Christian-Albrechts-Universität zu Kiel

Routing Optimization of QKD-Networks using Machine-Learning Based Prediction

Tim Johann[1], Daniel Giemsa[2], Sebastian Kühl[1], Annika Dochhan[1] and Stephan Pachnicke[1]

[1] Lehrstuhl für Nachrichtenübertragungstechnik, Christian-Albrechts-Universität zu Kiel

[2] Deutsche Telekom Technik GmbH

24. VDE ITG Fachtagung Photonische Netze

Leipzig, 22.05.2023

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

QuNET+ ML

Outline

1. **Motivation**
2. **Meshed QKD-networks**
3. **ML-based prediction**
4. **Results**
5. **Conclusion**

Motivation

- Progress in quantum computing challenges the conventional cryptography

Why QKD?

- Information-theoretical security

Challenges:

- No quantum repeaters available → limited reach
- How to realize meshed long-haul networks?
- How to control the network/which information should be shared?
- Limited keyrates

- Based on which rules should the routing take place?

- How to realize a QKD network in a German topology?
  - Nobel-Germany topology
    - → Extended with trusted nodes

Trusted Nodes (green):

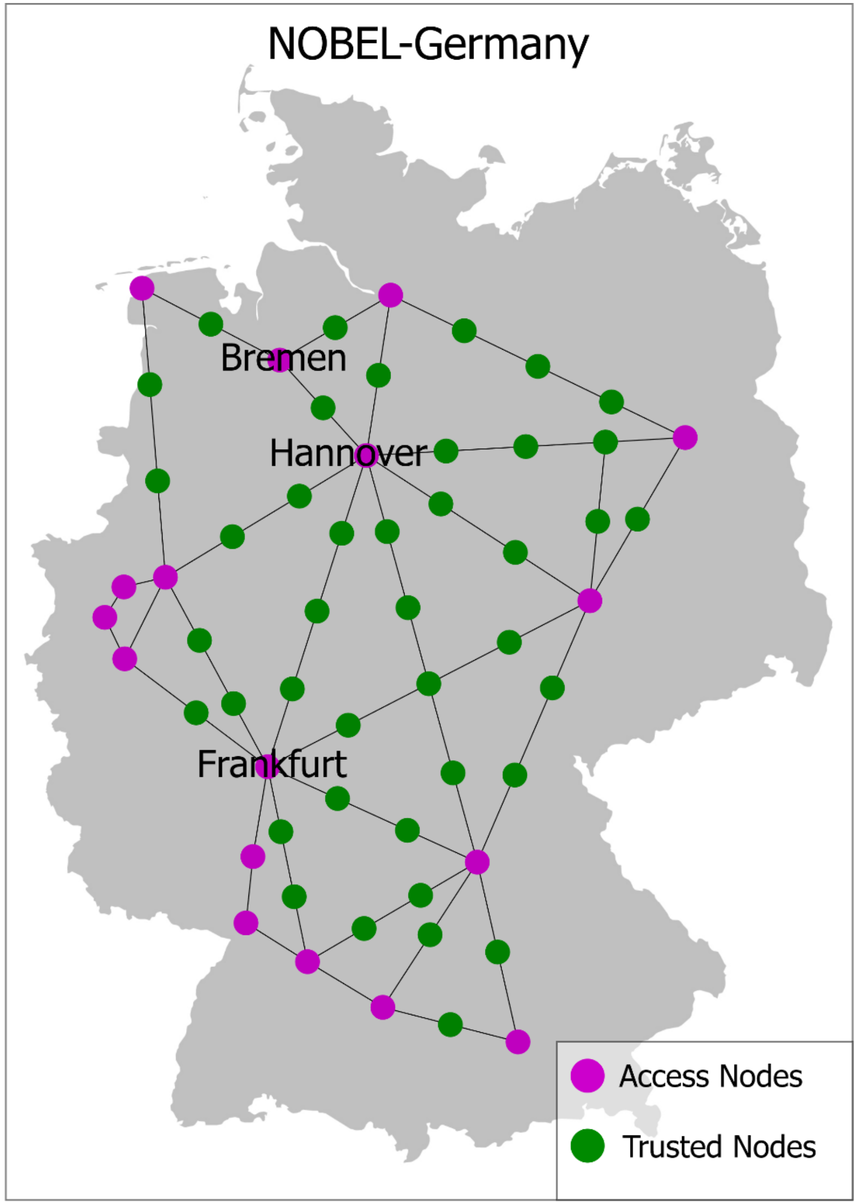
- Necessary due to reach limitations of QKD-devices
- Must be secured properly
- Placed equidistantly on the links

