Vehicular Communications and VANETs

Frank Kargl (frank.kargl@ulm.ccc.de)
CCC Ulm, Ulm University

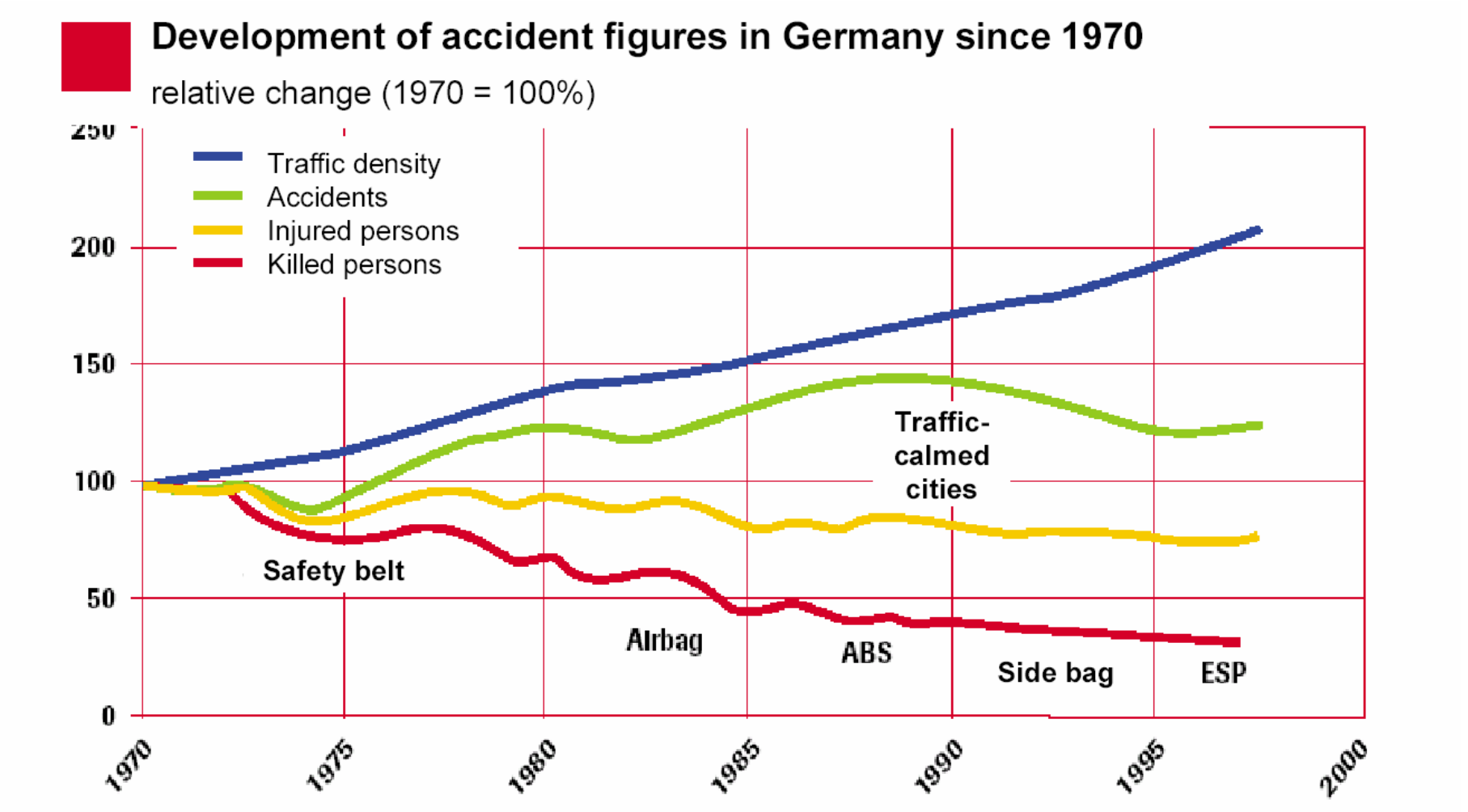
Overview

- Introduction
  - ***Motivation and Applications***
  - Technology Overview
- Communication
  - IEEE 802.11p
  - Position-based Routing
- Security and Privacy

Reasons for Vehicular Communications

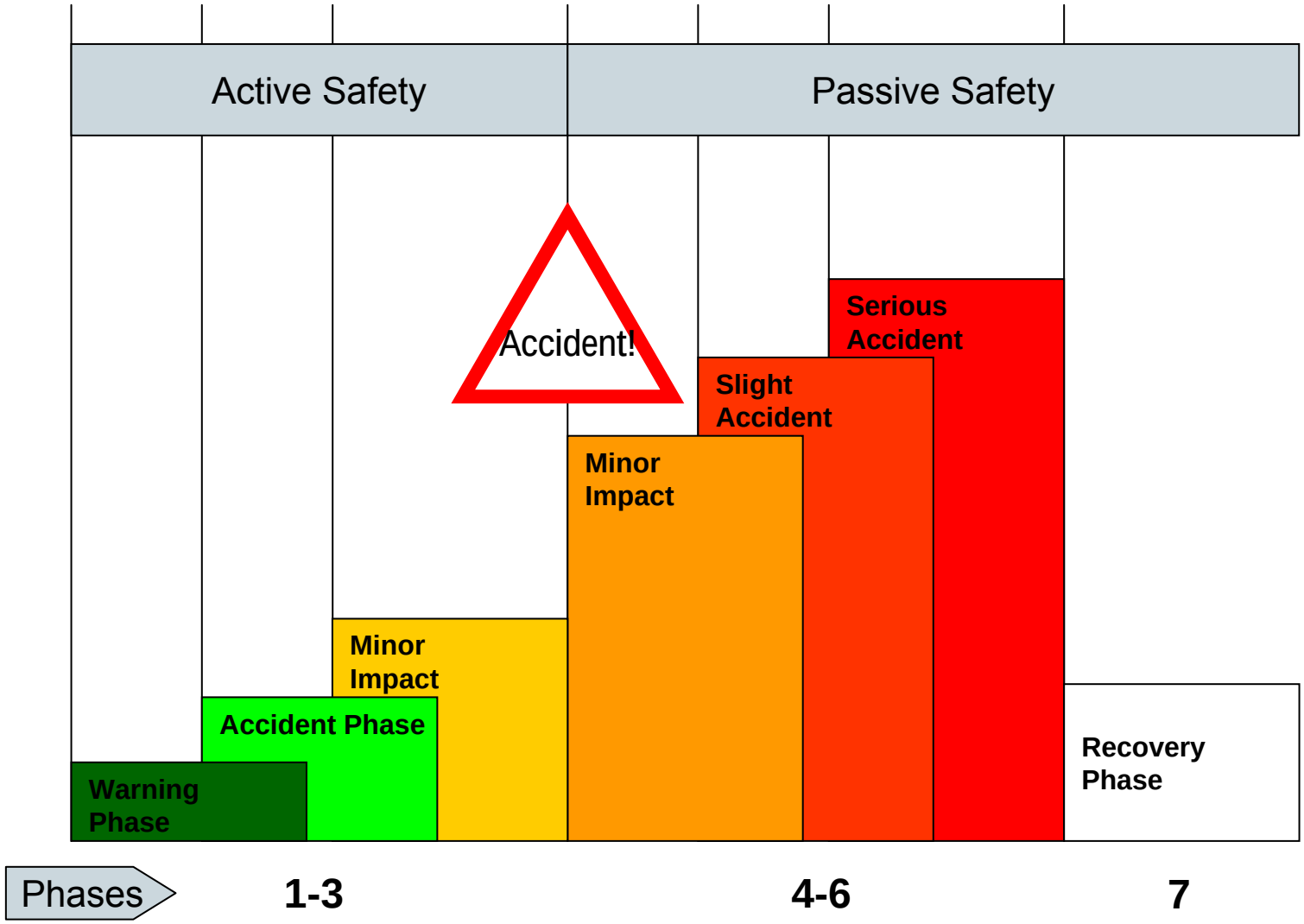
1. Research Grants and PhD titles;-)
2. Sell more cars ;-)
   - 80% of innovation in new cars is electronics, mostly software
3. Active Safety

