The Security and Privacy of Smart Vehicles

Jean-Pierre Hubaux

EPFL

Joint work with Srdjan Capkun,
Jun Luo, and Maxim Raya

http://lcawww.epfl.ch/

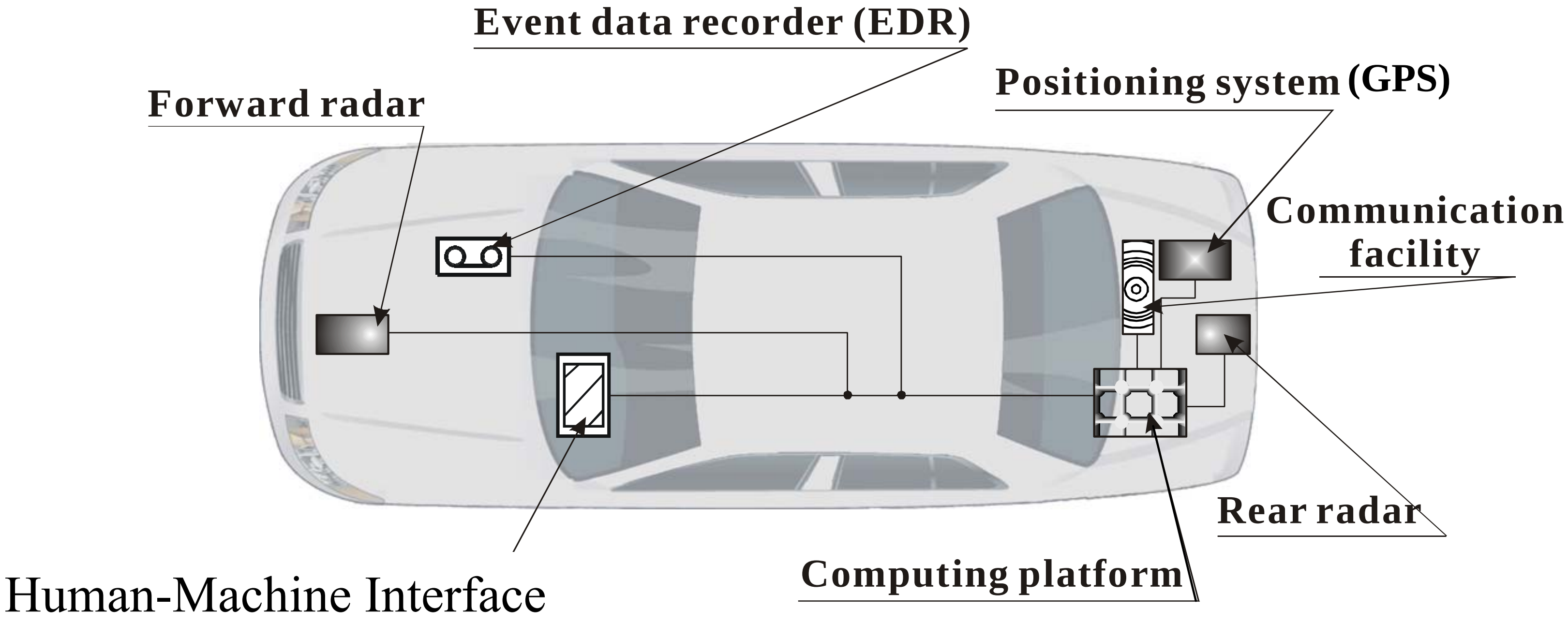
The Security and Privacy of Smart Vehicles

- Motivation
- Proposed model
- The case for secure positioning
- Security design options
- Conclusion

The urge for security in Vehicular Communications

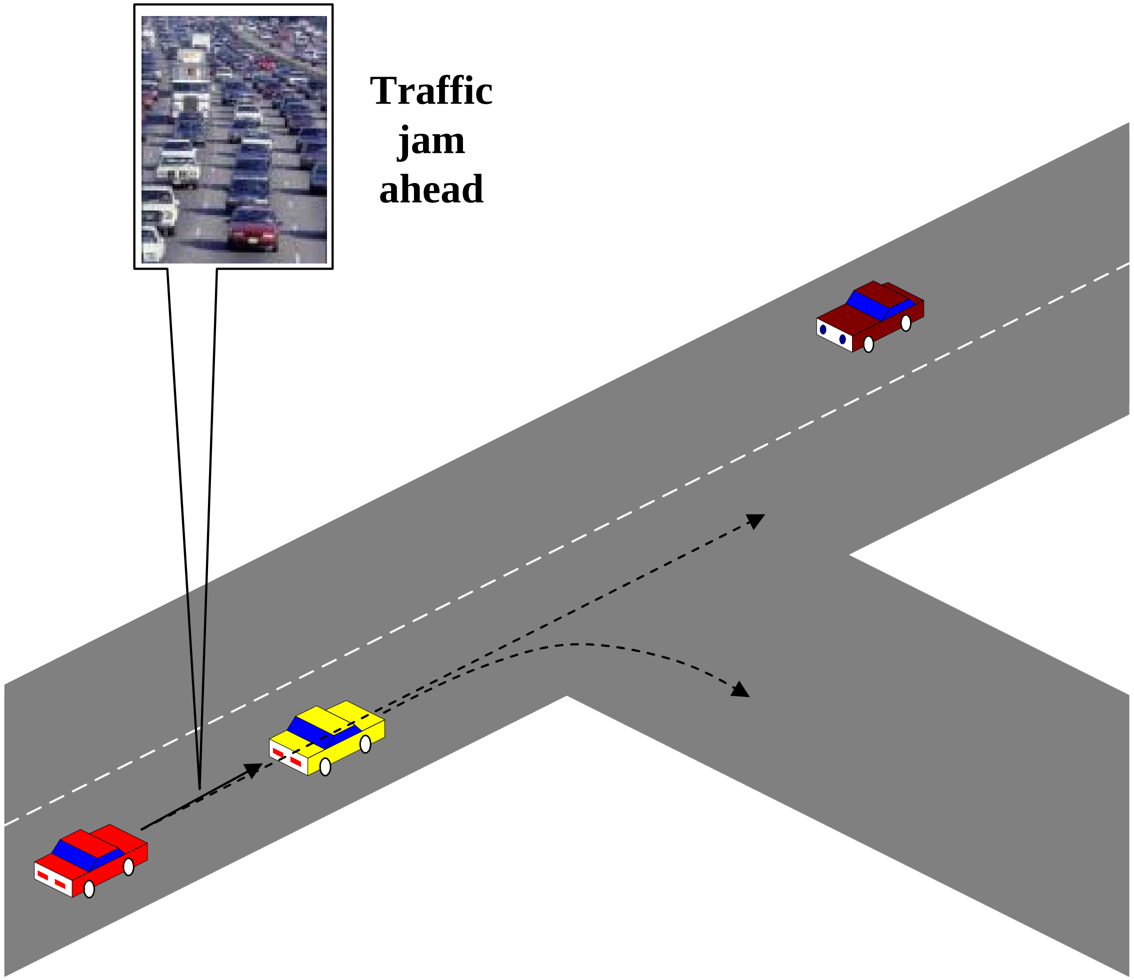
- Large projects have explored vehicular communications : PATH (UC Berkeley), Fleetnet,…
- No solution can be deployed if not properly secured
- The problem is non-trivial
  - Specific requirements (speed, real-time constraints)
  - Contradictory expectations
- Industry front: standards are still under development
  - IEEE P1556: Security and Privacy of Vehicle and Roadside Communications including Smart Card Communications
- Research front
  - ***No single paper*** on vehicular security in IEEE Vehicular Technology Conference (VTC) !

A smart vehicle



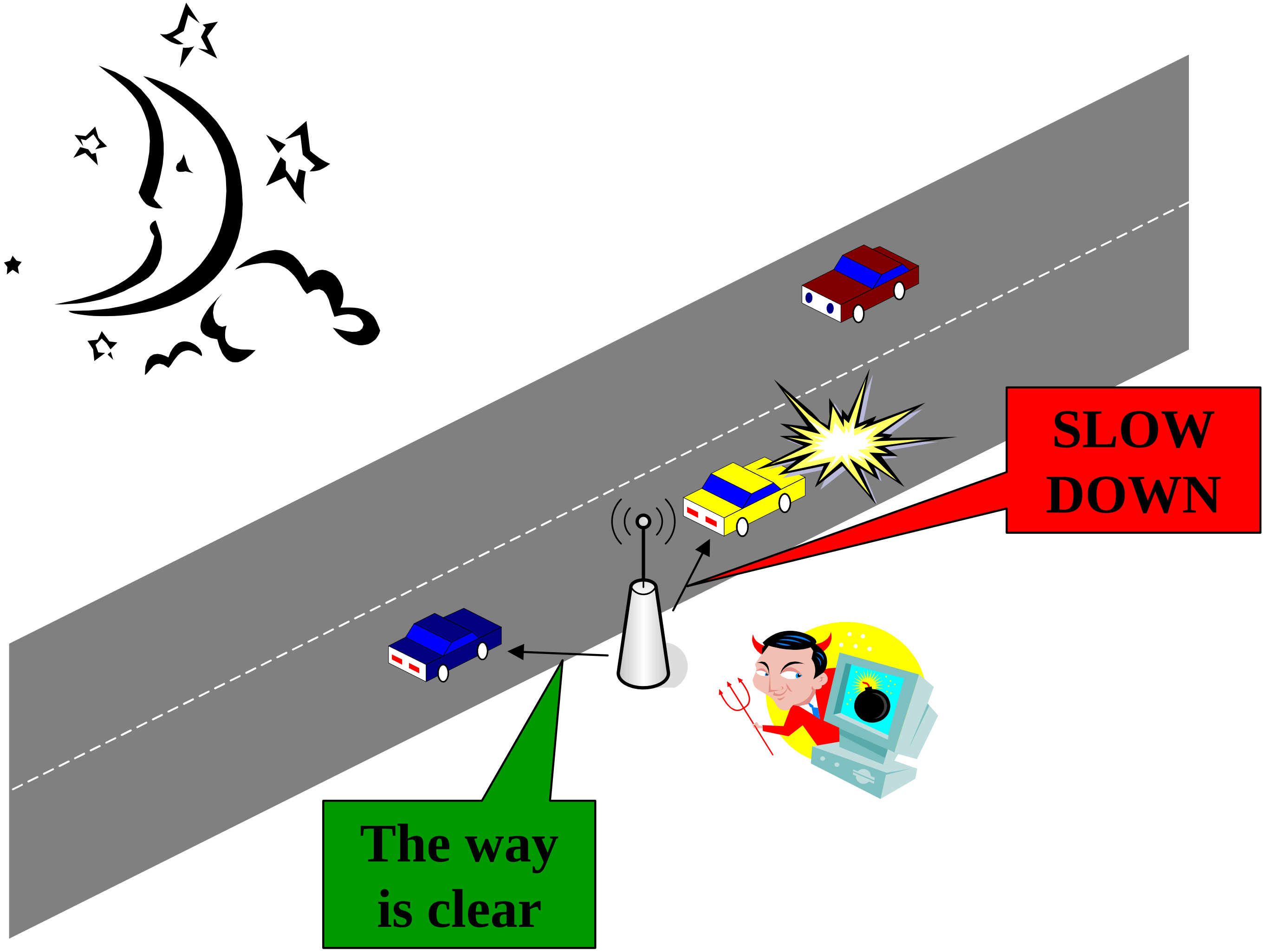
- Communication: typically over the Dedicated Short Range Communications (DSRC) (5.9 GHz)
- Example of protocol: IEEE 802.11p
- Penetration will be progressive (over 2 decades or so)
- Note: we will consider radars to be optional