Secret Keys:

- Limited keyrate
  - → Precious resource
- One key to encrypt one GByte of data

Keystores:

- One substore per link



Routing Challenges

Challenges:

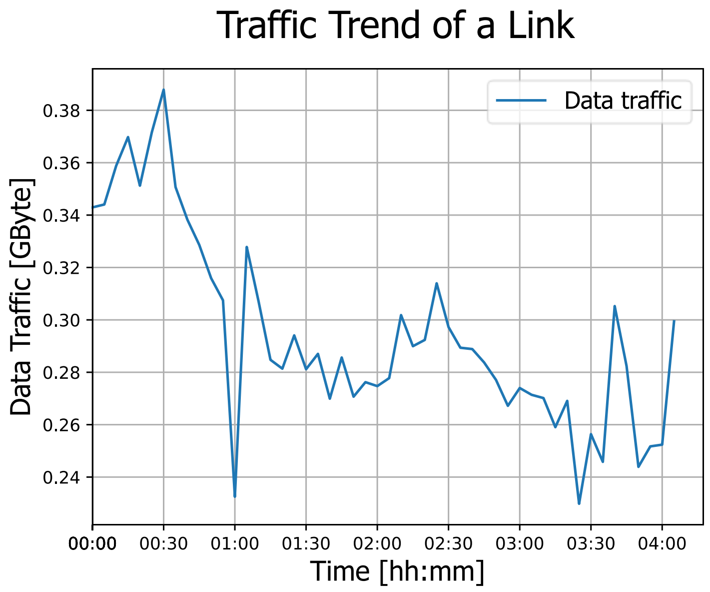
- Avoid keystores running empty

➢ What are the possibilities to route using limited information only?

- Simple hop-count based algorithm (Dijkstra)
- Include prediction of future key demands

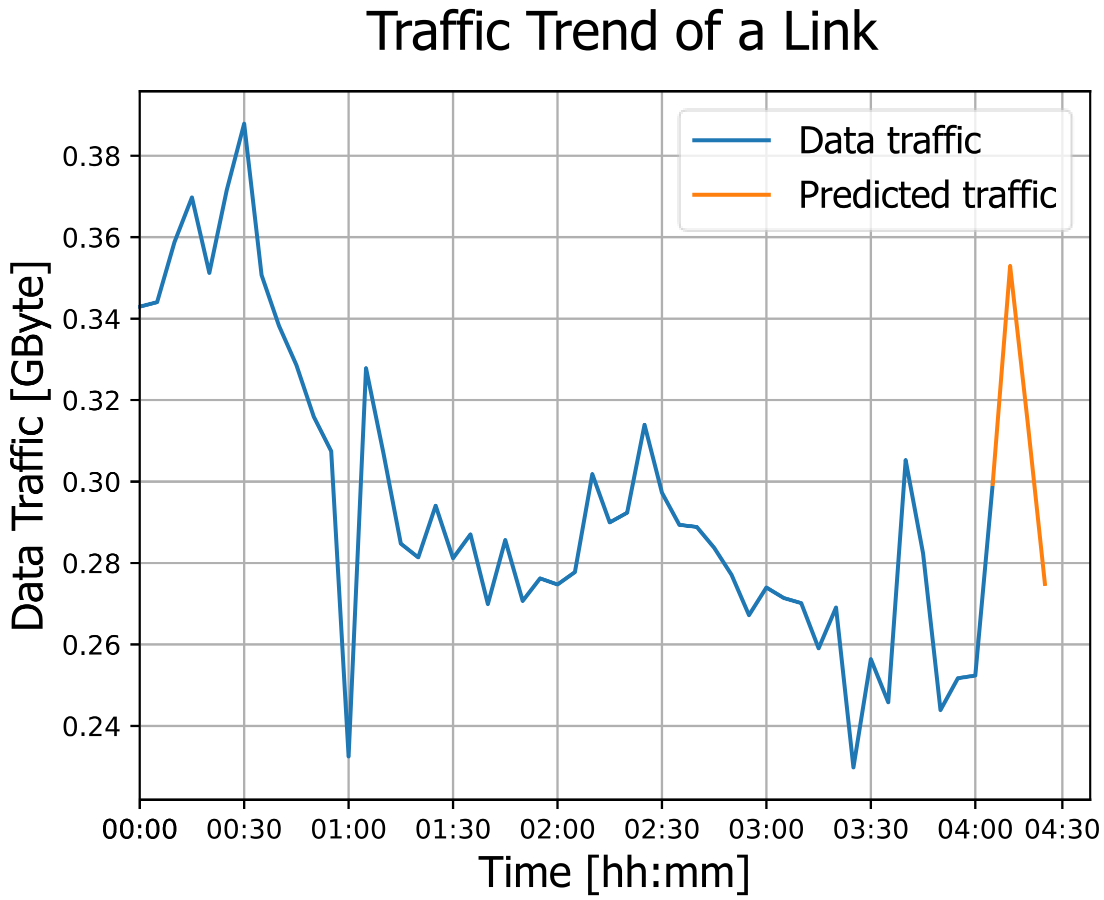
➢ Past demand matrices can be used to predict the future data traffic

