SIGNS WITH SMART CONNECTIVITY FOR BETTER ROAD SAFETY

PROBLEM SOLUTION FIT:

Smart intersections help to address increasing traffic density and improve road safety. By leveraging data from infrastructure sensors, and combining and supplying those data to road users, their perception can be improved. This aids in protecting vulnerable road users (VRUs) and acts as a crucial building block for enabling automated and autonomous driving.

Increasing volumes of traffic are using municipal road infrastructure, with severe consequences for traffic efficiency and the safety of road users. Vulnerable roads users (VRUs), such as pedestrians or cyclists, are involved in 46 % of lethal accidents [1]. Exchanging information between road users increases their perception and is thus a critical building block to improve this situation.

The Smart Intersection, developed by Fraunhofer Institutes IVI, AISEC, HHI and IIS in the IoT-COMMS project [L1] from 2018 to 2019, installs cameras at traffic junctions to monitor traffic. Those cameras send real-time and high-quality video to a road-side-unit (RSU), which detects and classifies objects such as pedestrians or cars. Together with additional information such as position, speed and direction of movement, they are stored in a dynamic object map. The object map is then transferred from the RSU to cars via WLANp or LTE/5G-V2X.

This approach facilitates the cooperative perception of surroundings, enabling road users to utilise information from other sensors. Thus, they can recognise obstacles and other road users out of plain sight, which prevents accidents and allows more efficient traffic flows (Figure 1).

While modern cars can already utilise sensor-based object detection, parametrisation and categorisation of objects from within the moving car is challenging. Shifting those tasks to road infrastructure, on the contrary, allows reliable distinction between static and dynamic objects. Using spatially stationary cameras permits “learning” the area under surveillance, enabling early detection of critical situations and a quick reaction to them.

Previous approaches lack the bandwidth to transmit raw camera images between infrastructure components and thus transfer only detected objects. This limits the effectiveness of the object detection and impedes the comparison of detected objects, as each camera sees only a particular part of the big picture.

Design

The smart intersection, on the other hand, utilises high-speed mmWave transmission technology by Fraunhofer HHI to transmit raw video frames from multiple cameras to the RSU. There, object detection is performed using background subtraction algorithms developed by Fraunhofer IVI. Subsequently, objects are classified, for example “passenger car”, “cyclist” or “pedestrian” from multiview data. To do so, Fraunhofer HHI employs convolutional neural networks. In addition, classification accuracy is improved over time and trajectories can be calculated, permitting tracing of temporarily occluded objects.

The key benefit of this centralised detection and classification approach is that information from all cameras can be used. Thus, the same object can be seen in multiple perspectives, improving the detection quality significantly and increasing the area that can be perceived.

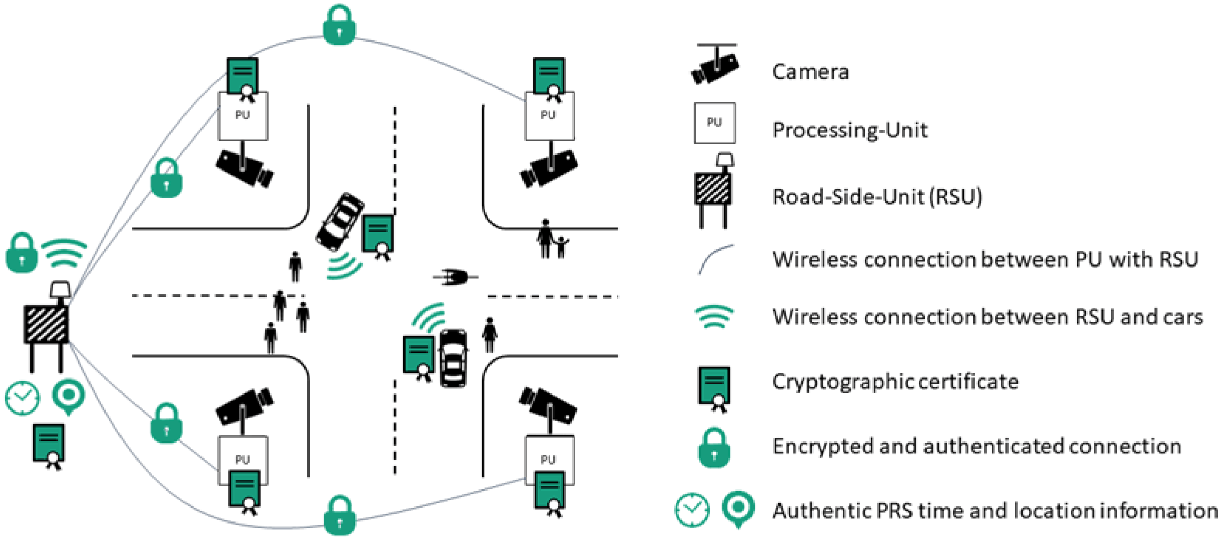
The object map is then written into a standardised collective perception message (CPM) and transferred from the RSU to cars via WLANp or LTE/5G-V2X. Thus, vehicles are enabled to expand the range of their own sensors significantly and safety-critical situations can be detected and controlled earlier or more safely at higher speeds.

Security and Privacy Concept

Another key component of the Smart Intersection is the security concept for protecting data against attackers. To provide security by design, the modular risk assessment (MoRA) method of Fraunhofer AISEC was applied [2]. MoRA permits systematic collection and assessment of security goals, threats and countermeasures, resulting in a holistic and traceable security concept.

Human drivers and, in the near future, autonomous cars base decisions on information supplied by the smart intersection, relying on the authenticity of information. Thus, it is important to ensure that the smart intersection captures authentic information and that the data has not been altered throughout transmission and storage.

To ensure camera image authenticity, the RSU utilises a PRS Snapshot Sensor by Fraunhofer IIS, which captures tamper-proof Galileo PRS signals. This is used to apply unforgeable position- and time-stamps on the camera images and the generated object list. Public-key cryptography is used to sign and encrypt all messages during transmission and storage. Tamper-proof hardware prevents physical attacks. Figure 2 shows the smart intersection and the security concept.


PU
PU
PU
PU
Camera
PU
Processing-Unit
Road-Side-Unit (RSU)
Wireless connection between PU with RSU
Wireless connection between RSU and cars
Cryptographic certificate
Encrypted and authenticated connection
Authentic PRS time and location information

To comply with data protection regulations, the centralised detection and classification of objects permits the localisation and anonymisation of number plates and faces of pedestrians in camera images. However, authorities desire to use the raw, i.e. not anonymised, video data captured by the smart intersection to investigate accidents. Confidentiality and authenticity of those images is ensured via cryptography as described above. Unlike standard camera surveillance systems, our solution stores all camera data encrypted in a trust-storage hosted in a high-security facility. Thus, these data can only be accessed after a judicial decision.

A proof-of-concept demonstration of the smart intersection has been deployed at Fraunhofer IVI in Dresden and will be used in further evaluation. We plan to enhance the intersection with further data-acquisition capabilities, transforming it into a primary building block of smart cities