Attack 1 : Bogus traffic information



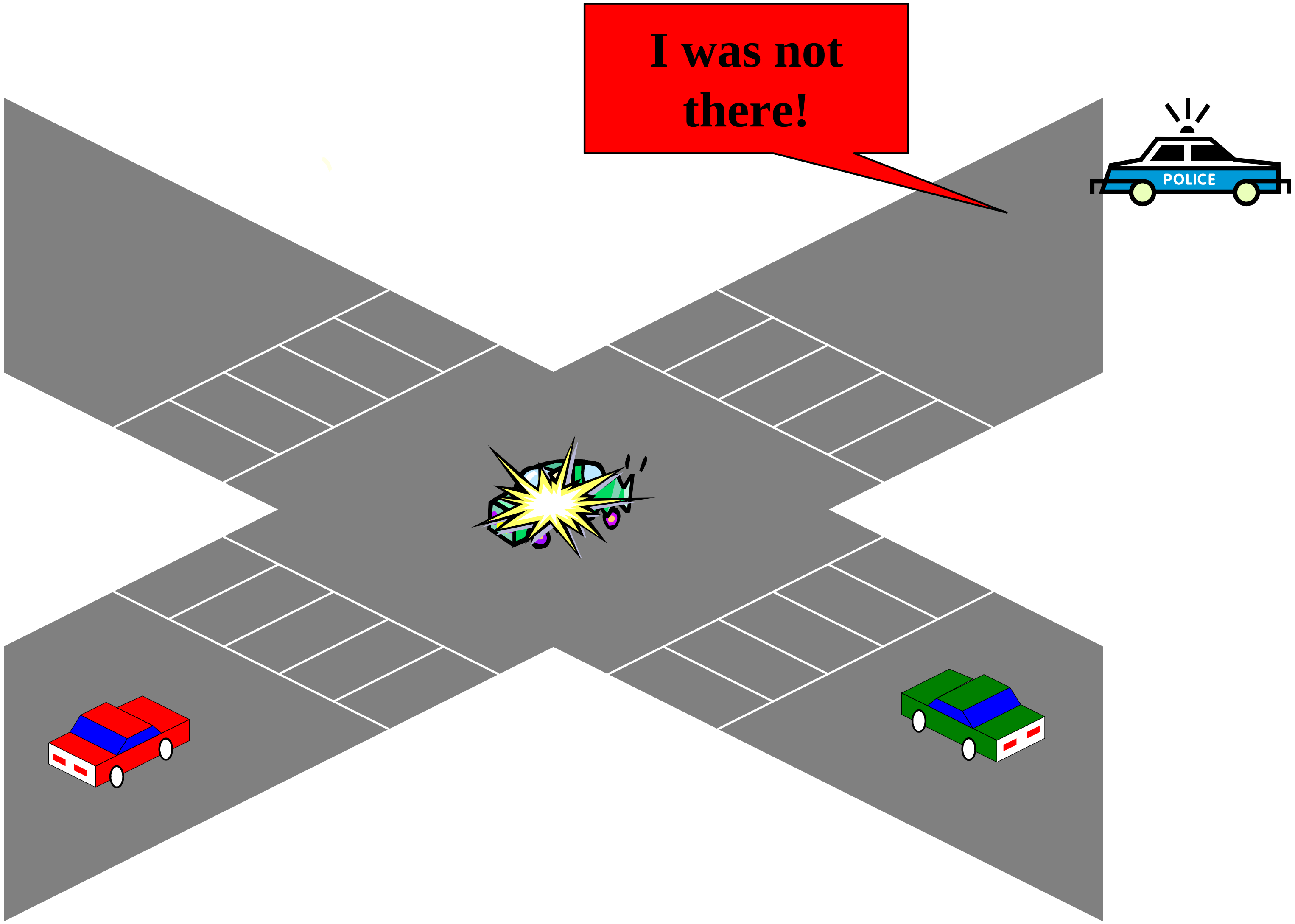
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



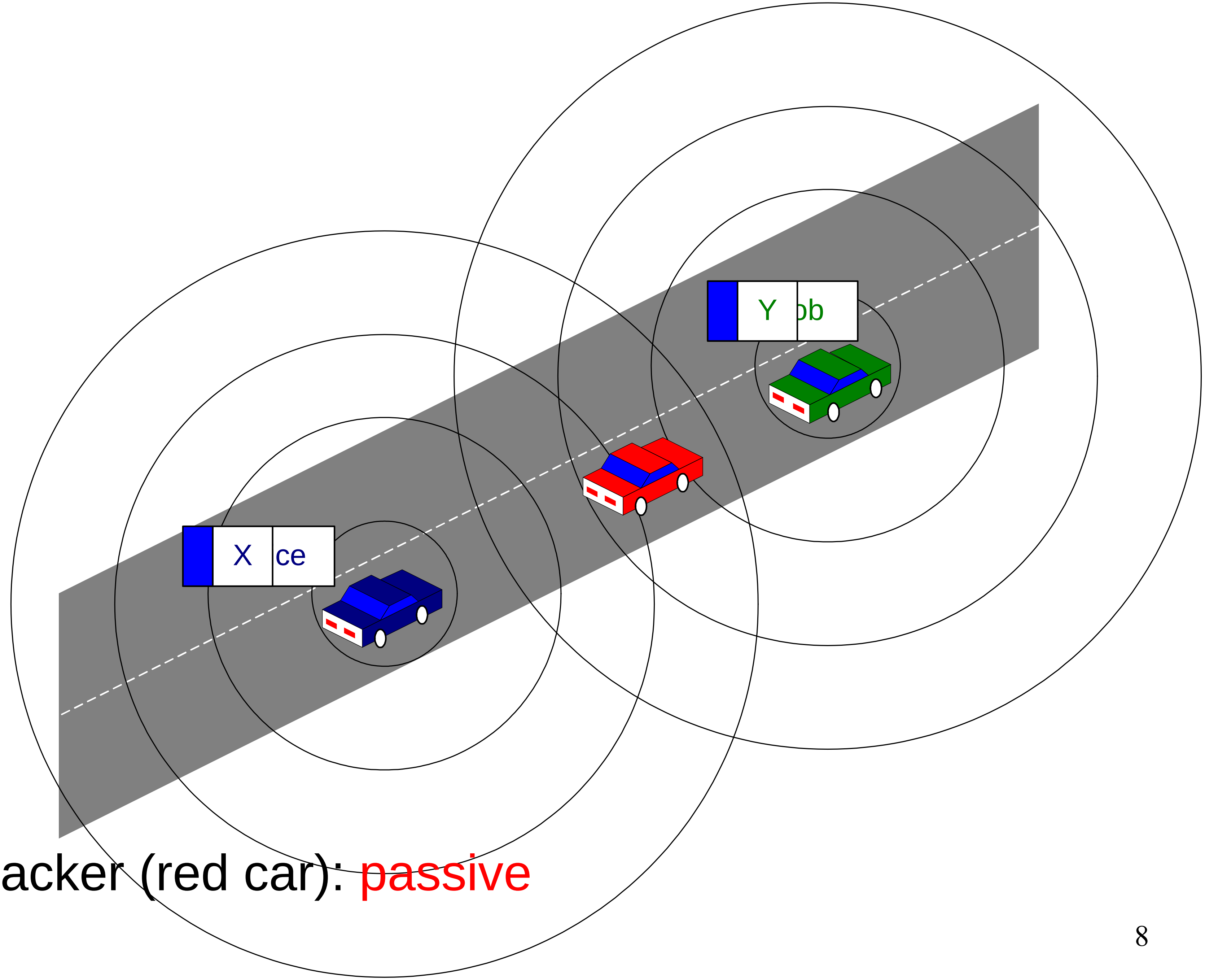
- Attacker: malicious, active

Attack 3: Cheating with identity, position or speed



- Attacker: insider, rational, active

Attack 4 : Uncovering the identities of other vehicles



- Attacker (red car): passive

DSRC APPLICATIONS
PUBLIC SAFETY and PRIVATE

PUBLIC SAFETY

- APPROACHING EMERGENCY VEHICLE (WARNING) ASSISTANT (3)
- EMERGENCY VEHICLE SIGNAL PREEMPTION
- ROAD CONDITION WARNING
- LOW BRIDGE WARNING
- WORK ZONE WARNING
- IMMINENT COLLISION WARNING (D)
- CURVE SPEED ASSISTANCE [ROLLOVER WARNING] (1)
- INFRASTRUCTURE BASED – STOP LIGHT ASSISTANT (2)
- INTERSECTION COLLISION WARNING/AVOIDANCE (4)
- HIGHWAY/RAIL [RAILROAD] COLLISION AVOIDANCE (10)
- COOPERATIVE COLLISION WARNING [V-V] (5)
- GREEN LIGHT - OPTIMAL SPEED ADVISORY (8)
- COOPERATIVE VEHICLE SYSTEM – PLATOONING (9)
- COOPERATIVE ADAPTIVE CRUISE CONTROL [ACC] (11)
- VEHICLE BASED PROBE DATA COLLECTION (B)
- INFRASTRUCTURE BASED PROBE DATA COLLECTION
- INFRASTRUCTURE BASED TRAFFIC MANAGEMENT – [DATA COLLECTED from] PROBES (7)
- TOLL COLLECTION
- TRAFFIC INFORMATION (C)
- TRANSIT VEHICLE DATA TRANSFER (gate)
- TRANSIT VEHICLE SIGNAL PRIORITY
- EMERGENCY VEHICLE VIDEO RELAY
- MAINLINE SCREENING
- BORDER CLEARANCE
- ON-BOARD SAFETY DATA TRANSFER
- VEHICLE SAFETY INSPECTION
- DRIVER'S DAILY LOG

