An Architecture for Detection of Anomalies in Deterministic Time within Real-Time Communication Networks

Christian Maier, Jia Lei Du, Stefan Farthofer, Peter Dorfinger

email: christian.maier@salzburgresearch.at

salzburgresearch

Intelligent Connectivity

Salzburg, Austria

IARIA

CORETA 2021

November 14, 2021 to November 18, 2021

Presenter‘s Resume

- Studies of pure mathematics at TU Munich (BSc) and LMU Munich (MSc)
- Researcher and Data Scientist in the Intelligent Connectivity group of Salzburg Research since 2018

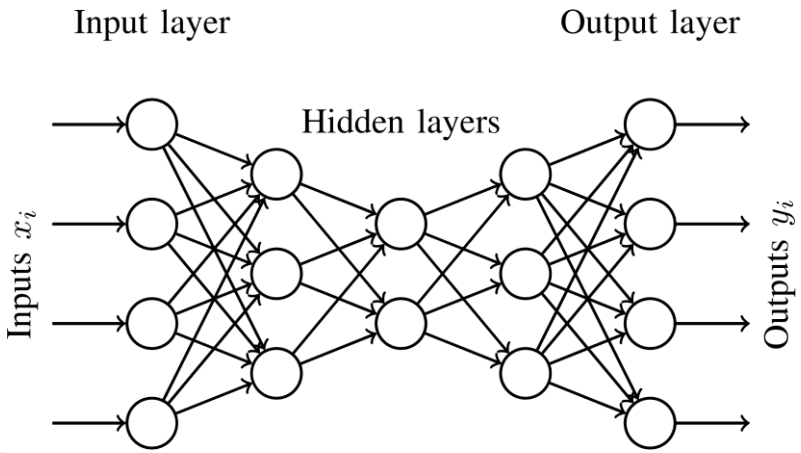
- Main topic of interest: Application of machine learning methods to networking
  - Supervised, unsupervised and reinforcement learning, mostly using (deep) artificial neural networks
  - In particular: Network modeling and performance prediction with Graph Neural Networks (GNNs)

Introduction & Motivation

- Current research topics in the networking domain:
  - Real-time communication networks
  - Application of Machine Learning (ML) methods, e.g., for anomaly detection
- Increasing relevance of real-time communication in cyber-physical systems within critical domains (e.g., manufacturing, smart energy grids)
- Crucial: **Timely** detection of anomalies in such scenarios
- ML approach / model mostly used for anomaly detection: Unsupervised learning with autoencoder neural networks
- **Combine real time communication networks and ML to provide an architecture for detection of anomalies in deterministic time**

Autoencoder Neural Networks (ANNs)

- Special types of Multi-Layer Perceptrons
- Input layer, output layer, hidden layers $h_1, \dots, h_k$
- Fewest neurons are located in the middle
- Number of inputs = Number of outputs



- Mean Squared Error (MSE) as loss function:

$$E = \sum (x_i - y_i)^2$$

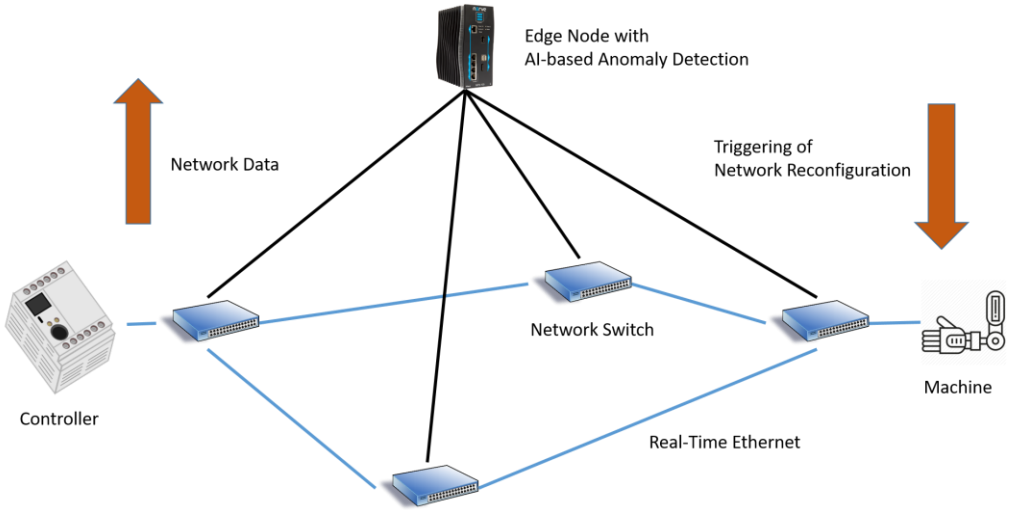
- $\rightarrow$ ANN learns to reproduce the inputs on the outputs
- $\rightarrow$ Information on the thinnest hidden layer serves as a low-dimensional representation of the input data
- ANNs can be interpreted as a composition $g \circ f$ of an encoding function f followed by a decoding function g

