Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com

Chapter 2: (secowinet.epfl.ch):

Mesh Networks, MANET, VANET, RFID, and Sensor Networks

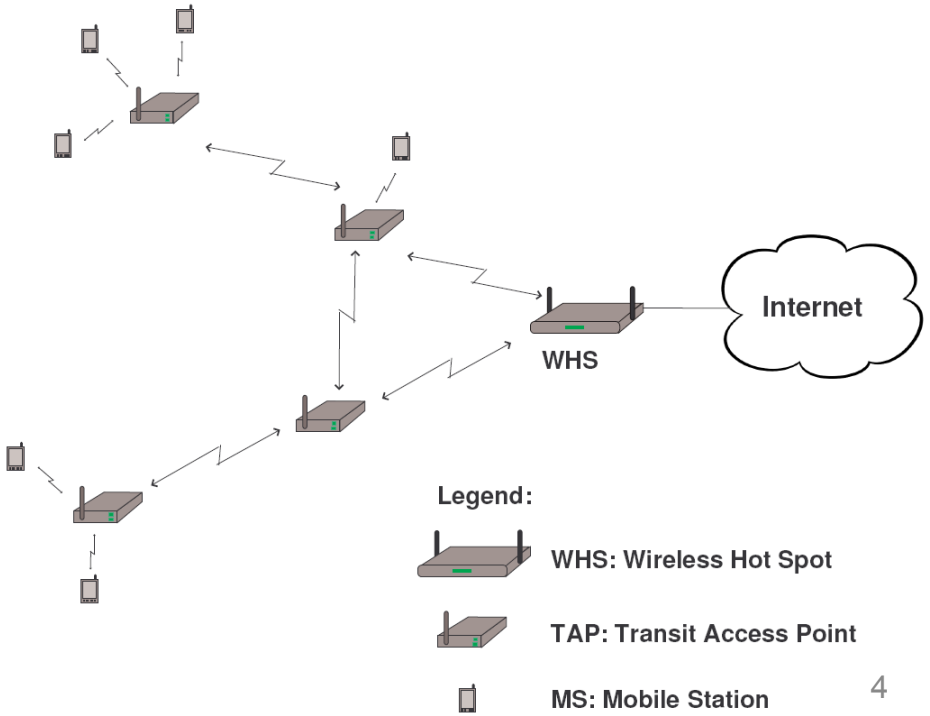
UPCOMING WIRELESS NETWORKS

Introduction

- Upcoming wireless networks:
  - Personal communications:
    - Wireless mesh networks
    - Hybrid ad hoc networks
    - Mobile ad hoc networks
  - Vehicular networks
  - Sensor networks
  - RFID
  - Mobility in the Internet

Wireless Mesh Networks

- **Mesh network:**
  - One Wireless Hot Spot (WHS)
  - Several Transit Access Points (TAPs)
  - Mobile Stations



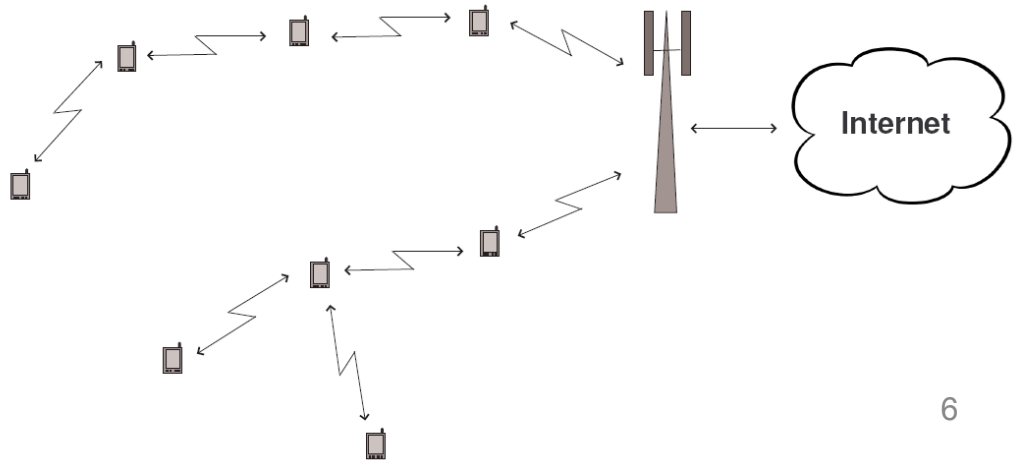
Wireless Mesh Networks

- **Easy to deploy:**
  - Single connection point to the Internet
- **Providing Internet connectivity in a sizable geographic area:**
  - Much lower cost than classic WiFi networks
- **Fairness and security are closely related**
- **Not yet ready for wide-scale deployment:**
  - Severe capacity and delay constraints
  - Lack of security guarantees

Hybrid Ad Hoc Networks

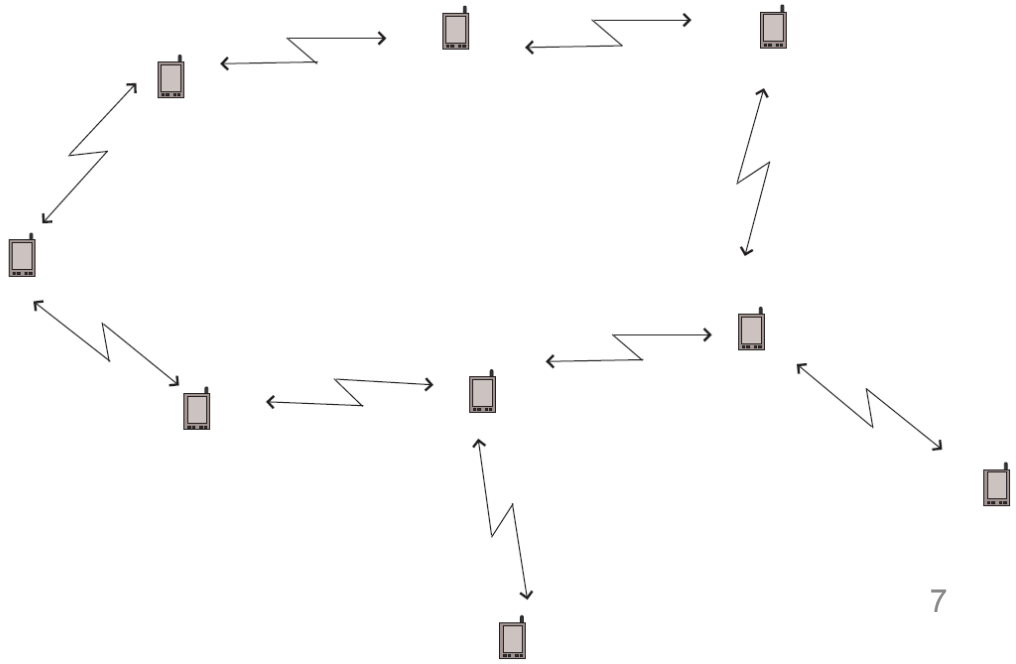
- **Hybrid ad hoc networks or multi-hop cellular networks:**
  - No relay stations
  - Other mobile stations relay the traffic

- **Problem of power management**



Mobile Ad Hoc Networks

- **Mobile ad hoc networks:**
  - Mobile ad hoc networks in hostile environments
  - In self-organized mobile ad hoc networks



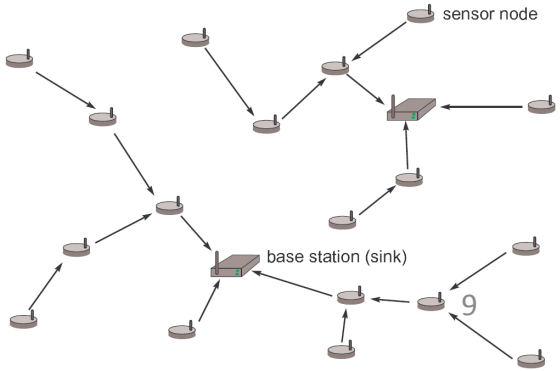
Mobile Ad Hoc Networks

- **Mobile ad hoc networks in hostile environments:**
  - Presence of a strong attacker: military networks
  - Security challenges:
    - Secure routing
    - Prevention of traffic analysis
    - Resistance of a captured device to reverse engineering and key retrieval.

- **In self-organized mobile ad hoc networks:**
  - No authority in the initialization phase
  - Nodes have to figure out how to secure the communications
  - Selfishness can be a serious issue:
    - Nodes selfishly refuse to forward packets
    - Greedily overuse the common channel

Sensor Networks

- Large number of sensor nodes, a few base stations
- Sensors are usually battery powered:
  - Main design criteria: reduce the energy consumption
- Multi-hop communication reduces energy consumption:
  - Overall energy consumption can be reduced, if packets are sent in several smaller hops instead of one long hop
  - Fewer re-transmissions are needed due to collisions



Sensor Networks

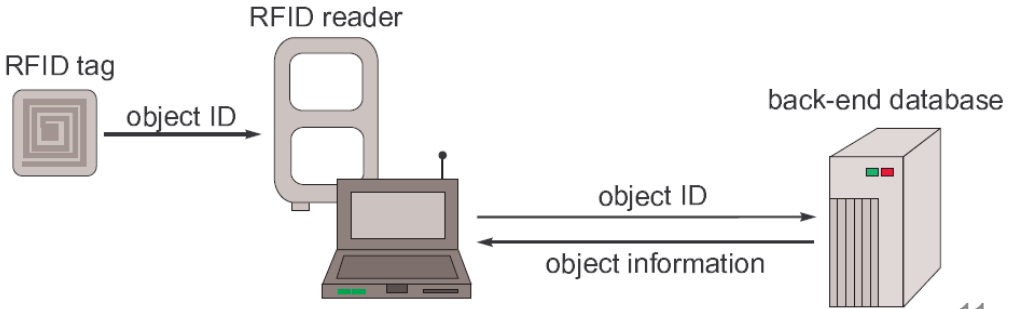
- **Security requirements:**
  - Integrity
  - Confidentiality
  - Availability

- **Special conditions:**
  - Energy consumption
  - Computing and storage capacity of sensors is limited
  - Access to the sensors cannot be monitored

RFID

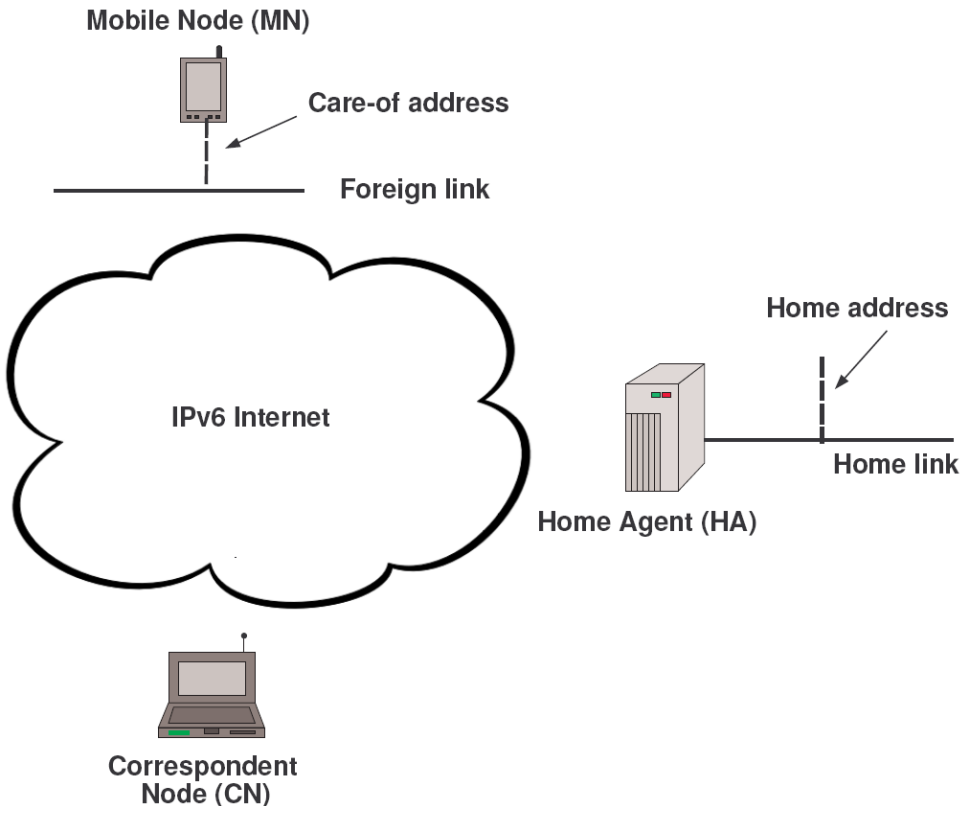
- **RFID systems:**
  - RFID tags
  - RFID readers
  - Back-end databases