Motivation for Vehicle Comm.: Active Safety

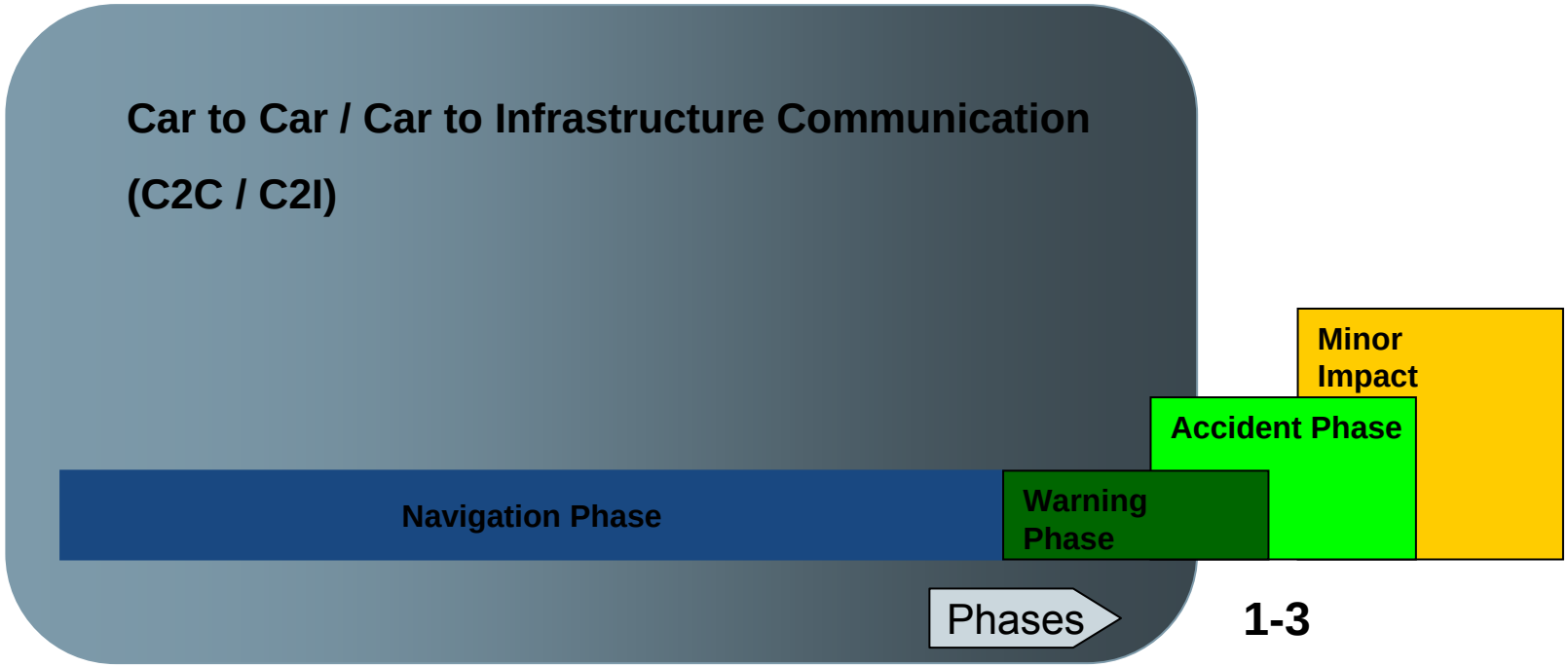


Source: Statistisches Bundesamt, Audi AG

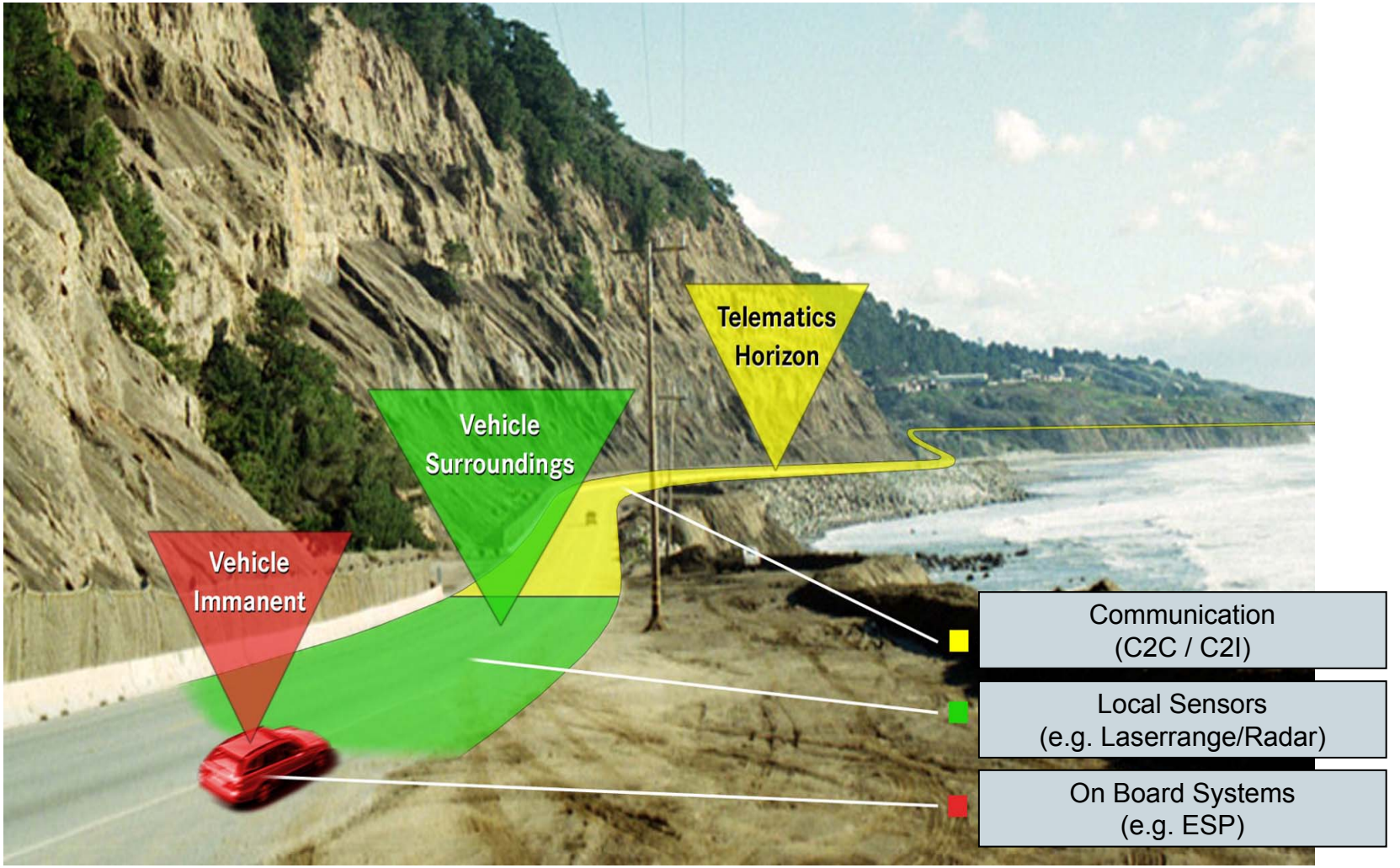
Accident Phases



Car to Car / Car to Infrastructure Communication

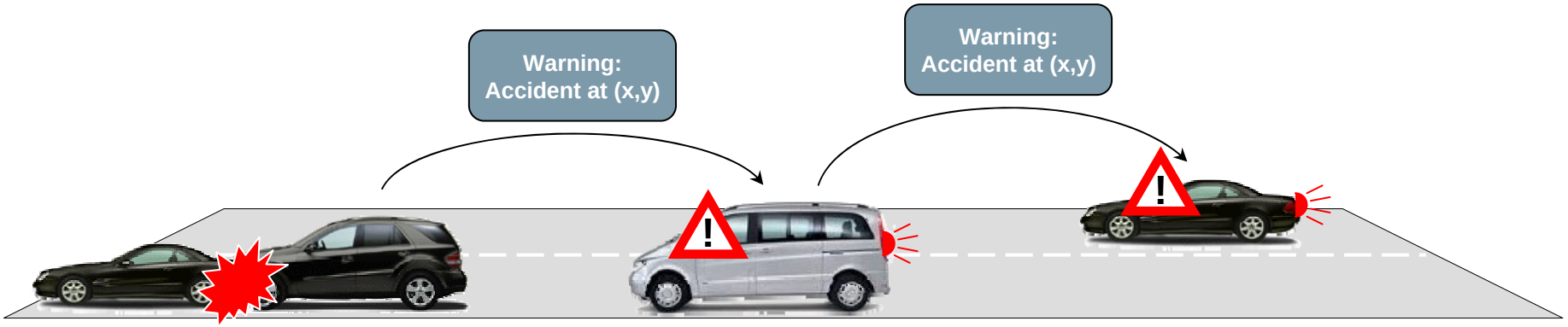


Telematics Horizon

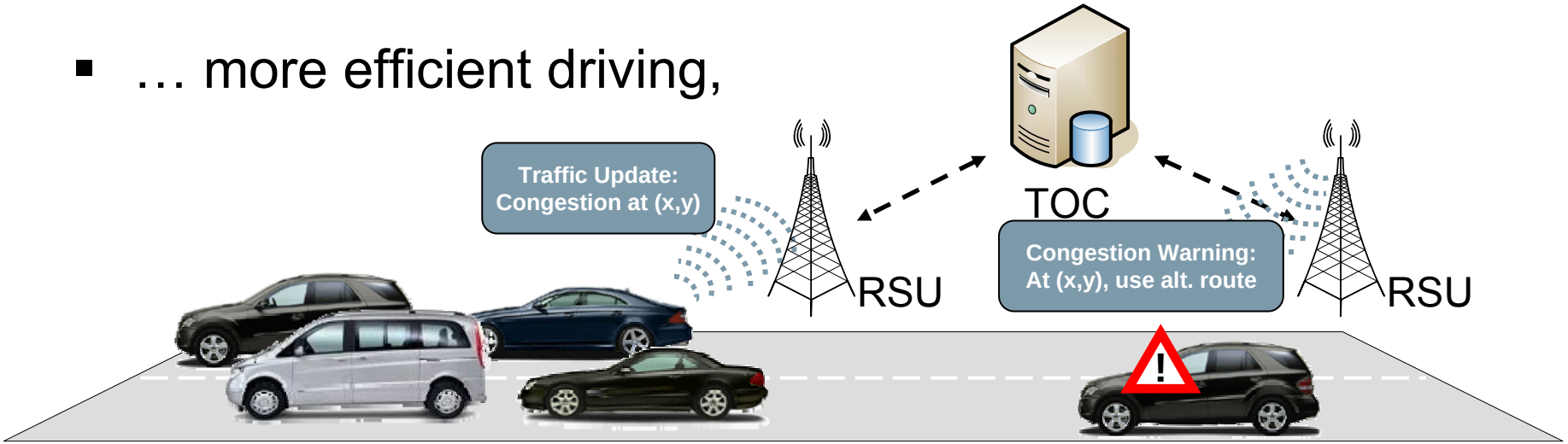


Vehicle Communication (VC)

- VC promises safer roads,

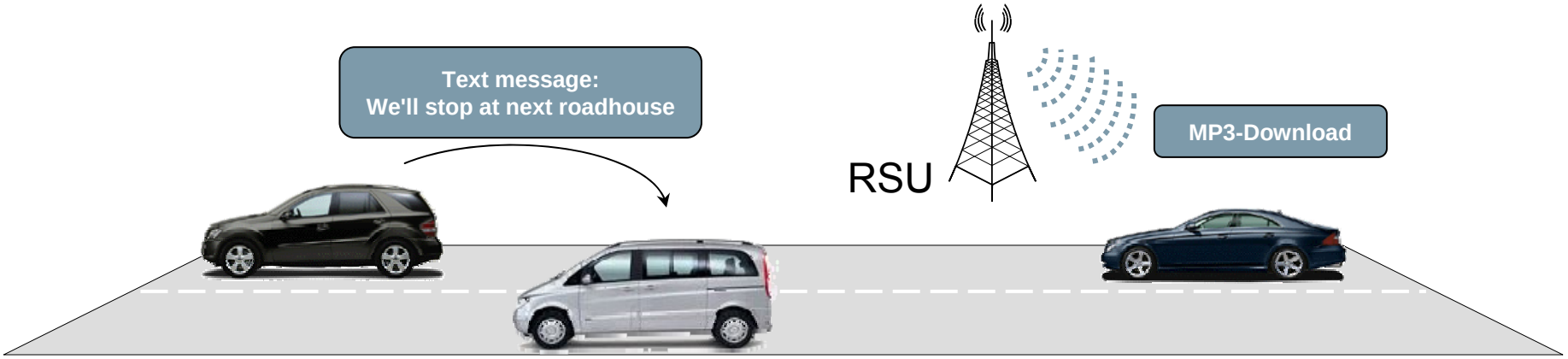


- … more efficient driving,

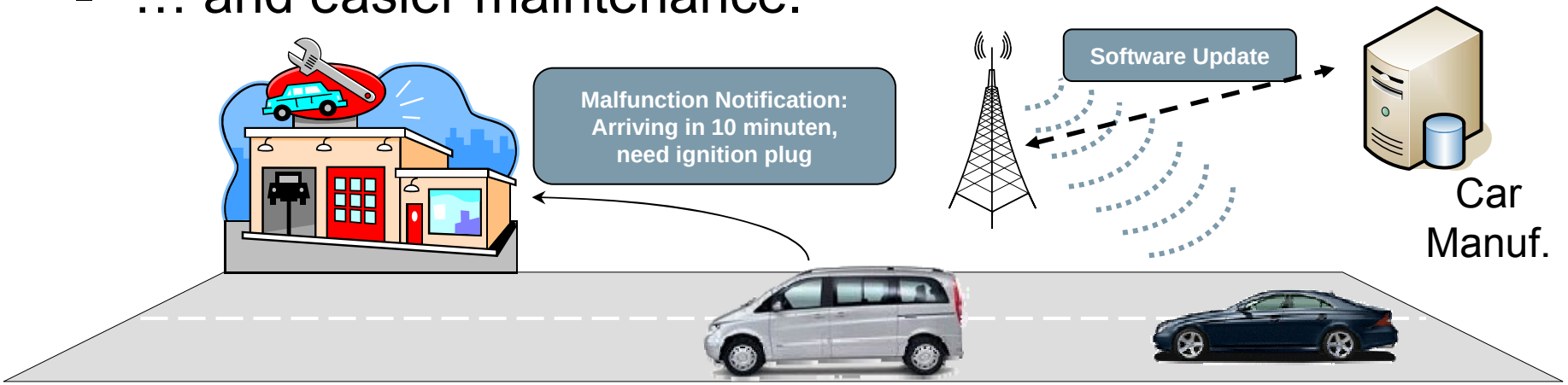


Vehicle Communication (VC)

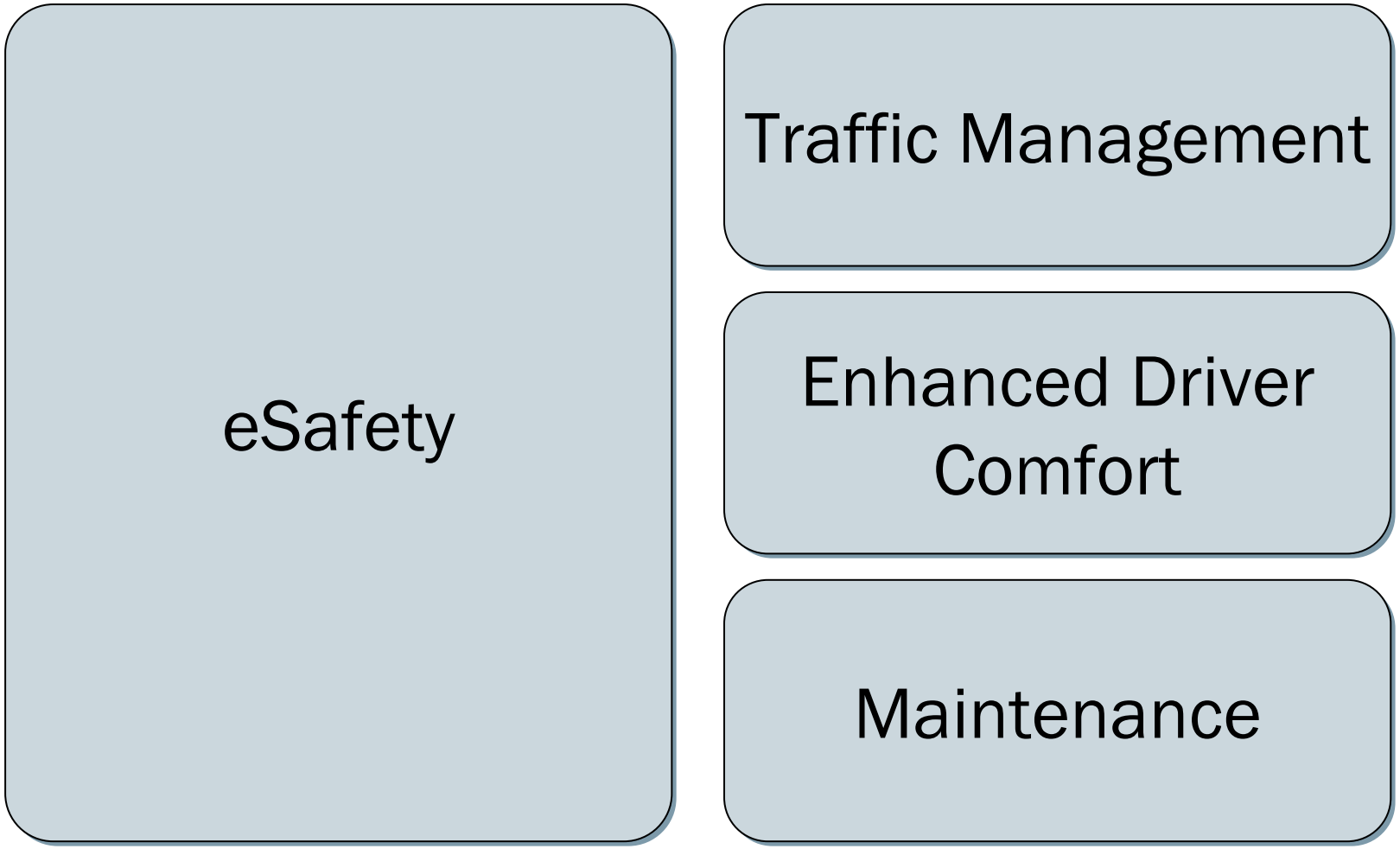
- … more fun,



- … and easier maintenance.



