Image based Anomaly Detection in Automotive Networks

Mohammad Fazel Soltani supervised by Prof. Franz Korf

Contact: mohammadfazel.soltani@haw-hamburg.de *Hamburg University of Applied Sciences (HAW) Dept. Computer Science Berliner Tor 7, D-20099-Hamburg*

Attack Detection in vehicle networks

Discovered vulnerabilities on attack surfaces can make the **in-vehicle network susceptible to attacks** [1], emphasizing the need for robust **security measures**. With the increasing use of **real-time Ethernet to ensure Quality of Service** [2] in future in-vehicle networks, it becomes crucial to detect anomalies in network behavior. Real-time communication exhibits distinct temporal and structural patterns as normal behavior. **Attacks cause anomalies** of the normal network behavior that are **detectable with image-based deep learning models** [3,4,5].

Foundation of the approaches

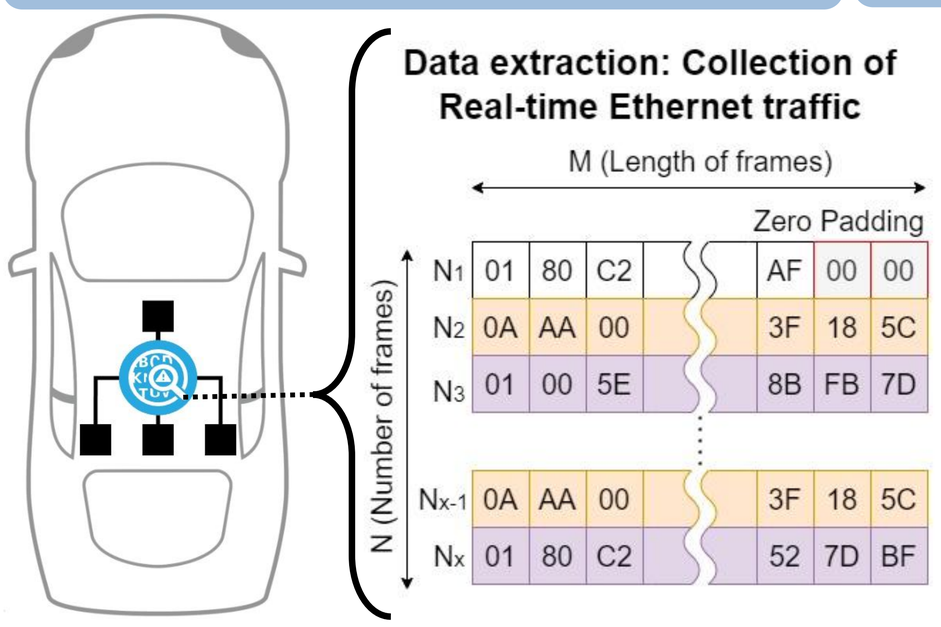
Similar steps of Jeong, S. et al. [4] and Han, M.L. et al. [5] can be used in the following to detect anomalies in automotive networks:

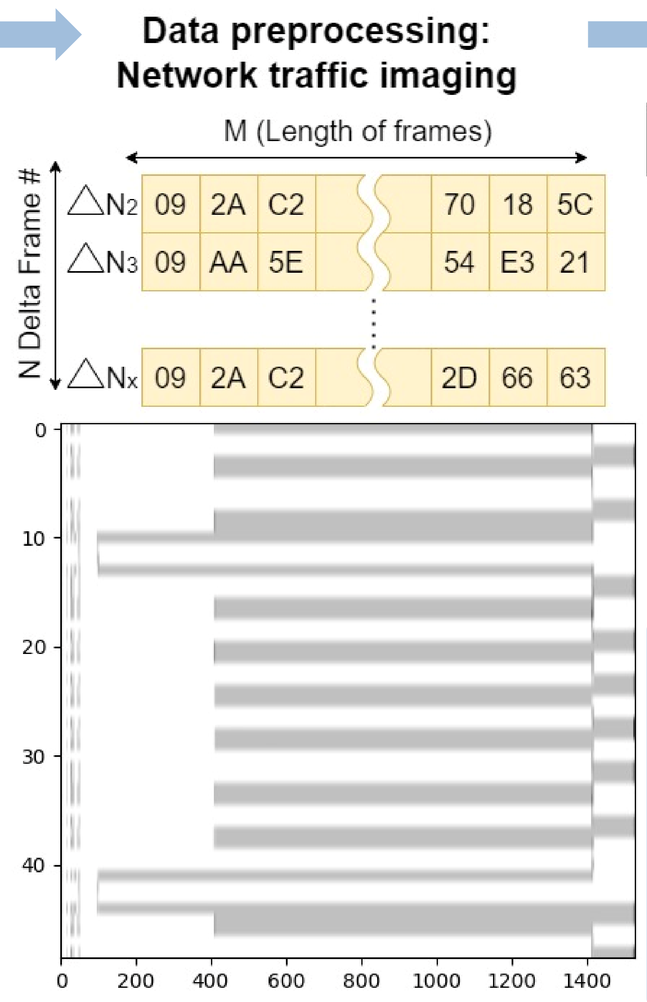
- **Data extraction:** A number of frames (N) with different lengths (M) are extracted. M has to fit to a desired length. Frames can come from single [4] or multiple [5] network traffic and represent normal communication behavior.
- **Data preprocessing:** Delta frames are computed from sequences of frames and transformed to images [4,5].
- **Data analysis:** For anomaly detection, the generated images serve as input and are trained with them. The reconstruction of each image ideally corresponds to the input.