- **RFID tag: microchip and antenna**
  - Active: have battery
  - Passive: harvest energy from the reader's signal



Mobility in the Internet

- When a node changes location: its address changes
- Mobile IP: solves this problem at the IP layer



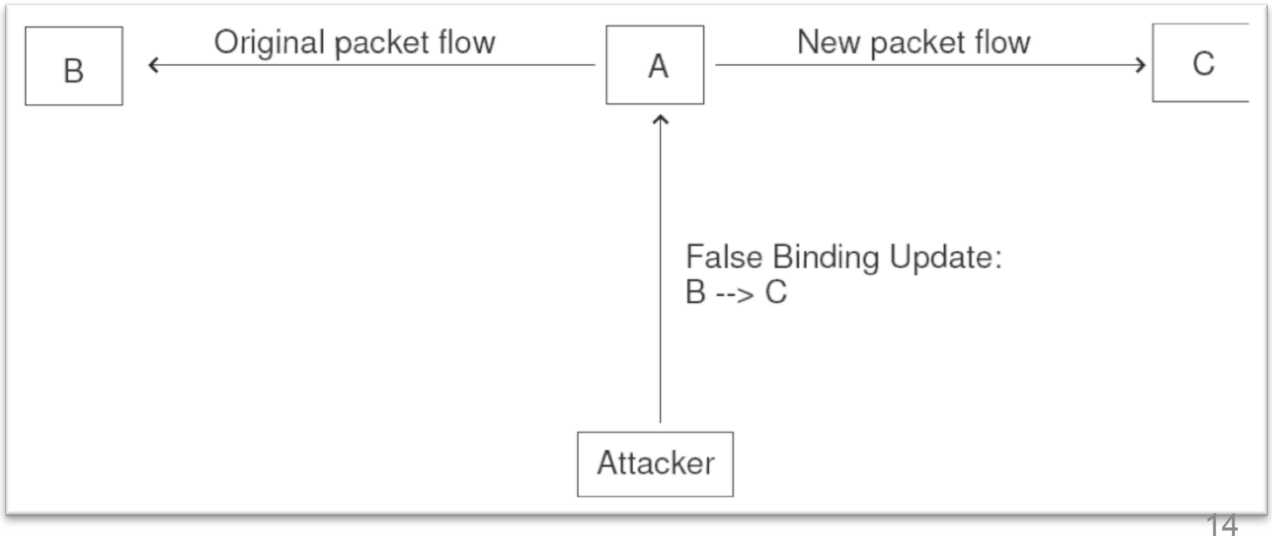
Mobility in the Internet

- **Care-of address:**
  - Address used by the mobile node while it is attached to a foreign link
- **Binding:**
  - Association of a care-of address with a home address
- **Bidirectional tunneling:**
  - Mobile node tunnels the packets for the correspondent node through its home agent
  - Home agent tunnels the packets to the mobile node via its care-of address
- **Route optimization:**
  - Mobile node registers its current address binding with the correspondent node
  - Packets are sent directly to the mobile node's care-of address
  - Use the optimal route between the mobile and correspondent node

Mobility in the Internet

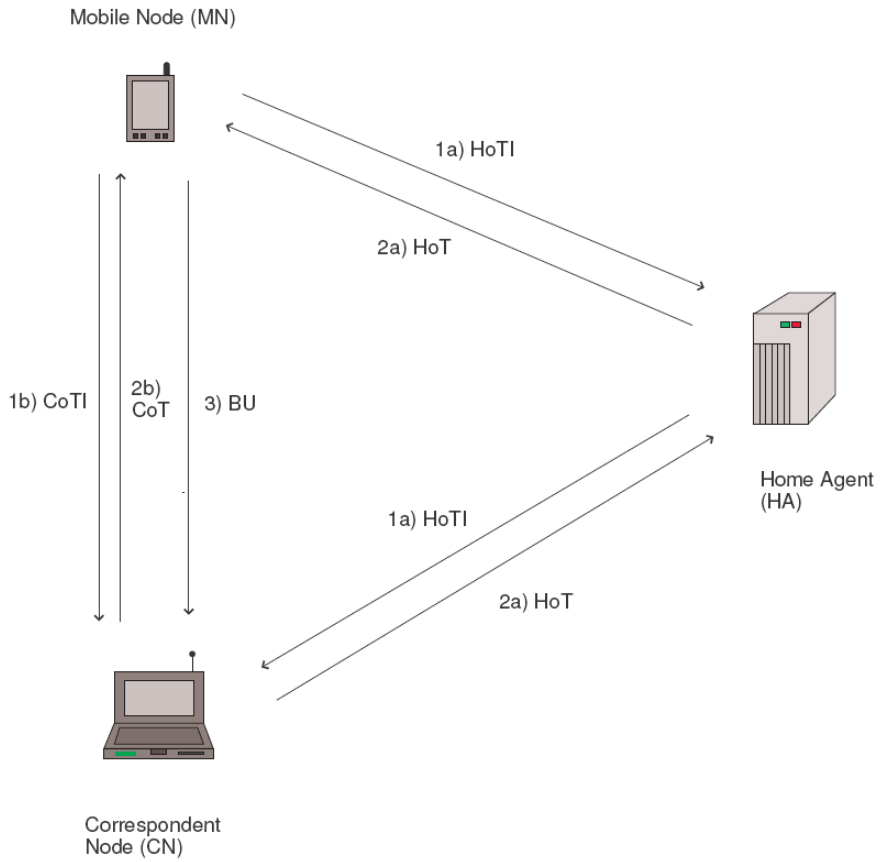
- **Address stealing:**
  - If binding updates were not authenticated: an attacker could send spoofed binding updates

- **DoS:**
  - Sending spoofed IP packets that trigger a large number of binding update protocol instances



Mobility in the Internet

- Protection mechanism: Return Routability (RR)
  - Non-cryptographic solution
  - Assumption of an uncorrupted routing infrastructure



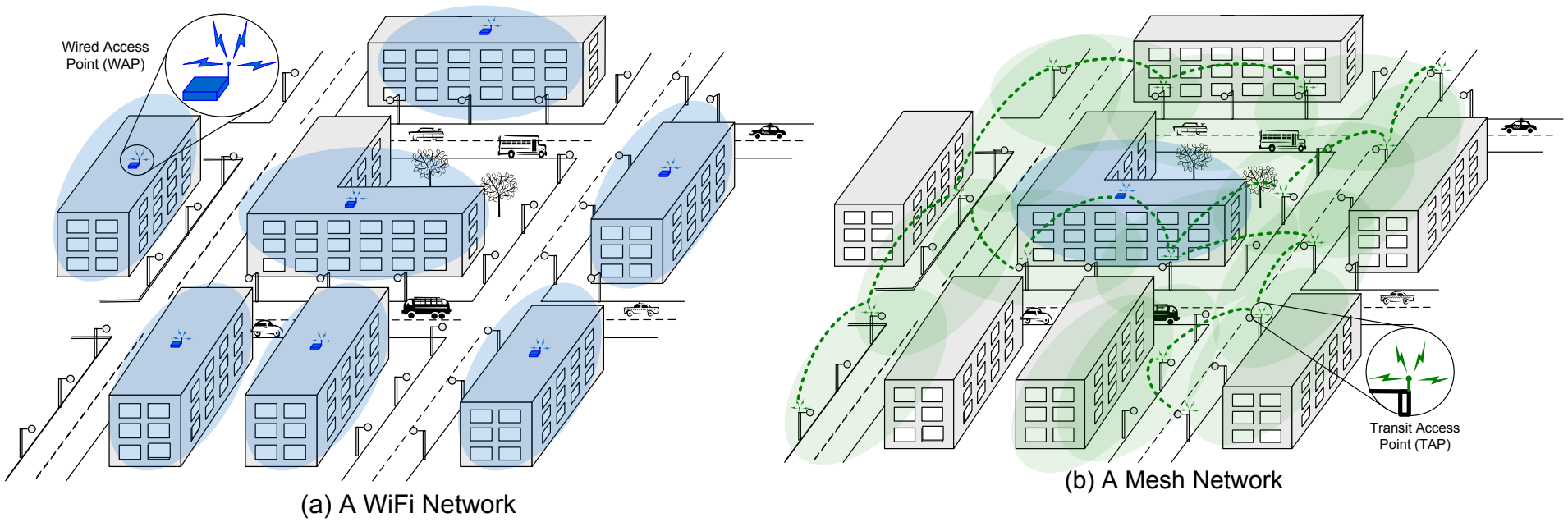
Return Routability

- Mobile Node MN checks the routability to the Correspondent Node CN:
  (a) via the Home Agent HA (HoTI)
  (b) directly (CoTI)

- CN replies to both of them: HoT and CoT

- Once MN has received both HoT and CoT:
  – MN sends a Binding Update to CN

Wireless Mesh Networks

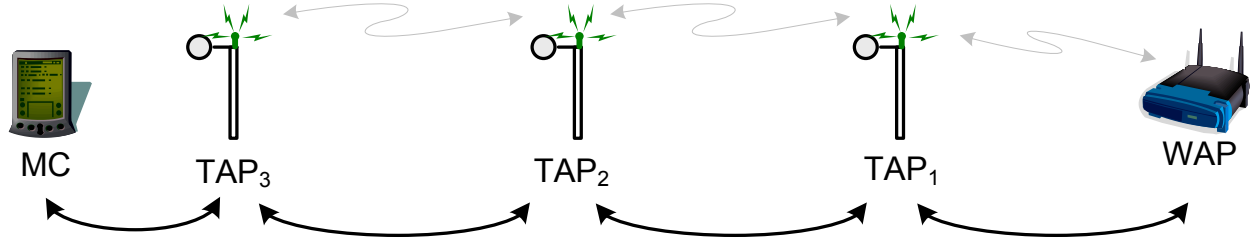


(a) A WiFi Network

(b) A Mesh Network

- Wireless Mesh Network (WMN): Same coverage as with WiFi networks but with only one WAP (and several TAPs).
- WMNs allow a fast, easy and inexpensive network deployment.
- However, the lack of security guarantees slows down the deployment of WMNs

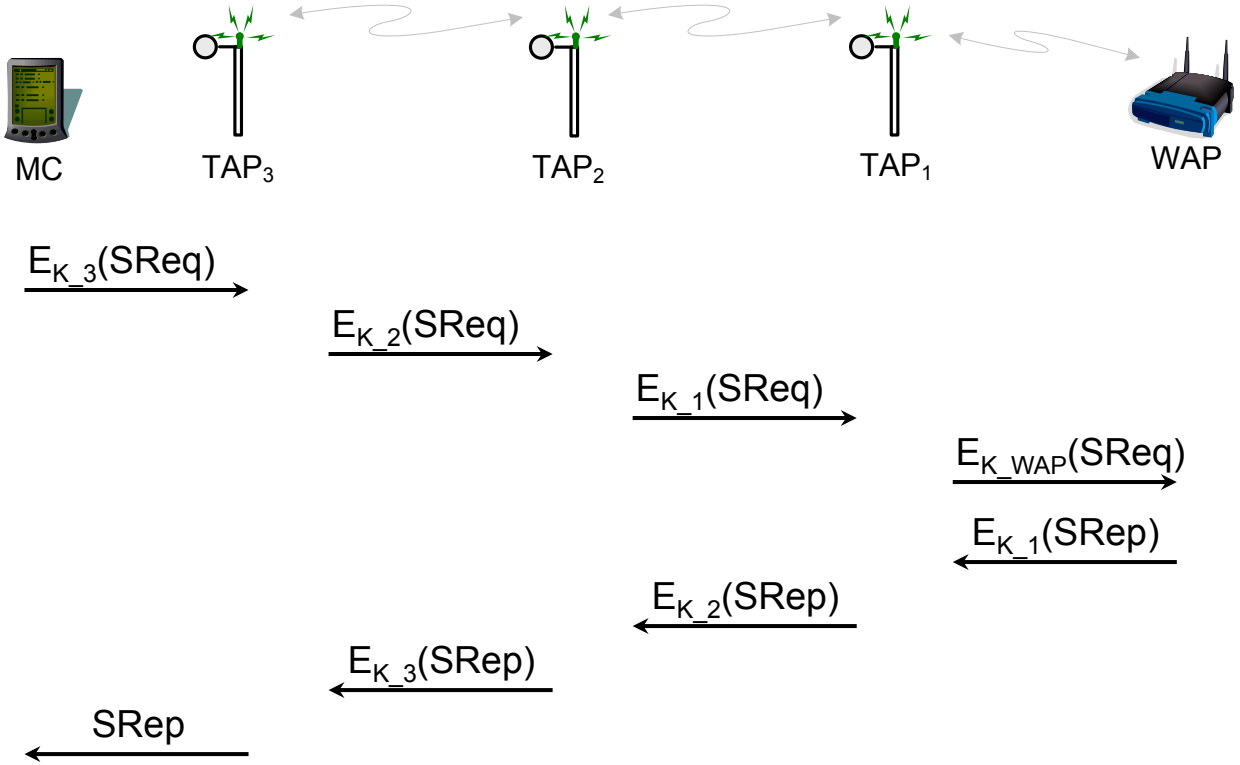
A Typical Communication in WMNs



- Several verifications need to be performed:
  - WAP has to authenticate the MC (Mobile Client).
  - MC has also to authenticate the TAPs
  - Each TAP has to authenticate the other TAPs in the WMN
  - The data sent or received by MC has to be protected (e.g., to ensure data integrity, non-repudiation and/or confidentiality).