Application Categories



eSafety Applications

- Traffic signal violation warning
- ***Stop sign violation warning***
- General in-vehicle signage
- Left turn assistant
- ***Intersection collision warning***
- Pedestrian crossing information
- ***Emergency vehicle approaching warning***
- Emergency vehicle signal preemption
- Emergency vehicle at scene warning
- Vehicle safety inspection
- Electronic license plate
- Electronic driver's license
- In-vehicle Amber alert (crime haunt)
- Stolen vehicles tracking
- Post-crash/breakdown warning
- SOS services
- Pre-crash sensing
- Event data recording
- Work zone warning
- Curve-speed warning (rollover warning)
- ***Vehicle-based road condition warning***
- Infrastructure-based road condition warning
- Cooperative (forward) collision warning
- Emergency electronic brake lights
- Blind spot warning / lane change warning
- Wrong way driver warning
- Rail collision warning

Traffic Management Applications

- ***Highway merge assistant***
- Cooperative adaptive cruise control
- Cooperative platooning
- Adaptive drivetrain management
- Intelligent traffic flow control
- ***Road surface conditions to TOC***
- Vehicle probes provide weather data to TOC
- Crash data to TOC
- Origin and destination to TOC
- Fleet management
- ***Area access control***
- Electronic toll payment
- Rental car processing
- Hazardous material cargo tracking

Maintenance and Enhanced Driver Comfort

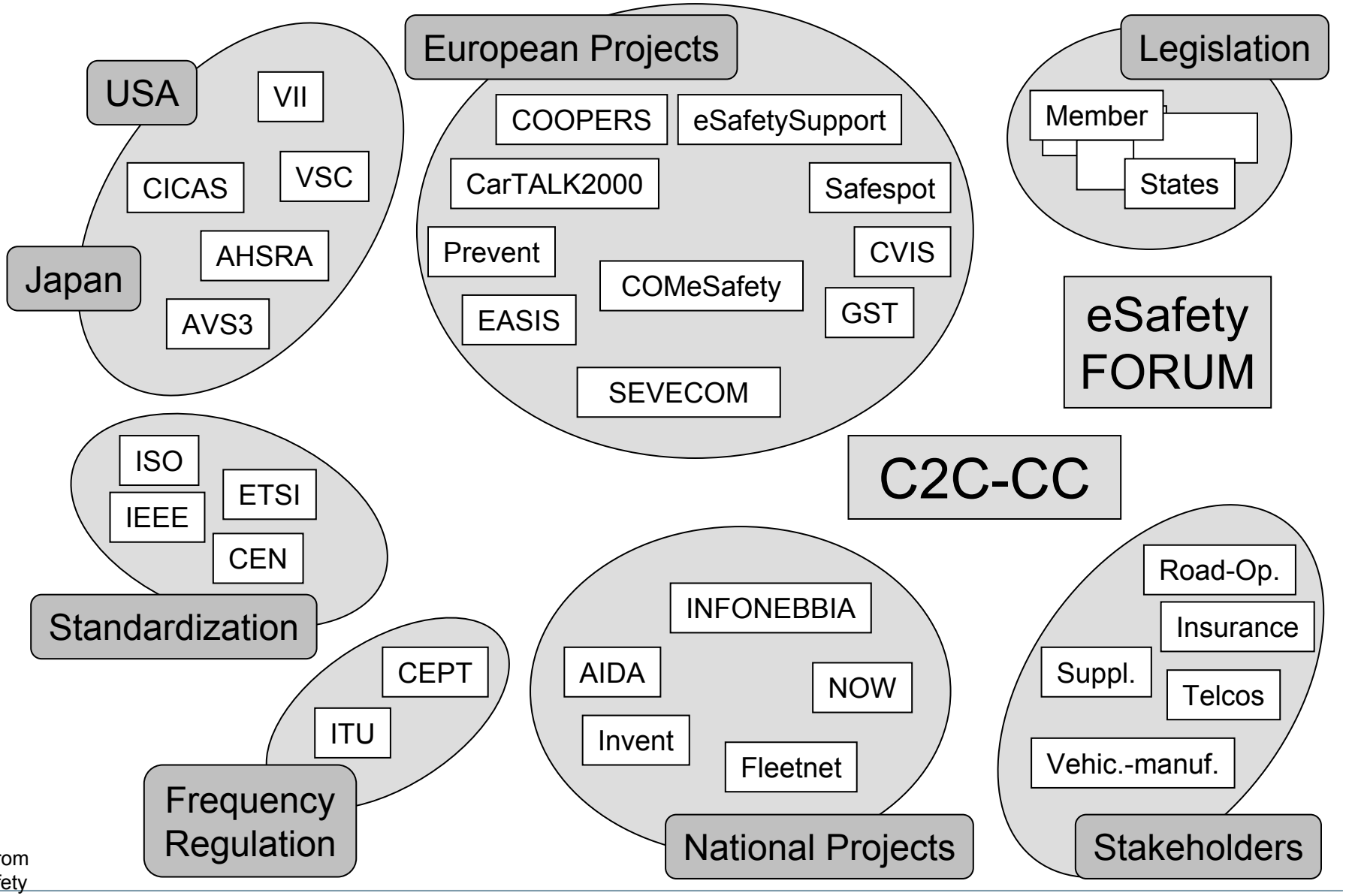
- Maintenance Applications
  - Safety recall notice
  - Just-in-time repair notification
  - Wireless Diagnostics
  - ***Software update/flashing***
- Enhanced Driver Comfort
  - Visibility enhancer
  - ***Cooperative glare reduction / headlamp aiming***
  - Parking spot locator
  - Enhanced route guidance and navigation

- Enhanced Driver Comfort (cont.)
  - Map download/update
  - GPS correction
  - Cooperative positioning improvement
  - ***Instant messaging (between vehicles)***
  - Point-of-interest notification
  - Internet service provisioning / info fueling
  - Mobile media services
  - Mobile access to vehicle data (PDA, Handy,…)

Scope of Vehicular Communications Research

- Today mostly warnings and assistance mechanisms
- Potential for automatic reaction and driving, but
  - User acceptance
  - Legal issues
  - Insurance issues
- <Videos go here>

Lot of Involved Parties



adopted from COMeSafety

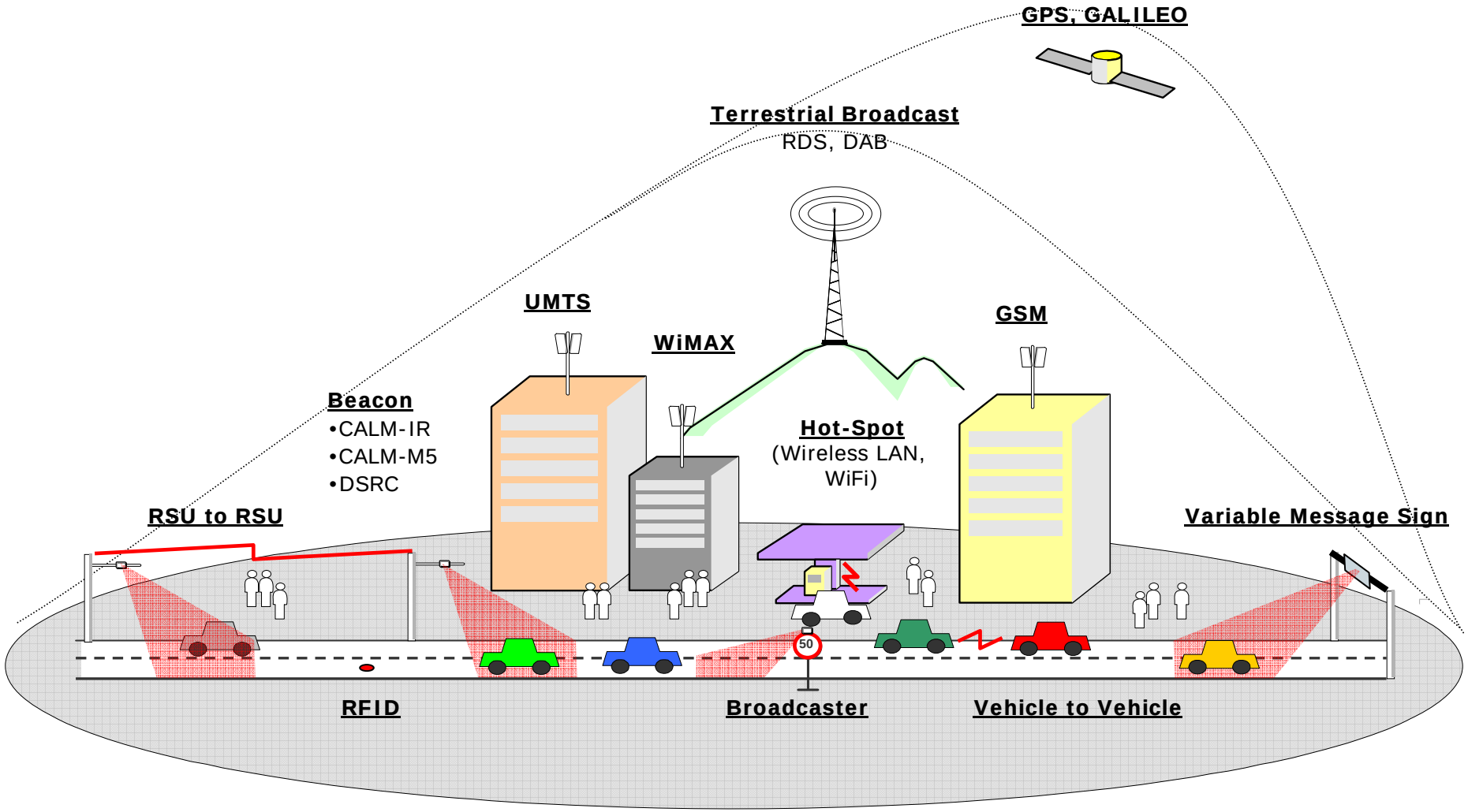
Overview

- Introduction
  - Motivation and Applications
  - ***Technology Overview***

- Communication
  - IEEE 802.11p
  - Position-based Routing

- Security and Privacy

Lot of Involved Technologies



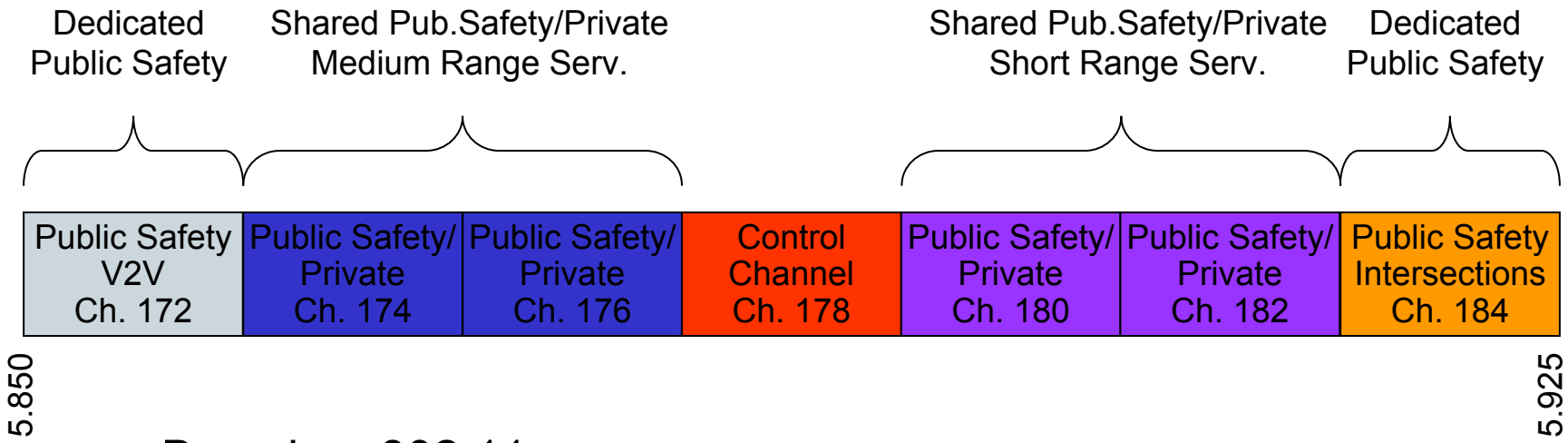
Overview

- Introduction
  - Motivation and Applications
  - Technology Overview
- Communication
  - ***IEEE 802.11p***
  - Position-based Routing
- Security and Privacy

DSRC – WAVE – IEEE 802.11p

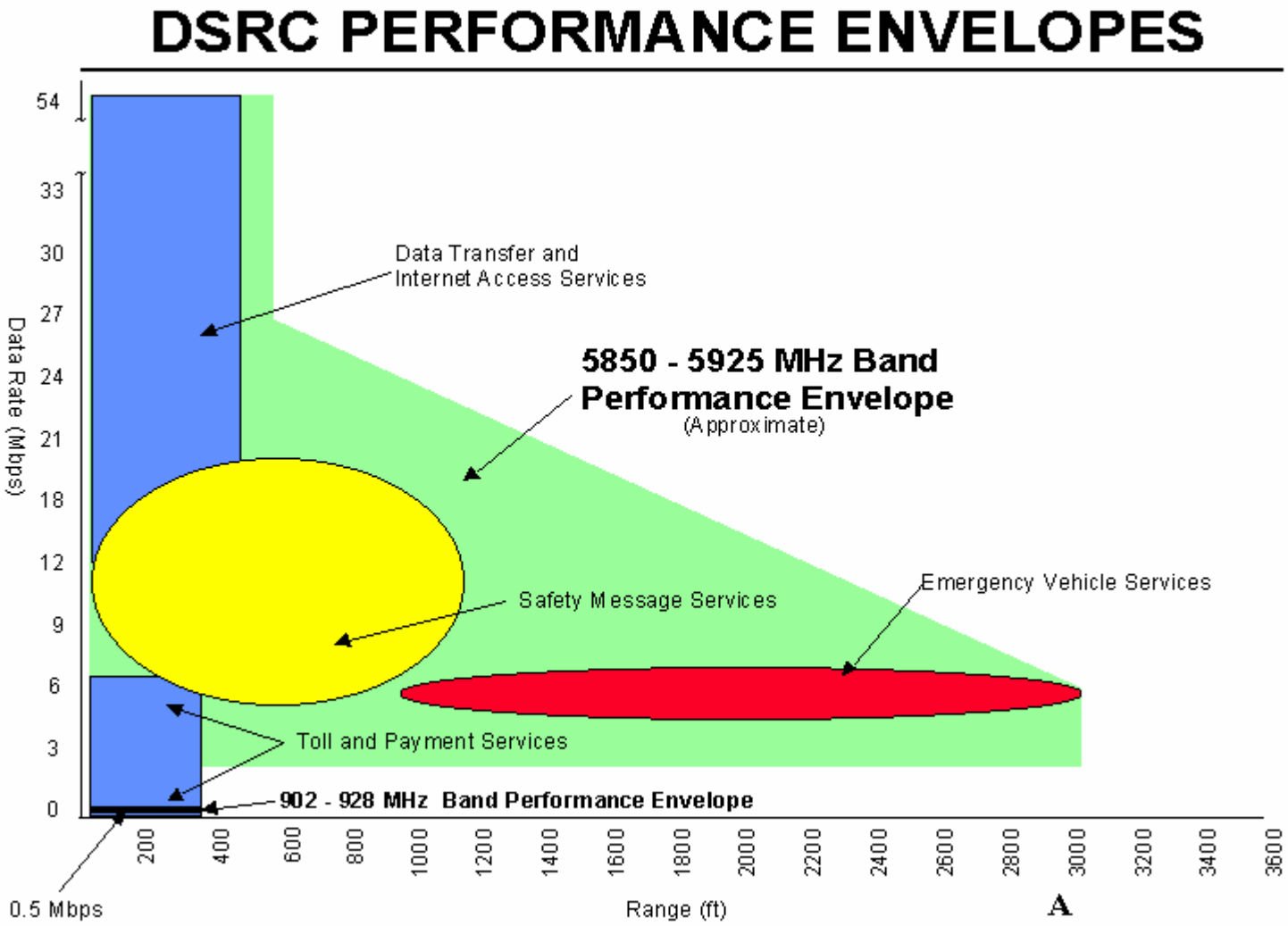
- DSRC: Dedicated Short Range Communication
  - 75 MHz spectrum set aside vor VC
- WAVE: Wireless Access in Vehicular Environments
  - Set of standards (incl. 802.11p) for VC
- IEEE 802.11p: 802.11a modification for VC
  - V2V: Vehicle-to-Vehicle Communication
  - V2I: Vehicle-to-Infrastructure Communication