Architecture

- Real-time detection of anomalies for security (intrusion detection) or safety (component failure prediction)
- Edge node sniffs data from network, represented by vector $\boldsymbol{x} = (x_1, \dots, x_n)$ which changes over time
- Online training of ANN at edge node to obtain low dimensional representation of $\boldsymbol{x}$
- Stop training if MSE is sufficiently small (i.e. if MSE < ε for a chosen treshhold $\varepsilon > 0$)
- Monitoring mode: If MSE $\gg \varepsilon$, the vector $\boldsymbol{x}$ is assumed to be anomalous
- Computation of output values of ANN can be done in deterministic time
- $\rightarrow$ If all the connections in the network are real-time connections, the detection of anomalies is done in deterministic time as well

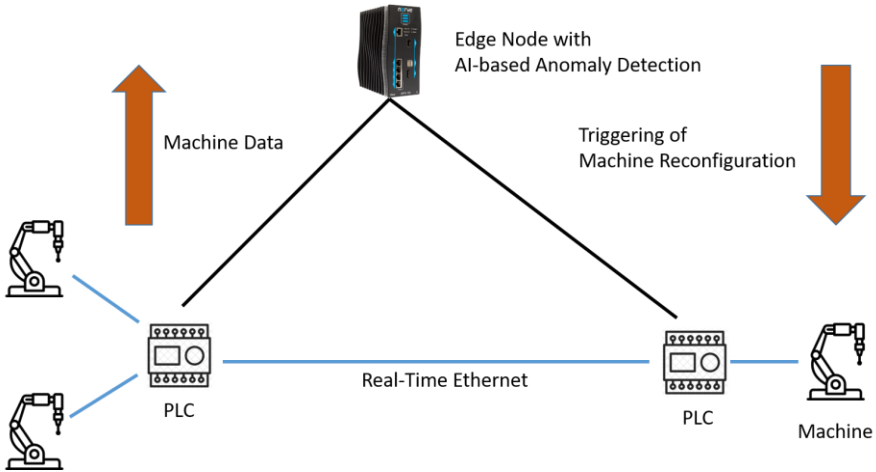
Architecture – Use Case 1

- Network data (delay values, jitter, traffic load, number or configuration of flows, …) collected at edge node
- Detected anomaly may indicate issue or attacker
- Edge node triggers SDN building blocks to reconfigure network configuration



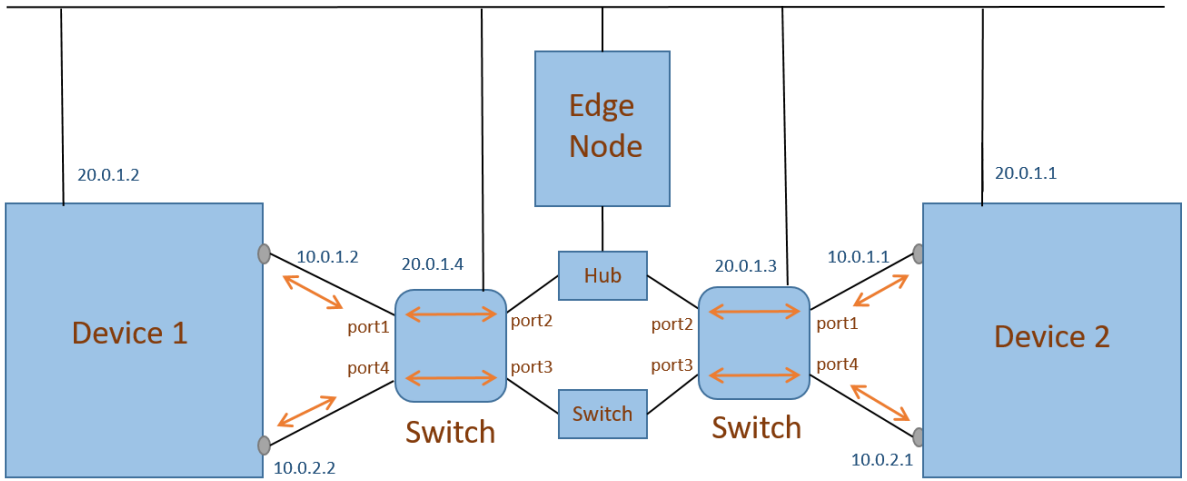
Architecture – Use Case 2

- Sensor values of machines collected at edge node
- Detected anomaly may indicate machine error
- Edge node triggers machine reconfiguration (predictive maintainence)



Proof of Concept Implementation

- Realized in our laboratory
- Devices connected through real-time Ethernet network



Proof of Concept Implementation

- Neural network at edge node implemented in Python, using TensorFlow framework
- 16 inputs $x_1, \ldots, x_{16}$
- 3 hidden layers with 12/8/12 neurons
- ANN achieved performance of $\mathrm{MS}E = 0.01$ after online training with $\approx 10^4$ samples
- Detected anomaly yields reconfiguration of network flows (e.g. shutting down network path, switching to another network path)
- All components operate in deterministic time → deterministic anomaly detection loop

Conclusion and Future Work

- Architecture for end-to-end deterministic anomaly detection system in real-time networks
- Autoencoder neural network at edge node detects anomalies
- Two use cases provided
- Demo implementation in one use case – Proof of concept
- **Future Work:**
  - **Perform measurements of the actual reaction time from anomaly detection to reconfiguration**
  - **Compare results to existing anomaly detection systems**

salzburgresearch

Thank you!

Christian Maier, MSc

Salzburg Research Forschungsgesellschaft m.b.H.
Jakob-Haringer-Straße 5/3 | Salzburg, Austria

Tel. +43 662 2288-457

christian.maier@salzburgresearch.at