secVI

Security for Vehicular Information

HAW HAMBURG

easycore

automotive engineering iav

Sponsored by the
Federal Ministry
of Education
and Research

Introduction

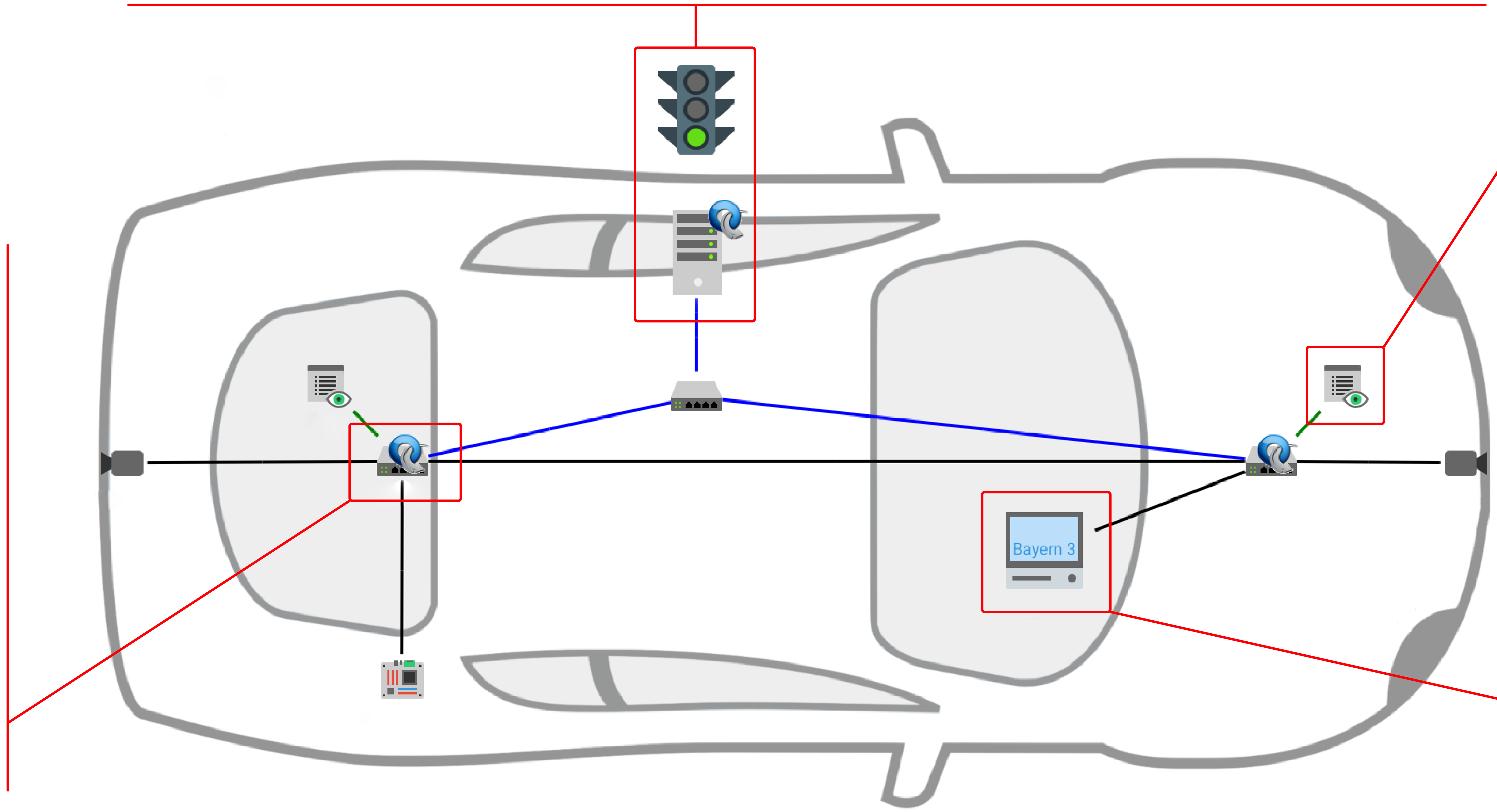
SecVI designs and analyses network security architectures that are flexible, robust, and of reduced complexity to protect the entire communication system of a vehicle. Work includes the verification of online updates as well as continuous monitoring of flows between ECUs and network components. Flow monitoring is a good technique to prevent cyber-attacks on the vehicle in a robust way while keeping most existing components of the vehicle unchanged.

Software-Defined Networking

- The control plane of network devices is separated from the data plane.
- An SDN-Controller is introduced to program the network devices.
- The flow based forwarding devices of the data plane are connected to the SDN controller via the OpenFlow protocol.
- This allows for a central management of all flows with comprehensive control functionality, management applications and security functions.

Security Cluster

- The Security Cluster monitors the security state of the in-vehicular network.
- It hosts the SDN-Controller and is connected to the forwarding devices in a separate control network.
- Has knowledge about all implemented flows and is able to add, modify and delete flows.
- Collects the reported anomalies of NADS's and flow table misses of forwarding devices.
- The Security Cluster initiates adequate countermeasures if possible.
- Defence mechanisms range from adding or removing flows to disconnecting certain nodes at the forwarding devices.



Network Anomaly Detection System

- An NADS is connected to each switch.
- NADS analyses network metrics such as the utilised bandwidth and average frame size per flow.
- Machine learning with the K-means clustering algorithm is used to learn the flow behaviour.
- Outliers of the learned clusters are recognised as anomalies and reported to the Security Cluster.

Attack Scenarios

Simple Message Attack

- Messages do not match any existing flows.
- First switch on the path reports a flow table miss to the Security Cluster.

Flow Hijack Attack

- Messages match an existing flow and are forwarded along the programmed path.
- The NADS detects misbehaviour and reports it to the Security Cluster.

In both scenarios the Security Cluster can execute countermeasures.

Website: https://secvi.inet.haw-hamburg.de