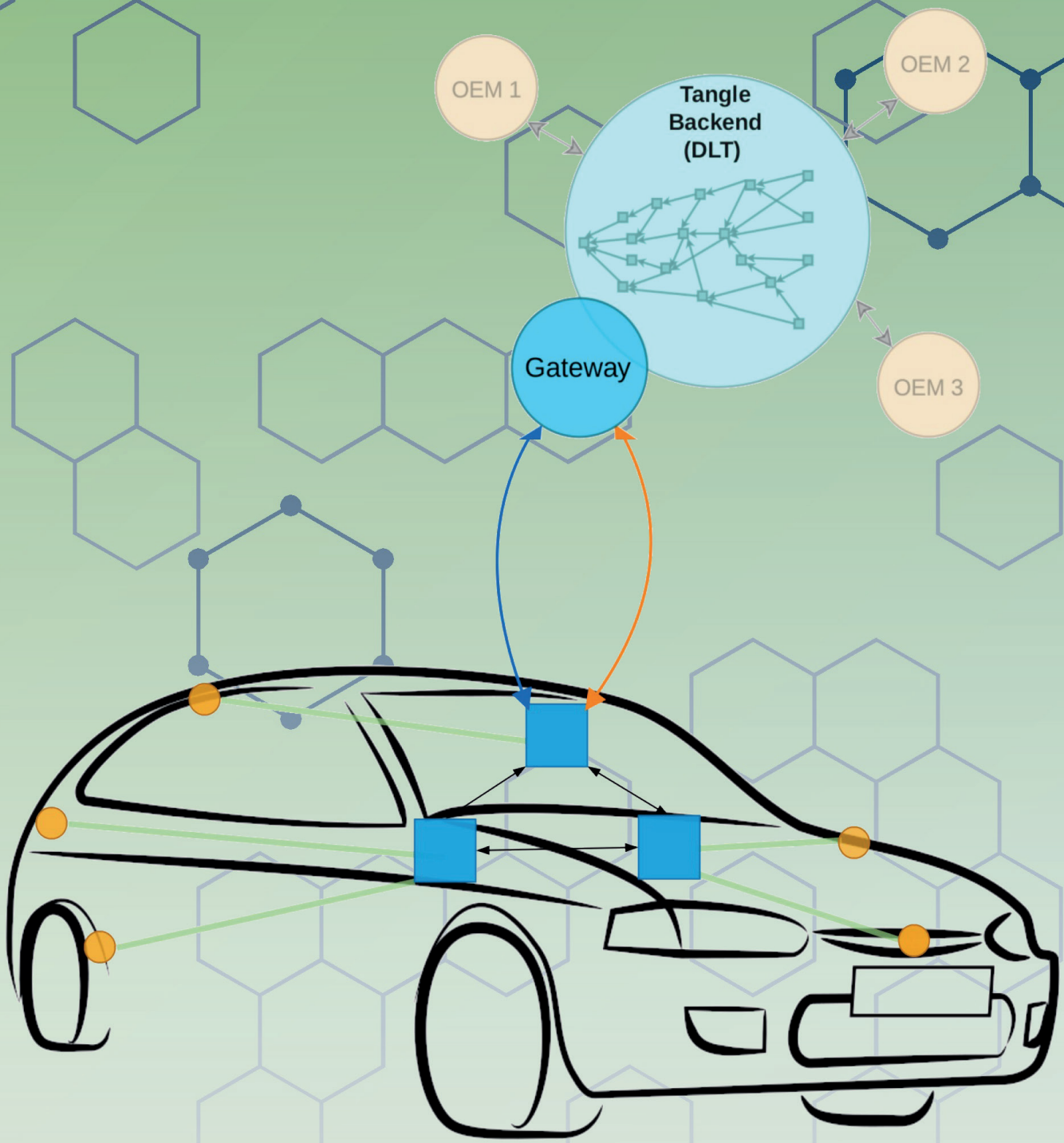
TECHNISCHE HOCHSCHULE DEGGENDORF



VITAF

SICHERE INTRA- UND INTERCAR-KOMMUNIKATION DURCH NACHWEISLICHE VERTRAUENSWÜRDIGE IDENTITÄTEN.