- Performing these verifications has to be efficient and lightweight, especially for the MC.

Securing a Communication in WMNs: An Example



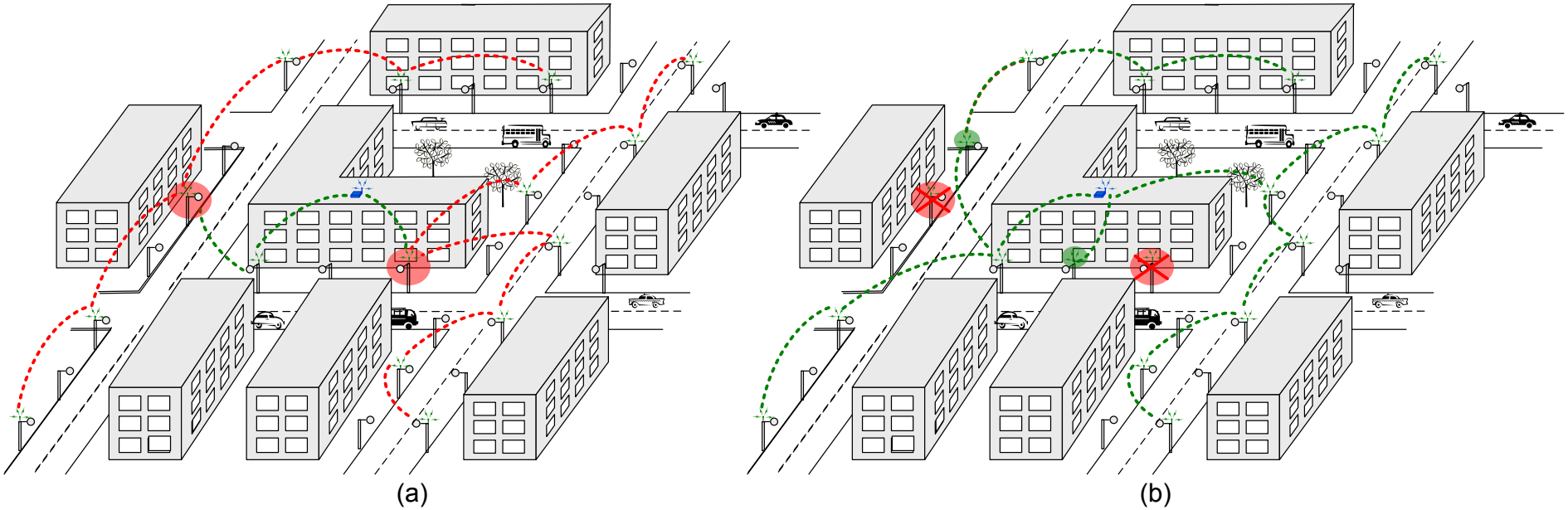
Example: SReq = E_{K_WAP} (ReqID, roamingInfo, SessionKey, Nonce)

Characteristics of WMNs

- **Multi-hop communications:**
  - ✧ Delayed detection and treatment of attacks
  - ✧ Routing becomes critical
  - ✧ Unfairness
- **The TAPs are not physically protected:**
  - ✧ Capture
  - ✧ Cloning
  - ✧ Tampering
- **Three fundamental security operations:**
  1. Detection of corrupt nodes
  2. Secure routing
  3. Fairness

Three Fundamental Security Operations

1. Detection of corrupt nodes



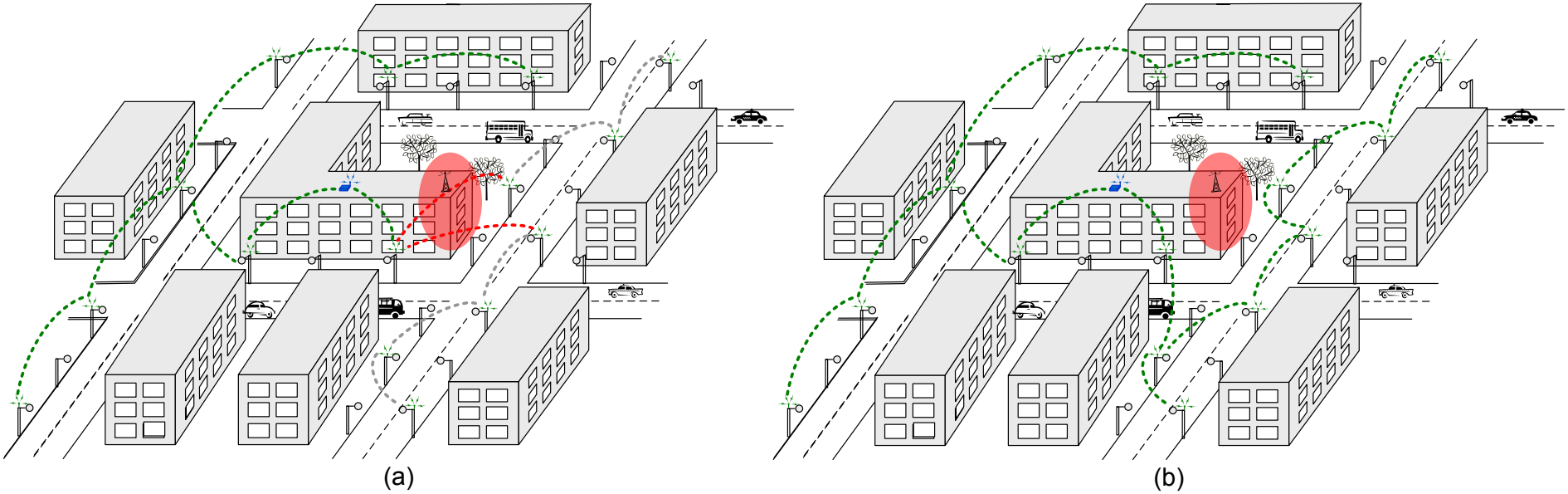
(a) An attacker compromises two TAPs

- Accessing the internal state
- Modifying the internal state

(b) The attack is detected and new routes are defined

Three Fundamental Security Operations

2. Routing

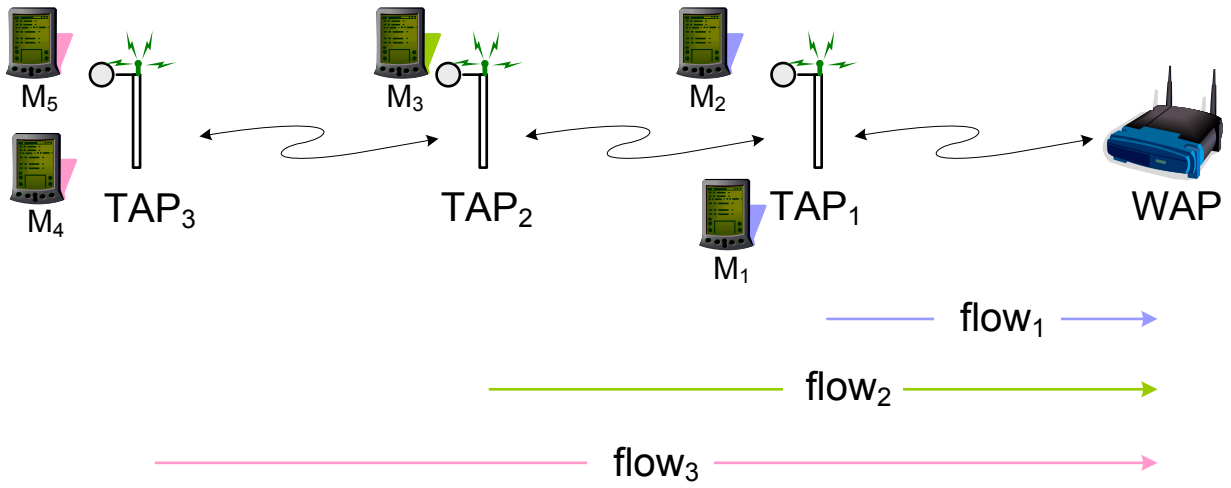


(a) Dos attack

(b) The attack is detected and new routes are defined

Three Fundamental Security Operations

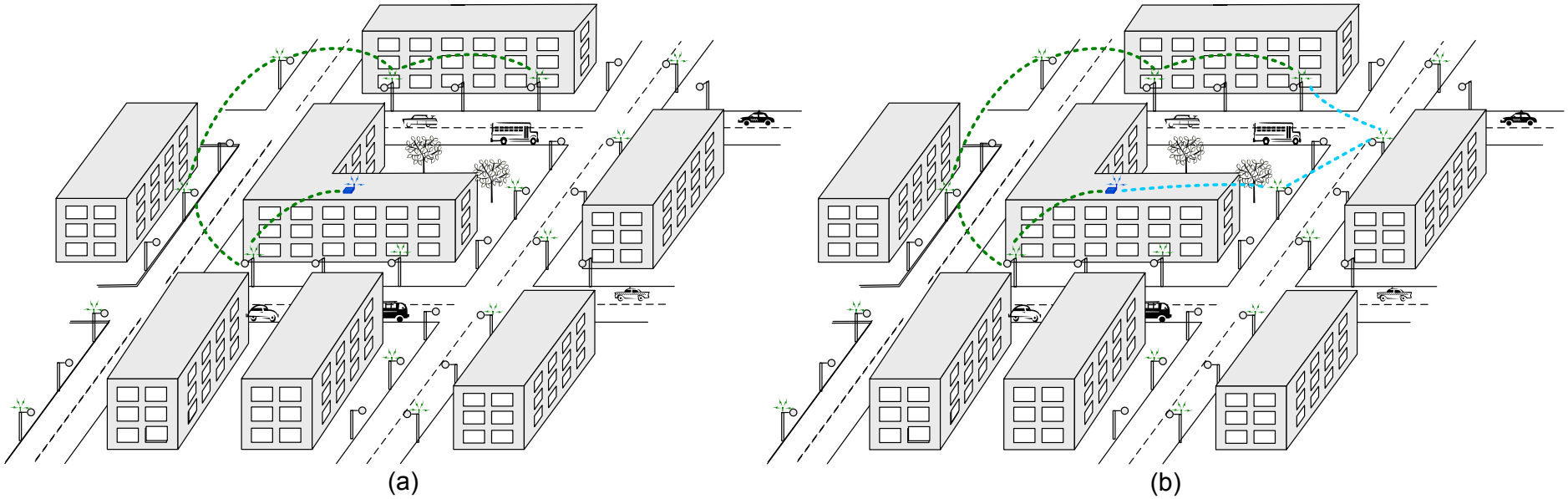
3. Fairness: Starvation problem



- Per-client fairness: $\rho_1=\rho_3=2*\rho_2$
- By attacking the routing, an adversary can affect fairness

