Data Generation and Knowledge Sharing

For Intrusion Detection Systems in the Internet of Things

Christian Rohner and Andreas Johnsson

Project financed by Vinnova

UPPSALA
UNIVERSITET

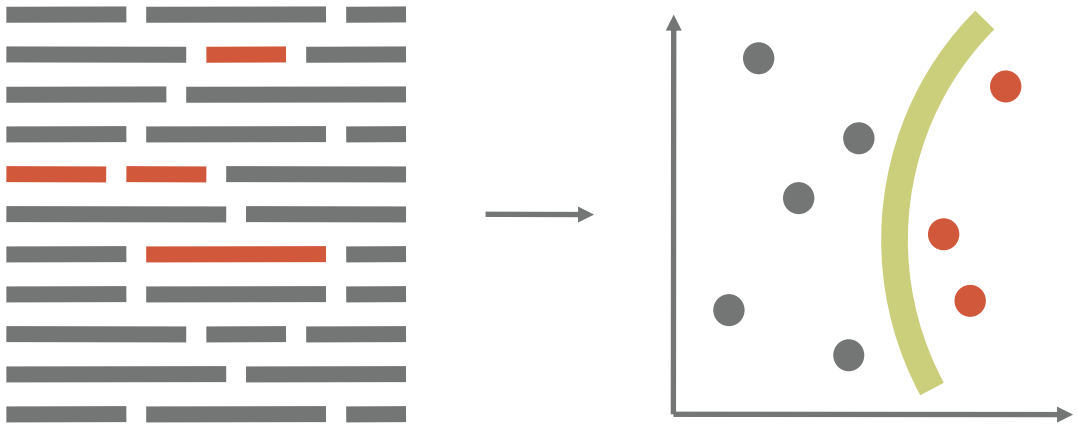
The Internet of Things

- Monitor and control an environment or process using multiple (wireless) sensors and actuators.
- Multiple possibly competing actors offering individual services.
- Often shared communication and computing infrastructures.

- IoT is target of attacks which severely impact privacy, robustness, performance and businesses of critical importance.
- Data-driven Intrusion Detection Systems (IDS): attacks and anomalies are detected and learned from previous examples.

