Sujash Naskar
Department of Information System and Technology (IST)
Contact: sujash.naskar@miun.se

Sensible Things that Communicate
Prof. Mikael Gidlund
Contact: mikael.gidlund@miun.se

Mittuniversitetet
MID SWEDEN UNIVERSITY

Privacy and Security in VANET

Introduction: What is already there and why is importantly needed to improve?

Vehicular-Ad-Hoc Network provides safety in intelligent transportation with self-driving, automated traffic management, etc.

- Increased Safety Measures
- Driving Efficiency
- Better Traffic Management

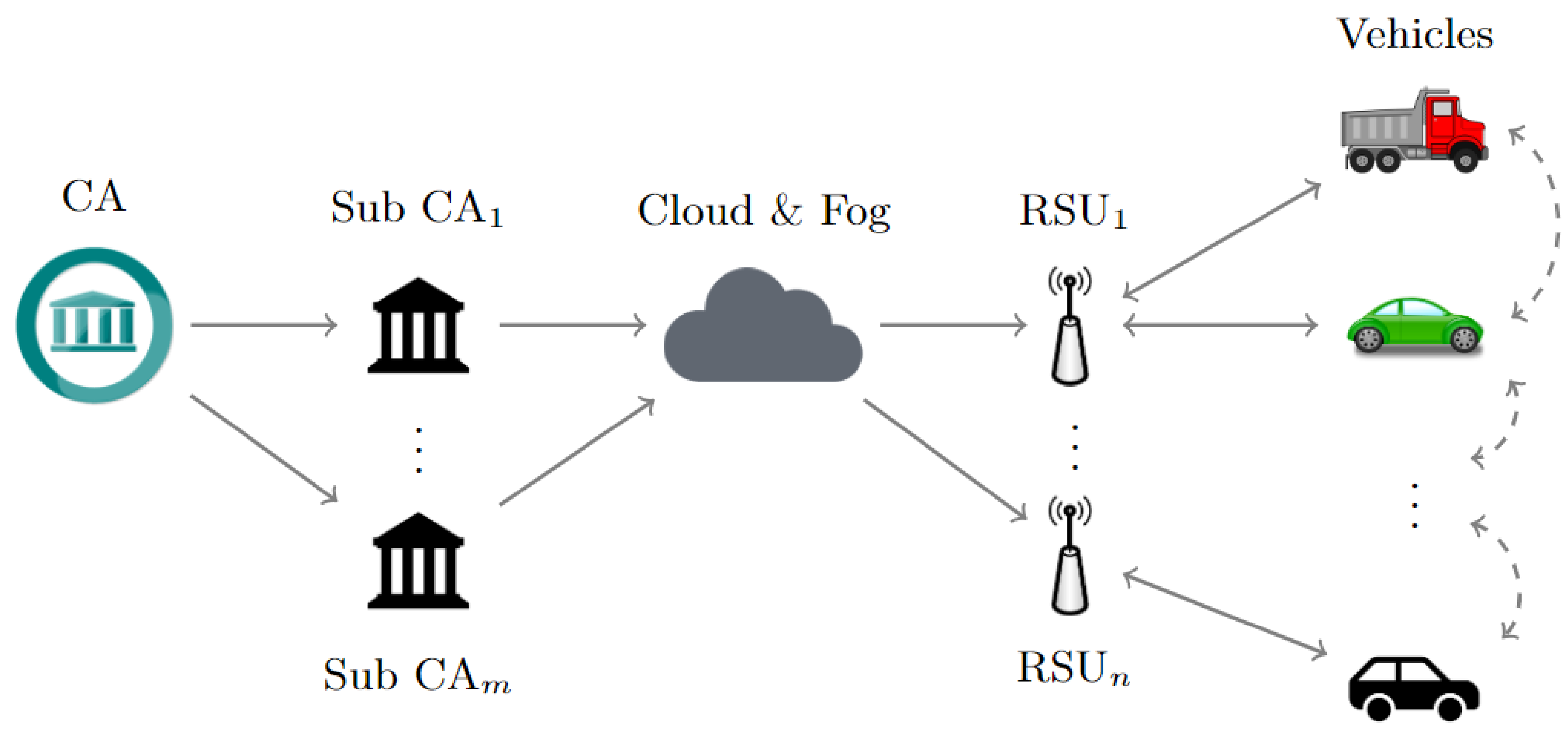


Fig.1: Centralized Classical VANET

Disadvantages

- Single Point of Failure
- High Delays!
- Message complexity!
- Third Party Mistrust!
- Scalability and Reliability Issues
- Fault Tolerance

Research Question: How can VANET be Decentralized with a Distributed Authentication and Revocation?

