

[Speed profiles

Author

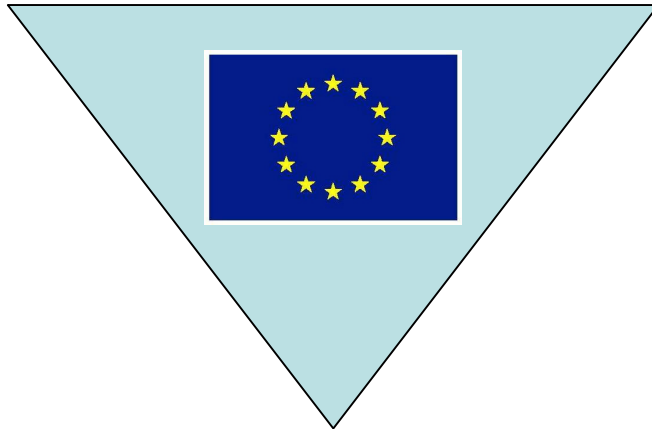
Nol Venema (Technolution)

Martin Kost (Humboldt Universität zu Berlin)

CVIS / eSecurity / PRECIOSA

Context of use case

- eSafety forum / eSecurity WG
- CVIS - PRECIOSA partnership concerning privacy
- European R&D Programme
- Use case inspired by a CVIS application