UPPSALA
UNIVERSITET

Data-driven Intrusion Detection Systems

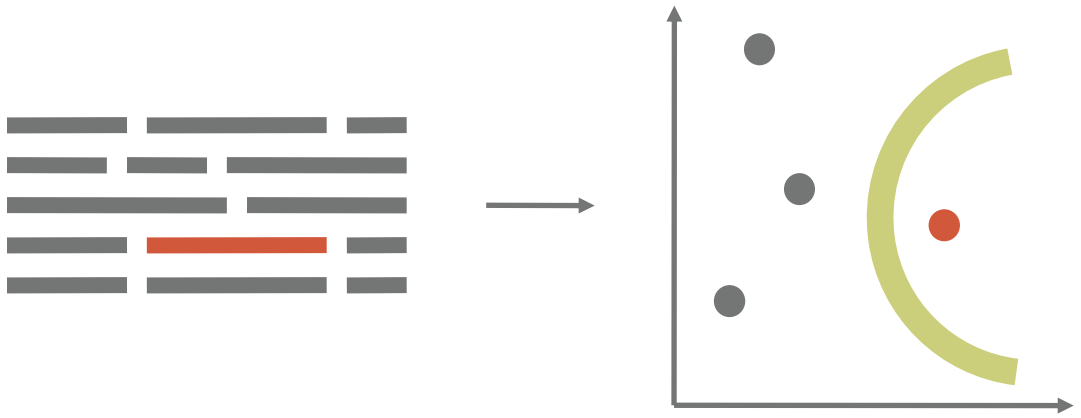


training data

classifier

Data-driven Intrusion Detection System

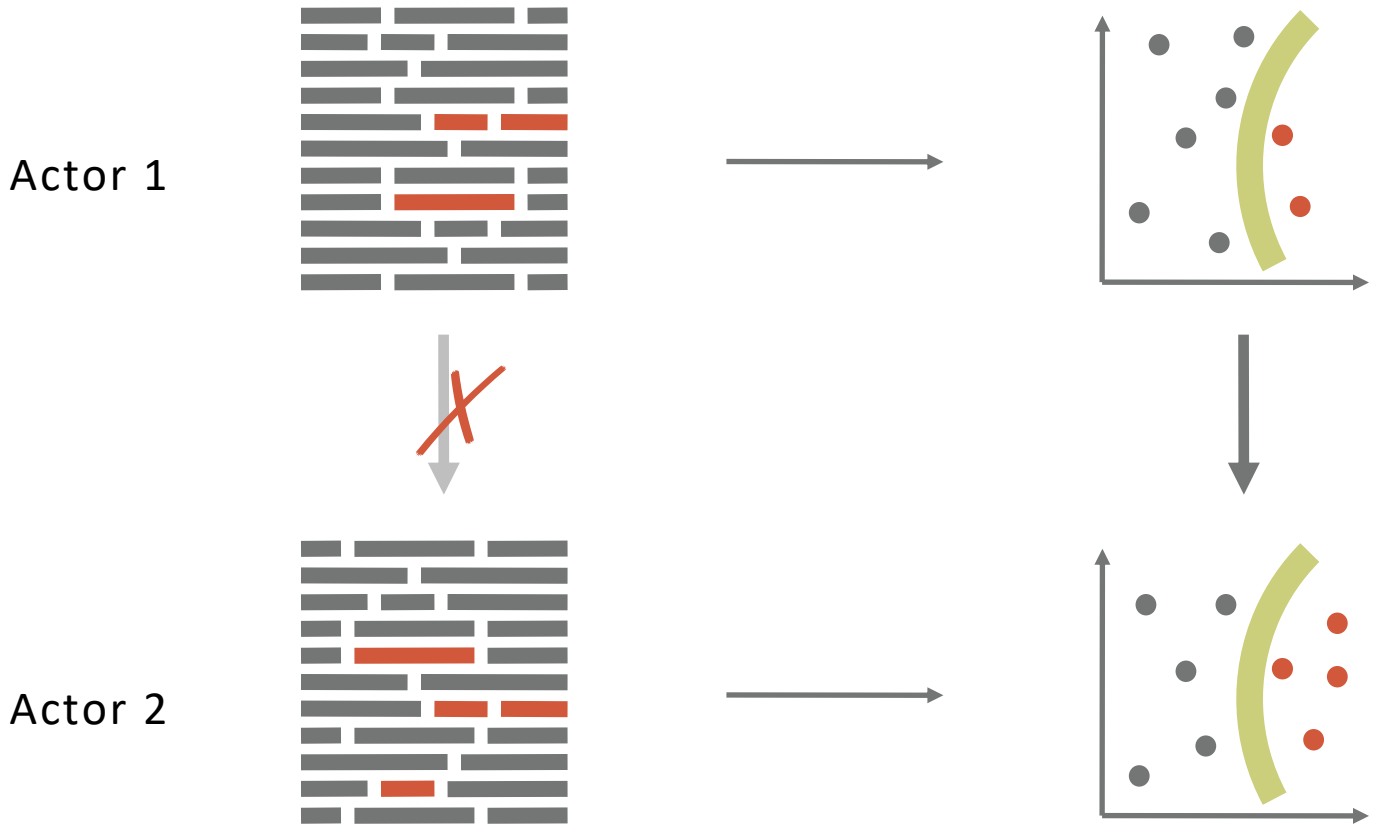
- Data availability Challenge: classification only as good as the data used to train