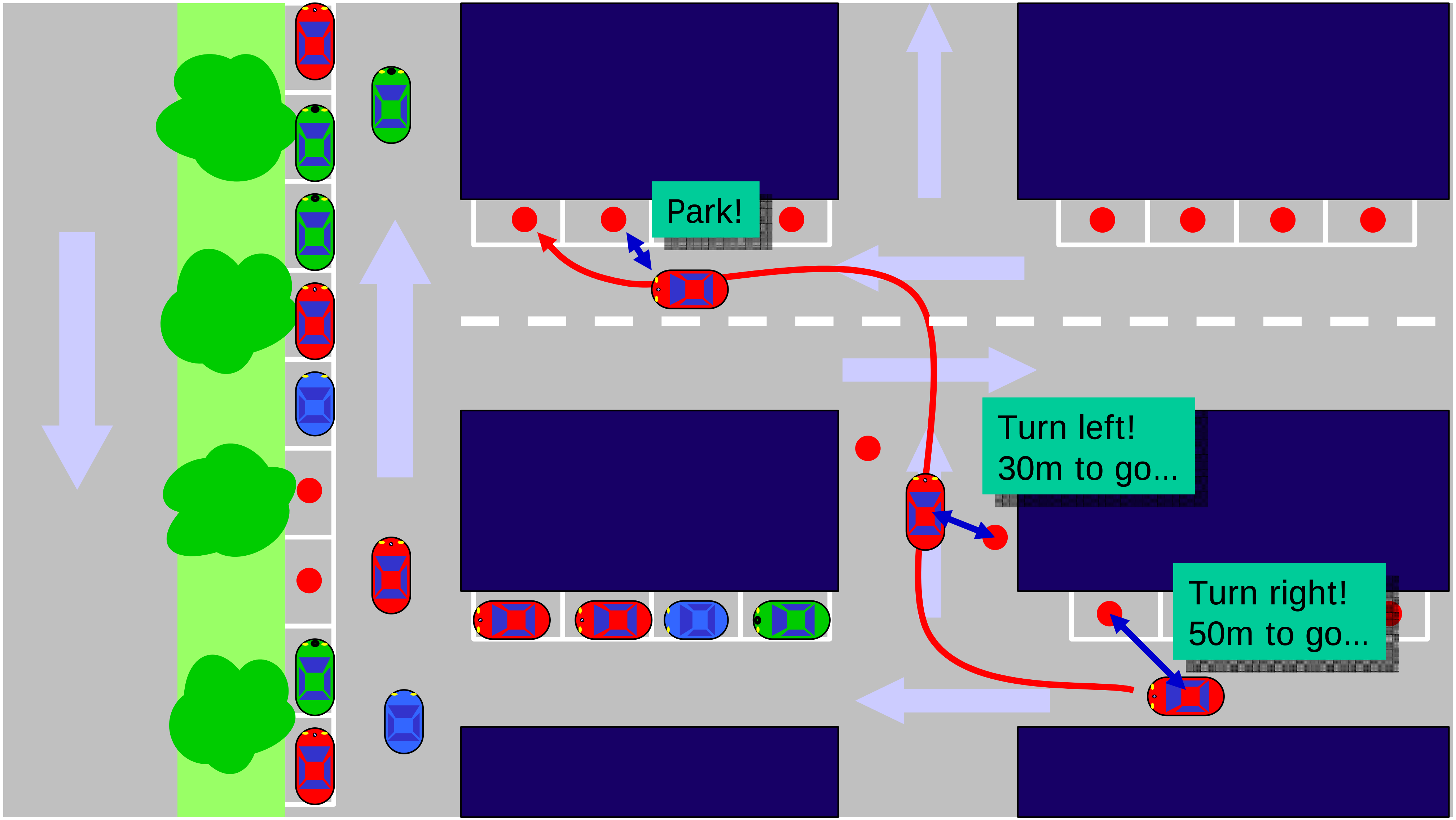
PRIVATE

- ACCESS CONTROL
- DRIVE-THRU PAYMENT
- PARKING LOT PAYMENT
- DATA TRANSFER / INFO FUELING (A)
  - ATIS DATA
  - DIAGNOSTIC DATA
  - REPAIR-SERVICE RECORD
  - VEHICLE COMPUTER PROGRAM UPDATES
  - MAP and MUSIC DATA UPDATES
  - VIDEO UPLOADS
- DATA TRANSFER / CVO / TRUCK STOP
- ENHANCED ROUTE PLANNING and GUIDANCE (6)
- RENTAL CAR PROCESSING
- UNIQUE CVO FLEET MANAGEMENT
- DATA TRANSFER / TRANSIT VEHICLE (yard)
- TRANSIT VEHICLE REFUELING MANAGEMENT
- LOCOMOTIVE FUEL MONITORING
- DATA TRANSFER / LOCOMOTIVE

ATIS - Advanced Traveler Information Systems
CVO - Commercial Vehicle Operations
EV - Emergency Vehicles
IDB - ITS Data Bus
THRU – Through
V-V – Vehicle to Vehicle
(#) – Applications Submitted by GM/Ford/Chrysler
(A- Z) – Applications Submitted by Daimler-Chrysler

(Slide borrowed from the DSRC tutorial: http://grouper.ieee.org/groups/scc32/dsrc/)

Another application : SmartPark



Courtesy: Matt Grossglauser, EPFL

http://smartpark.epfl.ch

Our scope

- We consider communications specific to road traffic: safety and traffic optimization (including finding a parking place)
  - Messages related to traffic information (and parking availability)
  - Anonymous safety-related messages
  - Liability-related messages
- We do not consider more generic applications, e.g. tolling, access to audio/video files, games,…

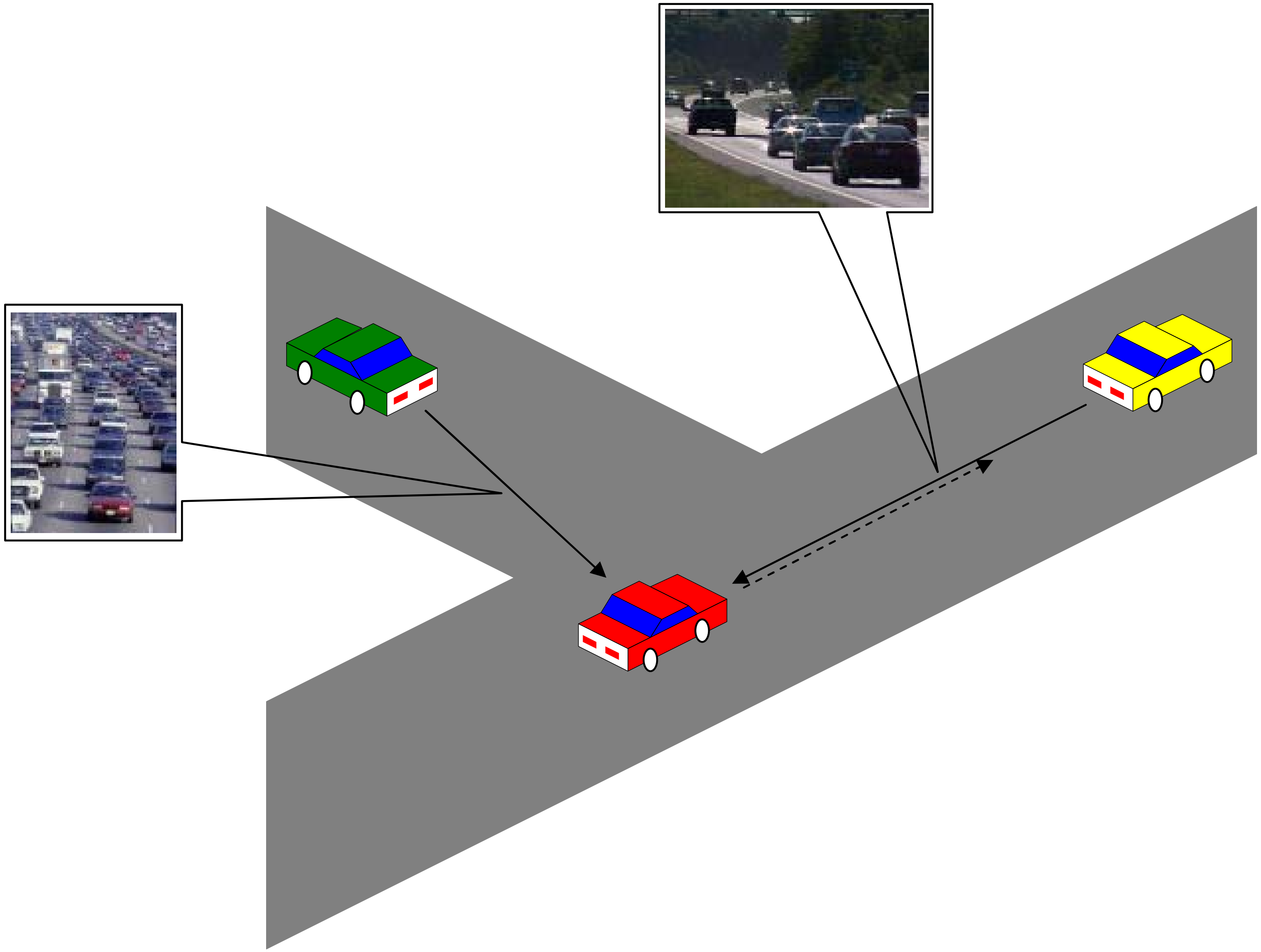
Message categories and properties

Property Category	Legitimacy	Privacy protection	
		Against other individuals	Against the police
Traffic information	☑	☑	☑
Anonymous safety-related messages	☑	☑	☑
Liability-related messages	☑	☑	
Guaranteed to	R, D	S, R, D	S, R, D

