ConnRAD – Connectivity and Resilience for Automated Driving

Final Presentation **23.10.2025**

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany
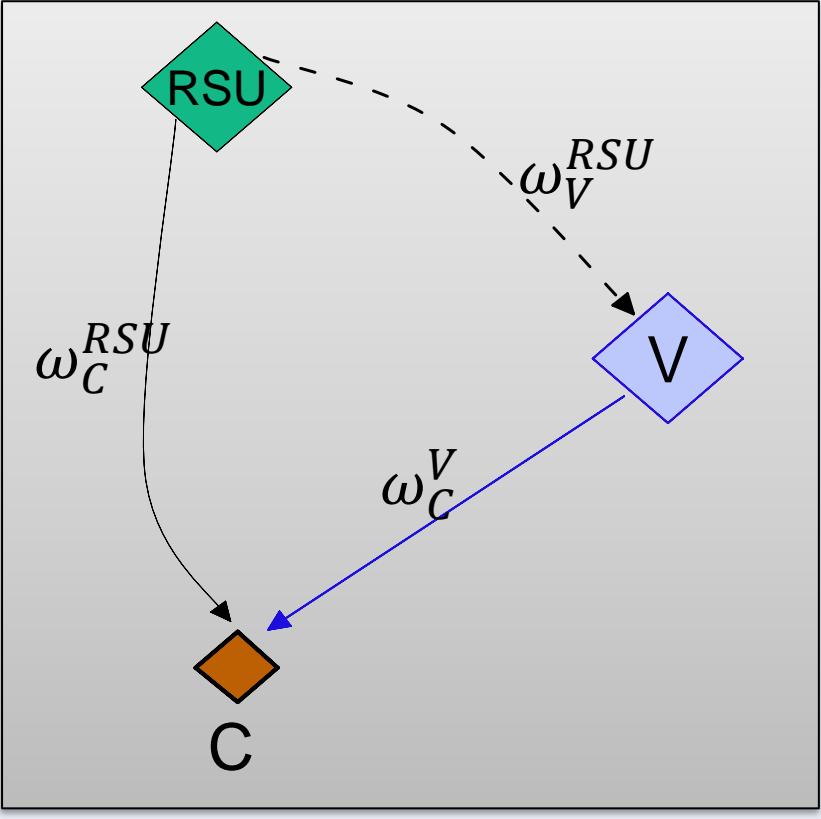
Representation of Trust Opinions in Messages and TAF

Artur Hermann, Dennis Eisermann, Nataša Trkulja, Frank Kargl
Institute of Distributed Systems, Ulm University