IEEE 802.11p Radio



- Based on 802.11a
- 7 channels á 10 MHz
  - Can combine two channels for additional bandwidth
  - 10MHz: 6 … 27 Mbps, 20 MHz: 6 … 54 Mbps
- Maximum Range: 1000m
  - Different transmission powers
- Some details still missing, e.g. channel reservation protocol

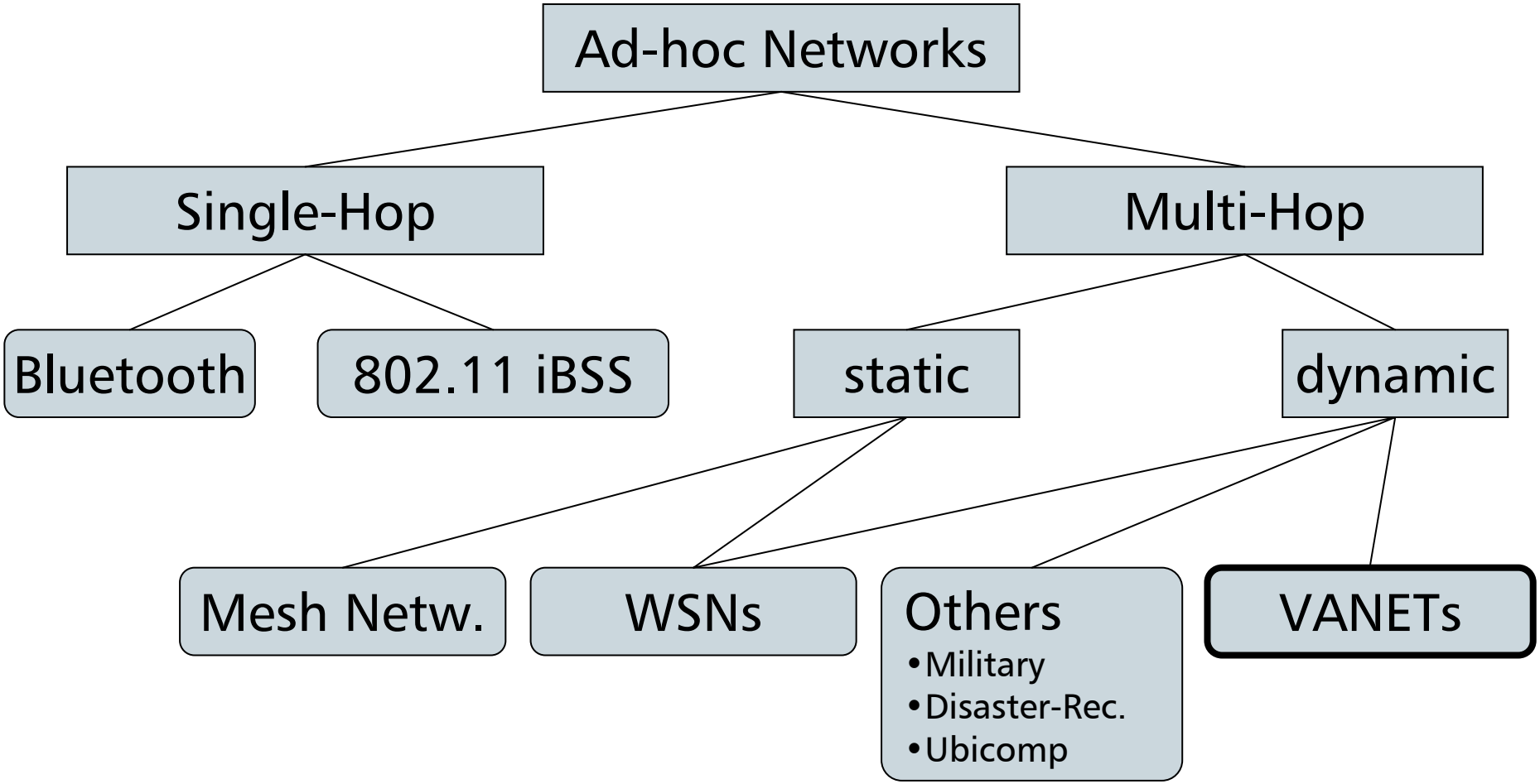
DSRC Performance



Overview

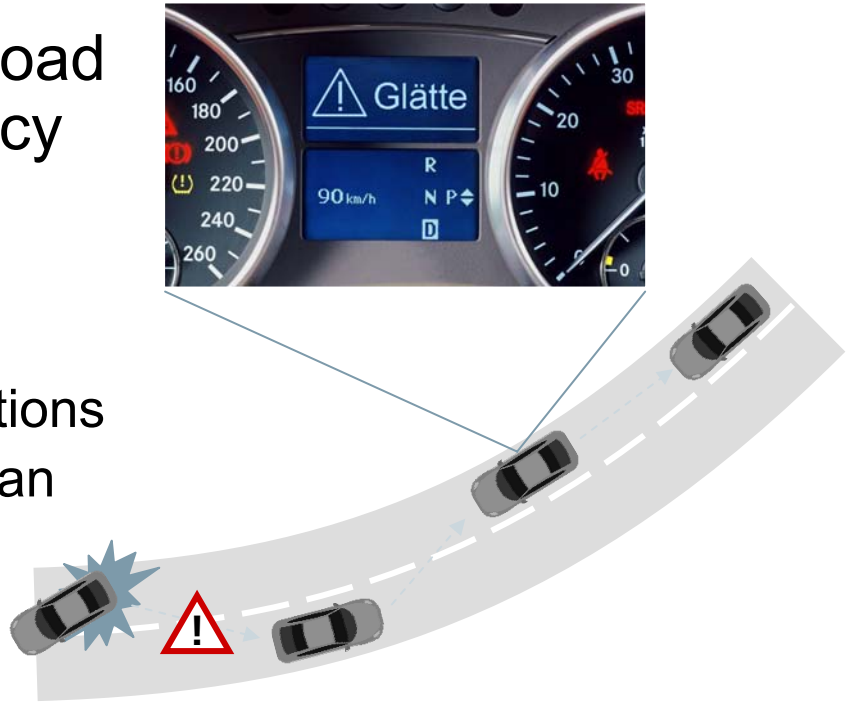
- Introduction
  - Motivation and Applications
  - Technology Overview
- Technology
  - IEEE 802.11p
  - ***Position-based Routing***
- Security and Privacy

Classification



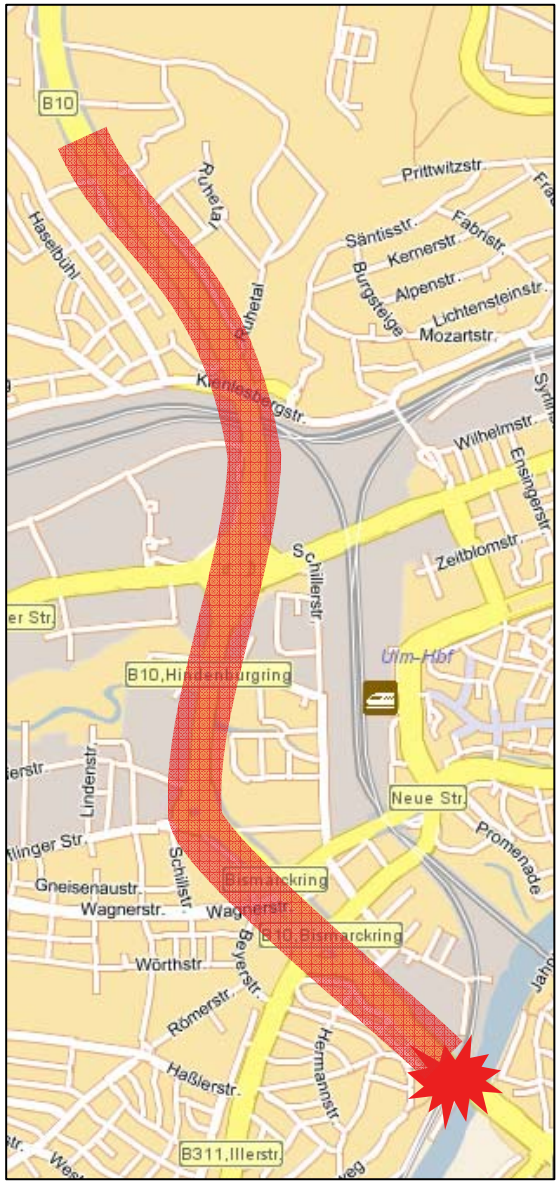
Example scenario for position-based routing: Road-Condition Warning

- Vehicles sense hazardous road or weather conditions (e.g. icy roads) using their on-board sensors (e.g. ESP)
- Information dissemination
  - Send weather and road conditions to all approaching vehicles in an area of interest
- Special properties compared to regular MANETs
  - Highly dynamic network topology
  - Different movement patterns (cities vs. highways)
  - Relatively good availability of resources (esp. energy) compared to small mobile devices



Routing in VANETs

- Often position based addressing
  - ***GeoBroadcast***: send to all nodes within a region “All cars in the area of Ulm/B10: Accident on Adenauerbridge when heading towards Neu-Ulm”
  - ***GeoAnycast***: send to arbitrary node within a region “How are traffic conditions three km ahead?“
- Fleetnet Routing Protocol
  - Address surrounding nodes:
    → Direct flooding of message in target region (“Area-Forwarding“)
  - Address remote nodes:
    → First „Line-Forwarding“, then Area-Forwarding
    - Cached Greedy Geocast (CGGC)

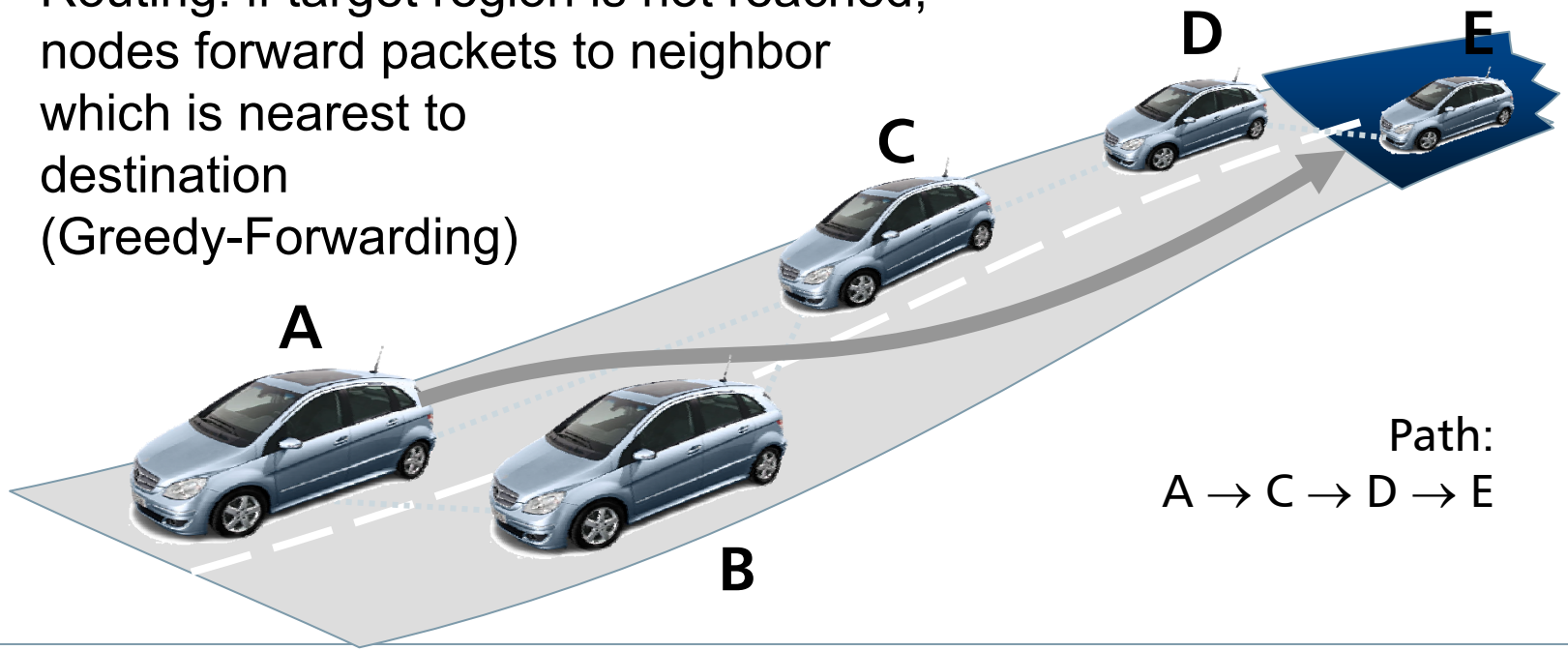


Source: www.map24.de

CGGC Line Forwarding

Line-Forwarding

- Destination: remote geographic position/region
- Each node announces its position periodically via broadcast to all reachable neighbors (Beaconing)
  → each node knows all other nodes and their position in its neighborhood
- Routing: if target region is not reached, nodes forward packets to neighbor which is nearest to destination (Greedy-Forwarding)