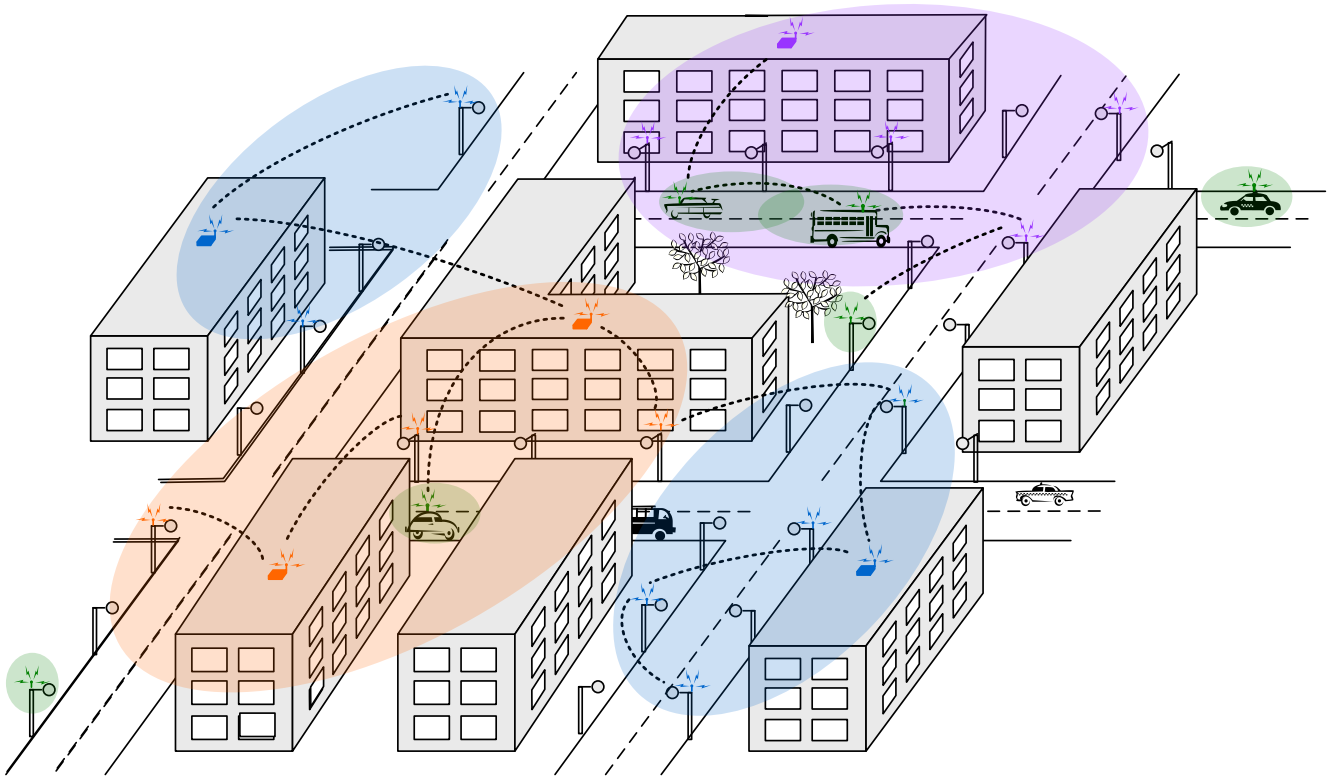
Three Fundamental Security Operations

- Fairness: Example



(a) Sub-optimal route
(b) Optimal route

Multi-operator WMNs

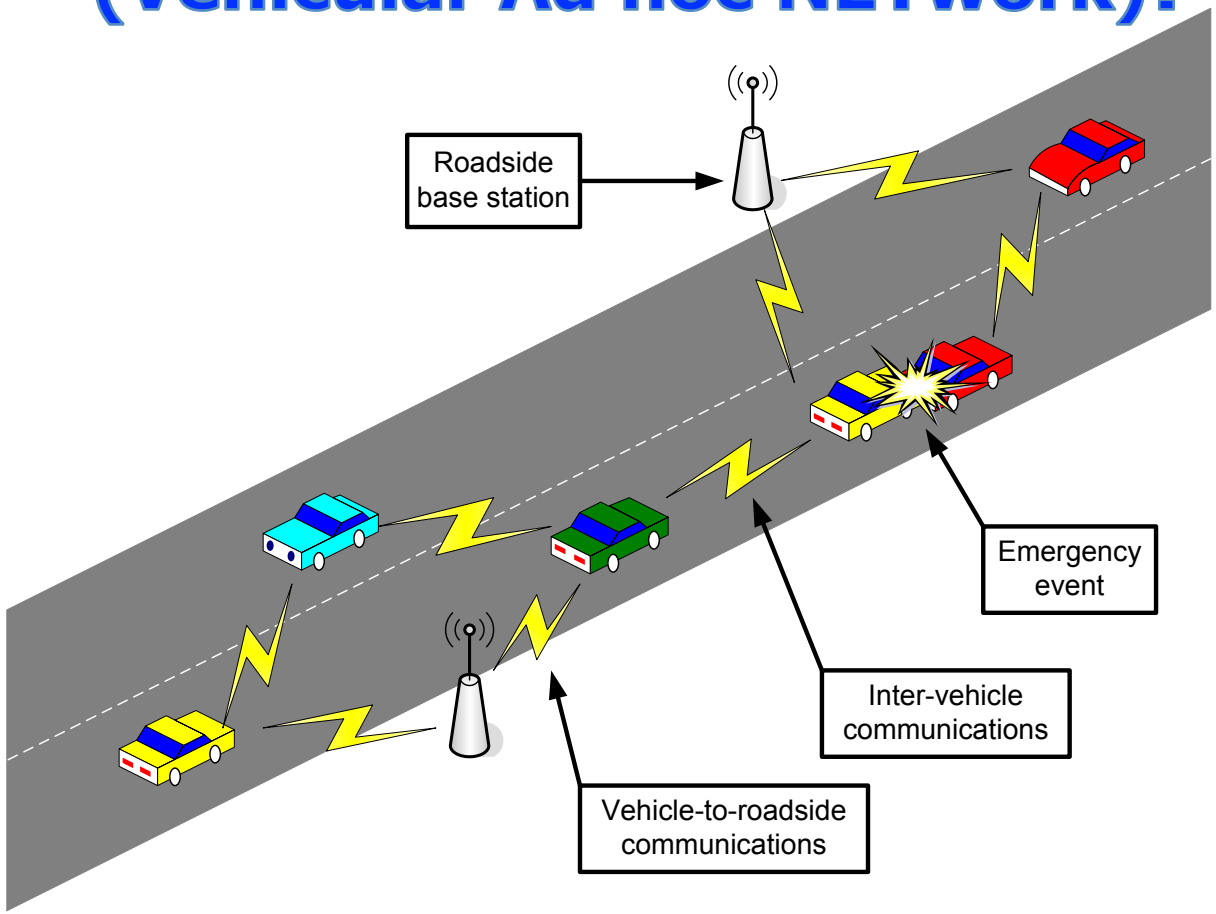


- **New challenges:**
  - Mutual authentication of nodes belonging to different “operating domains”
  - Competition for the channel (shared spectrum)

VANET

- Motivation
- Threat model and specific attacks
- Security architecture
- Security analysis
- Performance evaluation
- Certificate revocation
- Secure positioning
- Conclusion

What is a VANET (Vehicular Ad hoc NETwork)?



- 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)

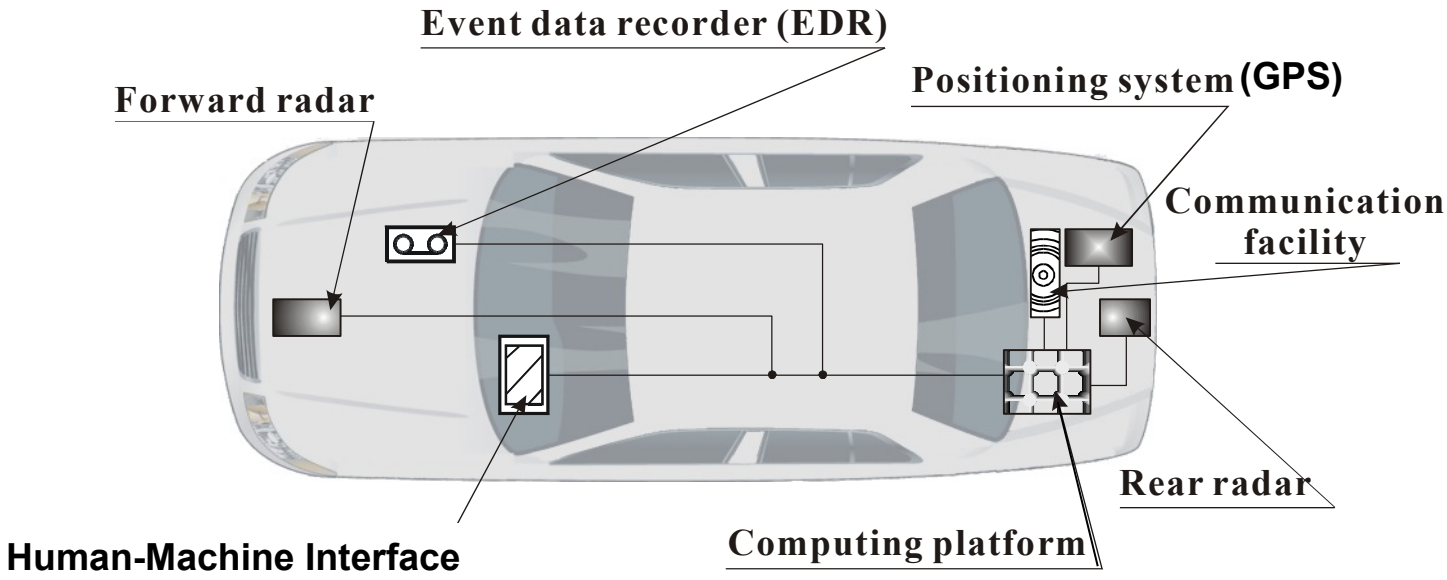
Vehicular communications: why?

- Combat the awful side-effects of road traffic
  - In the EU, around 40’000 people die yearly on the roads; more than 1.5 millions are injured
  - Traffic jams generate a tremendous waste of time and of fuel
- Most of these problems can be solved by providing appropriate ***information*** to the driver or to the vehicle

Why is VANET security important?

- Large projects have explored vehicular communications: Fleetnet, PATH (UC Berkeley),…
- 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 and suffer from serious weaknesses
  - IEEE P1609.2: Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages
- Research front
  - ACM International Workshop on VehiculAr Inter-NETworking, Systems, and Applications

