CONNECT - Continuous and Efficient Cooperative Trust Management for Resilient CCAM

CONNECT
CCAM TRUST & RESILIENCE

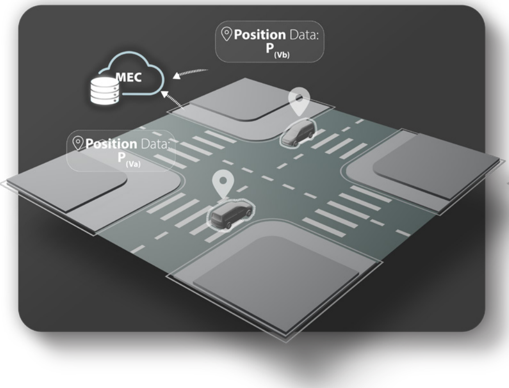
We are heading towards a future of **connected, cooperative, and automated mobility (CCAM)**. Fuelled by advances in automated driving and communication technologies like 5G cellular vehicle-to-everything (C-V2X), these developments will enhance the contemporary automated/autonomous driving functionalities and facilitate the next generation of cooperative autonomous driving applications (e.g., intersection movement assist, fleet management systems, cooperative routing, and parking services) and will extend the vision of Cooperative Intelligent Transport Systems (C-ITS) which was investigated and developed since the early 2000s to improve road safety, traffic efficiency, and sustainability.

With the increased connectivity and cooperation among different heterogeneous systems that are produced by different manufacturers, operate in highly dynamic, changing, and uncertain environments, and provide safety-critical services, the notion of trust is becoming a major concern and critical property of these systems [1]. The multiparty nature of these systems do not only include the vehicles themselves but also infrastructure technologies like **Multi-access Edge Computing (MEC)** and the cloud backends. Failures or attacks on one part of the system will have consequences throughout the overall System-of-Systems (SoS).

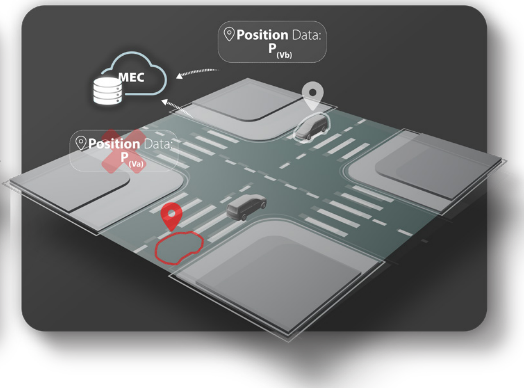
CONNECT's main mission is to enable a dynamic and continuous assessment of trust in a CCAM system and to investigate mechanisms that provide increased trust assurances compared to today's systems. By this, the abstract notion of trust should become quantifiable, assessable, and thus practically usable to enhance the security and safety of CCAM systems.

Motivational Example

The dynamic nature and the heterogeneity of the CCAM applications, as well as the dynamic environments in which the systems operate, dictate that no initial trust between entities can be assumed. In response, we follow the Zero Trust security principle: **"Never Trust, Always Verify"**. Therefore, we need to explicitly establish sufficient level of trust into remote entities, so they trust one another to collaboratively execute safety-critical tasks. For example, if we consider a scenario from the Cooperative Intersection Management use case [2], where two vehicles drive towards an intersection, then we require a trust assessment mechanism that answers the question "How much trust can vehicle V_A put into vehicle V_B to cooperatively execute a specific function (e.g., safely passing the intersection)?".



INTERSECTION CROSSING WITHOUT COLLISION



INTERSECTION CROSSING WITH A COLLISION

Two vehicles drive towards an intersection, and they communicate their state information (e.g., position p_a and p_b, for vehicle V_a and vehicle V_b, respectively) to the multi-access edge computing (MEC). MEC processes the received information and sends the vehicles their time slots (t_a and t_b). The first **animation** shows *Intersection crossing without collision*: V_a and V_b give correct information about their location to the MEC, and the MEC gives them respective timeslots for crossing. The second **animation** shows *Intersection crossing with a collision*. In this scenario, V_a is malicious and gives the MEC wrong information about its position. V_a is much closer to the center of the intersection in reality, than what V_a reports it to be. Based on the wrong information from V_a, the MEC gives the priority of passing to the V_b, but the vehicles end up crossing simultaneously, resulting in a collision

Solution: Trust Assessment!

Trust Assessment at runtime in the second scenario shall enable the MEC to assess the trust in the vehicles and also the vehicles to access the trust among each other. The trust Assessment ideally puts less trust in a malicious vehicle and the information that this vehicle shares, which prevents potential collisions.

To summarize, we think that trust management is a key ingredient to safe and secure CCAM systems. The requirement is that this assessment of trust relationships is quantifiable, verifiable, and assessable both at design- and runtime. CONNECT therefore works towards a technical implementation of such trust assessment in a trust management framework.