- Information can be used to optimize weight of network edges
- Machine Learning is used for prediction



Traffic Prediction

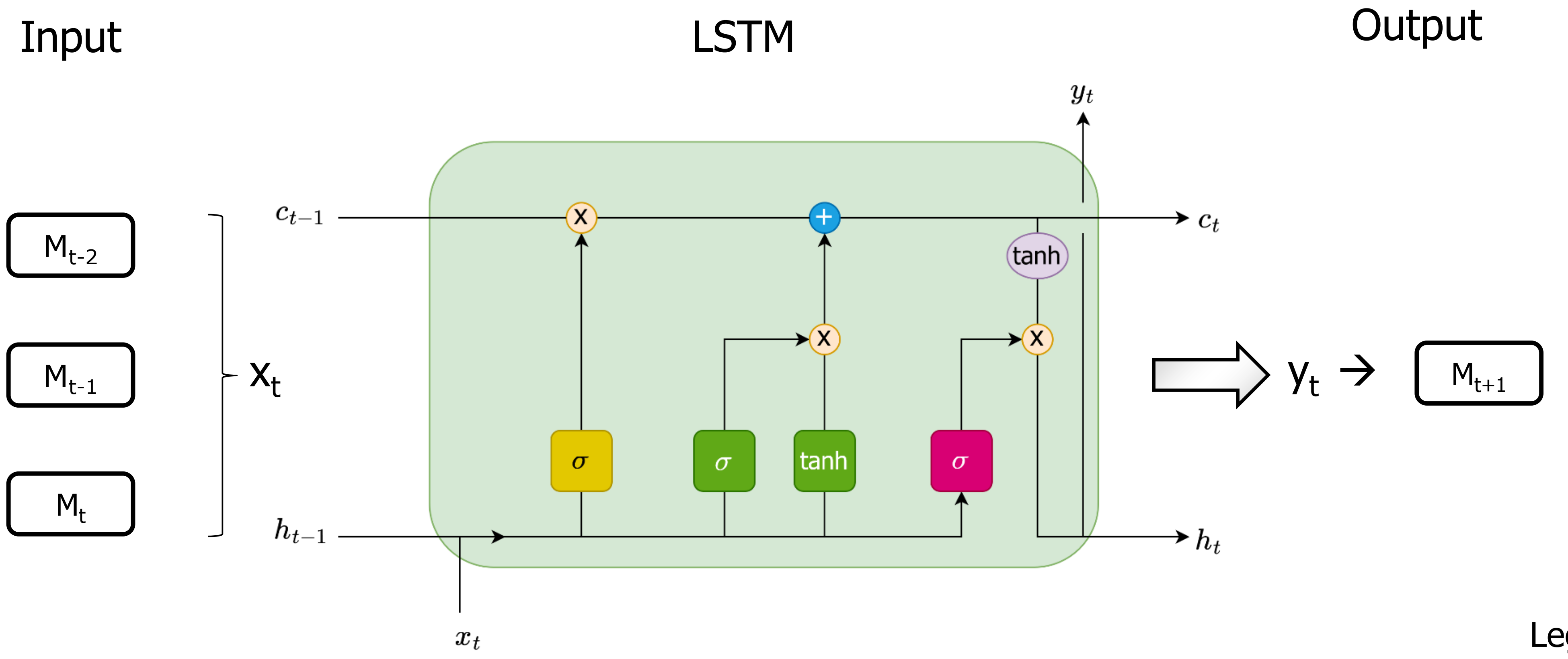
- Using prediction to proactively adapt edge weights
  - Execute Dijkstra based on these weights
    - → Leads to more balanced usage of network and avoids keystores to run empty