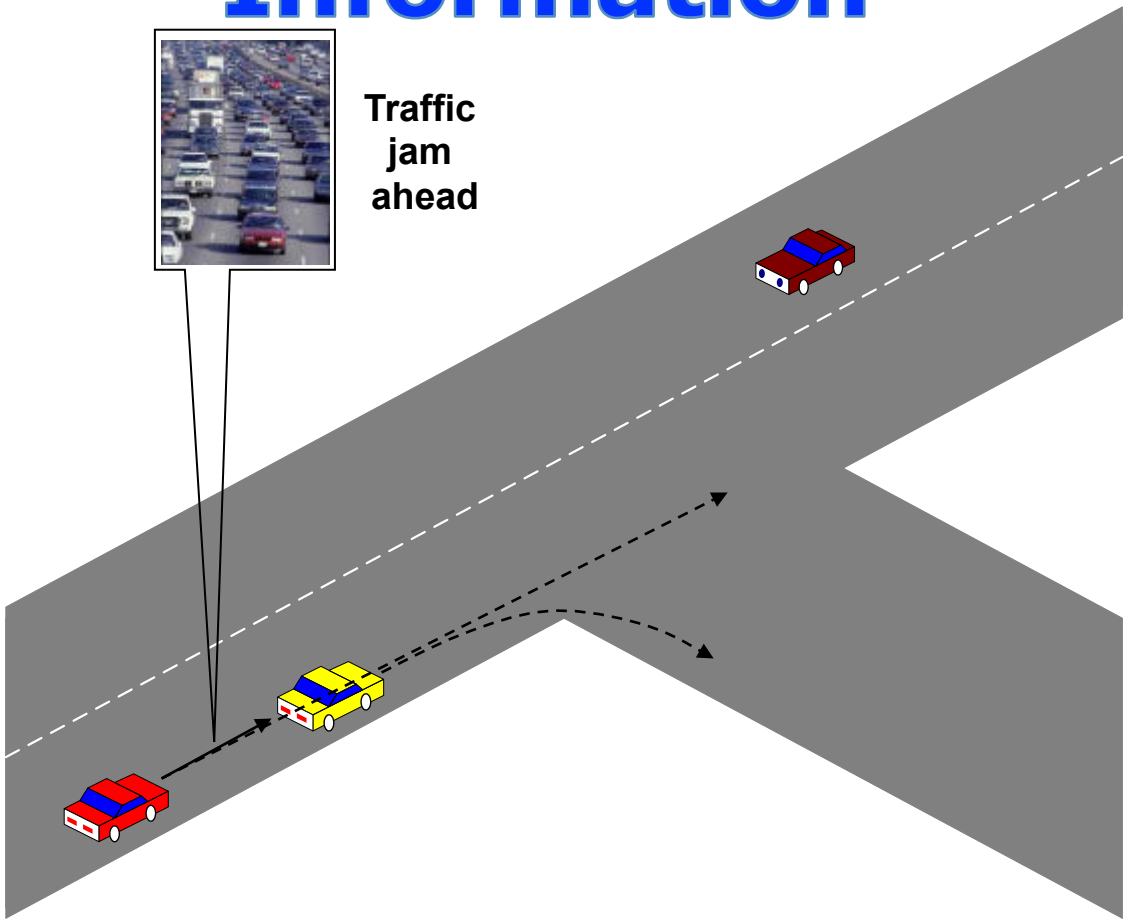
A Smart Vehicle



Threat Model

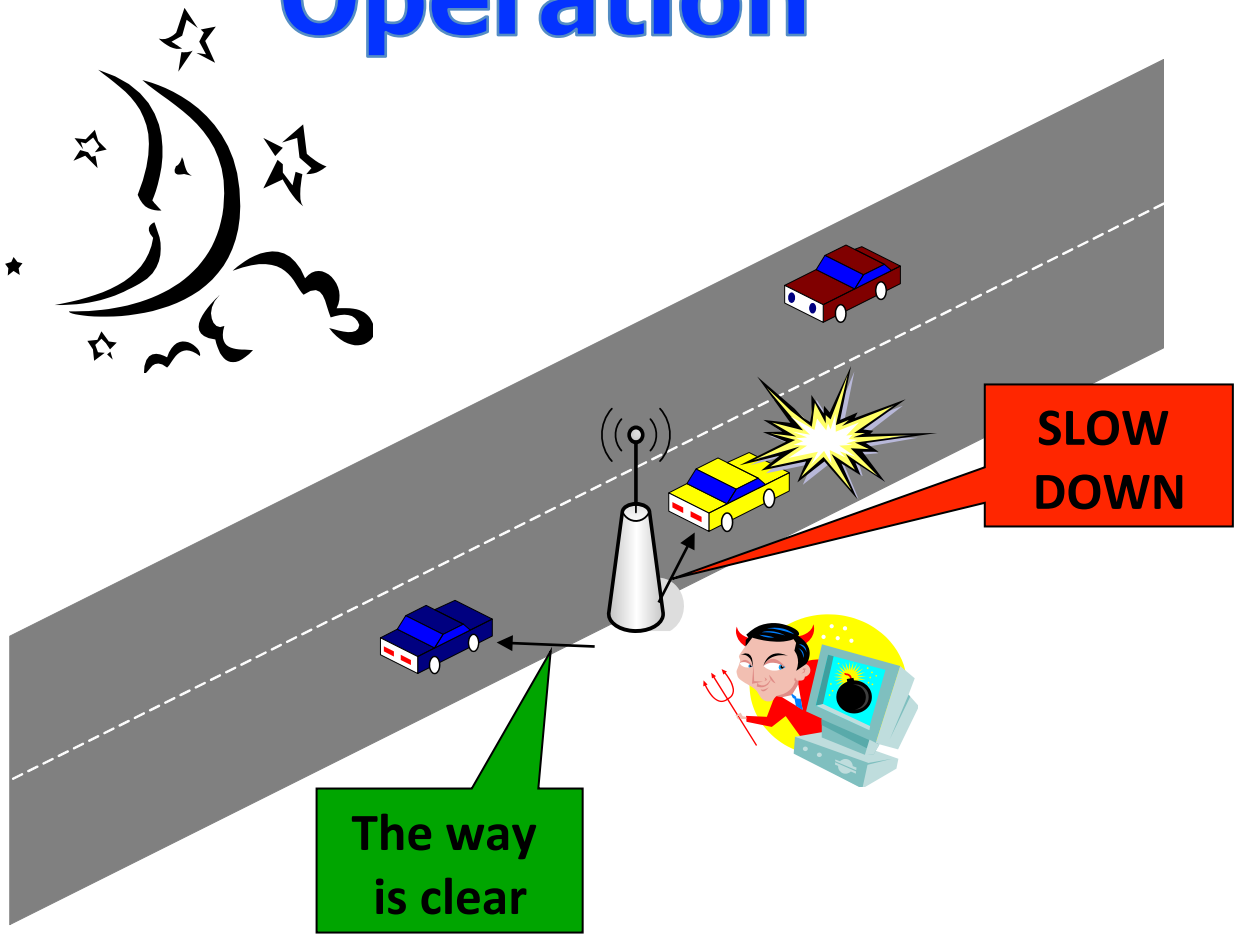
- **An attacker can be:**
  - Insider / Outsider
  - Malicious / Rational
  - Active / Passive
  - Local / Extended
- **Attacks can be mounted on:**
  - Safety-related applications
  - Traffic optimization applications
  - Payment-based applications
  - Privacy