Representation of Subjective Logic Opinions in the TAF

- Subjective Logic (SL) Opinions form the basic unit of trust representation in Subjective Logic and the TAF
- They express the opinion of an opinion holder on a proposition; which in the TAF represents the trustworthiness of data or an entity
- Therefore ω_X^S represents the opinion of subject S on statement X
- Example: ω_C^{V1} represents the opinion of vehicle V1 that a received CAM message C contains trustworthy information
- A Subjective Logic Trust Network allows to reason over complex and transitive trust relationships using fusion and trust discounting operators
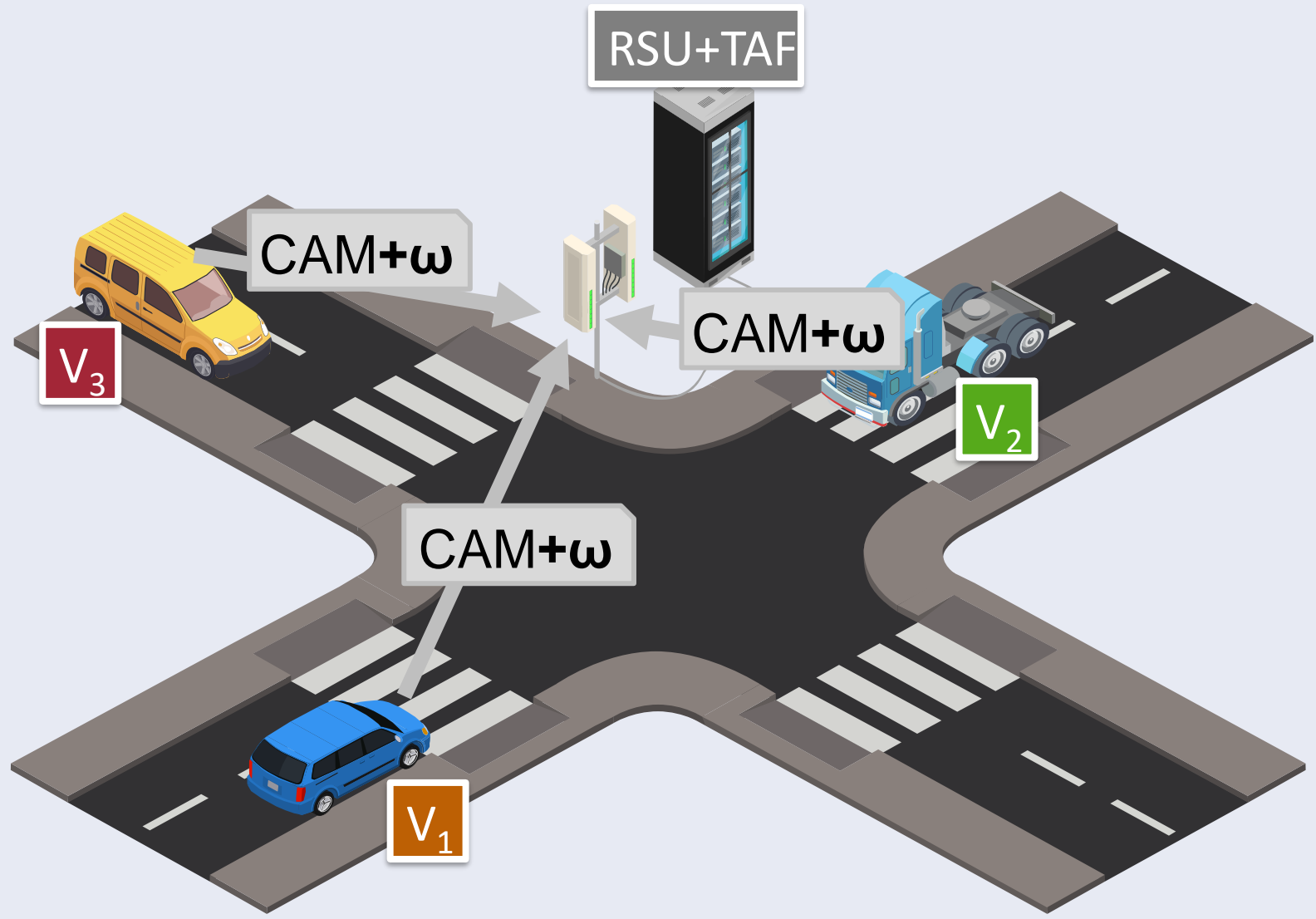
SL Trust Network Example

- For binomial propositions with $\omega_X^S \mid X = \{x, \bar{x}\}$ the opinion is represented by the tuple $\omega_X^S = (b, d, u, a)$ where $0 \leq (b, d, u, a) \leq 1$ and $b + d + u = 1$
- b represents the belief of X to be true (X = x)
- d represents the disbelief of X to be false ($X = \bar{x}$)
- u represents the uncertainty in the assessment of X due to lack of conclusive evidence
- a represents the prior probability of X to be true in the total absence of evidence to assess

Challenge 1: Including SL opinions in V2X messages increases channel load and can lead to packet loss

- Exchange of opinions is required for federated trust assessment in CCAM systems
- These should be included in and sent together with standard messages like CAMs, DENMs, or CPMs

Challenge 2: Limited accuracy of opinion representation introduces errors in trust assessment and reason

- In CPUs, (b, d, u, a) are typically represented as IEEE 754 Binary64
- When communicating opinions between nodes, we typically need to limit representation even further, using for example only 8, 16, or 32 bit per value
- Subjective logic operations inevitably introduce errors that can accumulate as the trust network grows in depth
- We conducted extensive analytical and simulation-based analyses to understand the nature and extent of these errors
  - For this purpose, we used interval arithmetic and simulations implemented in Haskell
  - We also considered even more restricted transfer encodings in messages
- Based on these insights, we propose guidelines for SL trust networks and implementation of SL operators
- We also propose integration and representations of SL opinions in standard messages