UPPSALA
UNIVERSITET

Private Knowledge Sharing

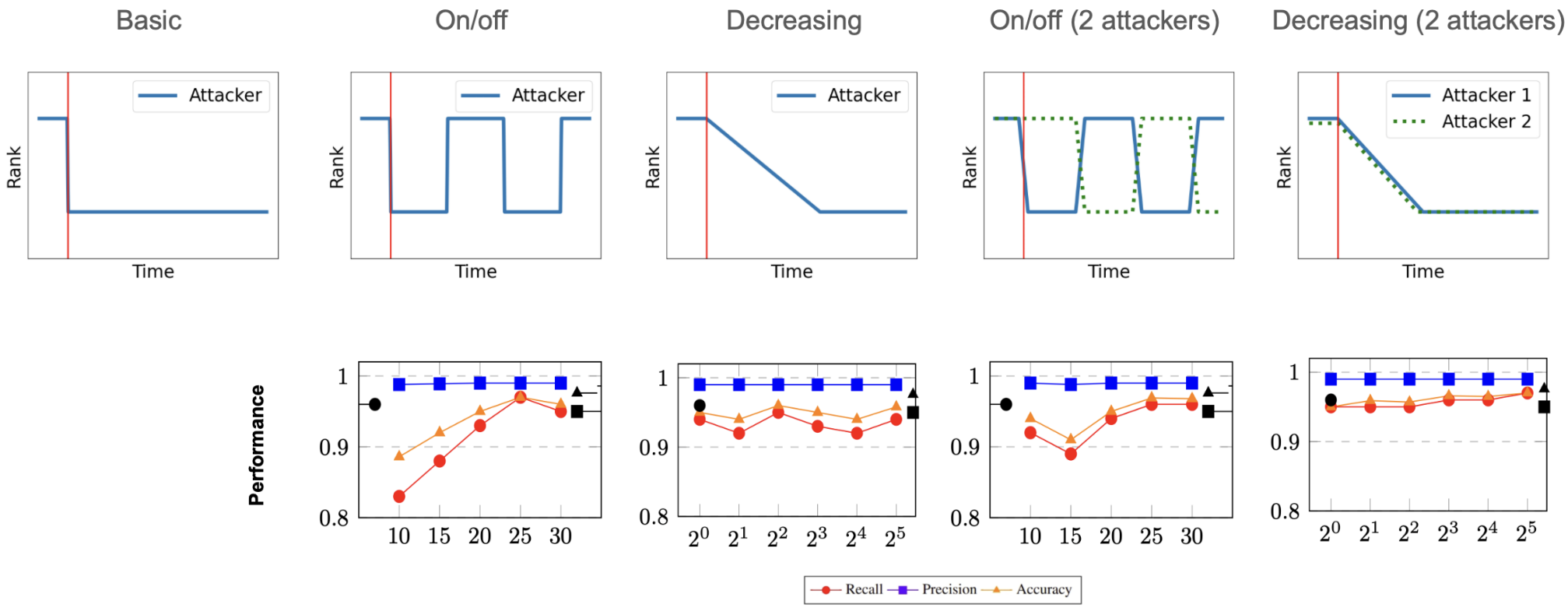
- Privacy Challenge: don't reveal attacks that were used in the training set



UPPSALA UNIVERSITET

Attack Variations for Robustness

- Blackhole Attack: change Rank in routing protocol to attract traffic.