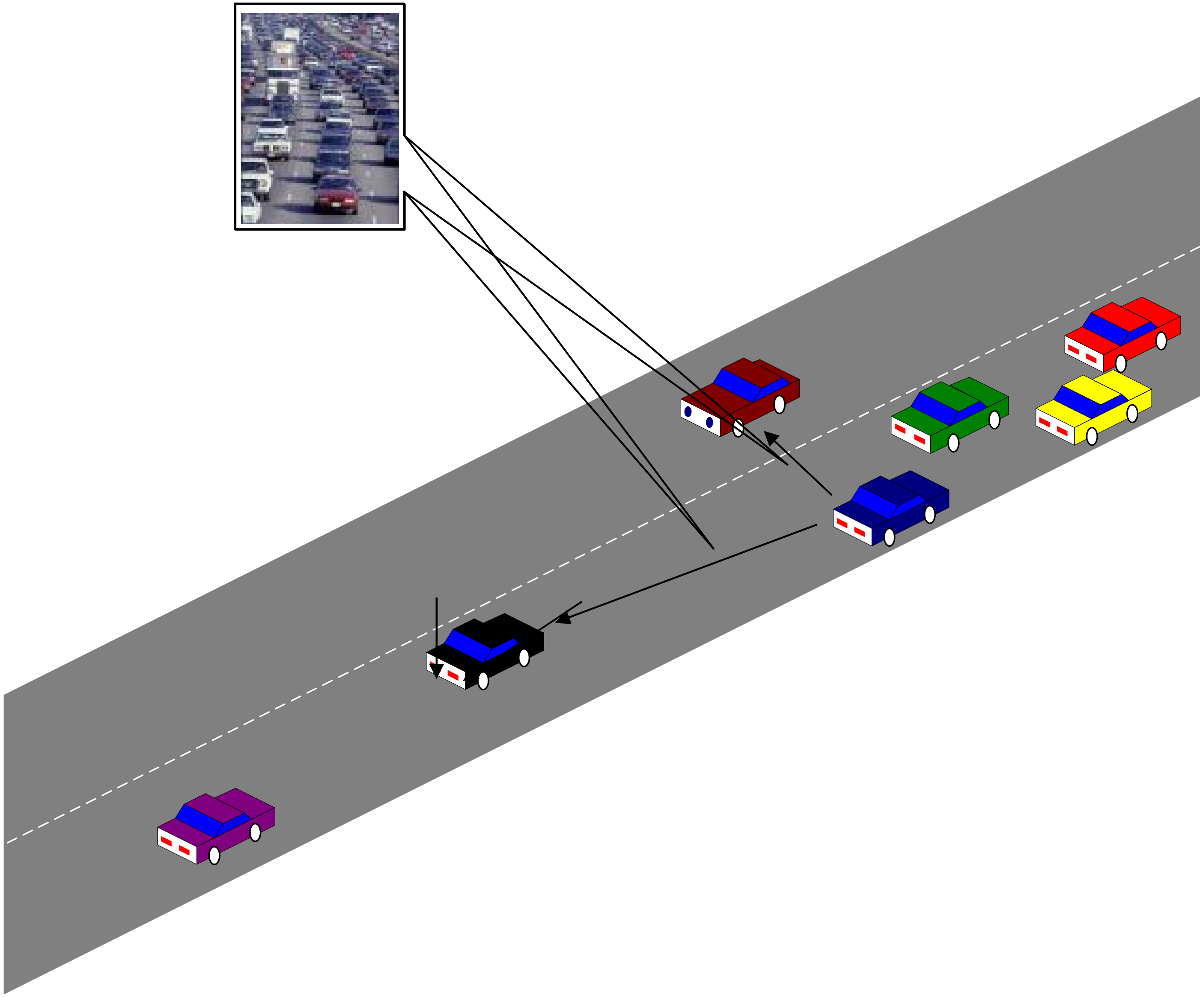
Real-time cons-traints

S: Source R: Relay D: Destination

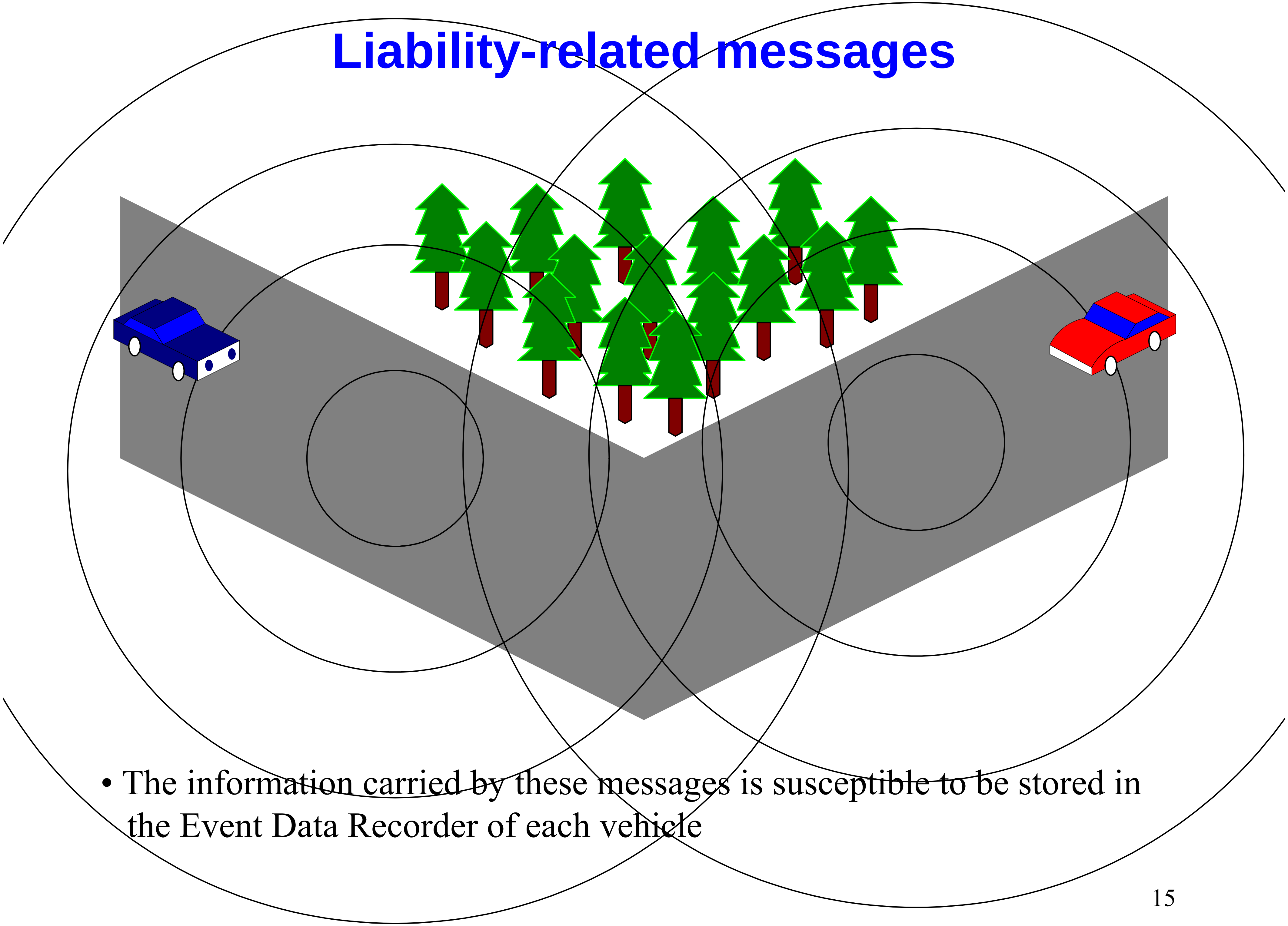
Messages related to traffic information



Anonymous safety-related messages

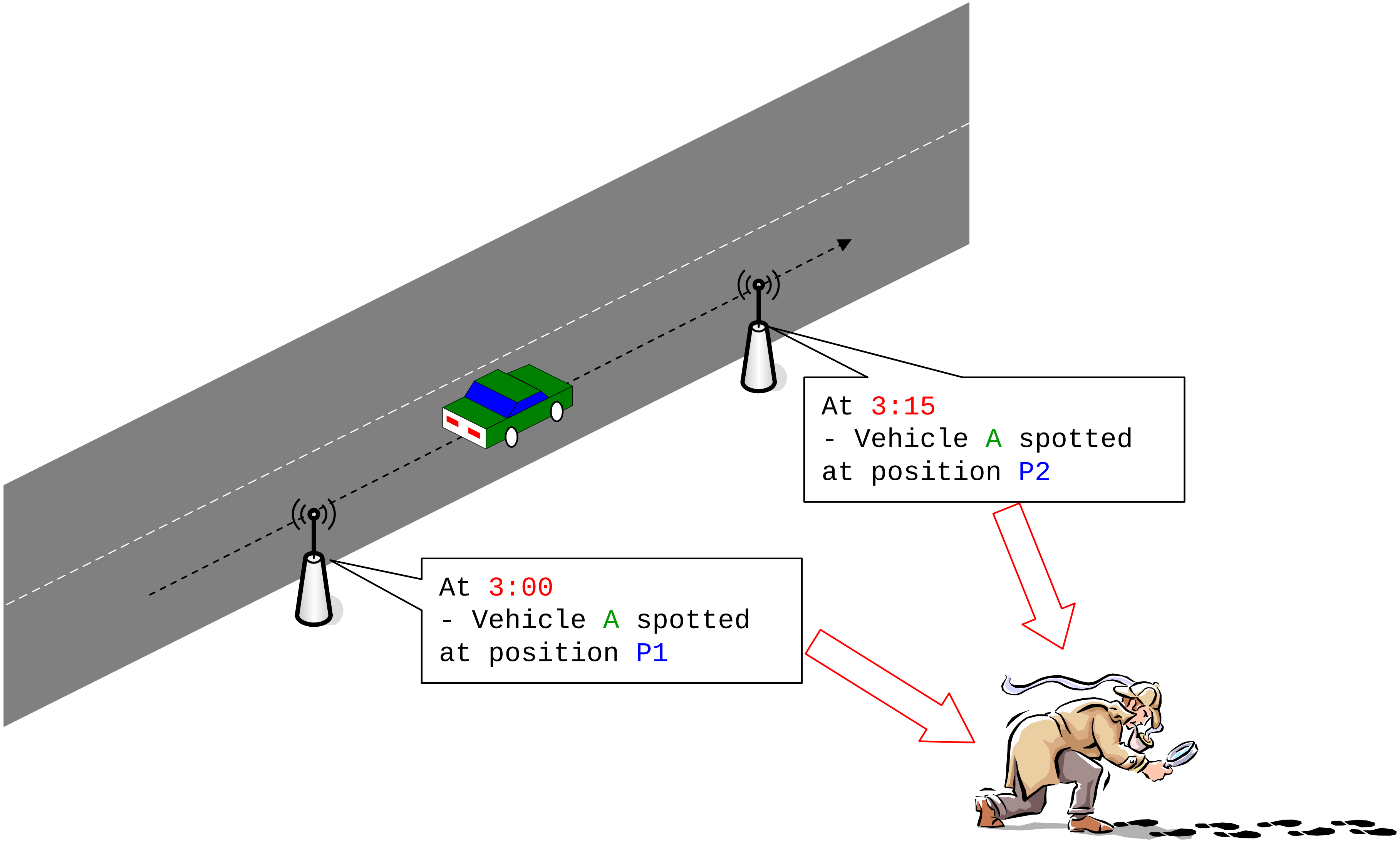


Liability-related messages



- The information carried by these messages is susceptible to be stored in the Event Data Recorder of each vehicle

Liability vs. Privacy: how to avoid the Big Brother syndrom

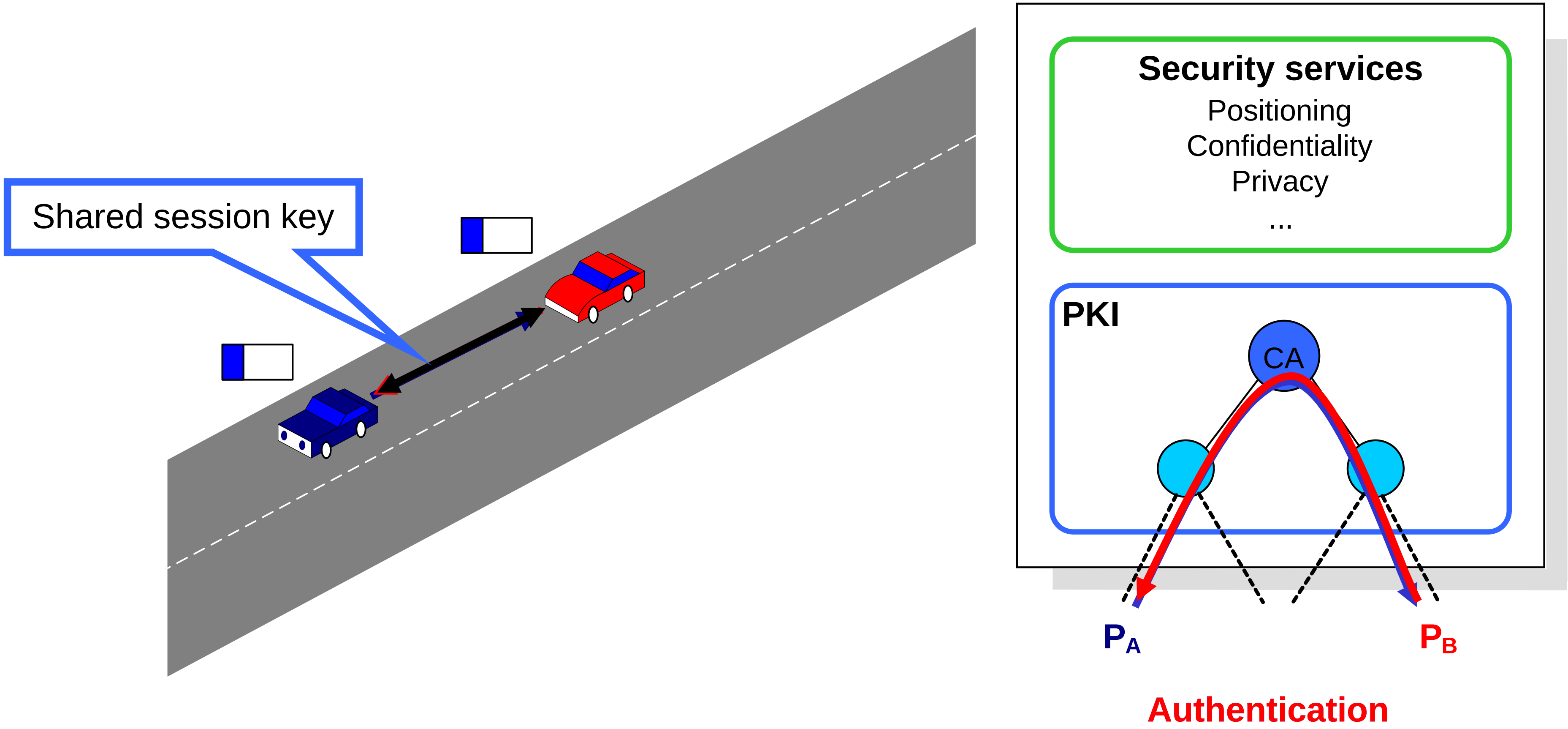


At 3:15
- Vehicle A spotted
at position P2