Simulation Fundamentals

- Dynamic traffic data: 24 hours → 5 minute intervals → 288 demand matrices → 73,512 demands
- Routing optimization based on (hypothetical) perfect prediction of demand matrices
- LSTM prediction of demand matrices based optimized routing algorithm
- One request per second
- Constant key generation
- Filled keystores (100,000 keys for each link)

LSTM for Prediction



- Three historic matrices as input
- One-step ahead prediction

Legend:

X_t = input

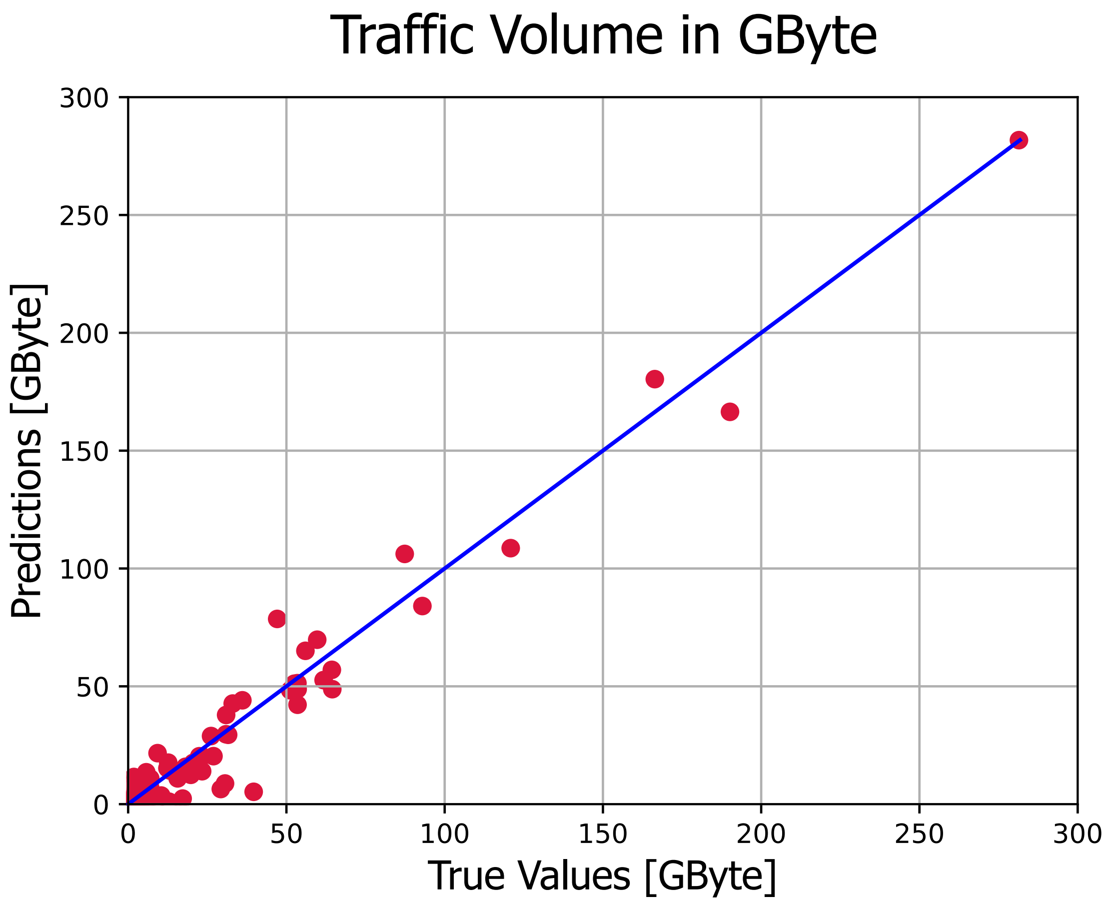