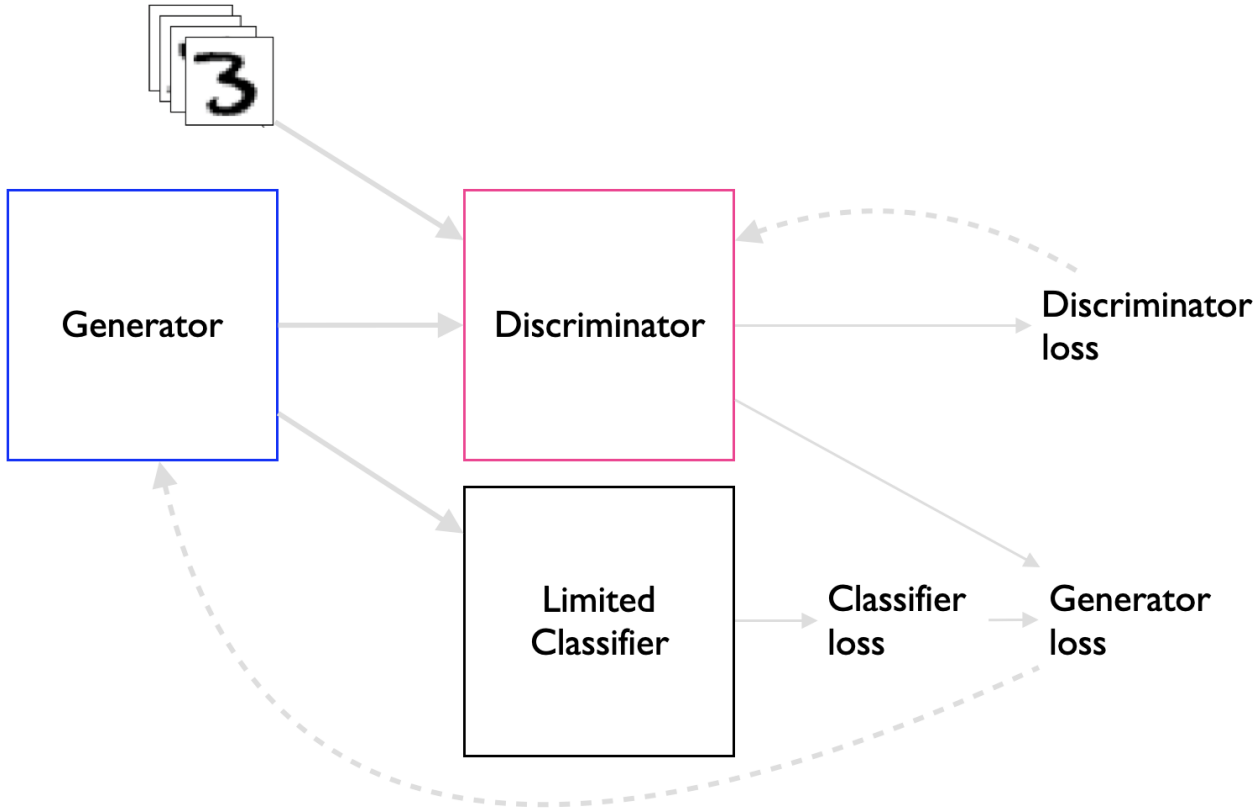


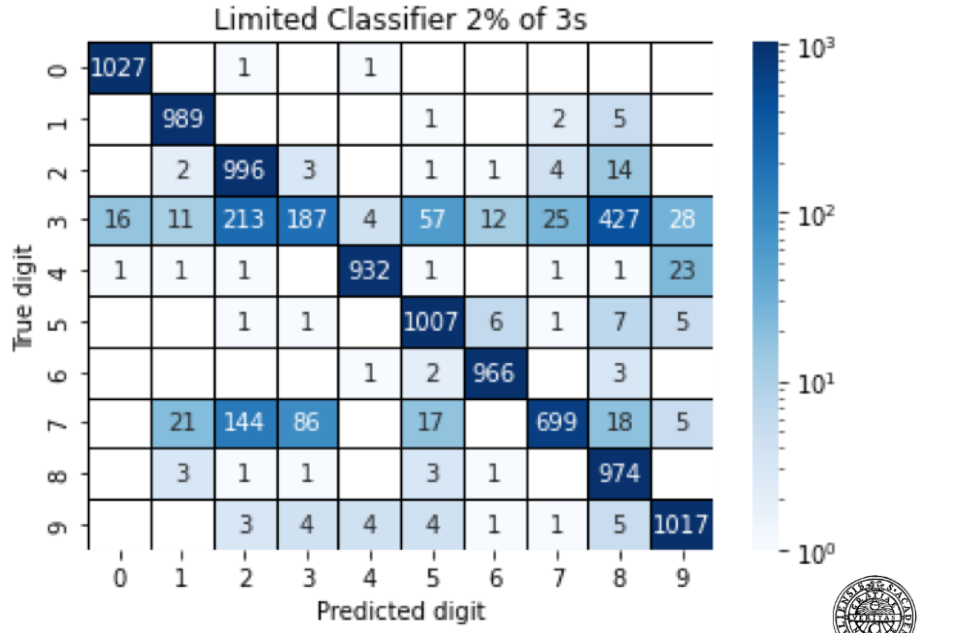
Credits: Amin Kaveh and Adam Pettersson

UPPSALA UNIVERSITET

Generative Adversarial Networks (GAN)

- Use GAN to create attack data variations.





Credits: Gustaf Bennmarker

UPPSALA UNIVERSITET

Contact

- Christian Rohner (Security and IoT expertise)
  christian.rohner@it.uu.se

- Andreas Johnsson (Network performance and ML expertise)
  andreas.johnsson@it.uu.se

UPPSALA
UNIVERSITET