Attack 1 : Bogus Traffic Information



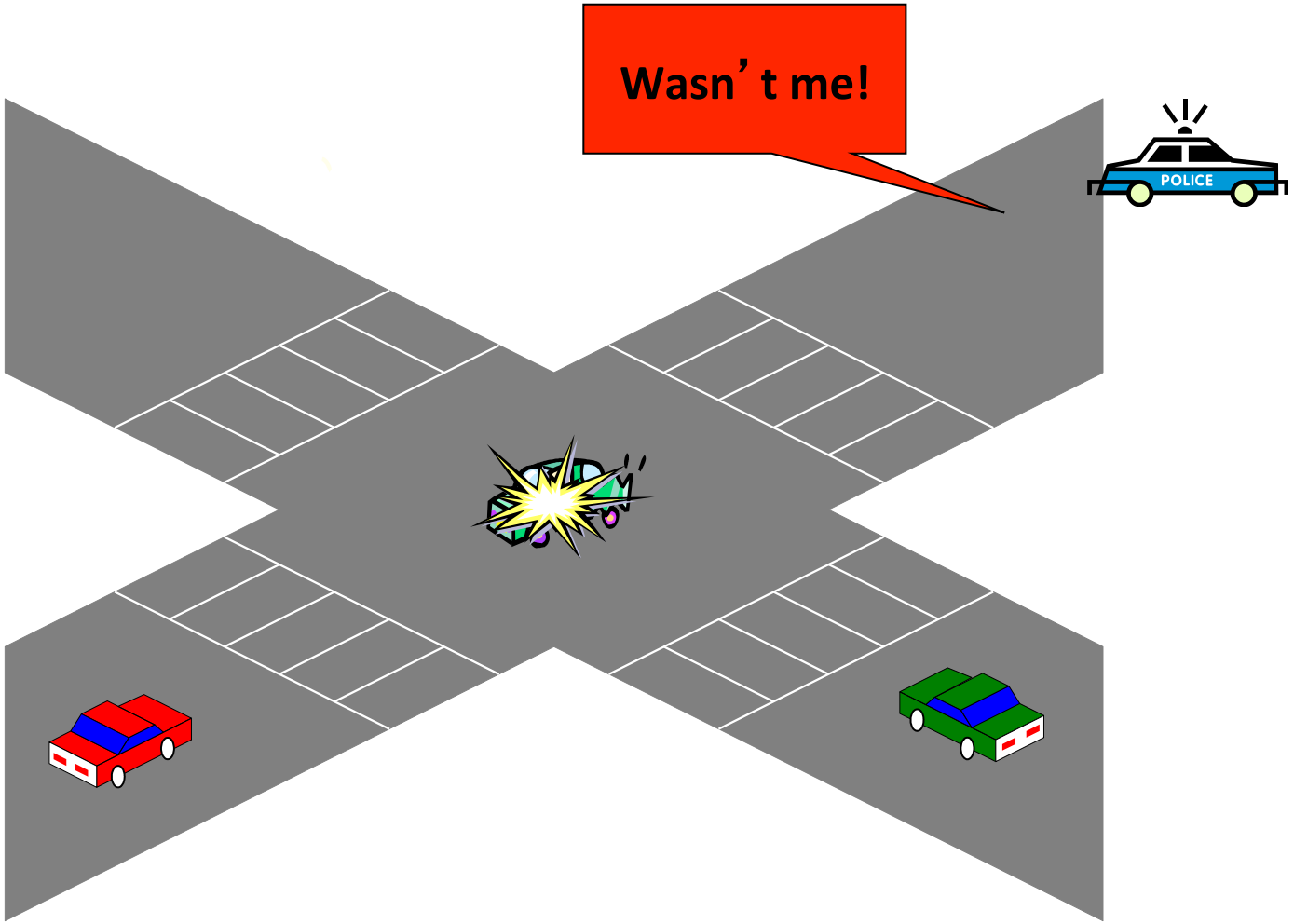
- Attacker: insider, rational, active

Attack 2 : Disruption of Network Operation



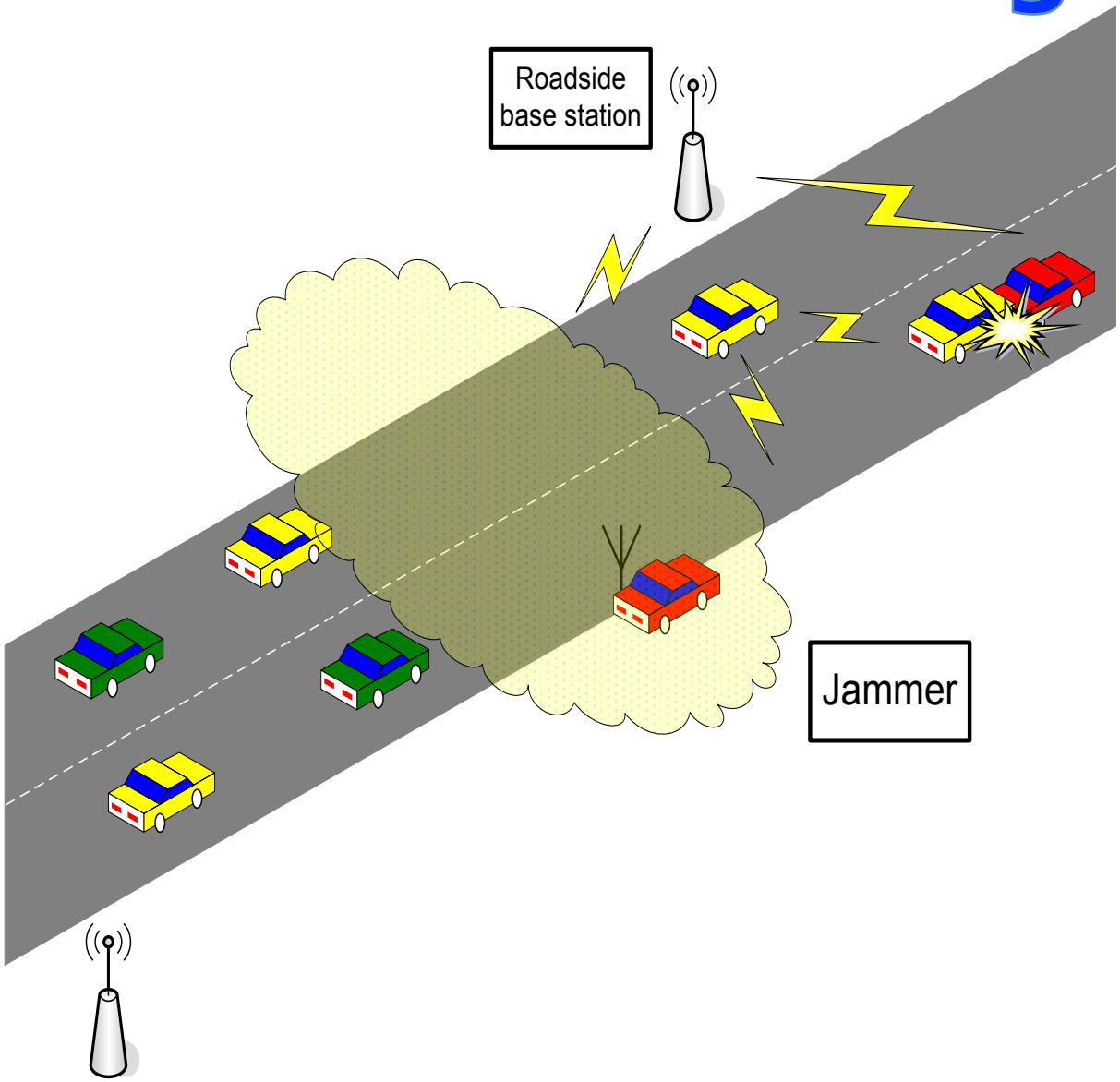
- Attacker: insider, malicious, active

Attack 3: Cheating with Identity, Speed, or Position

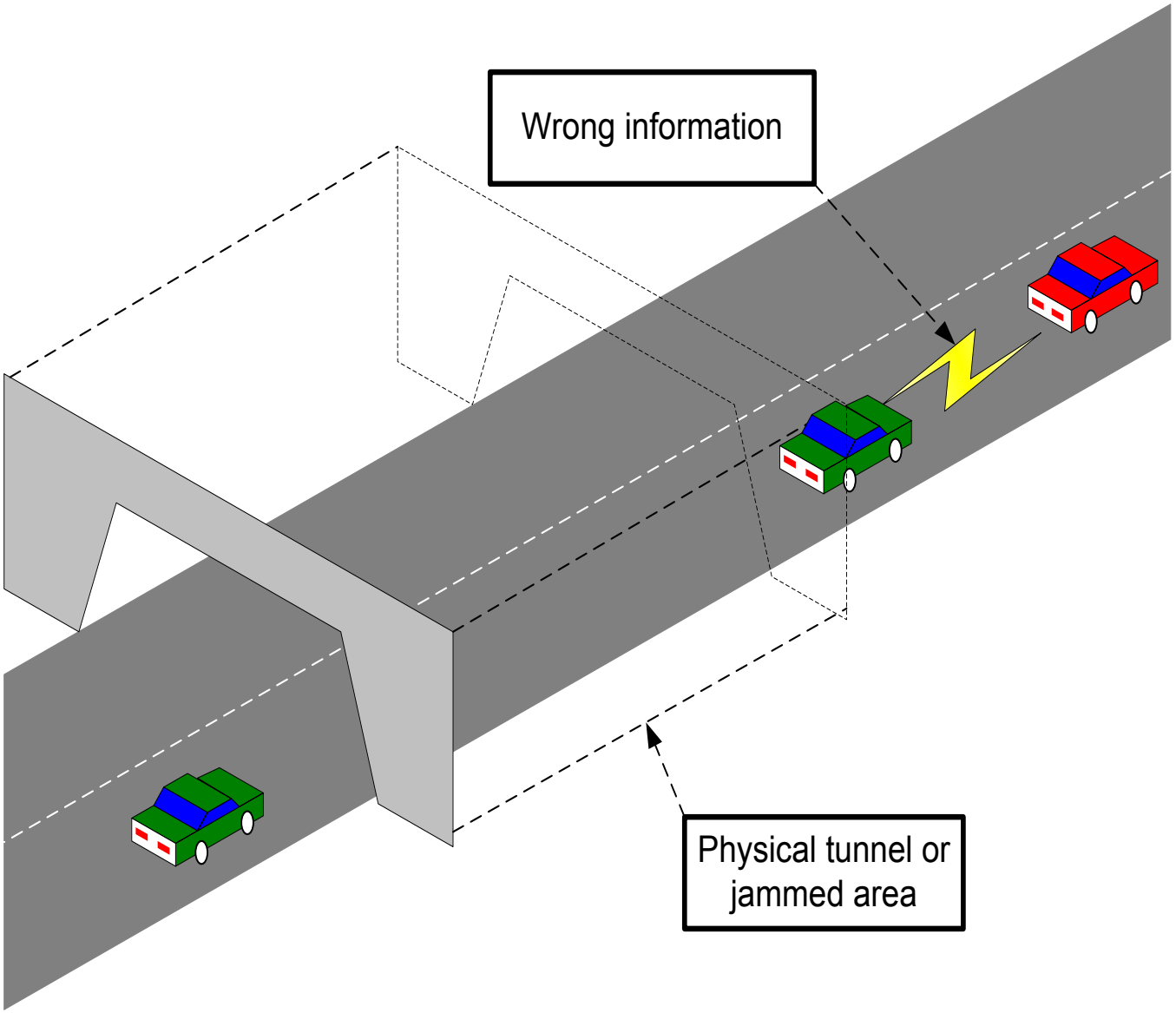


- Attacker: insider, rational, active

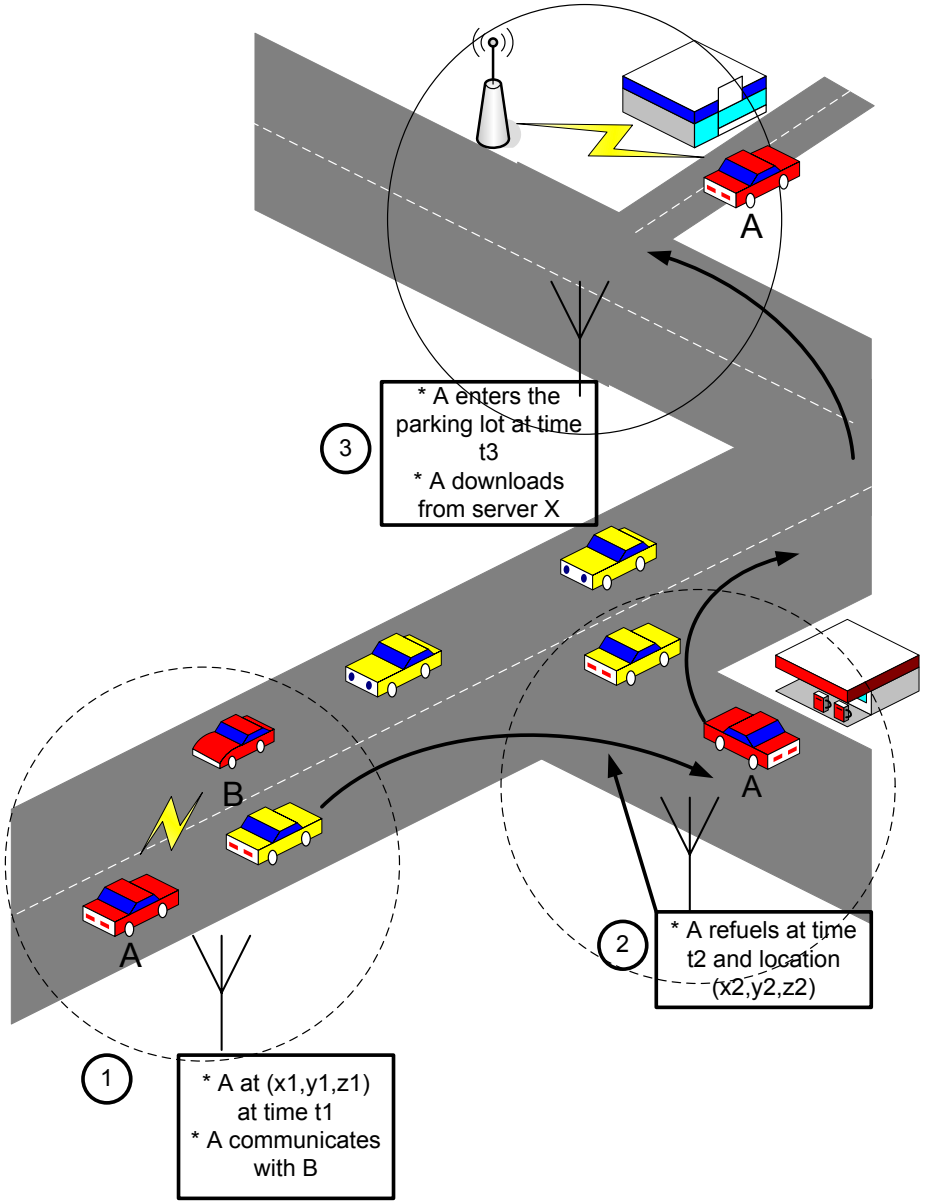
Attack 4: Jamming



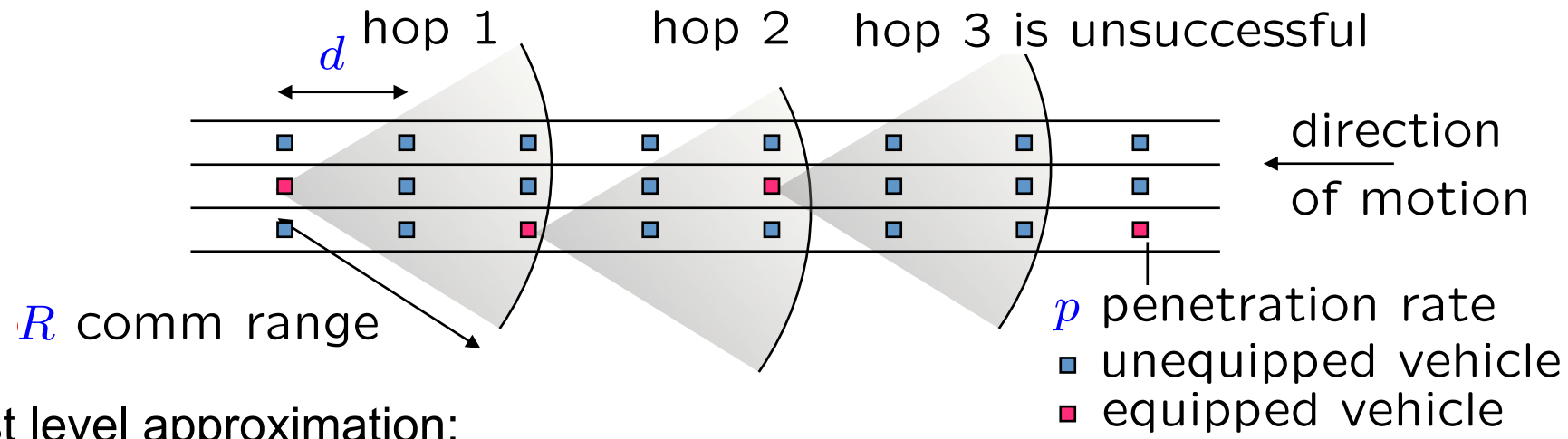
Attack 5: Tunnel



Attack 6: Tracking



Penetration and Connectivity



First level approximation:

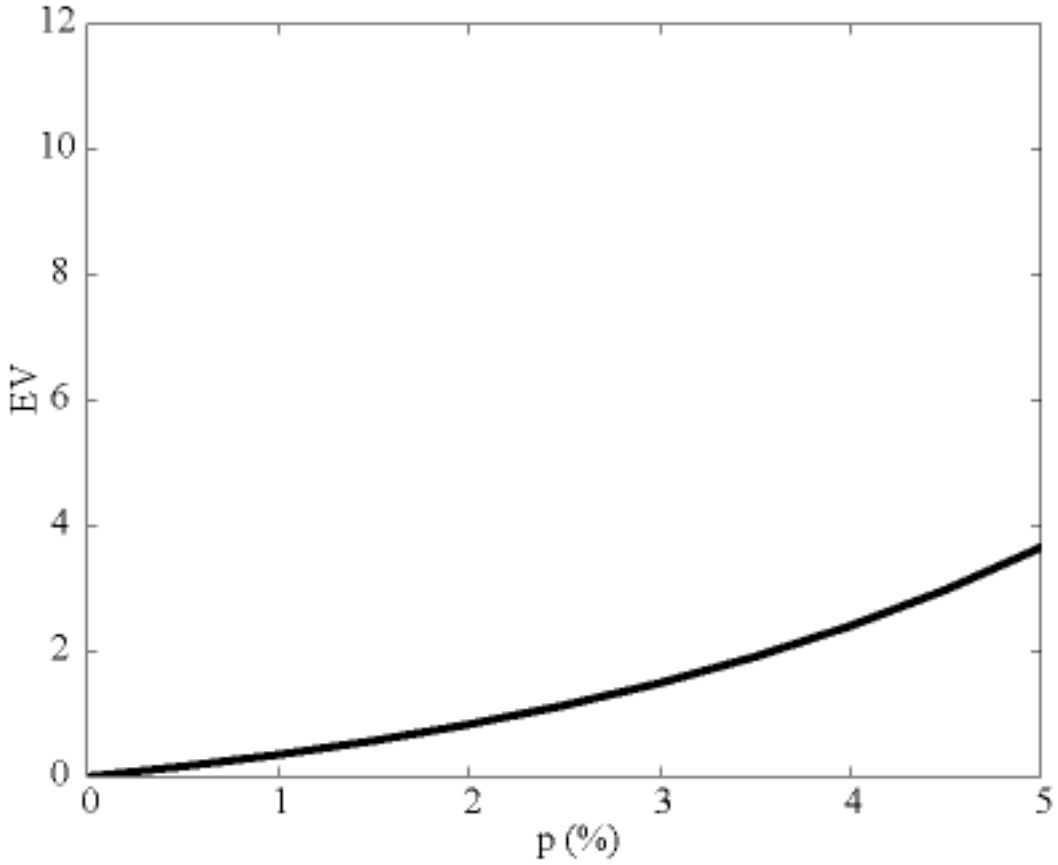
$$
\begin{aligned}
l &= \#\text{ of lanes} \\
N &= l \times R/d, \ \#\text{ vehicles in range} \\
V &= \#\text{ equipped vehicles reached} \\
P &= 1-(1-p)^N = \Pr(V>0) \\
\Pr(V=n) &= P^n(1-P) \\
E(V) &= 1/(1-p)^N - 1
\end{aligned}
$$