VITAF

Weitere Infos

Abstract

Projekttitel/ Project title:

VITAF – Vertrauenwürdige IT für Autonomes Fahren

Einleitung/ Introduction:

In Zukunft werden Kraftfahrzeuge zunehmend miteinander und mit der Außenwelt vernetzt sein. Sie legen Wegstrecken teil- oder vollautomatisiert zurück. Sowohl die Datenkommunikation als auch die Datenverarbeitung bedarf daher einer umfassenden Absicherung. Die Fahrzeuge müssen insbesondere vor Hackern geschützt werden, die in Fahrzeugsysteme einbrechen und diese manipulieren. Bisher scheiterten Sicherheitskonzepte häufig an nicht ausreichend zur Verfügung stehenden Rechenleistungen im Fahrzeug. Neue Formen lokal verteilter Datenverarbeitung (Edge- oder Fog-Computing) eröffnen nun neue Möglichkeiten.

Ziel/ Aim:

Ziel des Projektes VITAF ist es, ein System zu entwickeln, das Hackerangriffe auf autonome Fahrzeuge schnell erkennt und wirksame Gegenmaßnahmen einleitet. Dabei soll der Datenaustausch zwischen den Fahrzeugen und ihrer Infrastruktur nicht unterbrochen werden, damit ein sicherer Betrieb im Verkehr auch im Falle einer Cyberattacke gewährleistet bleibt. Zur sicheren Datenübertragung werden verschiedene Kommunikationsprotokolle etabliert: Zwischen einzelnen Steuergeräten im Fahrzeug selbst, zwischen den verschiedenen Fahrzeugen (Vehicle-to-Vehicle [V2V]) sowie zwischen Fahrzeugen und der Infrastruktur, wie etwa Verkehrsleitsystemen (Vehicle-to-Infrastructure, [V2I]). Daten vieler verschiedener Sensoren sollen ausgewertet und auf Auffälligkeiten in der Datenkommunikation untersucht werden. Bereits vorhandene, betriebsbewährte Ansätze aus der IT wie Datenverschlüsselung durch kryptografische Methoden werden weiterentwickelt und auf die Automobilwelt übertragen. Im Projekt werden darüber hinaus juristische Fragestellungen zum autonomen Fahren bearbeitet. Bereits bei der Technikgestaltung werden datenschutzrechtliche Fragen berücksichtigt – beispielsweise Probleme, die durch die Verschleierung der Fahrzeugidentität mit pseudonymisierten Token entstehen können. Die Evaluierung der neu entwickelten Technologie erfolgt abschließend an einem dafür entwickelten Demonstrator.

Methode/ Method:

Basierend auf der Theorie, dass innerhalb einer Fahrzeugarchitetkur eine Zero-Trust-Zone besteht, werden ,ausgehend von einer einzelnen ECU, (Electronic Control Unit) Methoden erforscht, um die Integrität zweifelsfrei nachzuweisen. Ausgehend von diesen Erkenntnissen wurde das Konzept zur Sicherung der Komponenten deduktiv auf die Gesamtarchitektur angewendet. Zur abgesicherten Kommunikation zwischen den ECUs innerhalb der Hierarchie wird ein leichtgewichtiges Verfahren entwickelt, was bereits auf Layer 2 des ISO/OSI-Modells angesiedelt ist. Diese Verbindung soll durch Verfahren der Post-Quantum-Kryptographie gesichert und dennoch ressourcenschonender als der MACsec-Standard (IEEE 802.1AE) sein.

Ergebnis/ Result:

Erfolgreiche Erzeugung eines simulativen Fahrzeugnetzwerkes mit hierarchischer Verifizierung der Gesamtintegrität, sowie sicherer Kommunikation der ECUs auf Sicherungssicht-Ebene. Weiterhin wurde nachgewiesen, dass das Auslagern von kryptographischen Operationen als ressourcenschonendes und effizientes Verfahren innerhalb einer Fahrzeugarchitektur genutzt werden kann.

Projektbeteiligte/ Project participants:

Enrico Weigelt, Kumar Ashutosh Anand, Paul Rauch, Diana Schramm

Projektpartner/ Project partners:

AVL-Solutions, b-plus, easycore, Frauenhofer SIT, Technische Universität München, Technische Hochschule Deggendorf

Gefördert durch/ Funded by:

Bundesministerium für Bildung und Forschung

Logos/ Logos:

Wird nachgereicht

insgesamt maximal 450 Wörter/ limit of 450 words in total