Problem analysis
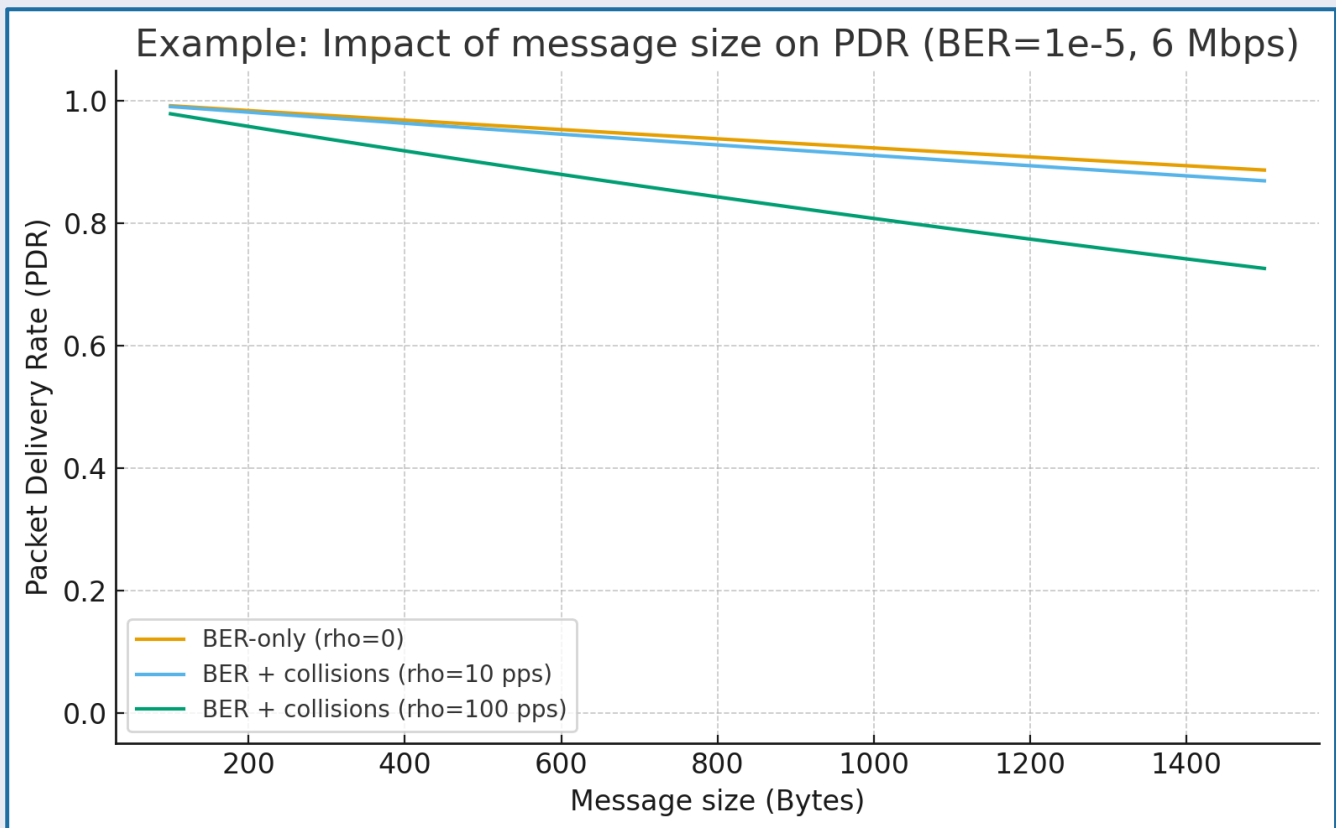
- **Where to