How to select the best neighbor: Greedy Routing Strategies

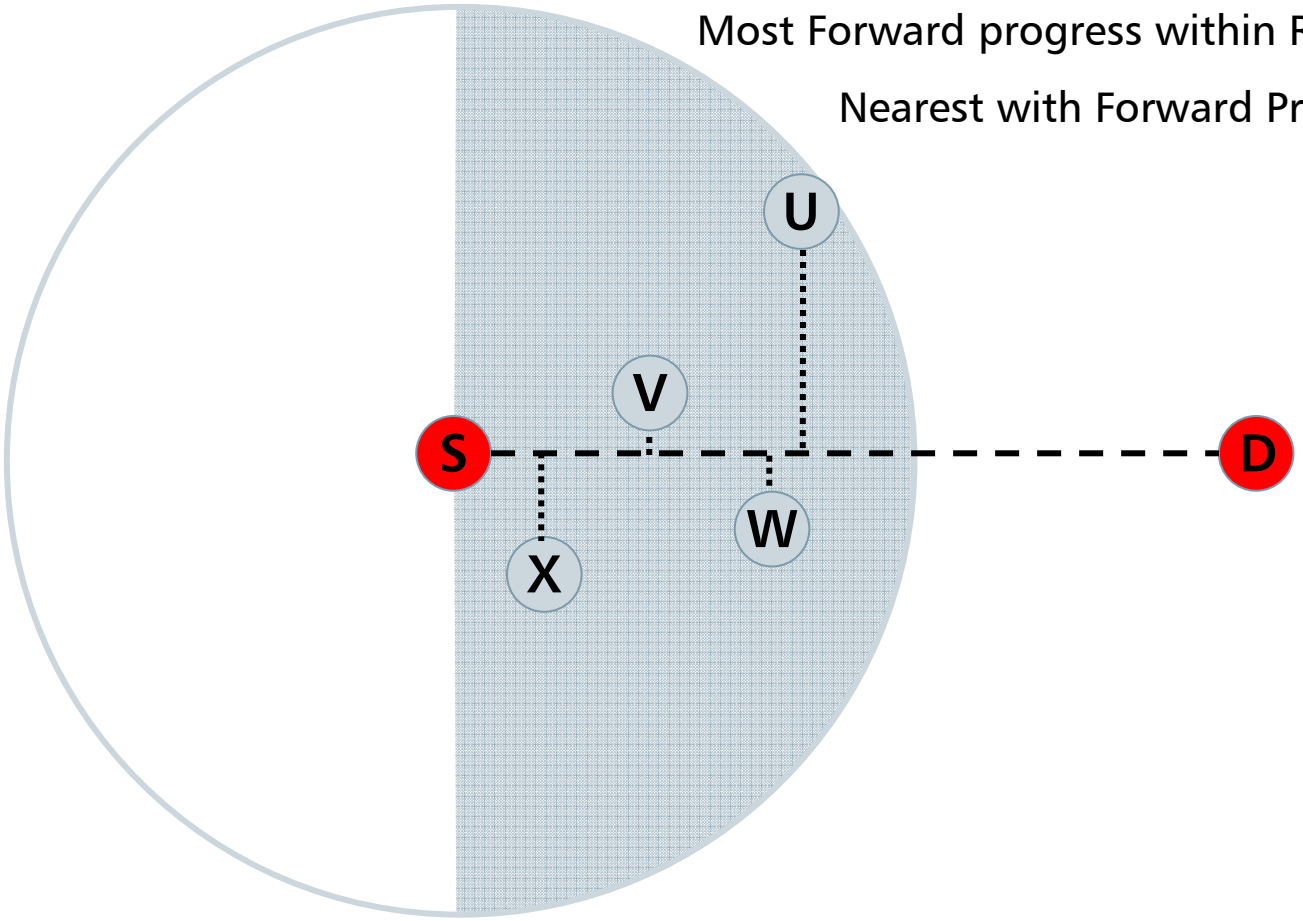
Greedy (W)

Most Forward progress within Radius - MFR (U)

Nearest with Forward Progress - NFP (X)

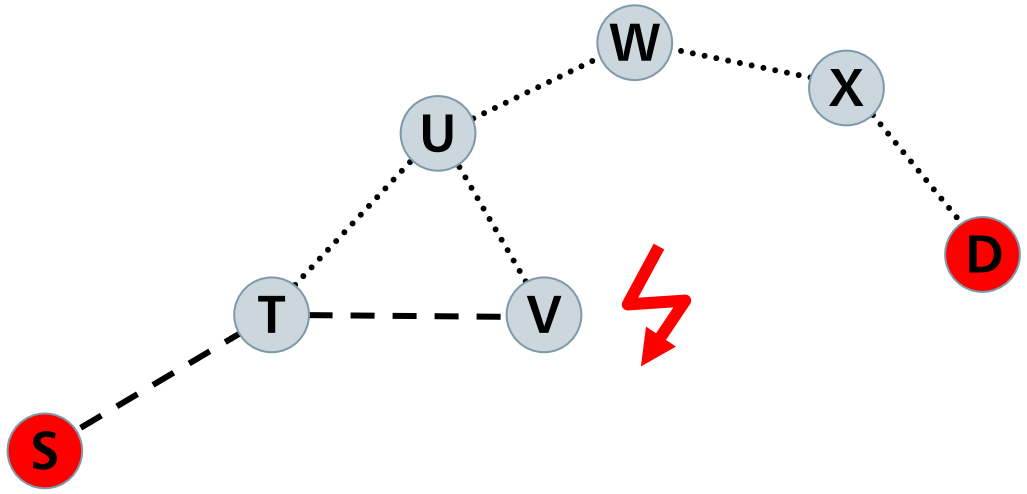
Compass (V)

Random



Local Maximum

- What to do when there is no better neighbor?
- Strategies
  - GPSR:
    parameter-Mode; left-hand rule to escape local maximum
  - CGGC:
    cache and let mobility resolve the local maximum



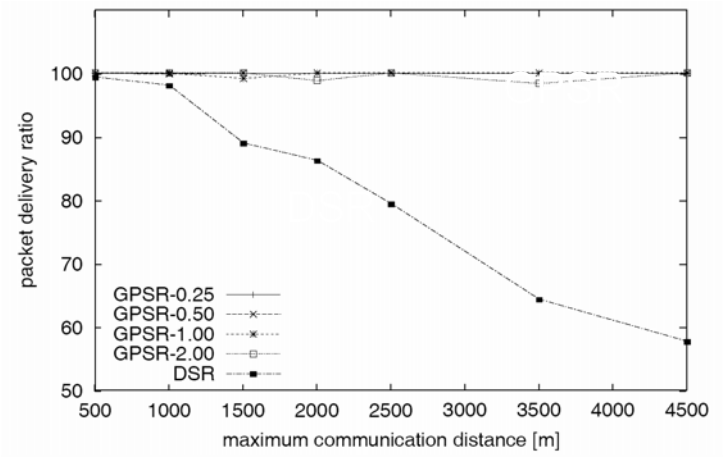
Position-based Routing

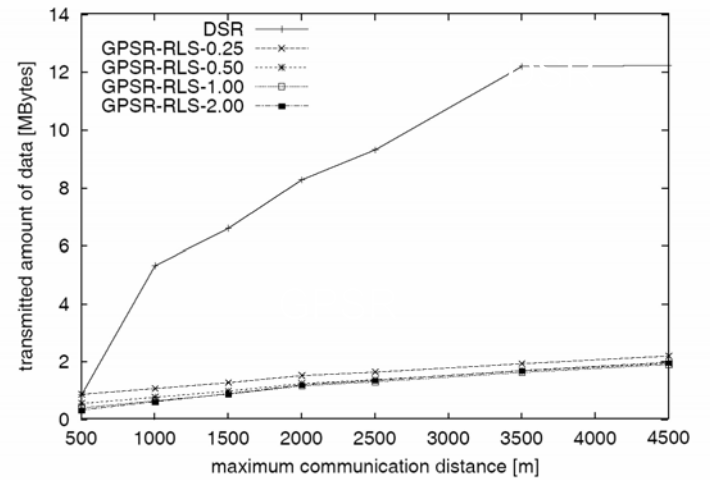
Advantages

- Applications often related to position
- No route discovery/management
  - Scalability
  - Well suited for high node mobility

Disadvantages

- Position needs to be known
  - VANETs: use GPS from navigation system
- Unicast-routing needs location service
  - Translate Node-ID → Location
  - Overhead





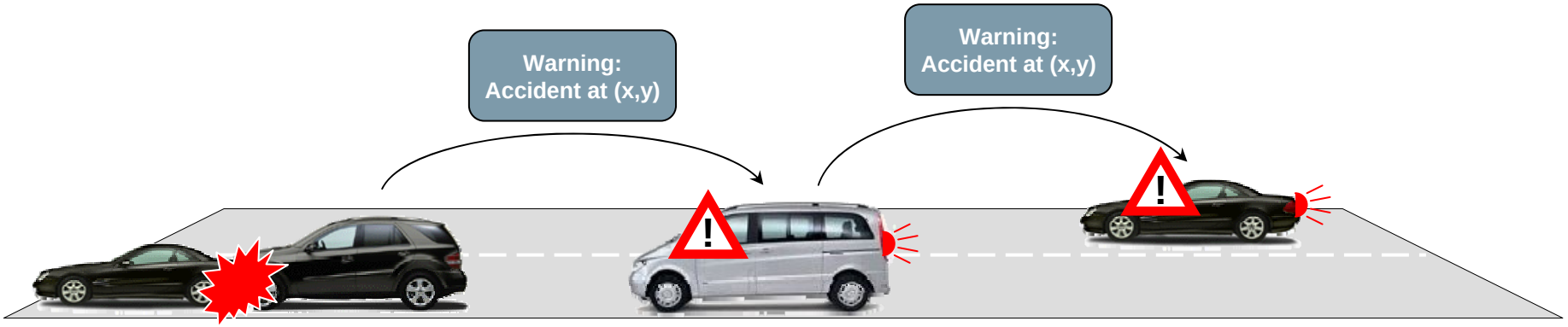
Source: Fleetnet Research Report

Overview

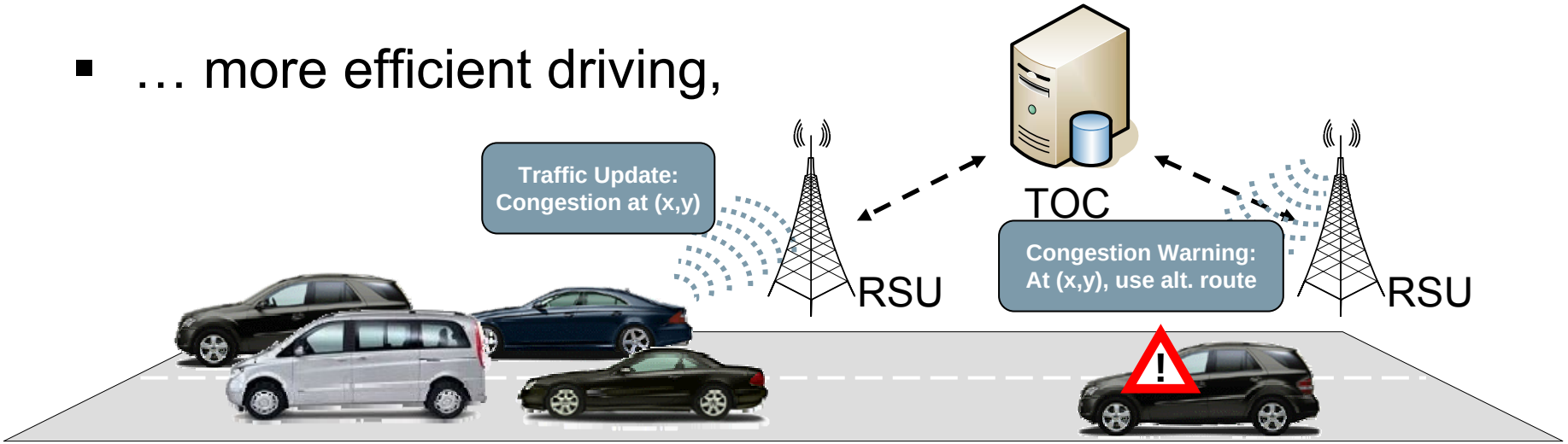
- Introduction
  - Motivation and Applications
  - Technology Overview
- Technology
  - IEEE 802.11p
  - Position-based Routing
- Security and Privacy

Vehicle Communication (VC)