"NEVER TRUST, ALWAYS VERIFY"

Authors:
Ana Petrovska, Nataša Trukulja, Artur Hermann, Frank Kargl

Find out more about this Project:
https://horizon-connect.eu

CONNECT
CCAM TRUST & RESILIENCE

Project Coordinator

Technikon, Austria

Technical Lead

Thanassis Giannetsos,
Ubitech
Greece

Scientific Lead

Frank Kargl,
University of Ulm
Germany

Call: HORIZON-CL5-2021-D6-01

Topic: HORIZON-CL5-2021-D6-01-04

Budget

€ 5.7 Million
100% EU-funded

Consortium

17 Partners
9 Countries

Duration

36 Months
09/2022 - 08/2025

Design of a Trust Management Framework

Implementing this trust management framework requires a number of challenges to be solved and solutions to be developed. Starting from a system model, we need a suitable representation of trust which allows us to model trust relationships in CCAM systems in a way that fulfils the requirements stated above. Second, we need to embed this trust model into a framework that can execute trust assessment and take decisions on whether the required trust is achieved or not.

Reasoning under uncertainties with subjective Logic

We approach the first challenge by using a well-establish logic framework called **Subjective Logic** that allows to reason about trust while also allowing to consider uncertainty in our judgement. This uncertainty can stem from incomplete evidence about trustworthiness that would prevent us from making dogmatic judgements.

In order to reflect this uncertainty, CONNECT uses Subjective Logic for trust assessment, i.e., for reasoning, assessing and quantifying trust in CCAM. The general idea of Subjective Logic is to enrich probabilistic logic by explicitly including uncertainty about probabilities and subjective belief ownership. Subjective Logic explicitly represents the amount of ‘uncertainty on the degree of truth about a proposition’ in a model called subjective opinion [3]. Based on this, **Subjective Trust Networks** allow to model complex trust relationships and to assess trust from the perspective of individual actors in our system.

Taking Trust Decision

Modelling and assessing trust using Subjective Trust Networks then form the basis for trust decisions, i.e., answering the question if there is sufficient trust in a specific situation to allow safe and trustworthy operation of a CCAM system and a specific driving function.

For this, two trust values have to be determined and compared. The first is the current level of trust also referred to as **Actual Trust Level (ATL)**. The second is the required level of trust among so that a specific function can be executed in a trustworthy manner – referred to as **Required Trust Level (RTL)**. Both can reference to a data item that an entity might receive and use in a driving function, or to another entity from which it consumes a service that it relies on. Only if the computed ATL exceeds the RTL, the execution of a specific function can proceed in a trustworthy manner.

Referring again to the motivational example: When we ask “How much trust is vehicle V_A required put into vehicle V_B to provide data correctly to safely engage in a maneuver at a cooperatively managed intersection?”, this determines Required Trust Level. On the contrary, if we ask “What is the actual level of trust that vehicle V_A has for data provided by vehicle V_B or to vehicle V_B in general with respect to performing a joint maneuver in a cooperatively managed intersection?”, then this determines the Actual Trust Level.

In CONNECT, we want to investigate, design, and develop this Trust Management Framework in order to bring Trustworthy CCAM closer to reality.

[1] https://upstream.auto/reports/global-automotive-cybersecurity-report/

[2] Ulm University, “Securing Cooperative Intersection Management through Subjective Logic”, presentation, 2022

[3] Jøsang, Audun. “A logic for uncertain proabilities.” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 9.03 (2001): 279-311.

[4] Jøsang, Audun. Subjective logic. Vol. 4. Cham: Springer, 2016

Partners

1. TECHNIKON
Technikon Forschungs- und Planungsgesellschaft mbH, Austria

2. UBITECH
Ubitech Ltd, Greece

3. HUAWEI
Huawei Technologies, Germany

4. Institute of Communication and Computer Systems, I-SENSE Research Group, Greece

5. uulm
University of Ulm - Institute of Distributed Systems, Germany

6. Red Hat
Red Hat Research, Israel

7. Trialog
Trialog, France

8. DENSO Crafting the Core
DENSO AUTOMOTIVE Deutschland GmbH, Germany

9. intel.
Intel Deutschland GmbH, Germany

10. Suite5
Suite5 Data Intelligence Solutions Ltd, Cyprus

11. uni.systems
Unisystems, Greece

12. UNIVERSITY OF TWENTE.
University of Twente, Department of Philosophy, Netherlands

13. FSCOM
FSCOM, France

14. STELLANTIS
Centro Richerche Fiat SCPA, Italy

15. Politecnico di Torino
Politecnico di Torino, Italy

16. SystemX
Institut de Recherche Technologique SystemX, France

17. UNIVERSITY OF SURREY
University of Surrey, Department of Computer Science, United Kingdom

Funded by
the European Union

Funded by the European Union under grant agreement no. 101069688. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Follow CONNECT on:

@connect_horizon

CONNECT Horizon Europe
project 101069688