add SL opinions in CAMs?**
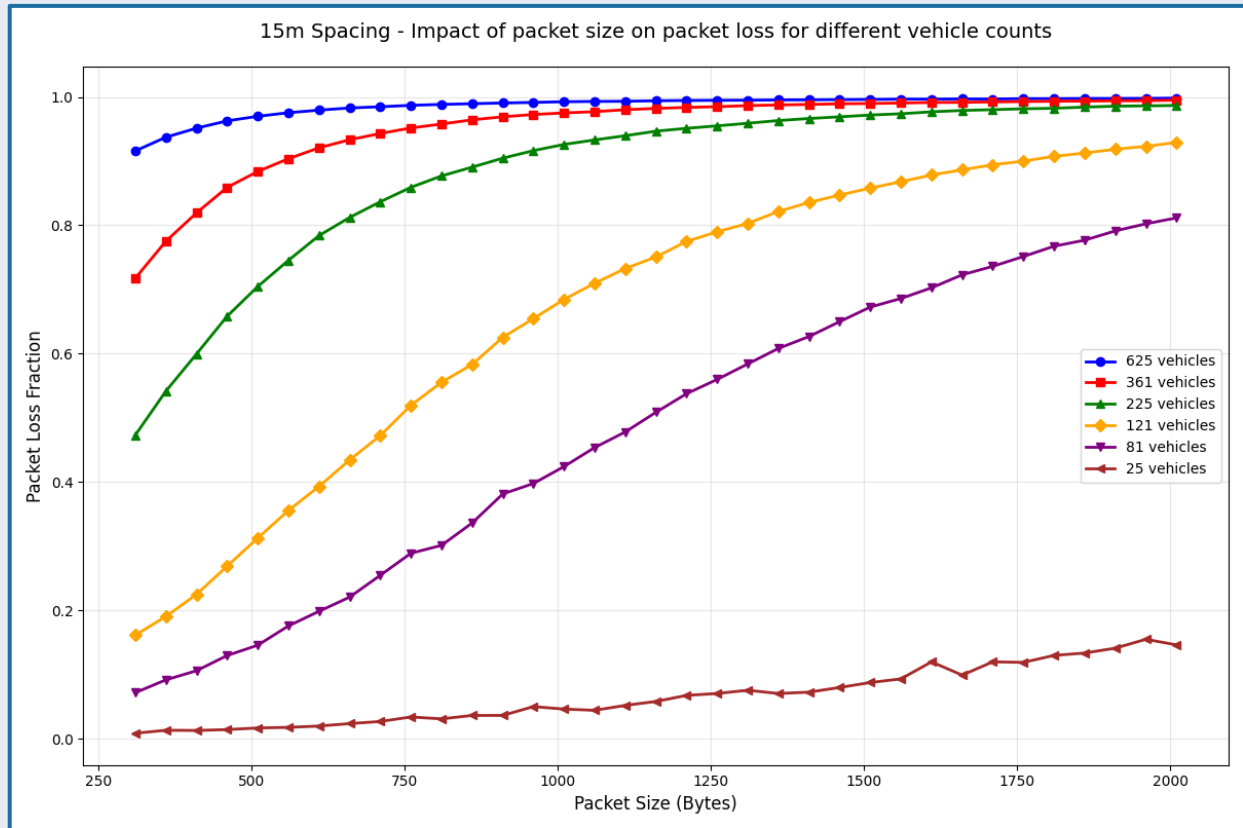