- VC promises safer roads,

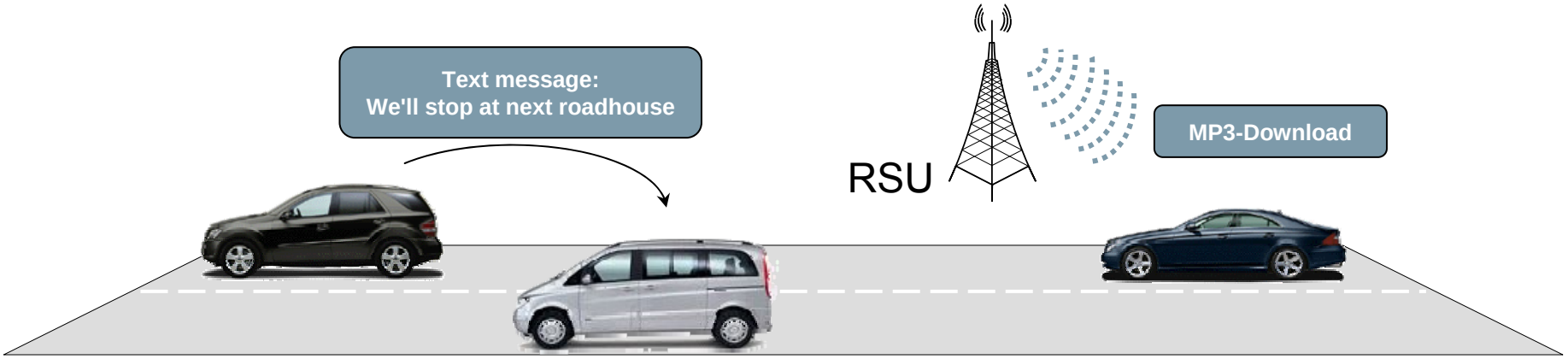


- … more efficient driving,

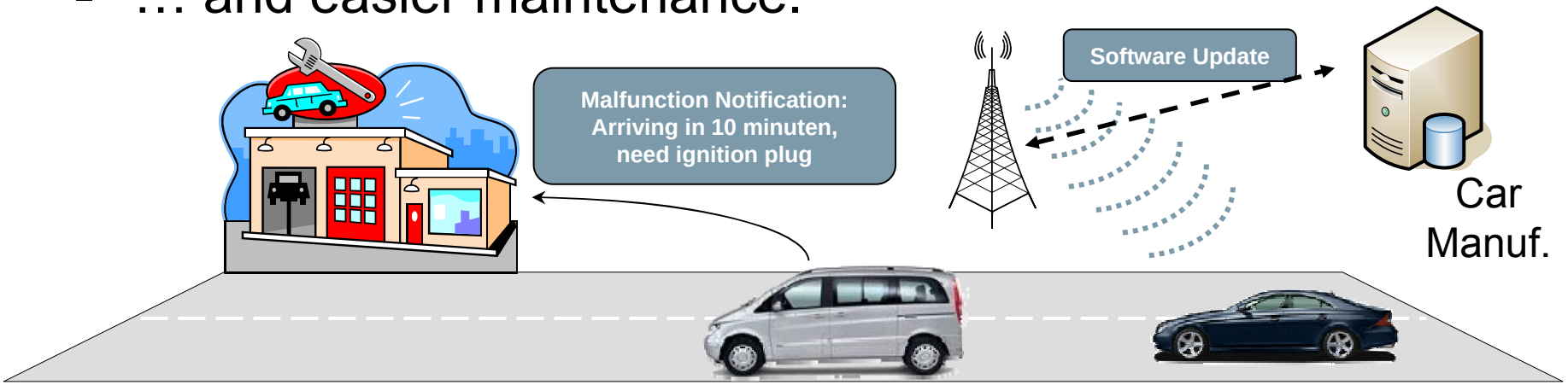


Vehicle Communication (VC)

- … more fun,



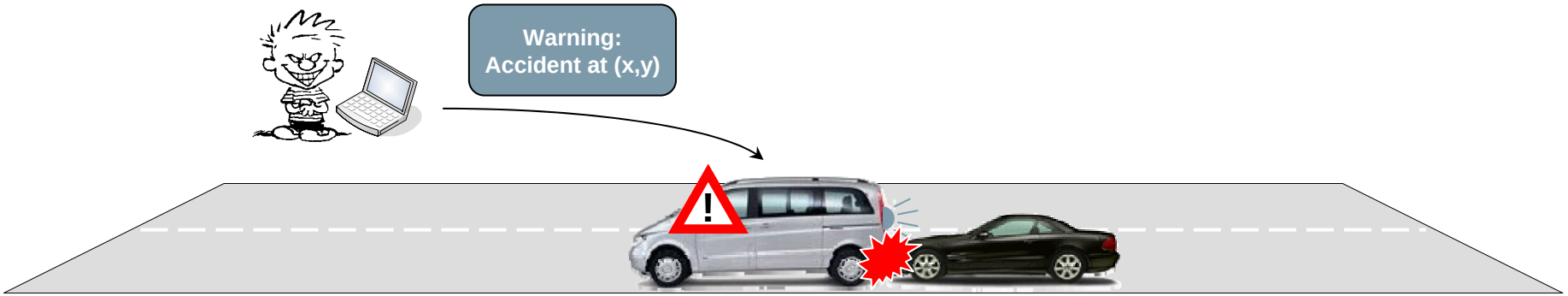
- … and easier maintenance.



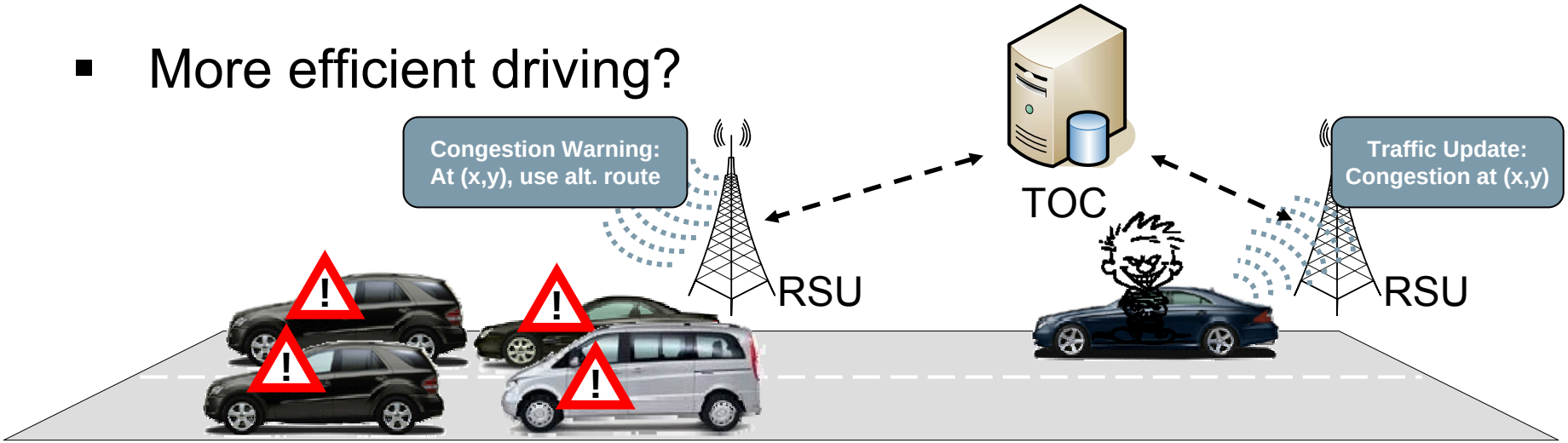

Sounds good
BUT ...

Security and Privacy???

- Safer roads?

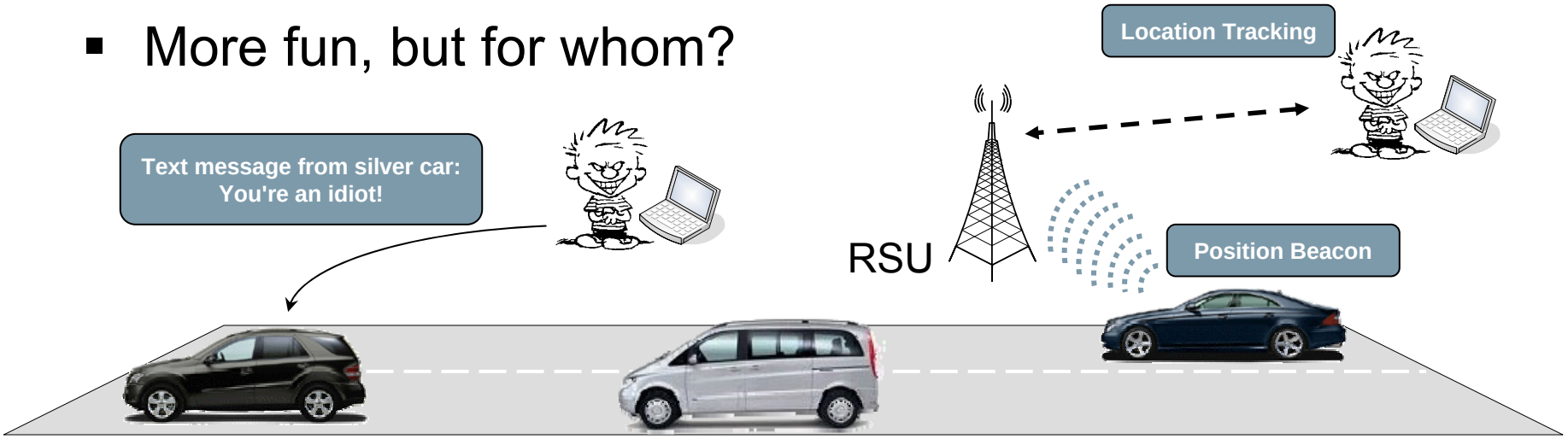


- More efficient driving?

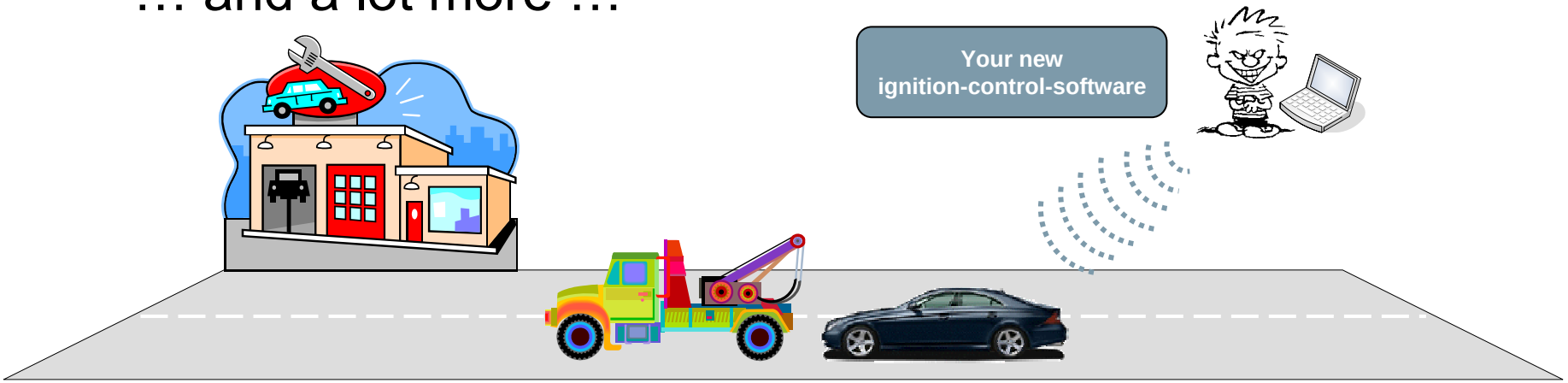


Security and Privacy???

- More fun, but for whom?



- … and a lot more …

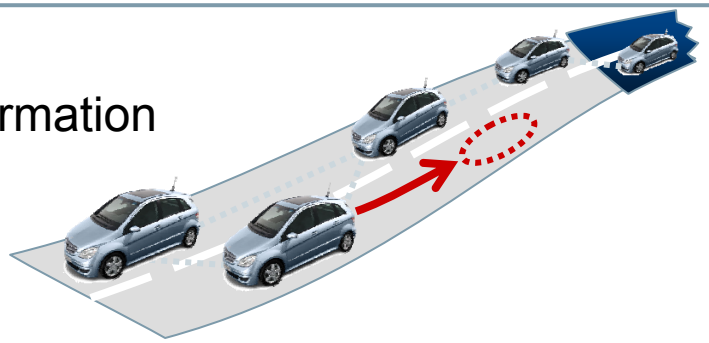


Security of Position Based Routing

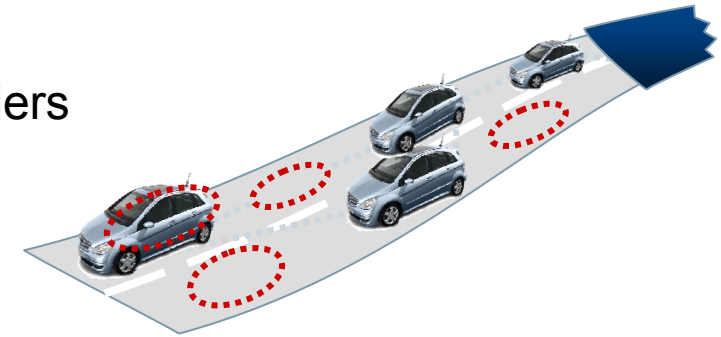
Attacking position based routing means to attack the beaconing mechanism

Attacks

- Using position information
  - Modify / falsify own position information in beacons
    - Reroute data
    - Intercept data