At 3:00
- Vehicle A spotted
at position P1

- Protection of privacy can be realized by **pseudonyms** changing over time
- Only the law enforcement agencies should be allowed to retrieve the real identities of vehicles (and drivers)

Electronic License Plates and Public Key Infrastructure



B

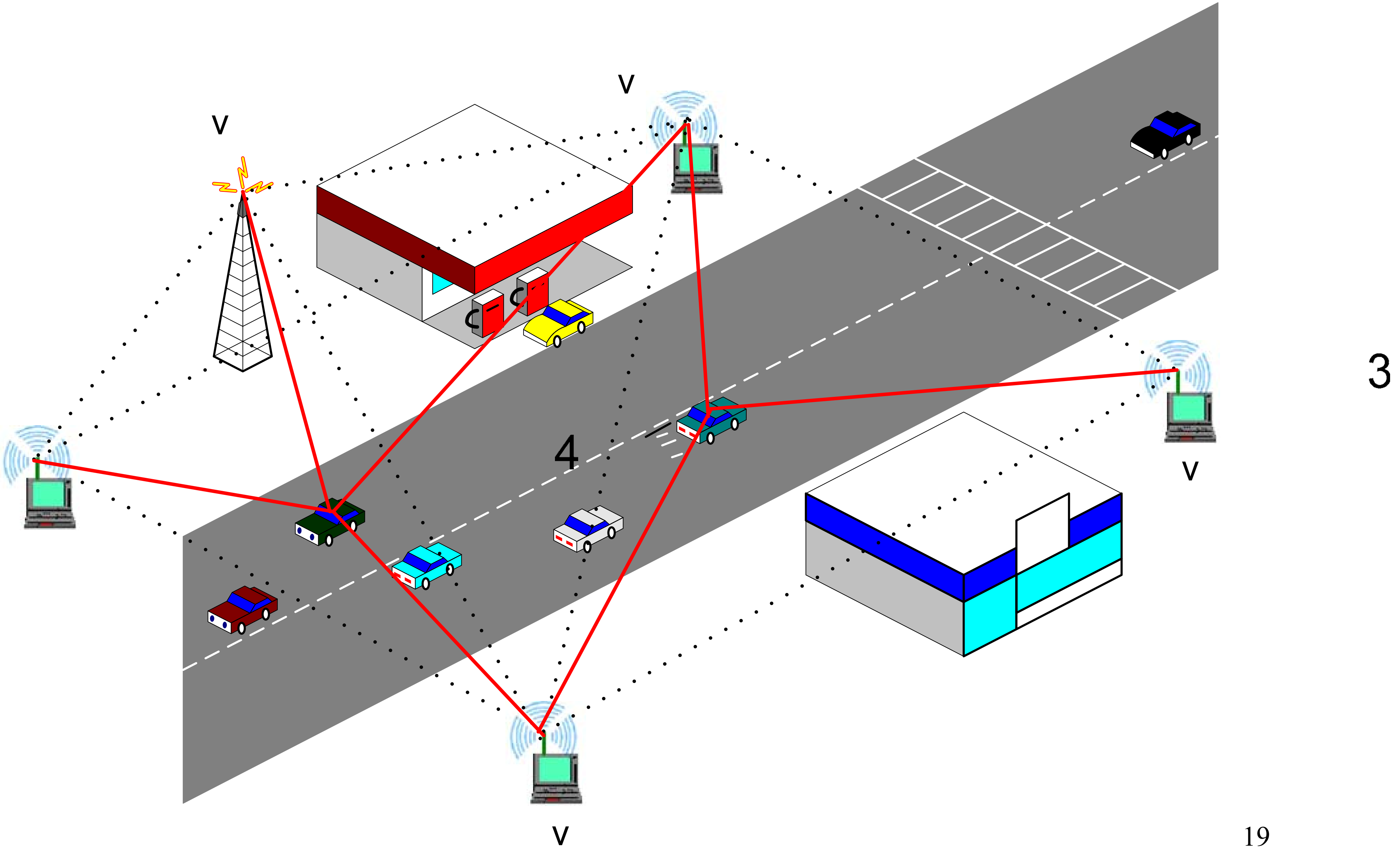
- Each vehicle carries a certified identity and public key (electronic license plate)
- Mutual authentication can be done without involving a server
- Authorities (national or regional) are cross-certified