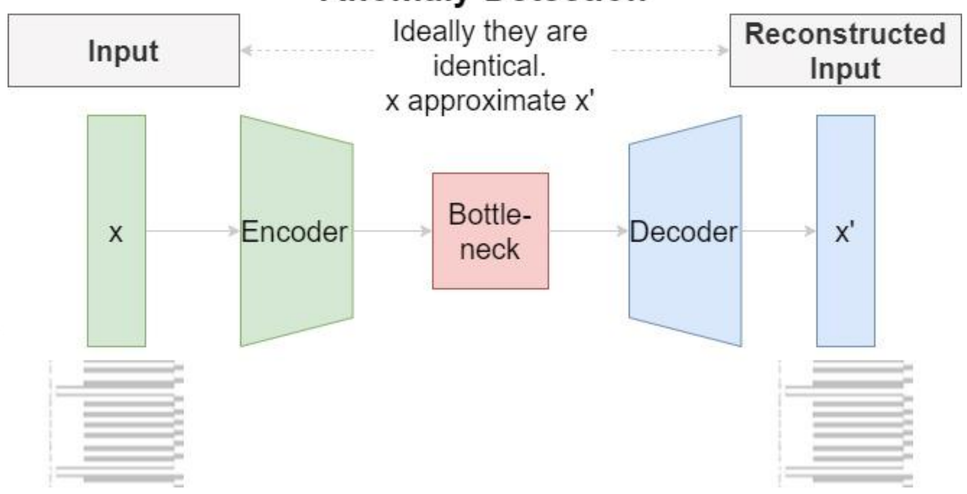
Potentials

This approach enables a **hybrid solution** combining anomaly detection and intrusion detection and could detect both known and unknown attacks.

Moreover, more **complex neural network structures** can be constructed from different input images. For example, images that uses temporal aspects in the automotive network can be additionally generated. The different input images are trained separately, and their output is passed as input to a deep learning architecture.







Future Roadmap

- **Base project**: Implementation of Tool Chain | Dataset generation from simulation based automotive network | Test framework
- **Main project**: Extend tool chain to generate temporal aspects in images and compare with targeted approach for anomaly detection.
- **Master thesis**: Research and development of an effective anomaly detection method for vehicular networks considering temporal aspects and the use of image-based data representations.

References

[1]: Checkoway, S., et al. "Comprehensive experimental analyses of automotive attack surfaces." USENIX security symposium. Vol. 4. No. 447-462. 2011.
[2]: IEEE 802.1 Working Group: IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks. Standard Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014), IEEE (Jul 2018).
[3]: Suzuki, A., et al. "Reverse Reconstruction of Anomaly Input Using Autoencoders." 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS). IEEE, 2018.
[4]: Jeong, S., et al. "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks." Vehicular Communications 29 (2021): 100338.
[5]: M. L. Han, et al. "TOW-IDS: Intrusion Detection System Based on Three Overlapped Wavelets for Automotive Ethernet." IEEE Transactions on Information Forensics and Security 18 (2022): 411-422.