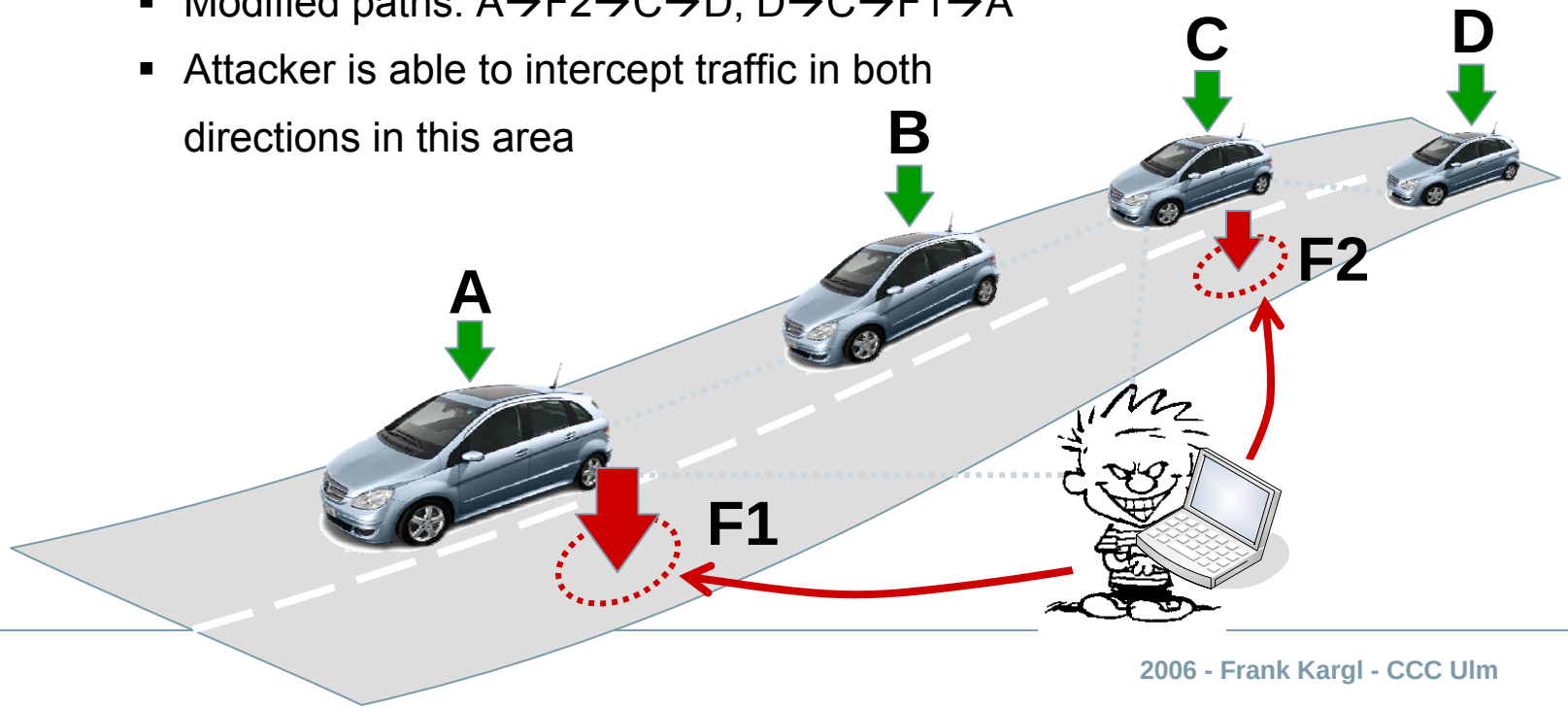


- Using node identifiers
  - Create (additional) node identifiers
    - Sybil Attack
  - Impersonate other nodes
    - Discredit other nodes

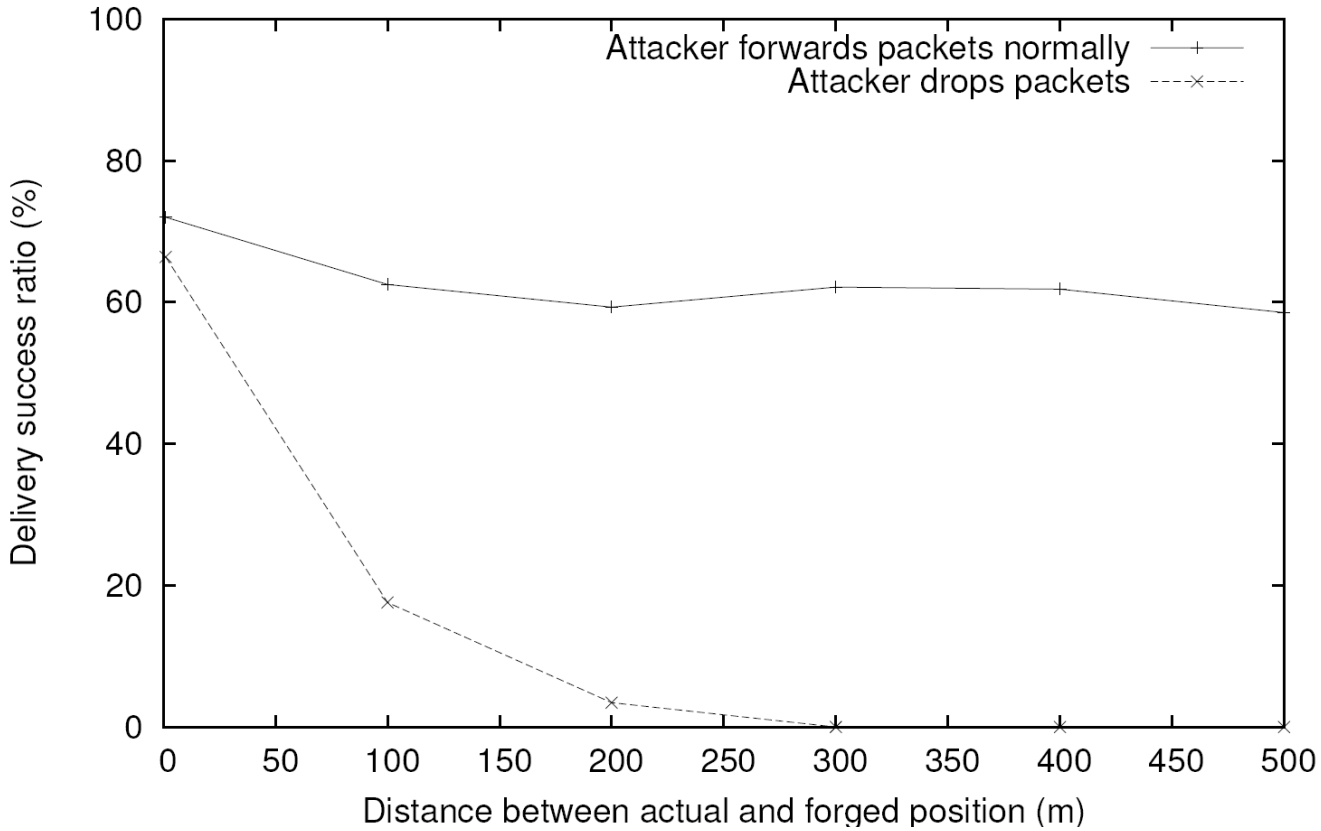


Position Faking Roadside Attacker

- Roadside attackers pretend to be part of the net and use properties of the comm. system to decrease net performance
- Example: Attacker emulates two fake nodes (F1 and F2)
  - Correct path between vehicle A and vehicle D: A→B→C→D
  - Attacker broadcasts positions for two fake vehicles
    - Modified paths: A→F2→C→D, D→C→F1→A
    - Attacker is able to intercept traffic in both directions in this area



Simulation Results: Stationary Roadside Attacker



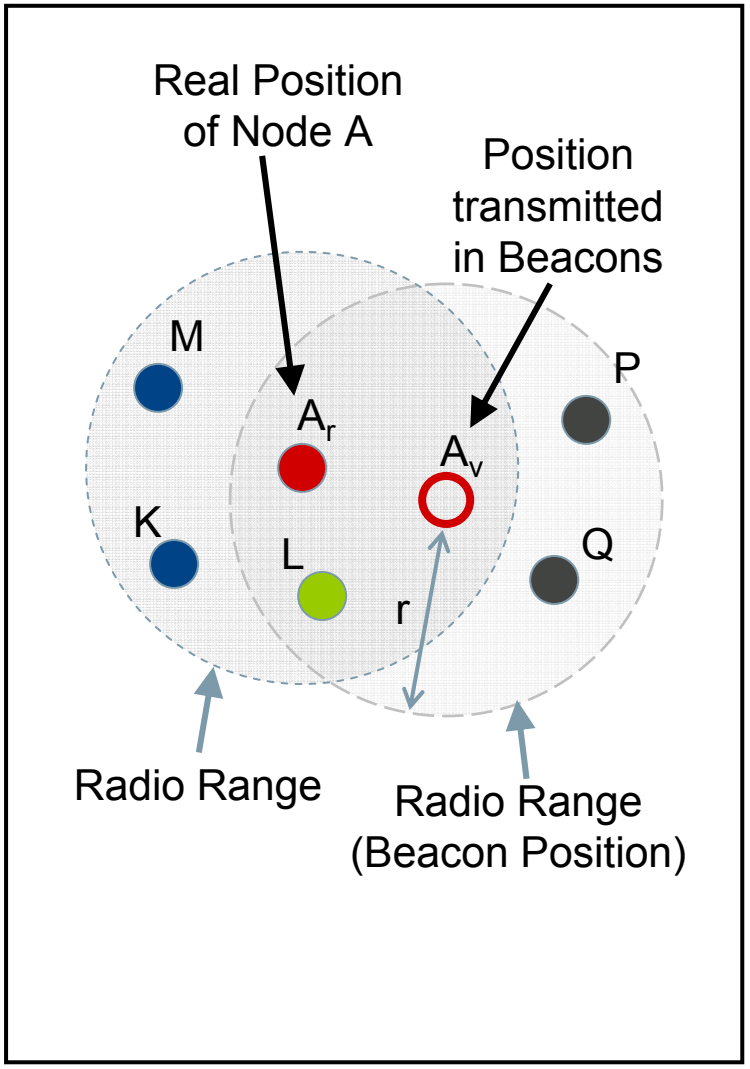
- Single roadside attacker is able to intercept and drop the entire data traffic in an area

Solutions

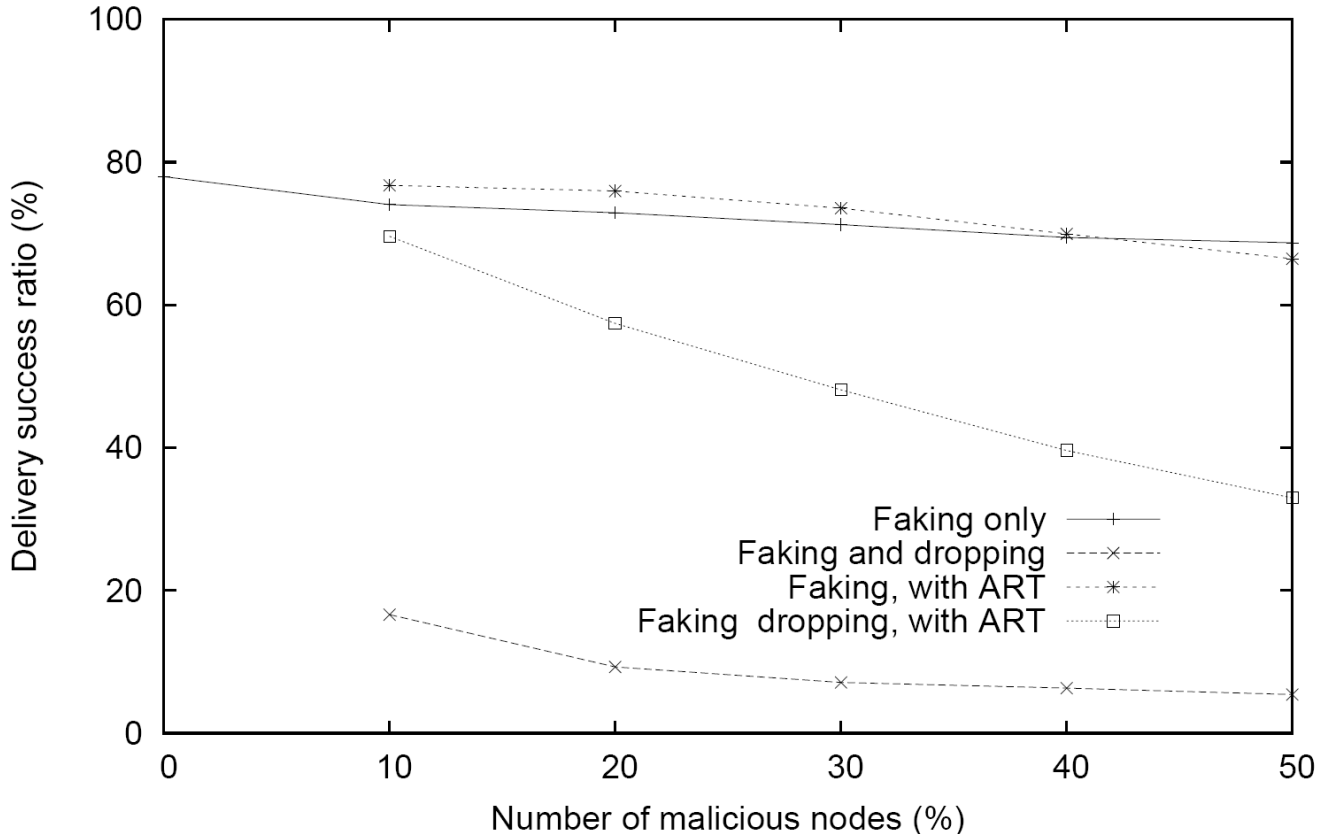
- Provable Positioning
  - Related work on secure GPS etc.
  - Change GPS???
- Physical Measurement
  - TOA, TDOA, …
  - Additional Hardware for positioning???
- Heuristics
  - Simple, easy
  - Sufficient effective?

