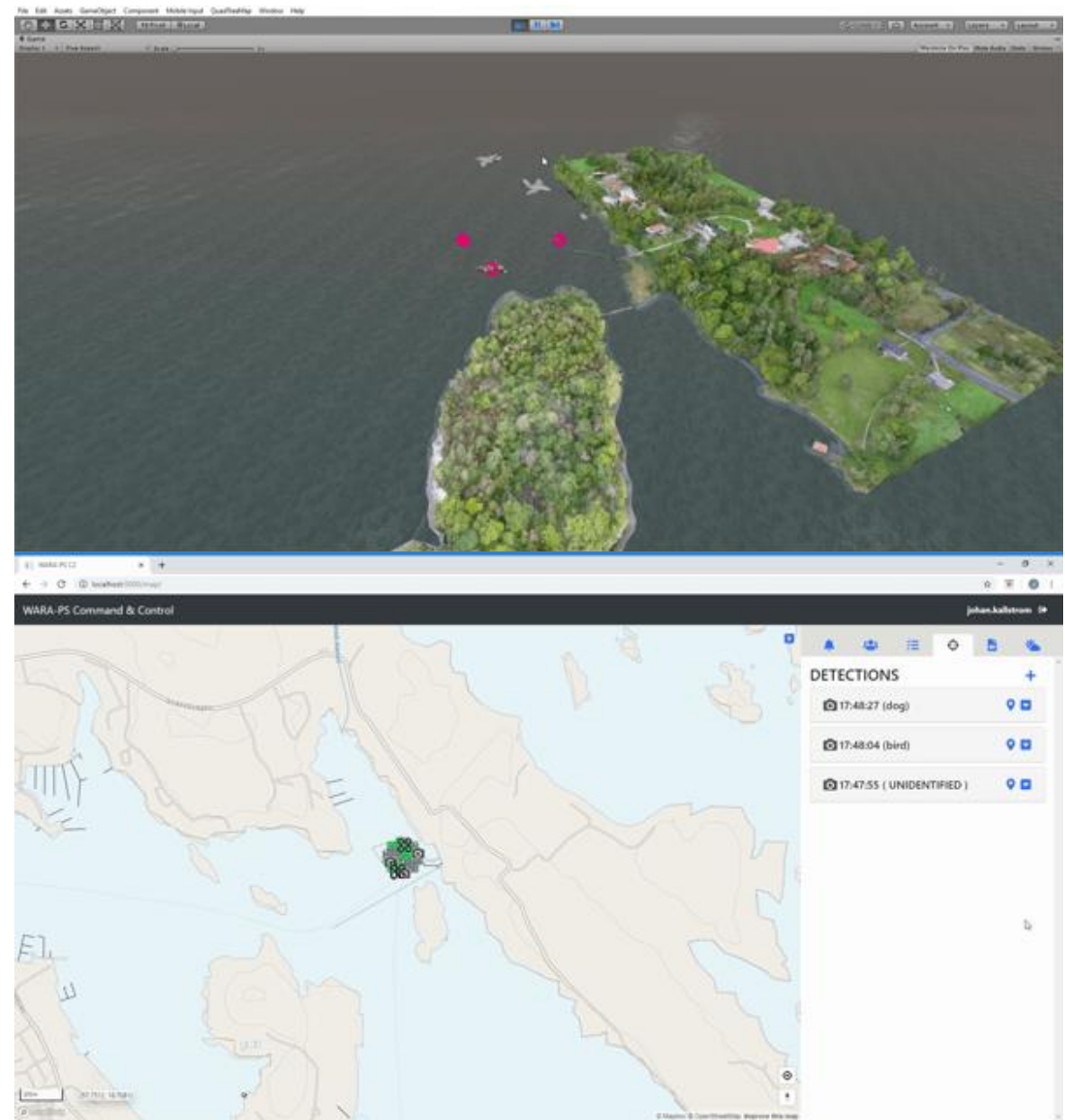
Project scope

- **Improve** an existing **Combitech WARA-PS simulator** and its **user interface**
- Utilize **multi-modal** interfaces



Result

- 3D visualization and sensor simulation
- AI object detector
- Improved interface
- Feedback on improvements from a professional operator



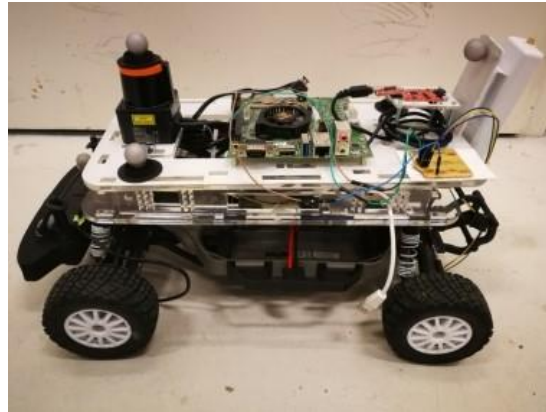
Shared automation between a traffic tower operator and an automated vehicle