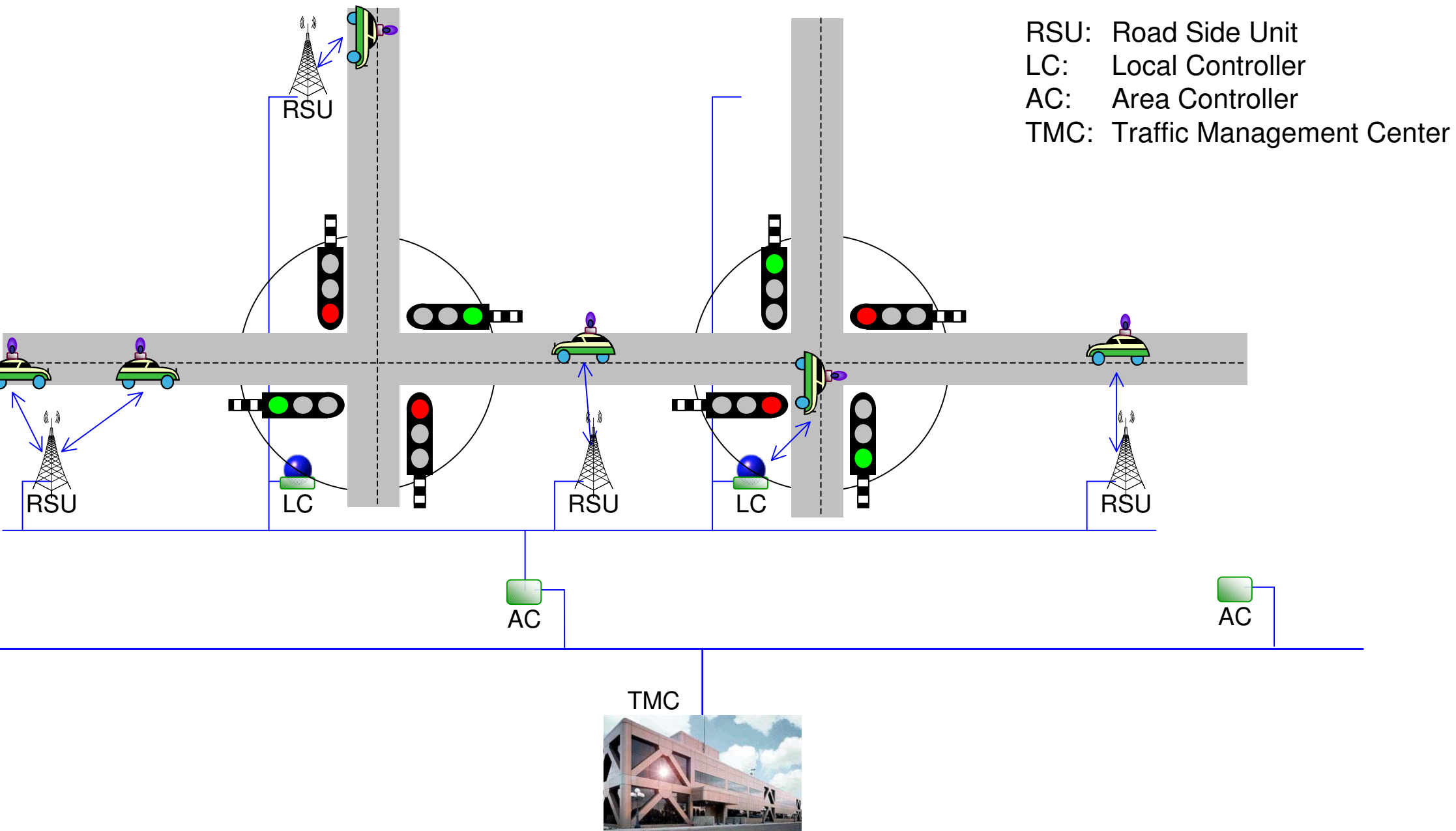


Summary



- The **Speed Profiles** application is used to harmonize traffic flow at an intersection. This is done by:
 - collecting data from vehicles
 - calculating optimal traffic light switching plan
 - providing speed profiles (recommendations) back to approaching vehicles
- This approach will improve efficiency, comfort and safety on the level of urban intersections