Our Approach: Introduce Multi-CA Model and apply Distributed Authentication using ECC

Step 1: Architecture and Protocols

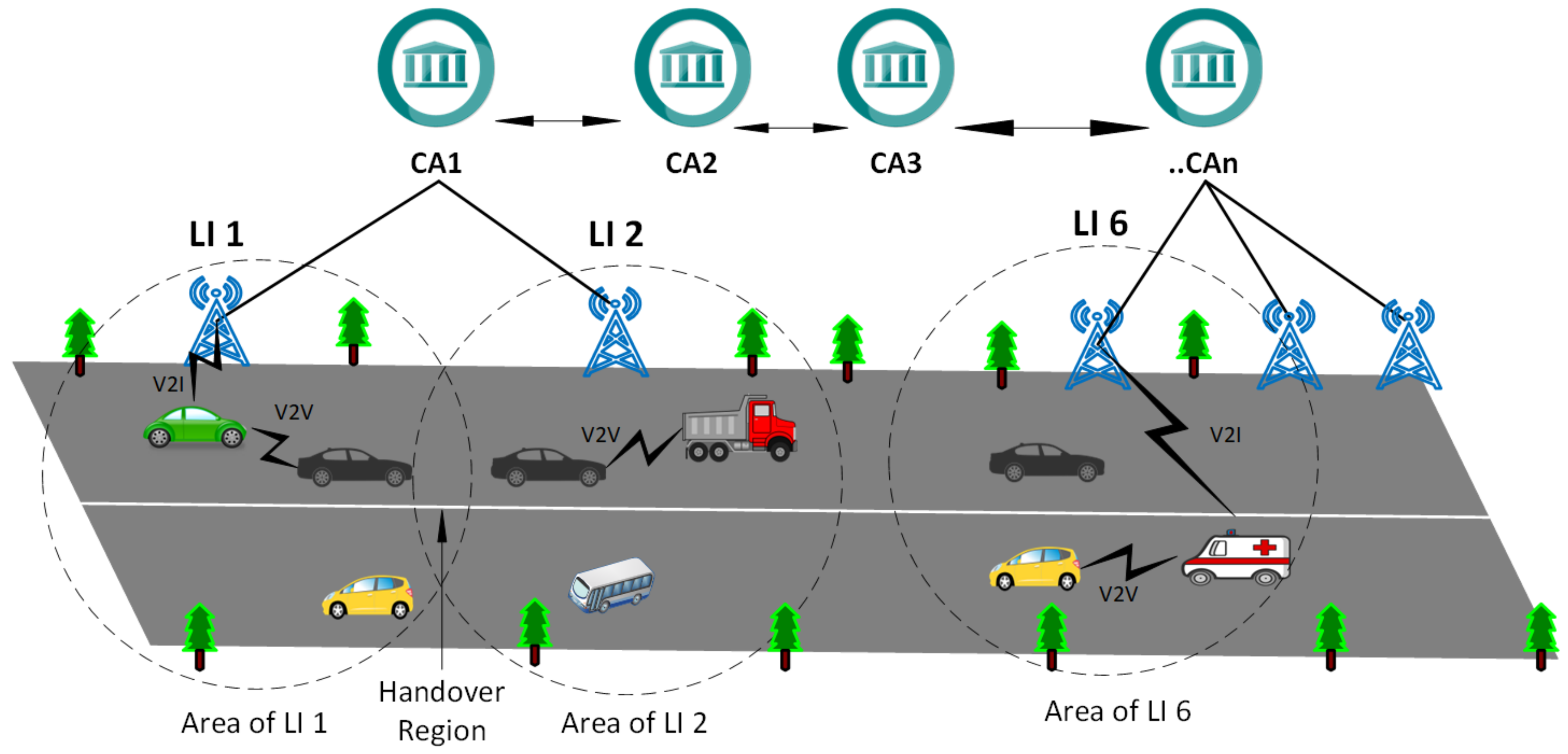
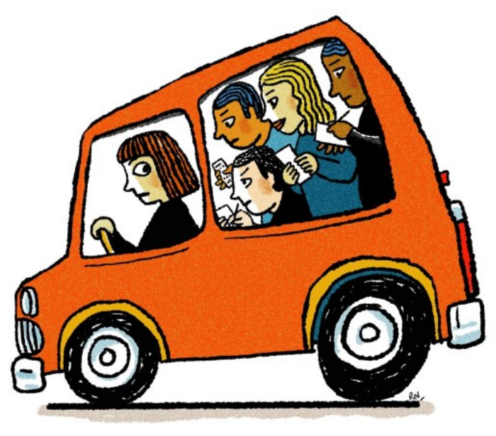