Example: Acceptance Range Threshold

- Based on the limited radio range
- Maximum ART := Δ_{max}
- Accept neighbors N where distance(Pos(N_i),Pos(N_j)) ≤ Δ_{max}, otherwise ignore them
- The bigger the distance between A_r und A_v, the more nodes will detect the falsified position
- Issues
  - Fixed threshold is not flexible enough
  - False positions within reasonable distance will not be detected by some neighbors
- Example
  - M, K: distance([M|K],A_v) > Δ_{max} ➔ ignore
  - L : distance(L,A_v) ≤ Δ_{max} ➔ accept
  - Q, P: no beacon received



Simulation Results: Delivery Success Ratio

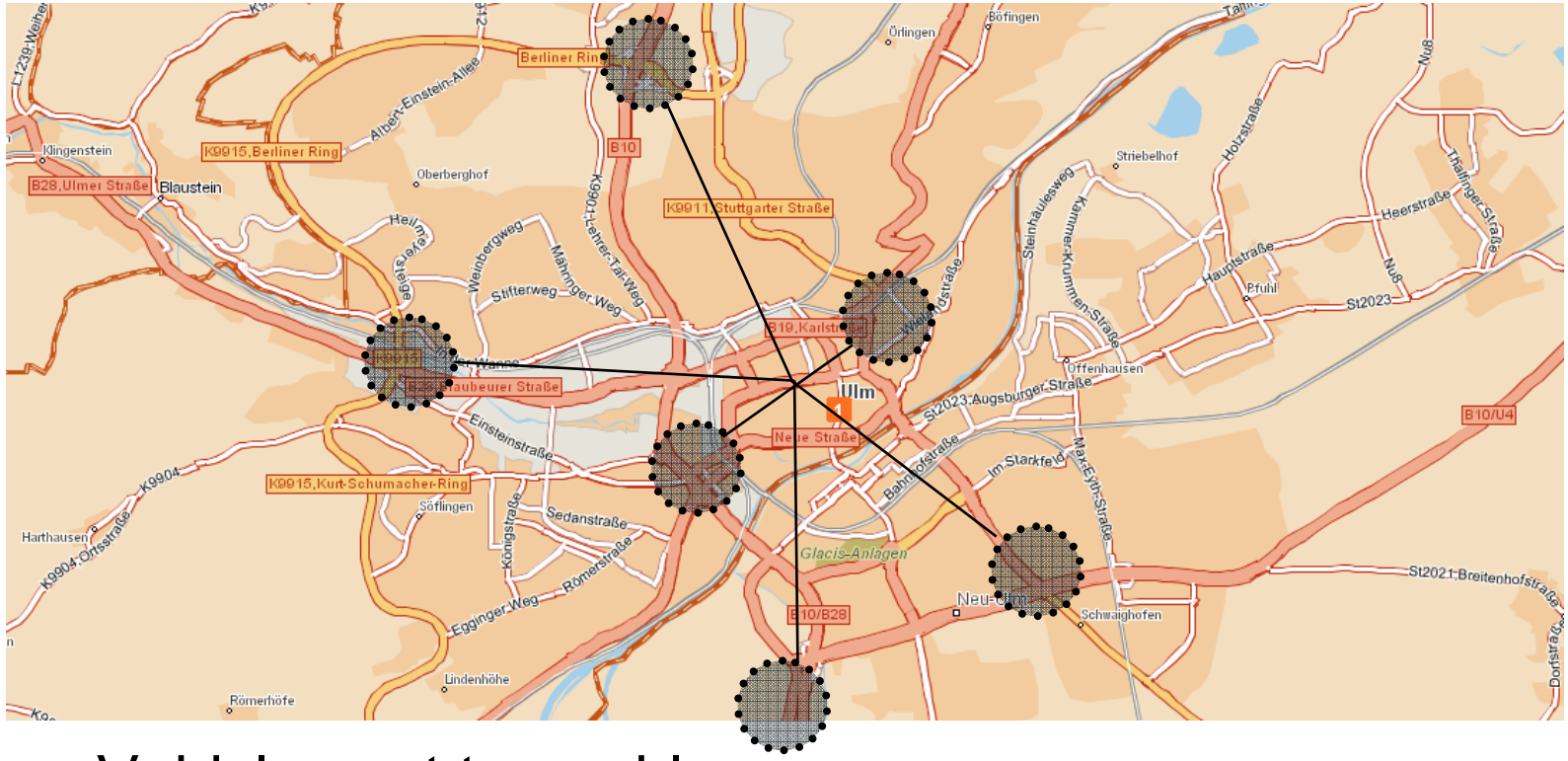


- Performance degradation reduces when applying the position verification system

Other Sensors

- Mobility Grade Threshold (MGT)
  - Based on limited velocity of nodes
  - Maximum node velocity := Vmax
- Overhearing
  - Nodes monitor data traffic of neighboring nodes and try to identify irregularities
  - Own packet is routed to a less suitable neighbor at the next hop
  - Other nodes forward packets to a node that normally should not be able to receive the packet
- Maximum Density Threshold (MDT)
  - Based on the fact that only a restricted number of physical entities can reside in a certain area
  - Maximum node density ρ_{max}
- Map-based Verification
  - Based on the assumption that vehicles move mainly on roads
- …

Privacy in VANETs



- Vehicles get traceable
  - Macroscopic tracing – e.g. over the country
  - Coarse-grain tracing – e.g. down to certain roads
  - Fine-grain tracing – exact positions and times

Map source: www.map24.de

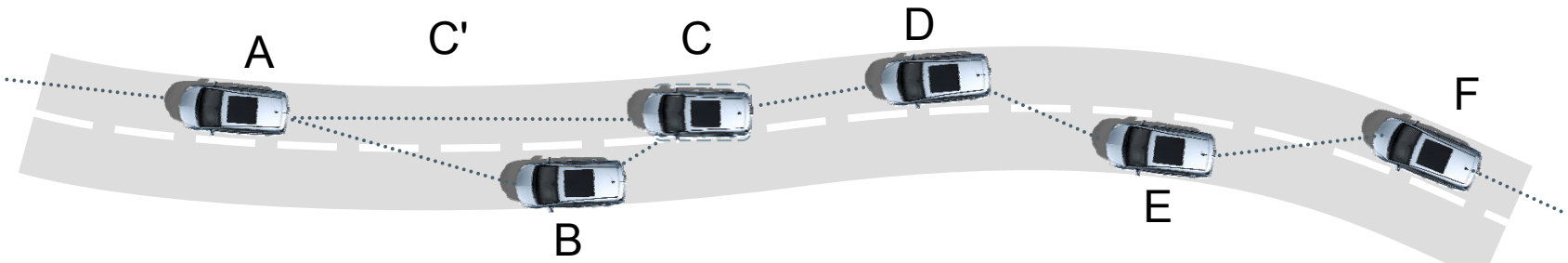
Changing Pseudonyms

- Concept:
  - → Nodes change their ID from time to time
  - → Observations cannot (trivially) be linked
- Drawbacks
  - Linking pseudonyms might be possible due to
    - Correlation of identifiers between changes
      - Cross-layer issues, heuristics, hardware fingerprinting, …
      - Context of the node (e.g. unique itinerary, few nodes)
  - Operability of system is influenced
    - Sessions may be interrupted
    - Communication protocols may stall

→ What is the impact of changing pseudonyms on geographic routing?

Changing Pseudonyms

- If pseudonyms change frequently, privacy profits
  - Linking different pseudonyms together gets harder
- On the other hand, geographic routing performance declines due to invalid neighbor table entries
  - After a pseudonym change, old (ID,Position)-tupel remain in neighbor tables until expiration
  - Routing metric only respects neighbor position
  - → Probability of selecting outdated neighbors as next hop



- Selected route from A to F until beacon timeout still:

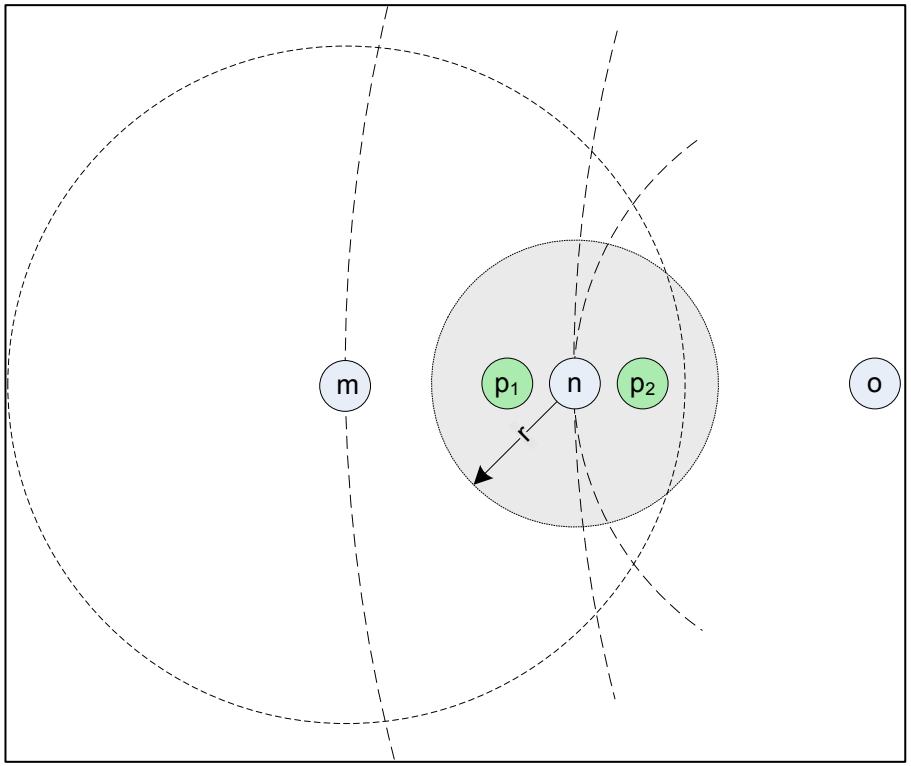
  $A \rightarrow C \rightarrow D \rightarrow E \rightarrow F$

Analytical Study of Impact

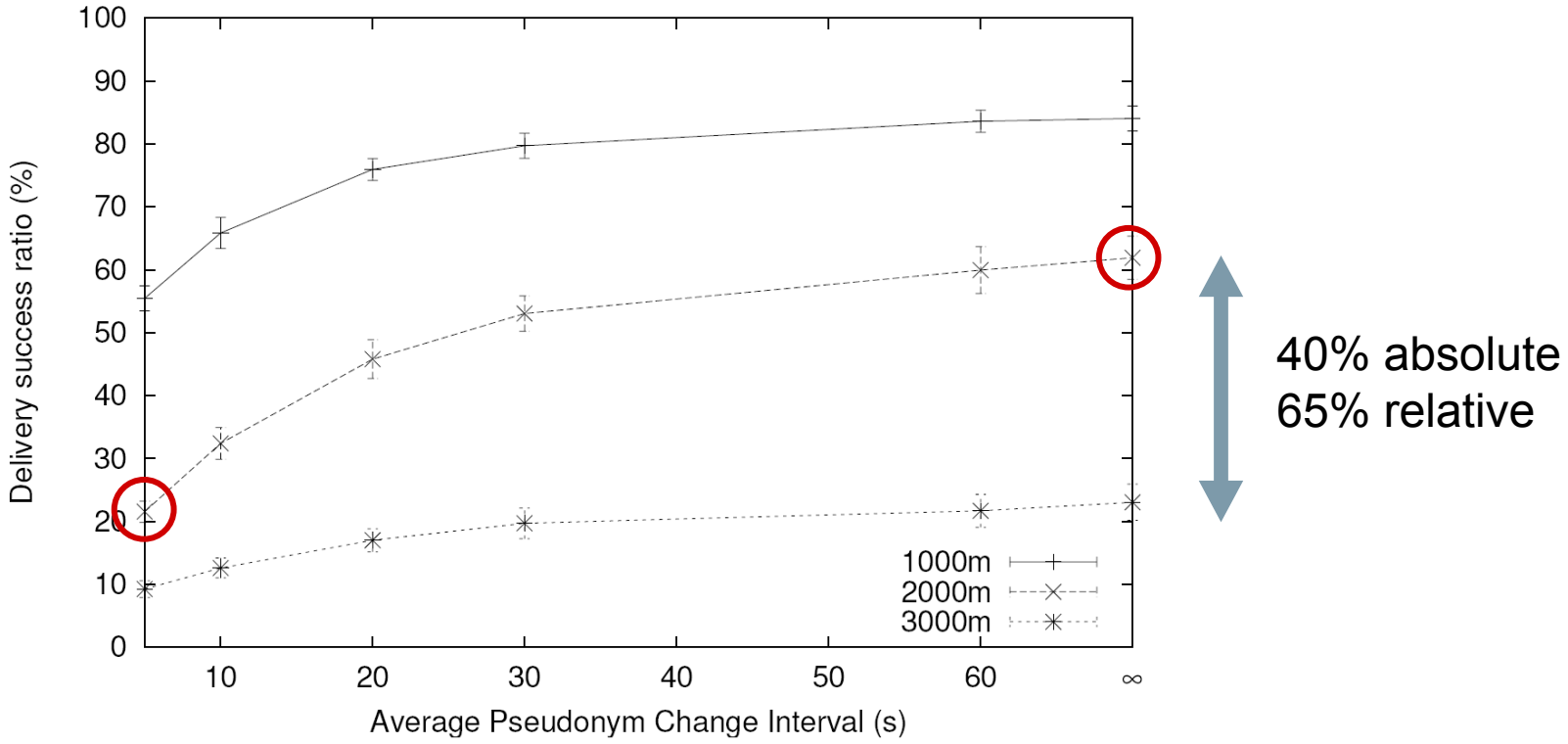
- Parameters
  - Beacon rate – *b*
  - Packet rate – *p*
  - Expiration timeout – t_0
  - Pseudonym change rate – *c*

- Total loss probability within one t_0 interval

$$P_{loss} = \frac{t_o}{2c}$$



Simulation results support these findings



- Notable decrease in delivery ratio with 5 seconds ID change interval
  - For 2000 x 2000 m, ~ 65% less packets delivered

SE-cure VE-hicle COM-munication

- Mission:
  practical solution to the problem of V2V/V2I security

- IST STREP Project. 1/1/2006-1/1/2009
- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Ricerche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

Security Mechanisms

- Identified ~20 different security mechanisms needed to conquer the most attacks
- Examples
  - PKI for VANET
    - Prevent sibyl attacks
    - Efficient revocation
    - Cheap operation
  - Anonymization layer
    - Pseudonyms with revocation
  - Routing and forwarding security
  - Consistency Checks
  - In-Vehicle protection mechanisms
  - …

Identification & Authentication Concepts
Identification
Authentication of sender
… and sender is
Authentication of receiver
Property authentication
Authentication of intermediate nodes
Privacy Concepts
Resolvable anonymity
Total anonymity
Location obfuscation
Integrity Concepts
Encryption
Integrity protection
Detection of protocol violation
Jamming protection
Tamper-resistant comm. system
DRM
Replay protection
Consistency/context checking
Attestation of sensor data
Location verification
Access Control/Authorization Concepts
Access control
Firewall/Checkpoint
Closed user groups
Filtering (e.g at intermediate nodes)
Sandbox

THE END!!! Questions?

Frank Kargl (frank.kargl@ulm.ccc.de)
IM: comram@jabber.ccc.de
CCC Ulm, Ulm University