- **Exchange of opinions is required for federated trust assessment in CCAM systems**
  - should be included in and sent together with standard messages like CAMs, DENMs, or CPMs
  - expressiveness increases the more fine-granular opinions you include
  - also makes the message size grow proportionally
- **Larger messages affect message delivery success, due to:**
  - Larger channel occupation and larger channel access latency
  - Increased risk of bit errors during transmission
  - Increased risk of collisions due to CMSA/CA random access with fixed backoff window
  - Increased risk of collisions due to hidden terminal constellations

Analysis based on analytical model of IEEE 802.11p: effects of BER and collisions on PDR
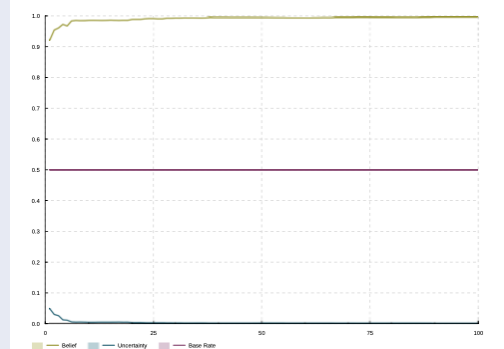
Simulations based on OMNET++ / VEINS / SUMO document effect of message size on PDR
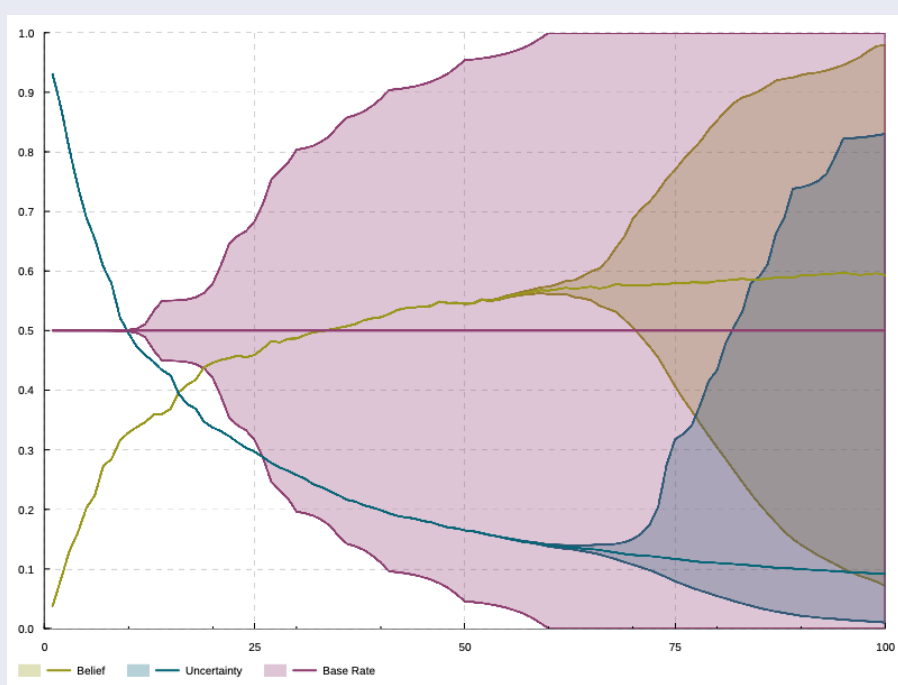
Simulation results

- Approach: repeated application of SL operation (different fusion operators & trust discounting) to identify when calculations become unstable
- Experiment 1: (Averaging) Fusion of opinions with binary32 representation show sudden shift from one extreme to the other
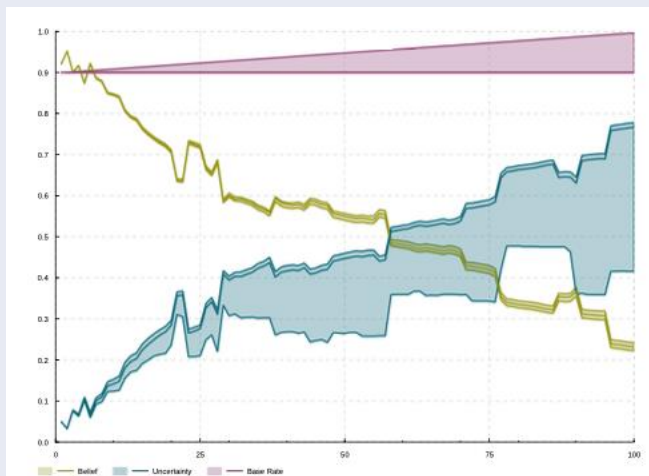 - Scenario: Jury-MostlyYes-Binary32-100
  - Not observed with binary64

- Experiment 2: Repeated cumulative fusion of opinions with high uncertainty leads to substantial growth of confidence intervals
  - Scenario: Reputation-MostlyUnknown-Binary64-100

- Experiment 3: Transmission as tuple (b, u, a), as fixed-point numbers of type UQ0.16 proofs stable in realistic scenarios (here: platooning)
  - Scenario: PlatoonUQ0_16-SpanishInquisition-Binary64-100
  - For smaller networks, the packed representation `(b: UQ0.11, u: UQ0.11, a: UQ0.10)` (32 bits total) might be sufficient

Conclusion 1

- Size of messages should be kept below 400 bytes in high-load scenarios
- Opinions per data field are not practical (considering current message sizes w/o opinions including already message payloads, headers, and security)
- More evaluations are required that investigate efficient encodings of opinions and also the accuracy of trust assessment that is achievable when having opinions per container or per message

Conclusion 2

- Normalize results and intermediate values (recalculation of disbelieve as d = 1 − b − u)
- binary64 for internal representation and UQ0.16 for transfer encoding recommended
- Many learnings for structure of trust networks
  - Avoid cumulative fusion of opinions with high uncertainty
  - Keep diameter of trust graphs < 20 (common in practice)
- Novel results and insights on SL; publication pending