[Pravin Varaiya]

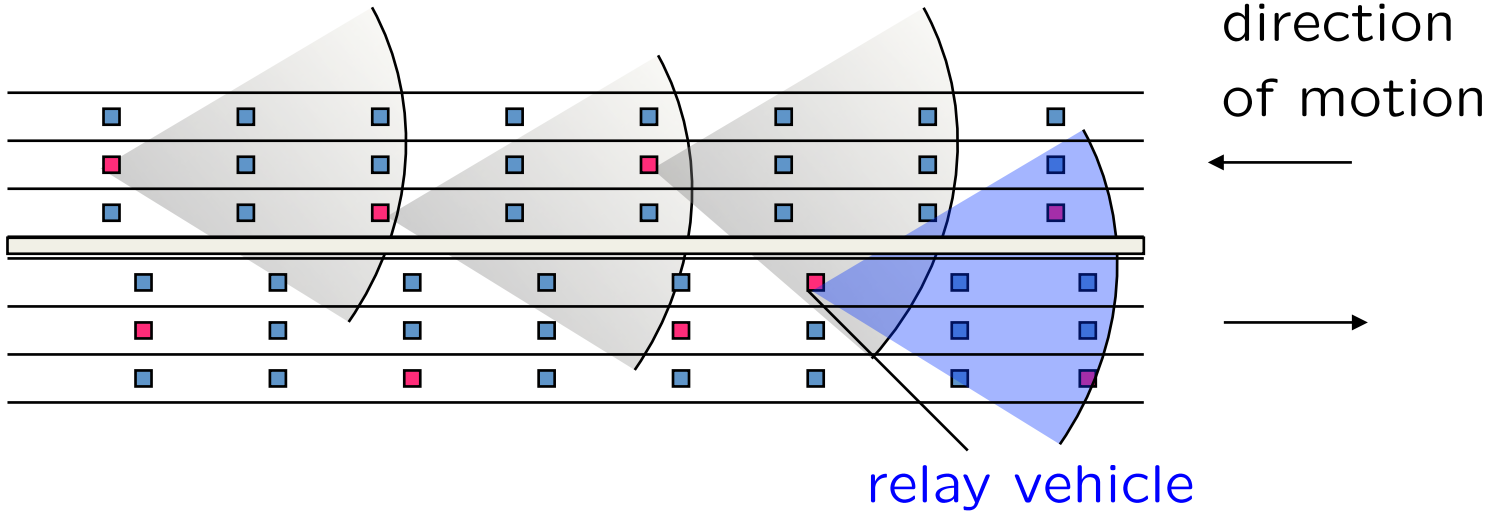
Number of Hops Vs Penetration (1/2)

R = 500m; $d = 50$m [speed = 25m/s; flow = 1,800 v/l/hour];

l = 3 lanes. Then $N = 30$; $EV = 1/(1-p)^{30} - 1$.



Hopping on vehicles in the reverse direction



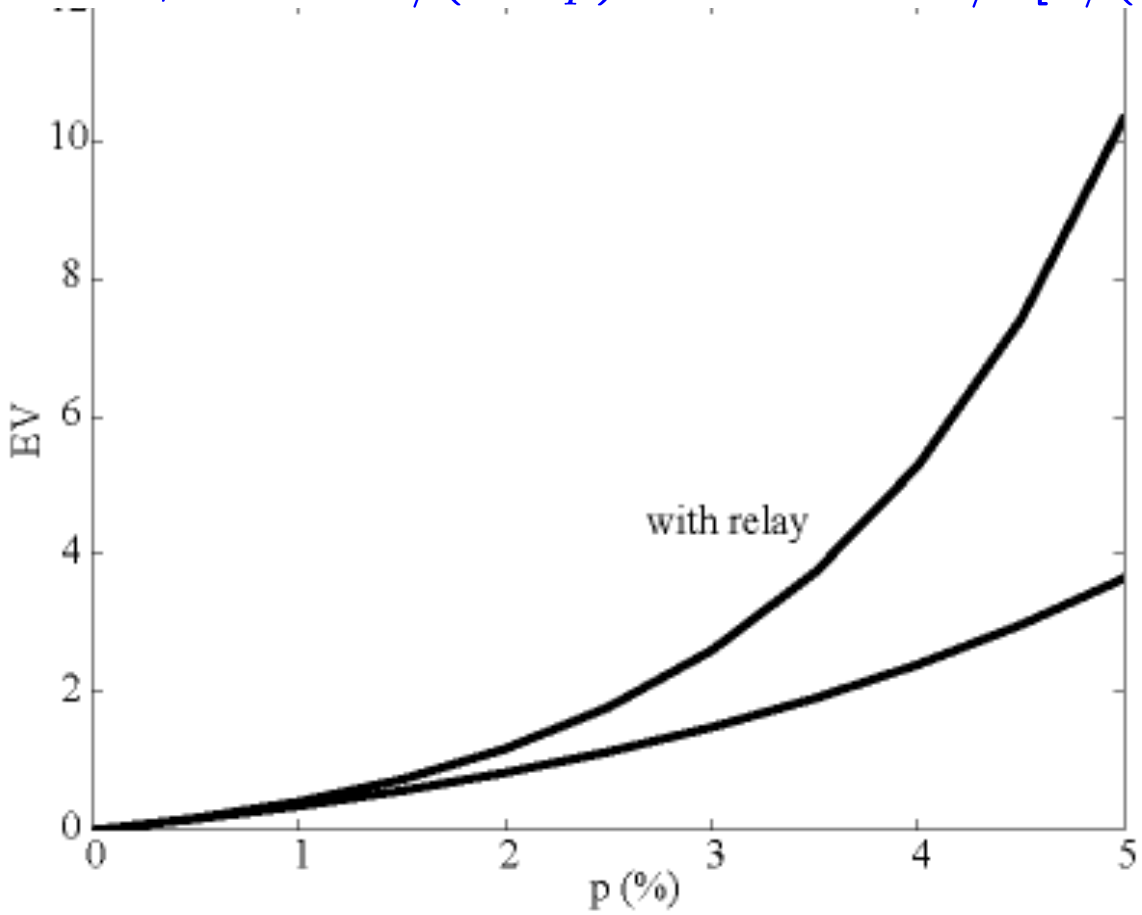
Equipped vehicles in other direction serve as relays. So $d \rightarrow d/2, N \rightarrow 2N$. However, only half the number of successful hops are useful on average, so $EV \rightarrow EV/2$,

$$EV = 1/2[1/(1-p)^{2N} - 1]$$

Number of hops Vs penetration (2/2)

R = 500m; d = 50m; speed = 25m/s; l = 3 lanes. Then

N = 30; $EV = 1/(1-p)^{30} - 1$ or $= 1/2[1/(1-p)^{60} - 1]$



Proposed Homework

Compute connectivity in this case ;-)

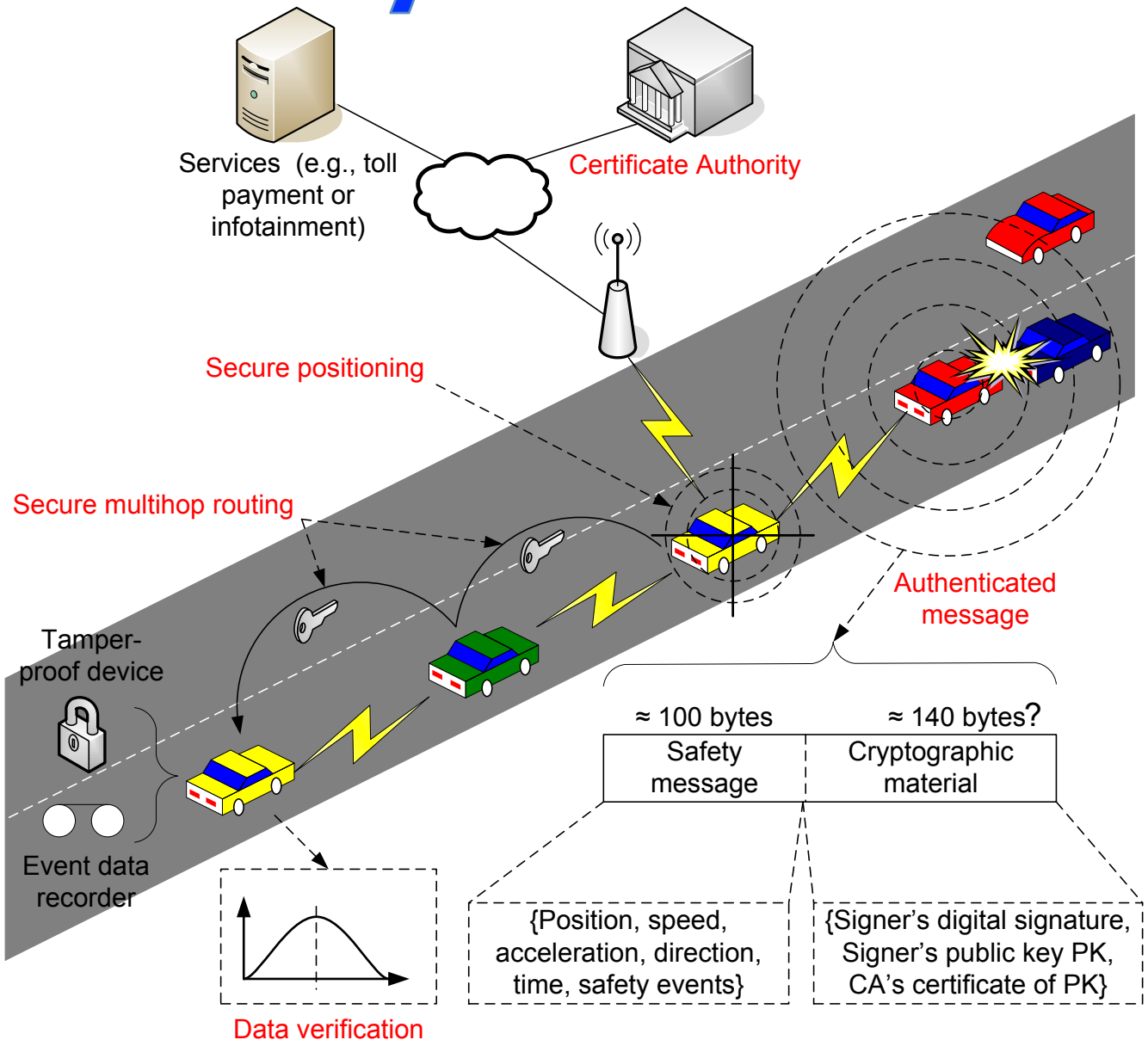
Our Scope

- We consider communications specific to road traffic: safety and traffic optimization
  - Safety-related messages
  - Messages related to traffic information
- We do not consider more generic applications, e.g. toll collect, access to audio/video files, games, …

Security System Requirements

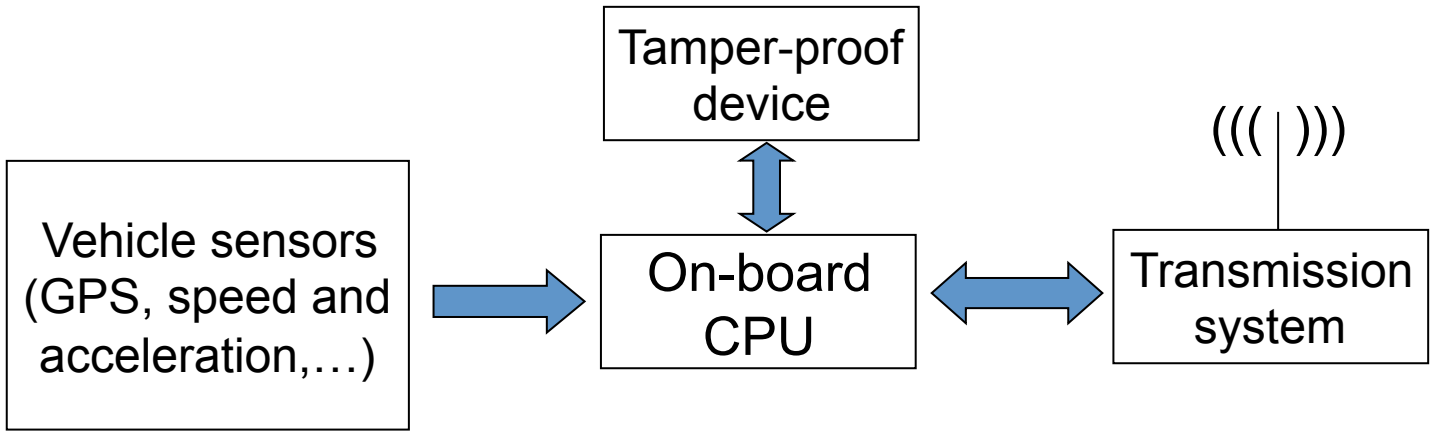
- Sender authentication
- Verification of data consistency
- Availability
- Non-repudiation
- Privacy
- Real-time constraints