Project members: Gonçalo Pedro Arrais Ivens Collares Pereira(KTH), Amber Zelvelder(Umeå), Masoud Bahraini(Chalmers), and Mohammad Nazari(Chalmers)

Project supervisors: Jonas Mårtensson (KTH), Linda Meiby (SCANIA)

Background

- Autonomous vehicles (AV) are still not capable of handling all situations and conditions safely.
- The idea of having a human driver per AV, partly defeats the purpose of an autonomous system, besides being unfeasible and too costly.
- Control towers for AVs are proposed in order to allow a human operator to take over control when a vehicle is in a situation it cannot handle. This allows an operator to serve many vehicles.
- This project consists of implementing and testing shared automation scenarios for the SVEA vehicles and the control tower available at the ITRL.



**ITRL – INTEGRATED TRANSPORT
RESEARCH LAB**

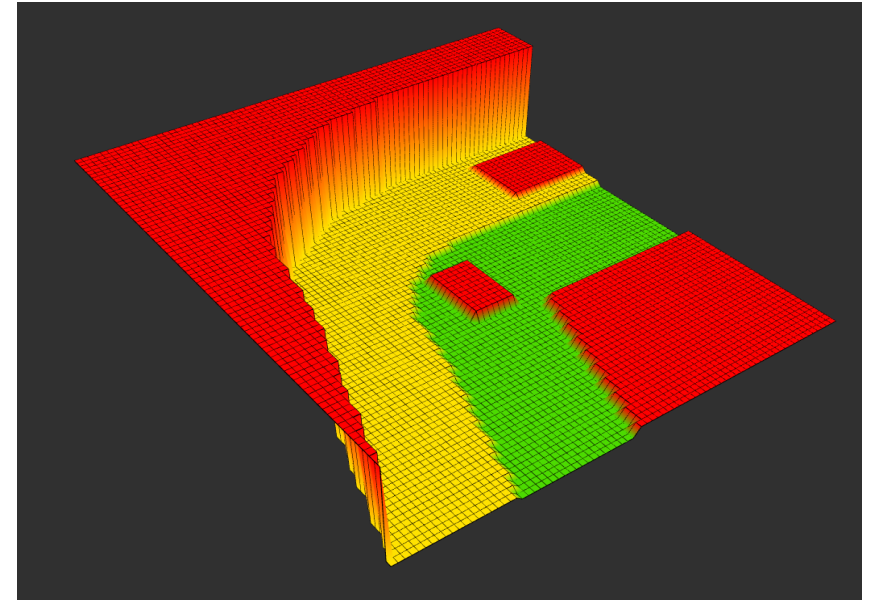
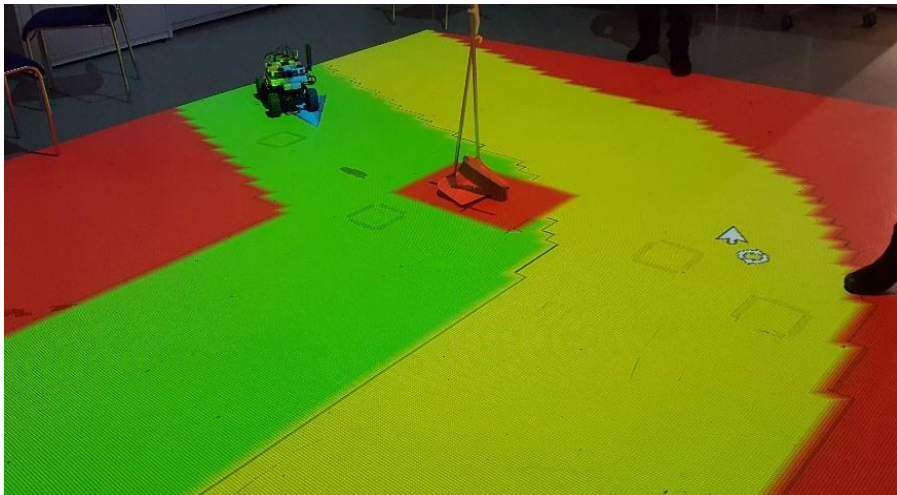
KTH ROYAL INSTITUTE OF TECHNOLOGY



SCANIA

Result

- 3 scenarios implemented:
 - Vehicle drives autonomously with no intervention;
 - Vehicle receives permission to execute plan and then drives autonomously;
 - Vehicle is denied permission to execute plan and then the operator takes over control and tele-operates the vehicle to the goal.



Thank you for your attention!

Don't miss the poster sessions where more details will be presented!