C_{t-1} = cell state

h_{t-1} = hidden state

Traffic Prediction Quality

Deviation between predictions and true values:

- Traffic matrices dominated by low volume demands

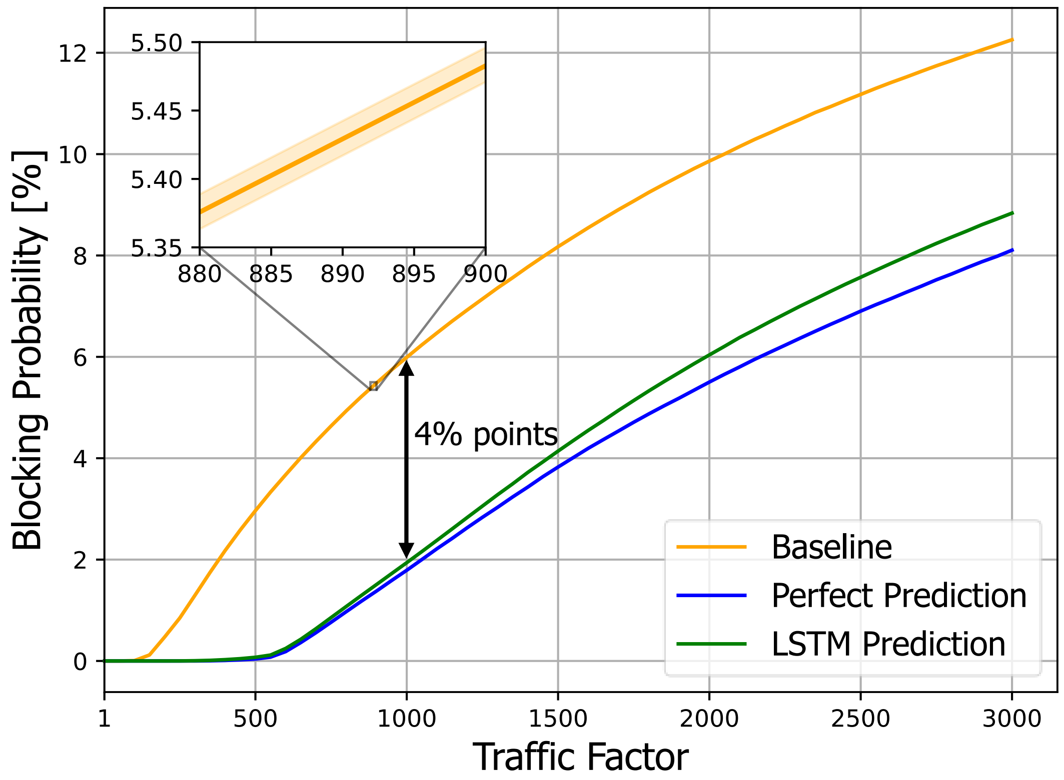


Investigation of Blocking Probability

➢ Increasing traffic factor for scaling of demands

Main goal: Reduction of blocking probability

- Significantly better performance of prediction-based algorithms (up to 4 percentage points)
- Higher traffic load factor → higher deviation between LSTM and perfect prediction