Fig.2: Proposed Distributed VANET

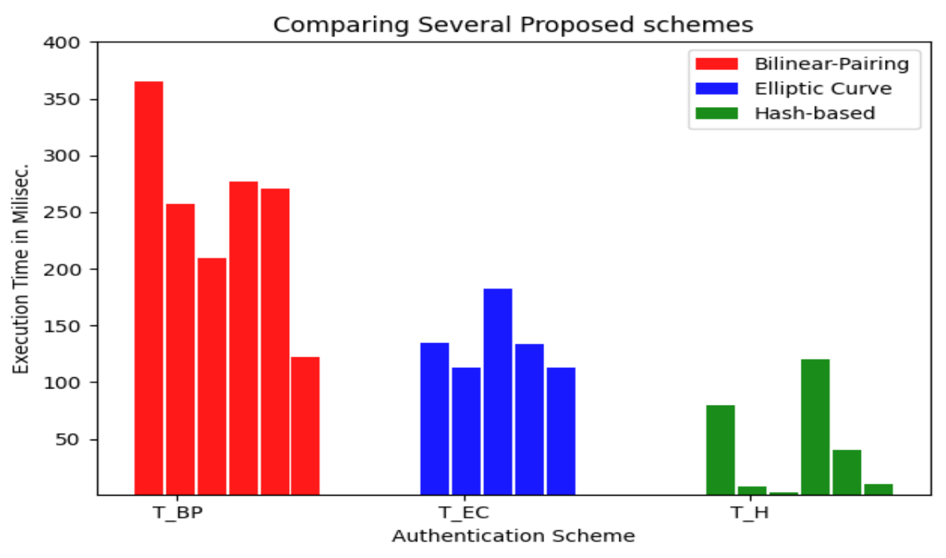
Step 1: Threat Model

Security Attack



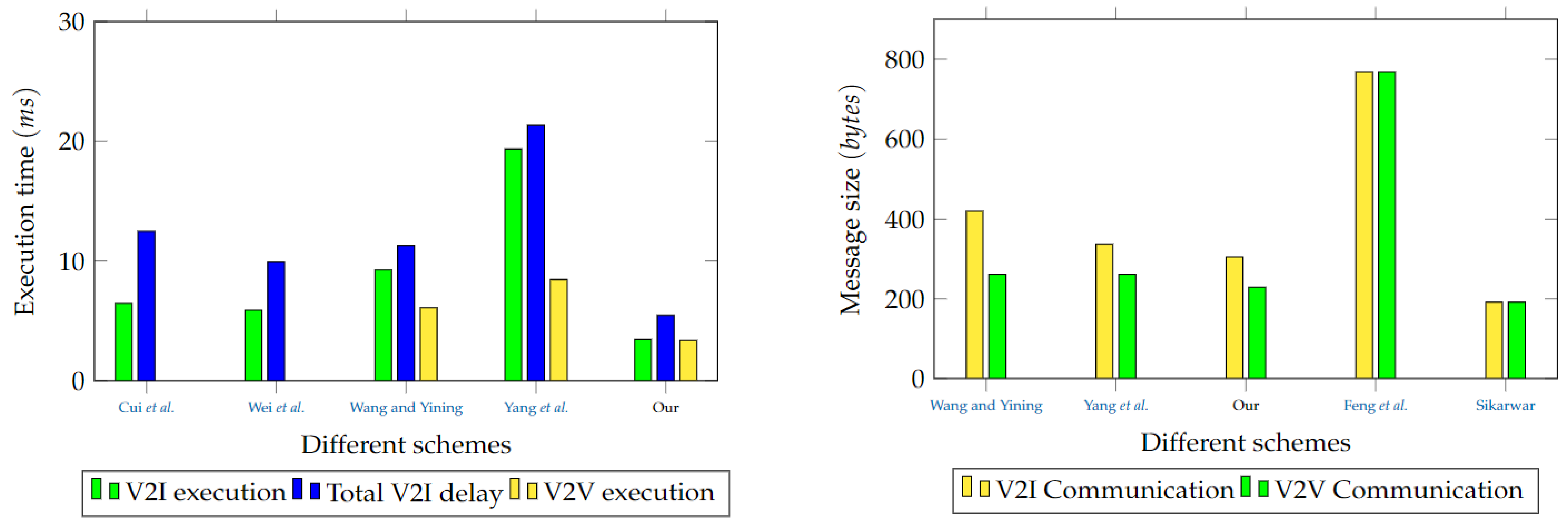
Privacy Issues

Step 3: Crypto Choices



- Elliptic Curves
- ECDSA
- Symmetric Enc/Dec
- NIZK

4. Results: Efficiency Gain in terms of Computation Cost, Communication Overhead and Overall Delay



(a) Comparison of V2I, V2V execution cost and V2I delay

(b) Comparison of V2I and V2V Communication cost

Fig.3(a,b): Results representing Efficiency gains

Efficiency Gains

- Lower delay in V2I authenticated key sharing (upto 3.9 times faster than others)
- Lower delay in V2V message sharing (upto 7.5 times faster than others)
- Strong security guarantees
- Revocation abilty

5. Research Collaborators and Possible Beneficiaries

Research Collaborators:

Simula UiB

Simula@UiB, Norway

Karlstads University, Sweden

Possible Beneficiaries:

- Vehicle Industries: Tesla, BMW, Audi, SCANIA
- Organizations: Gov. willing to implement a safe and smart trasportation system.