A

Attacker's model in Vehicular Communications

- An attacker can be an outsider or an insider and malicious or rational
- An attack can be active or passive
- Attacks against anonymous messages:
  - Bogus information
- Attacks against liability-related messages:
  - Cheating with own identity
  - **Cheating with position or speed**
- Attacks against both:
  - Uncovering identities of other vehicles
  - Disruption of network operation (Denial of Service attacks)

How to *securely* locate a vehicle



Positioning systems and prototypes

Satellites:

-**GPS, Galileo, Glonass** *(Outdoor, **Radio Frequency (RF) – Time of Flight (ToF)**)*

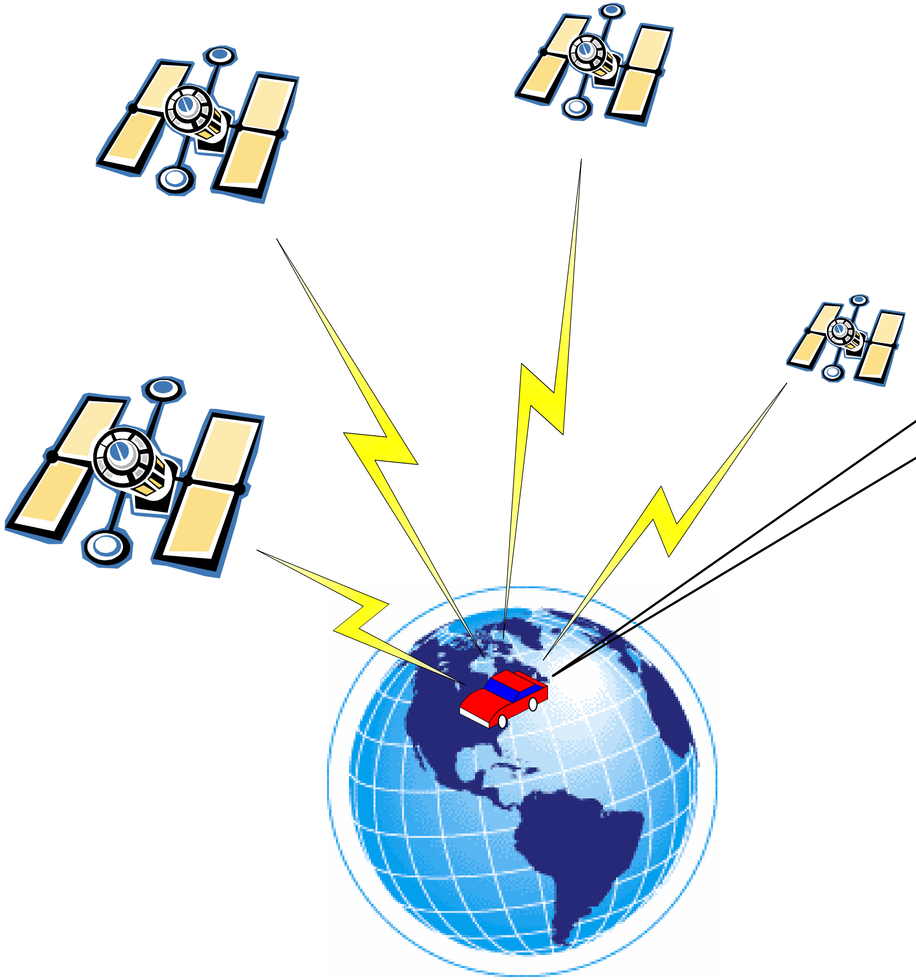
General systems:

- **Active Badge** *(Indoor, **Infrared(IR)**)*, Olivetti
- **Active Bat, Cricket** *(Indoor, **Ultrasound(US)**-based), AT&T Lab Cambridge, MIT*
- **RADAR, SpotON, Nibble** *(Indoor/Outdoor, **RF- Received Signal Strength**)*, Microsoft, Univ of Washington, UCLA+Xerox Palo Alto Lab
- **Ultra Wideband Precision Asset Location System,** *(Indoor/Outdoor, **RF-(UWB)-ToF**)*, Multispectral solutions, Inc.

Ad Hoc/Sensor Network positioning systems (without GPS):

- **Convex position estimation** *(**Centralized**)*, UC Berkeley
- **Angle of Arrival based positioning** *(**Distributed**, Angle of Arrival)*, Rutgers
- **Dynamic fine-grained localization** *(**Distributed**)*, UCLA
- **GPS-less low cost outdoor localization** *(**Distributed**, Landmark-based)*, UCLA
- **GPS-free positioning** *(**Distributed**)*, EPFL

GPS



- A constellation of 24 Earth-orbiting operational satellites

- Each receiver can see at least 4 satellites simultaneously (to improve accuracy)

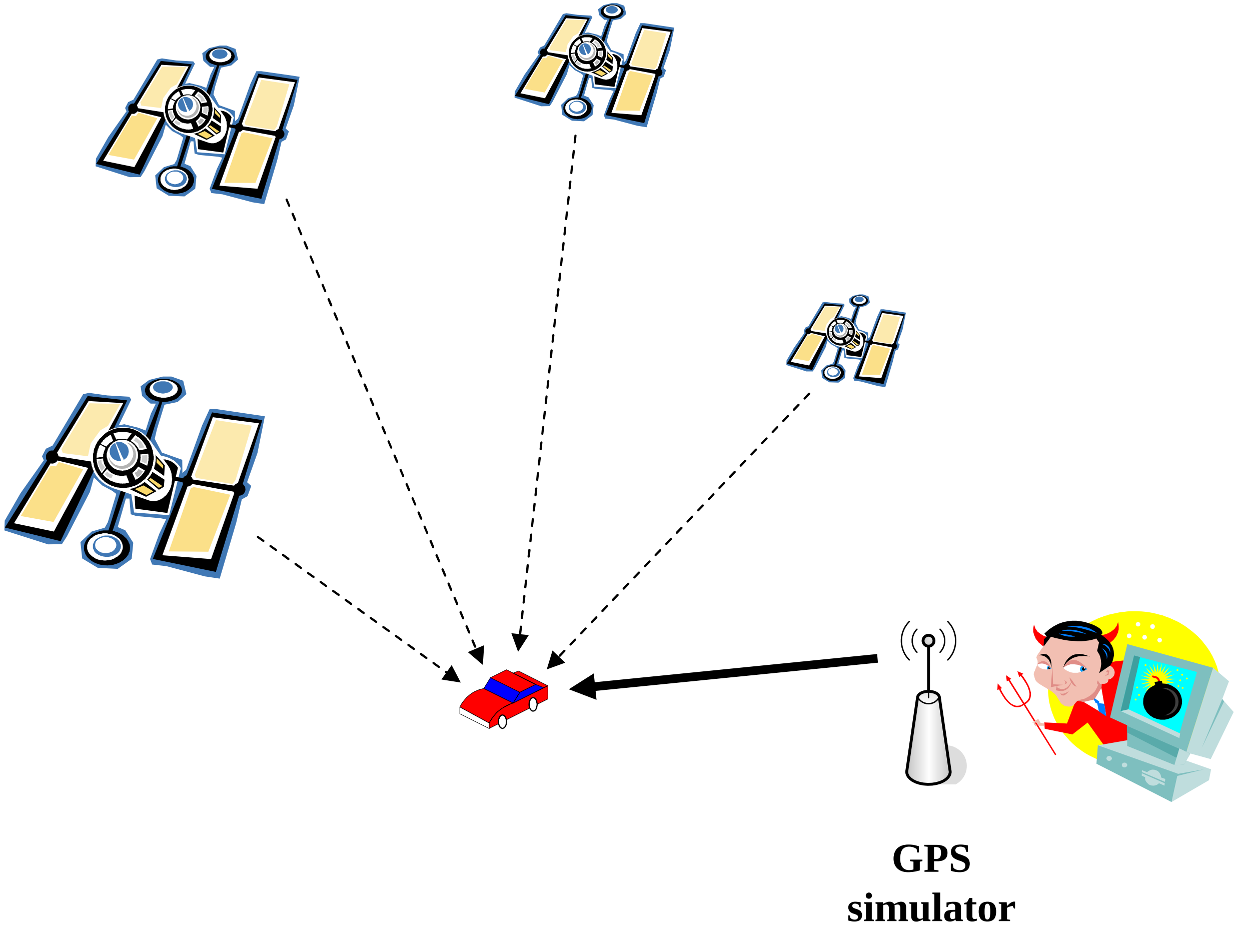
- Satellites emit low-power signals

- Positioning by 3-D trilateration

- Differential GPS can improve accuracy from several meters to a few centimeters.