Investigation of Keystore Filling Level

- Exemplary visualization of the keystore filling level for a traffic factor of 1000

Baseline:

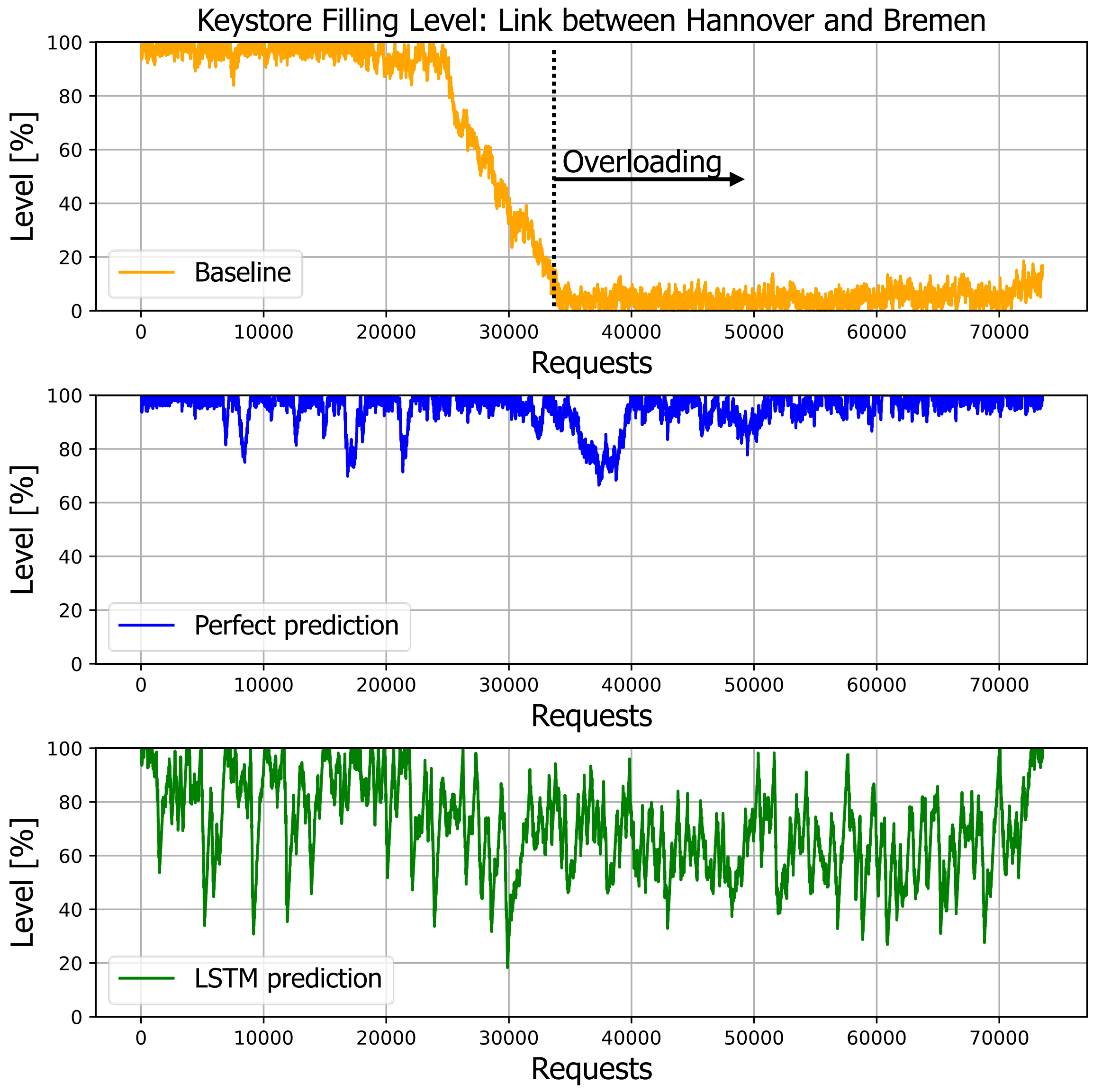
- Abrupt transition between „full"-state and a nearly empty keystore