Overview



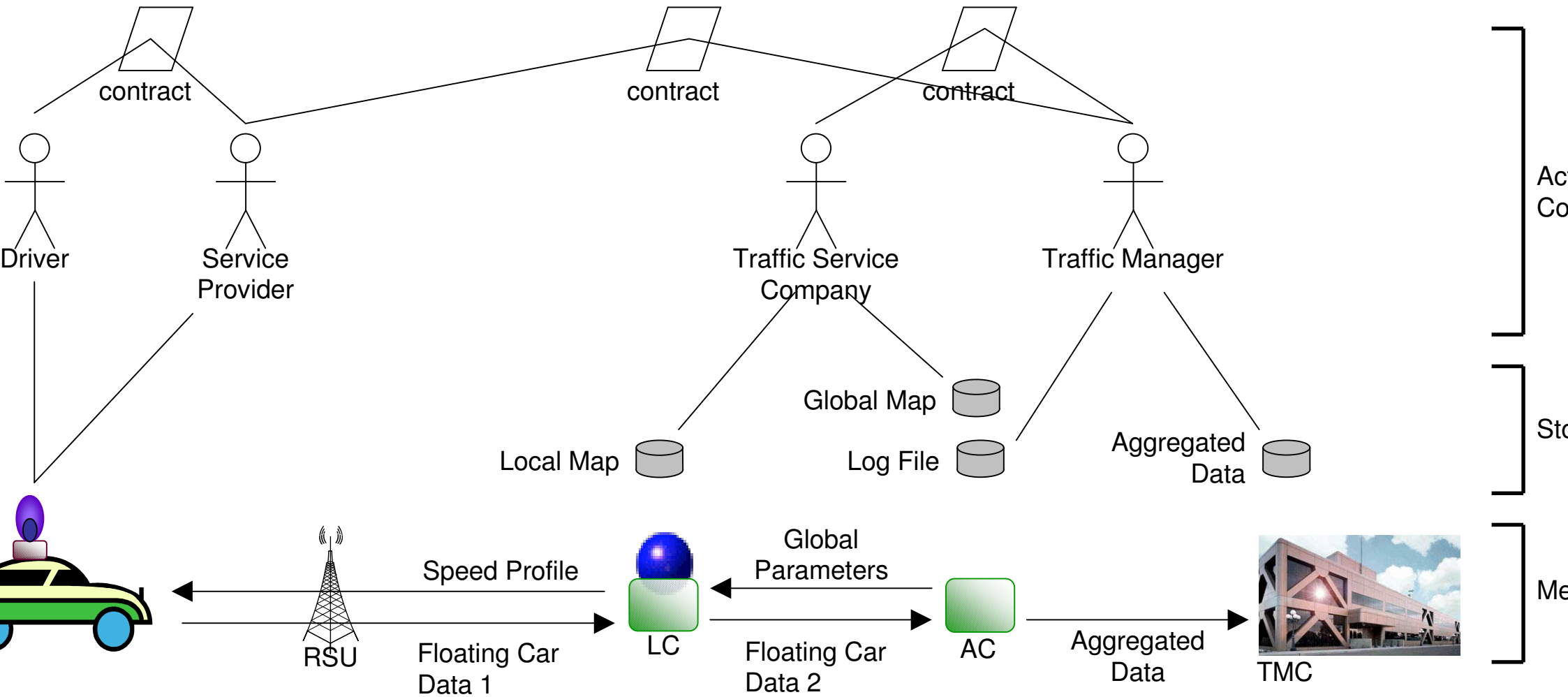
Description

- The **Local Controller** receives **Floating Car Data** (like vehicle ID, type of vehicle, actual speed, location, ...) from all nearby equipped **vehicles**
- **Local Controller** stores the **Floating Car Data** in a **dynamic map** that represents the local situation
- **Local Controller** calculates optimum switching plan for the traffic lights based on that **dynamic map**
- **Local Controller** calculates **Speed Profiles** based on the switching plan and sends it to the appropriate **vehicles**
- Equipped **vehicles** receive the **Speed Profiles** message and notify the drivers in a suitable way (e.g. scaling an up or down arrow)
- **Floating Car Data** is forwarded to the **Area Controller** and stores the data in a **Global Map** and in a **Log File** for analysis purposes
- The **Area Controller** performs global optimizations and sends **Global Parameters** back to the **Local Controller**
- The **Traffic Management Center** receives **Aggregated Data** from the **Area Controller**

Messages, Storage, and Access

RSU: Road Side Unit
LC: Local Controller

AC: Area Controller
TMC: Traffic Management Center



[Personal data

FCD 1/2 (Car > LC):

- Vehicle ID
- Time
- Vehicle type
- Vehicle position
- Vehicle speed
- Route fragment

Speed profile (LC > Car):

- Speed target

Log file:

- FCD records

Global parameters

- ??

Aggregated data:

- Road section / Direction
- Time slot
- Vehicle count
- ...

[PETs

- Data encryption v
 - Protect transmission of sensitive records (FCD)
- Logical access control v
 - Control access to systems in complete chain
- Data minimisation related v
 - Transmit, store and show only appropriate fields
 - aggregation
- Separation of identity domains x
- Improving Information quality x
- Anonymisation / pseudonymisation v
 - either hash vehicle ID after receiving
 - or use vehicle ID pseudonyms
- Policy enforcement (storage) v

[Data protection issues

■ Data controllers / Data processors

- Traffic Manager (TMC): data controller
- Traffic service Company: data processor

■ Purpose (or limitations)

- Short range tracking of vehicles
- Facilitate future research on optimisation
- Improve infra planning: traffic statistics

■ Legal Grounds

- either unambiguous consent (optional)
- or for the proper performance of a public law duty (mandatory)

■ Interoperability of systems

- not in this use case

■ Location technology impact

- low because of limited area and limited personal info

Storage policies

DPU	Storage Policies
Vehicle	<ul style="list-style-type: none">• No storage
RoadSideUnit	<ul style="list-style-type: none">• No storage
LocalController	<ul style="list-style-type: none">• Stores FCD data in Local Map as long as vehicle is “visible” (~5 min)
AreaController	<ul style="list-style-type: none">• Stores FCD data in Global Map for global optimisations (~1h)• Stores FCD data in Log File (~1 wk)
TrafficManagement Center	<ul style="list-style-type: none">• Stores Aggregated Data (anonymous) infinitely as historical data (~10 yr)

[Opinion

Privacy by design:

- Embed in development process and product lifecycle
- Improves visibility/awareness (technical and management level)
- Level of detail?

Concerning BATs:

- Builds on security BATs?
- Will it iterate quickly enough?

[Thanks