GPS Security – Example of attack

- A GPS simulator can send strong fake signals to mask authentic weak signals



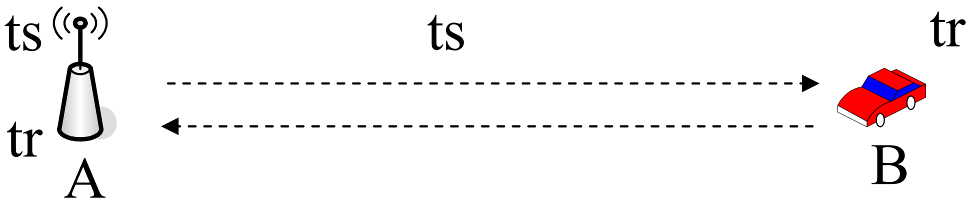
GPS Security

- Other vulnerabilities
  - Relaying attack: connects the receiver to a remote antenna
  - Signal-synthesis attack: feeds the receiver with false signals
  - Selective-delay attack: predicts the signal *Δt* earlier
- Security solutions
  - Tamper-resistant hardware
  - Symmetric crypto
    - Problem: an authenticated receiver can hack the system
  - Asymmetric crypto
    - Problem: additional delay

Distance measurement techniques

- Based on the speed of light (RF, Ir)

$d_{ABm}=(tr-ts-t_{procB})c/2$



ts

tr

A

ts

tr

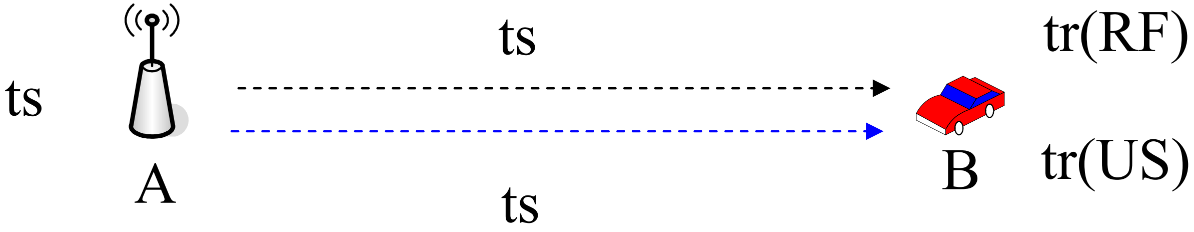
B

$d_{ABm}=(tr-ts)c$

(A and B are synchronized - ToF)

(A and B are NOT synchronized –
Round trip ToF)

- Based on the speed of sound (Ultrasound)



ts

A

ts

ts

tr(RF)

B

tr(US)

$d_{ABm}=(tr(RF)-tr(US))s$

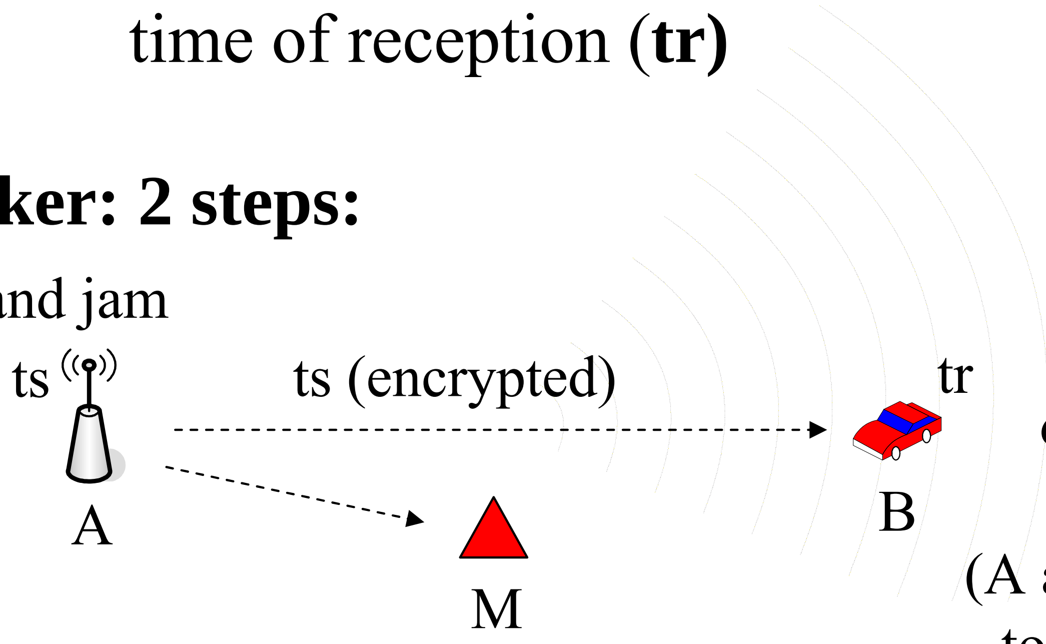
- Based on Received Signal Strength (RSS)

Attacks on RF and US ToF-based techniques

- **Insider attacker:** cheat on the time of sending (**ts**) or time of reception (**tr)**

- **Outsider attacker: 2 steps:**

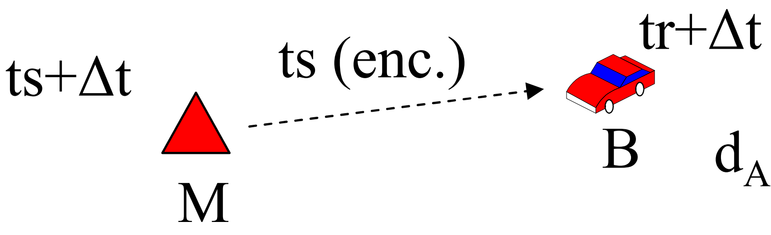
1. Overhear and jam



d_{ABm}=(tr-ts)c

(A and B are assumed to be synchronised)

2. Replay with a delay Δt



d_{ABm}=(tr+Δt-ts)c

=> d_{ABm}>d_{AB}

Summary of possible attacks on distance measurement

	Insider attackers	Outsider attackers
RSS (Received Signal Strength)	Distance enlargement and reduction	Distance enlargement and reduction
Ultrasound Time of Flight	Distance enlargement and reduction	Distance enlargement and reduction
Radio Time of Flight	Distance enlargement and reduction	Distance enlargement only

The challenge of secure positioning

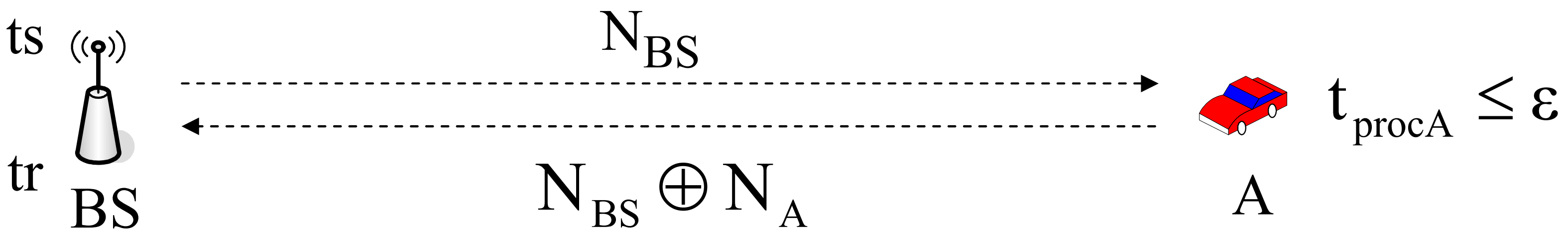
- **Goals:**
  - preventing an **insider attacker** from **cheating about its own position**
  - preventing an **outsider attacker** from **spoofing the position of an honest node**

- **Our proposal: Verifiable Multilateration**

Distance Bounding (RF)

- Introduced in 1993 by Brands and Chaum (to prevent the Mafia fraud attack)

$$\begin{aligned}
A &: \text{ generate random nonces } N_A, N'_A \\
&: \text{ generate commitment } commit = h(N_A, N'_A) \\
A \rightarrow BS &: \ commit \\
\\
BS &: \text{ generate random nonce } N_{BS} \\
BS \rightarrow A &: \ N_{BS} \\
A \rightarrow BS &: \ N_{BS} \oplus N_A \\
BS &: \text{ measure the time } t_{BSA} \text{ between} \\
& \text{ sending } N_{BS} \text{ and receiving } N_{BS} \oplus N_A \\
\\
A \rightarrow BS &: \ N'_A,\ sig_{K_A}(A, N'_A) \\
\\
BS &: \text{ verify if the signature is correct} \\
& \text{ and if } commit = h(N_A, N'_A)
\end{aligned}$$



$d_{real} \leq db = (tr\text{-}ts)c/2$ (db=distance bound)

Distance bounding characteristics

- RF distance bounding:

- nanosecond precision required, 1ns ~ 30cm

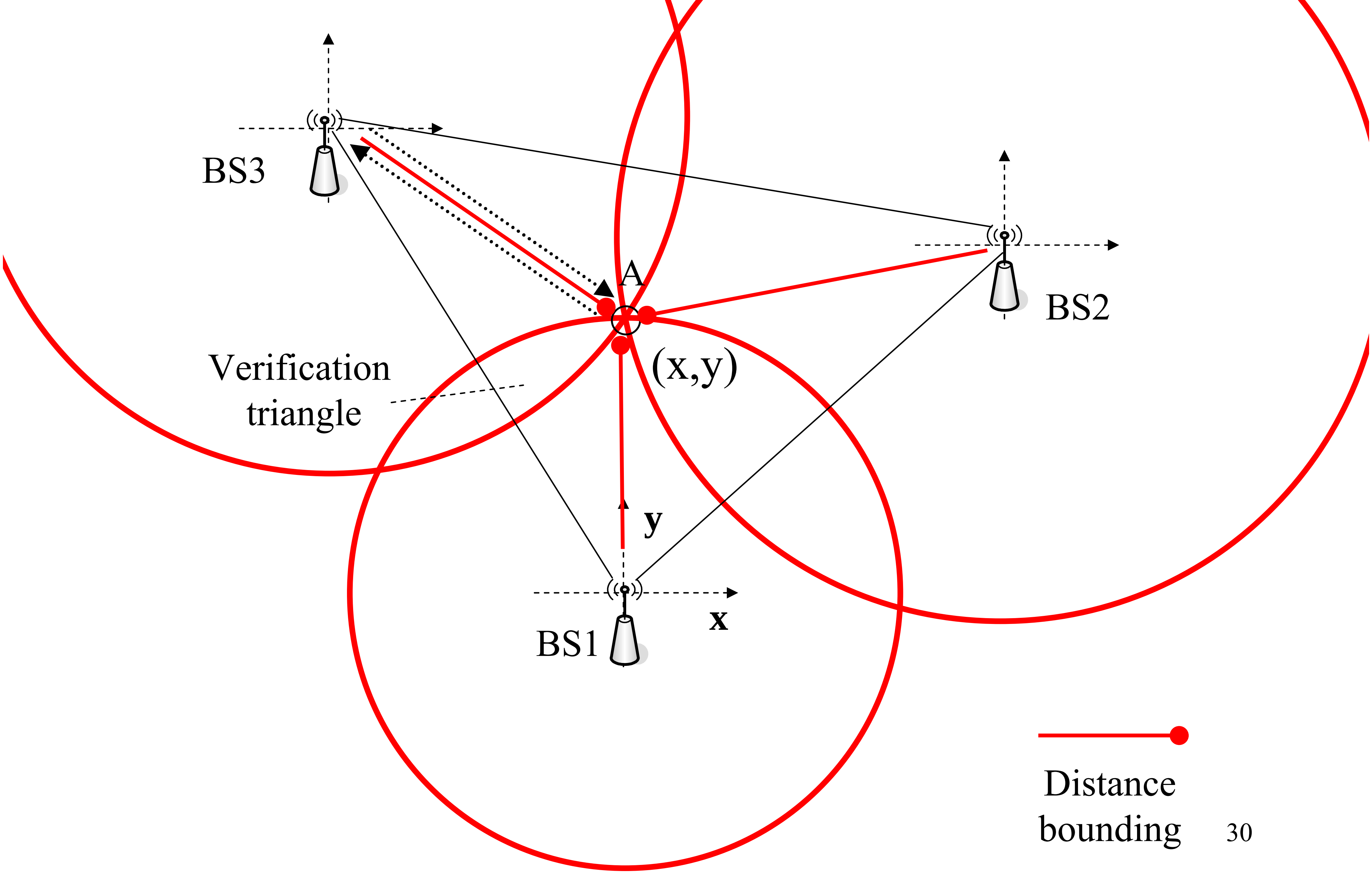
- UWB enables clock precision up to 2ns and 1m positioning indoor and outdoor (up to 2km)

- US distance bounding:

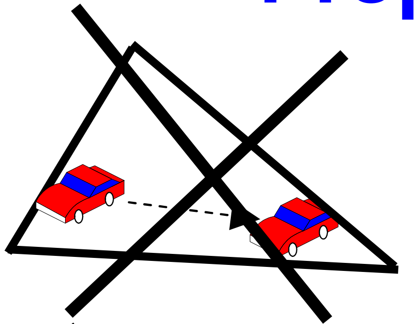
- millisecond precision required,1ms ~ 35cm

RF Distance Bounding	Distance enlargement only	Distance enlargement only
US Distance Bounding	Distance enlargement only	Distance enlargement and reduction

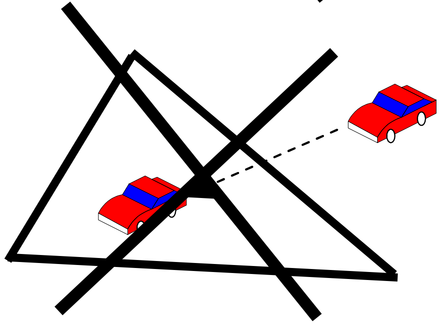
Verifiable Multilateration (Trilateration)



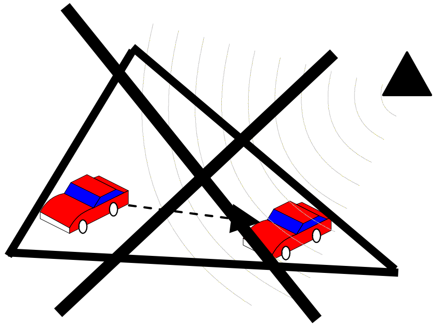
Properties of Verifiable Multilateration



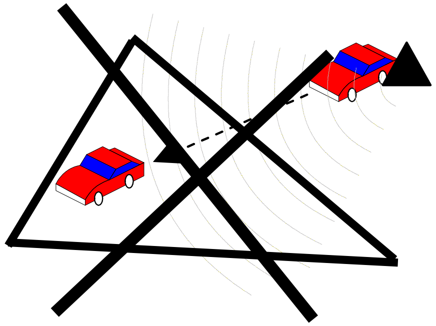
- a vehicle located within the triangle cannot prove to be at another position within the triangle except at its true position.



- a vehicle located outside the triangle formed by the verifiers cannot prove to be at any position within the triangle



- an outsider attacker cannot spoof the position of a vehicle such that it seems that the vehicle is at a position different from its real position within the triangle



- an outsider attacker cannot spoof the position of a vehicle such that it seems that it is located at a position within the triangle, if the vehicle is out of the triangle

The same holds in 3-D, with a triangular pyramid instead of a triangle

Conclusion on secure positioning

- New research area
- Positioning *tout court* is not yet completely solved (solutions will rely on GPS, on terrestrial base stations, and on mutual distance estimation)
- Time of flight seems to be the most appropriate technique
- More information available at: http://lcawww.epfl.ch/capkun/spot/

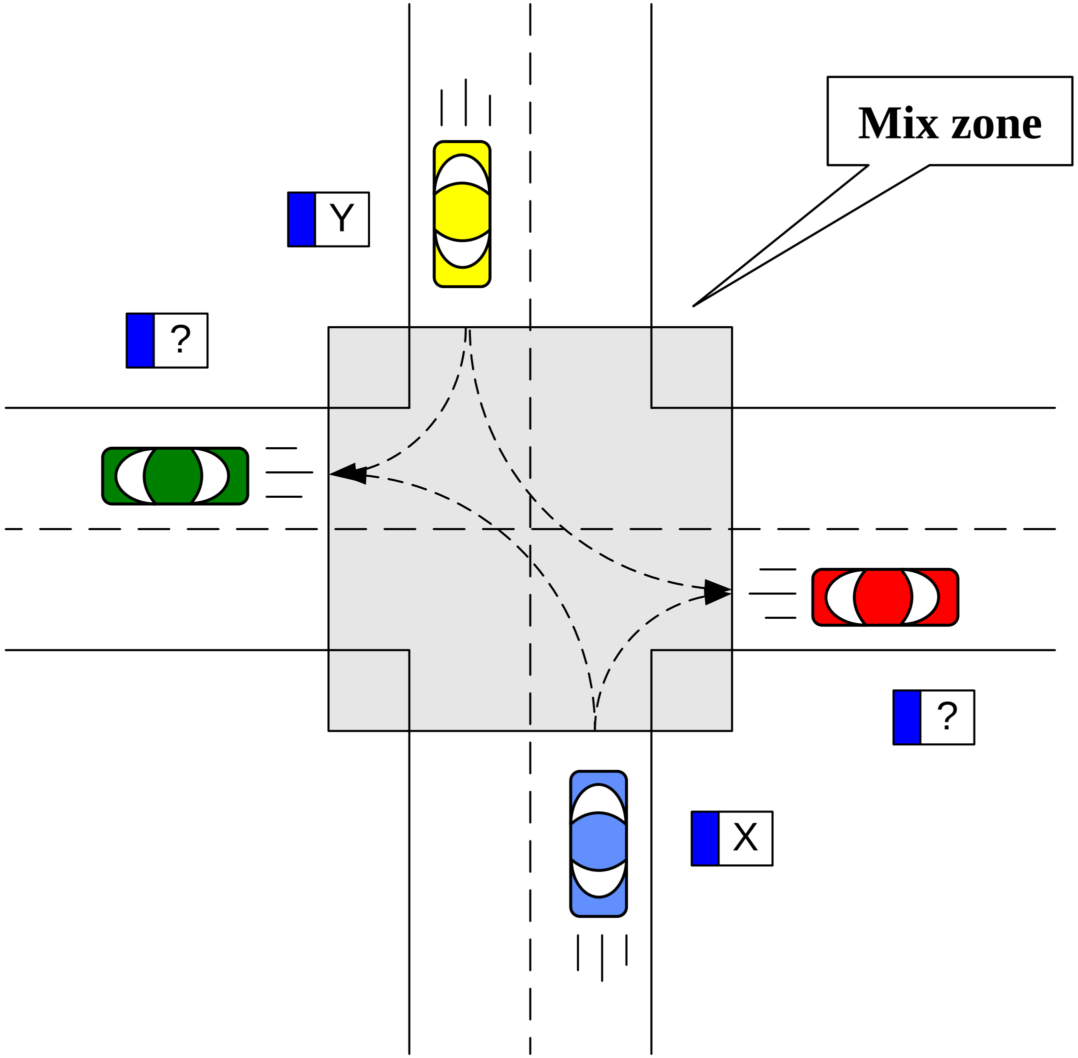
Srdjan Capkun and Jean-Pierre Hubaux
Secure Positioning of Wireless Devices with Application to Sensor Networks

Accepted for Infocom 2005

Security design options

- Each vehicle possesses a large set of certified anonymous public keys
- Keys have short lifetimes
- Pseudonyms replace vehicle identities
- Authentication of real identities is required for liability-related messages
- Police abuse can be prevented by distributing the law enforcement authority
- Secure positioning guarantees position correctness

Alternative technique to change pseudonyms: Mix zones



Security analysis

- Attacks against anonymous messages:
  - Bogus information: correlation of traffic reports
- Attacks against liability-related messages:
  - Cheating with own identity: certificates are signed by a trusted authority
  - Cheating with position or speed: secure positioning
- Attacks against privacy:
  - Uncovering of other vehicles' identities: anonymous keys + pseudonyms + mix zones
- Disruption of network operation
  - Denial of Service: alternative technologies (e.g., UWB, UTRA-TDD, and Bluetooth) can temporarily support communications

Conclusion

- The security of vehicular communications urgently needs to be considered
- Security includes secure positioning
- Major challenge: cope with the conflicting constraints of liability and privacy
- Tricky question: who delivers and certifies the cryptographic keys: a governmental agency or the vehicle manufacturers?

- More information available at: http://ivc.epfl.ch