(hypothetical) Perfect prediction:

- Keeps high level of remaining keys

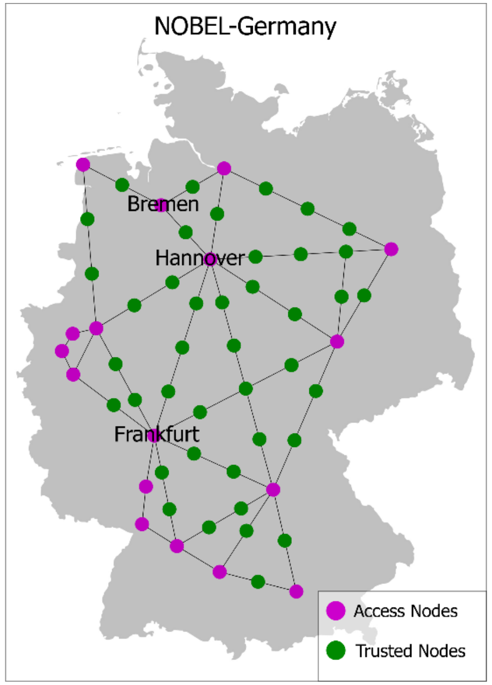
LSTM prediction:

- Higher fluctuation
- No overloading



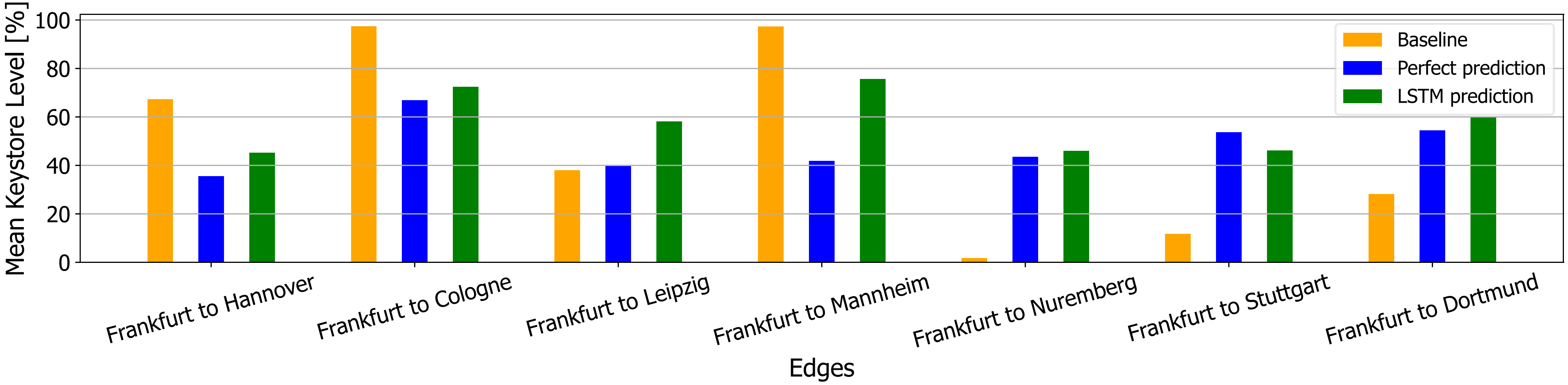
Investigation of Mean Keystore Level

- Frankfurt is one of the most heavily used nodes in the network



Results for a traffic factor of 1000:

- LSTM prediction enables more evenly distributed utilization
- Higher variance for the Baseline due hop-based approach
- (hypothetical) Perfect prediction performs similar to LSTM prediction



Conclusion

- Keystores running empty can be avoided by traffic prediction
- LSTM prediction performs better than hop-based routing

  → Blocking probability is reduced by up to 4 percentage points

  → Traffic load is distributed more evenly
- No sensitive information required

tim.johann@tf.uni-kiel.de

Acknowledgements:

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

QuNET+ ML

Thank you!