Security Architecture



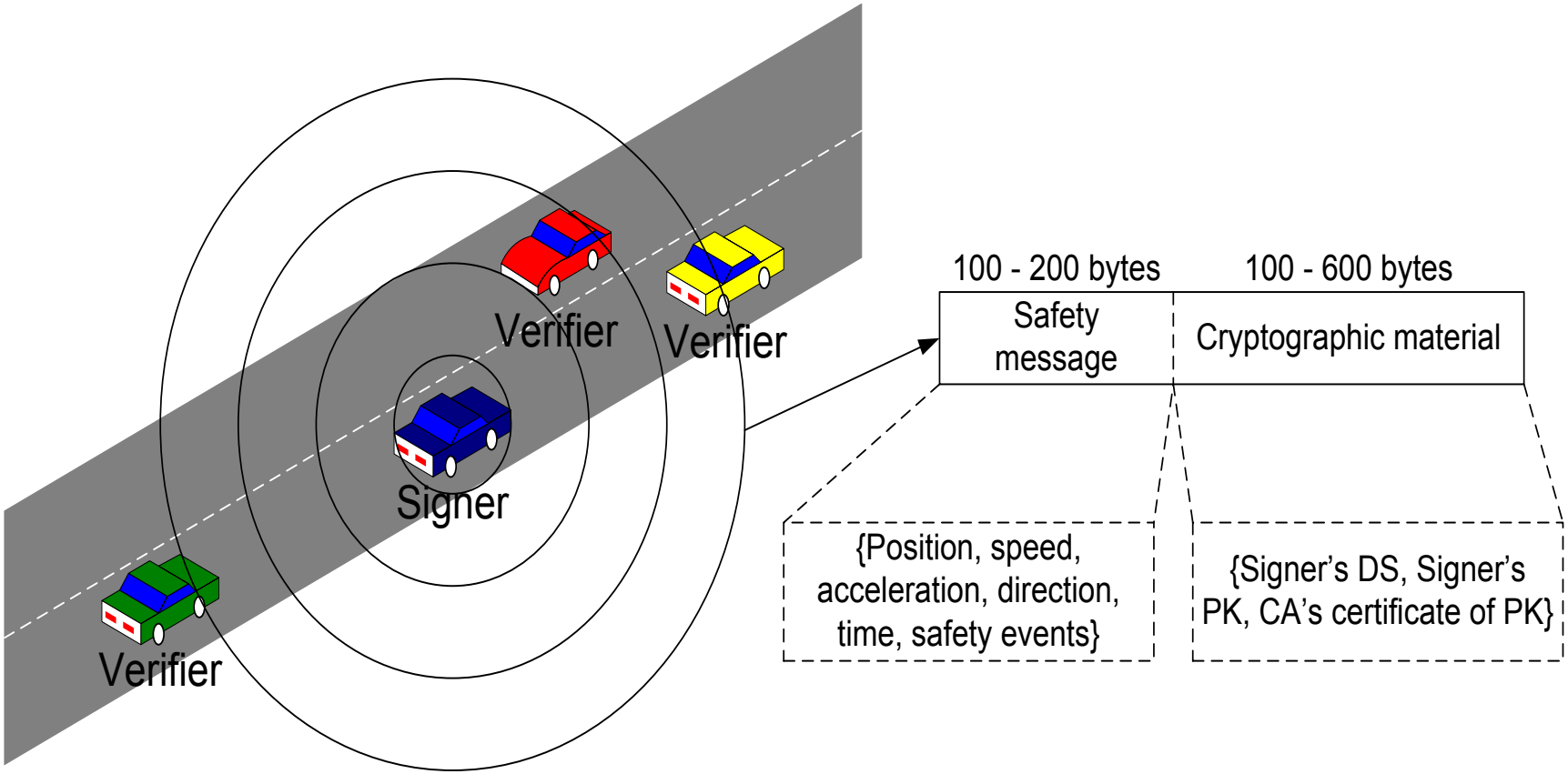
Tamper-Proof Device

- Each vehicle carries a **tamper-proof device**
  - Contains the secrets of the vehicle itself
  - Has its own battery
  - Has its own clock (notably in order to be able to sign timestamps)
  - Is in charge of all security operations
  - Is accessible only by authorized personnel



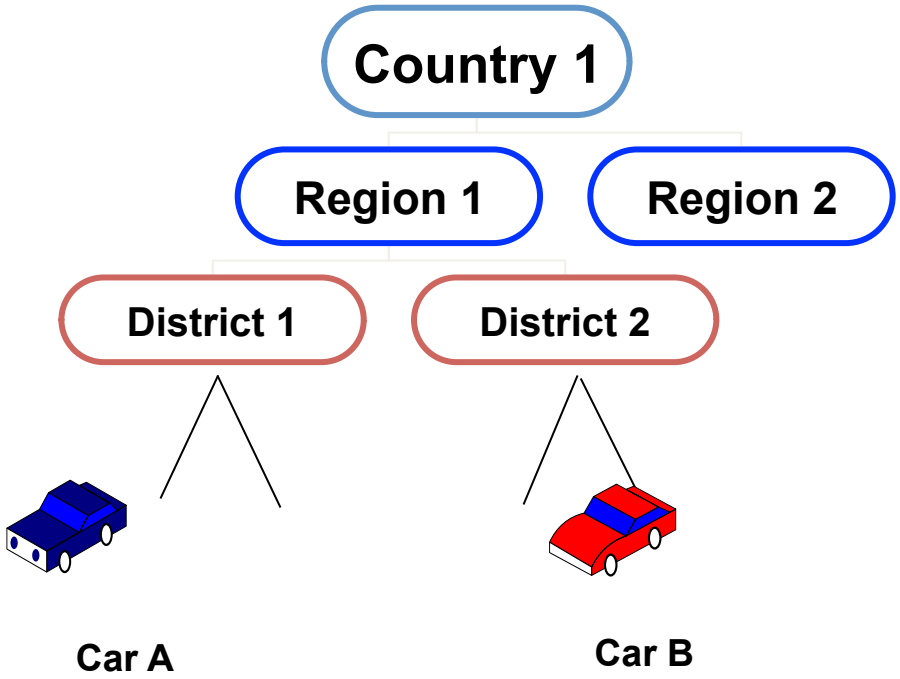
Digital Signatures

- Symmetric cryptography is not suitable: messages are standalone, large scale, non-repudiation requirement
- Hence each message should be signed with a DS
- Liability-related messages should be stored in the EDR



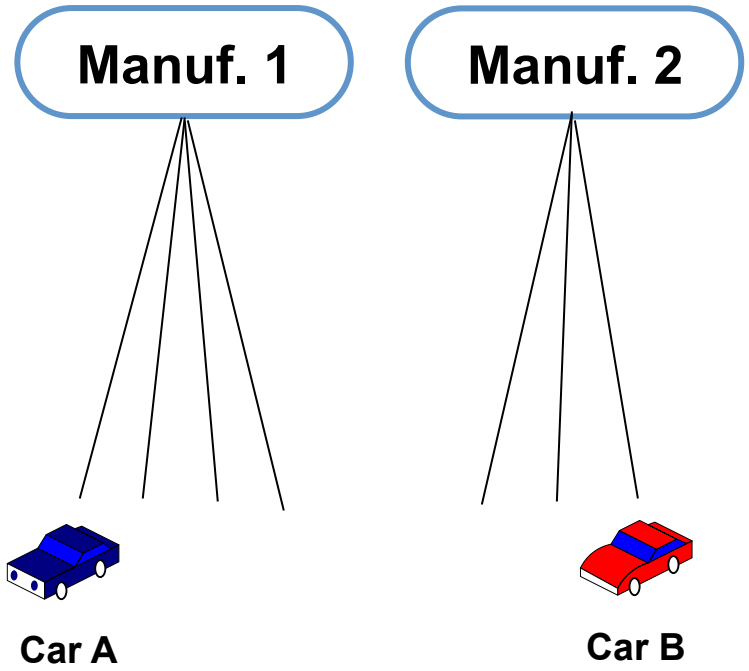
The CA hierarchy: Two Options

1. Governmental Transportation Authorities



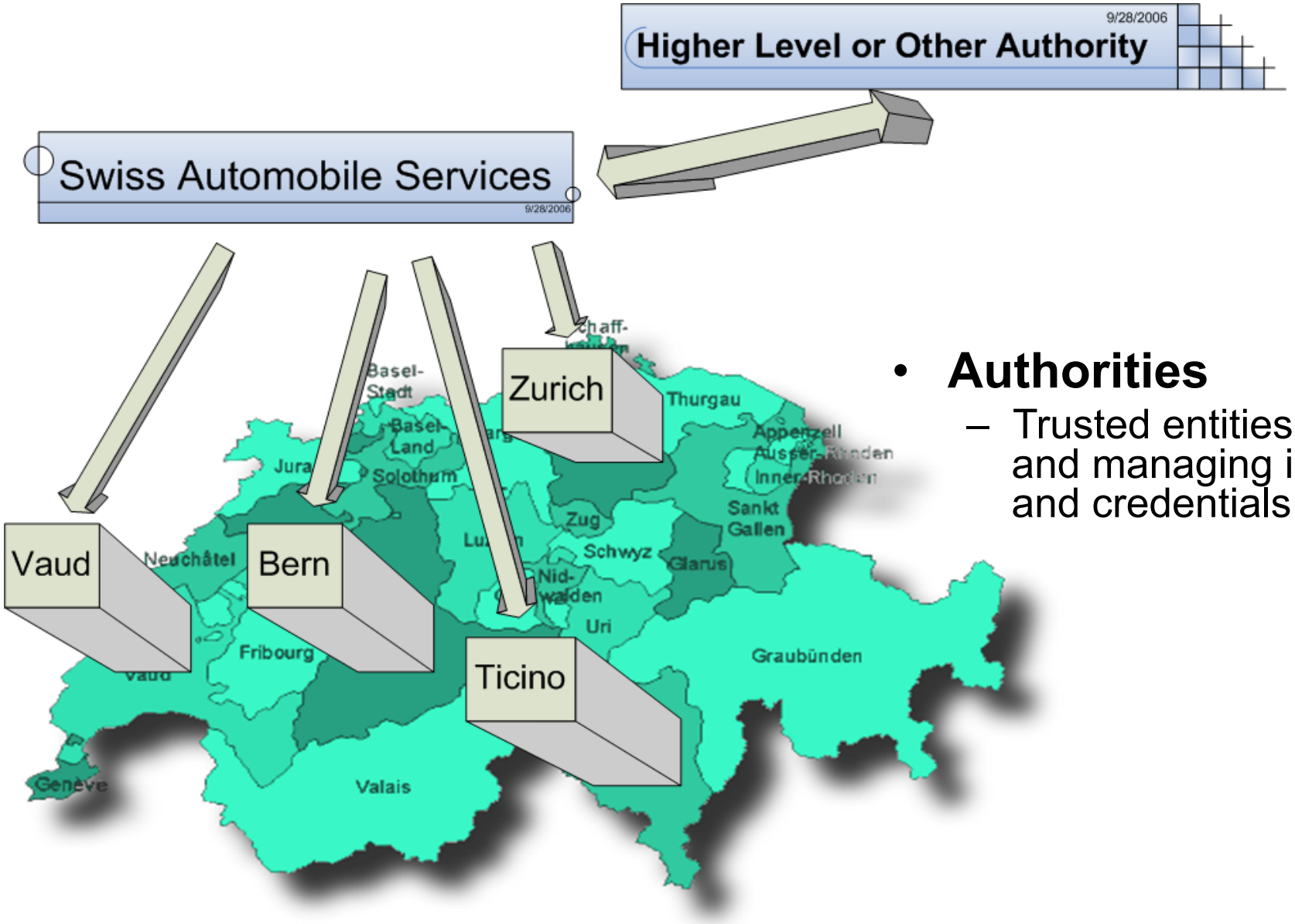
- The governments control certification
- Long certificate chain
- Keys should be recertified on borders to ensure mutual certification

2. Manufacturers



- Vehicle manufacturers are trusted
- Only one certificate is needed
- Each car has to store the keys of all vehicle manufacturers

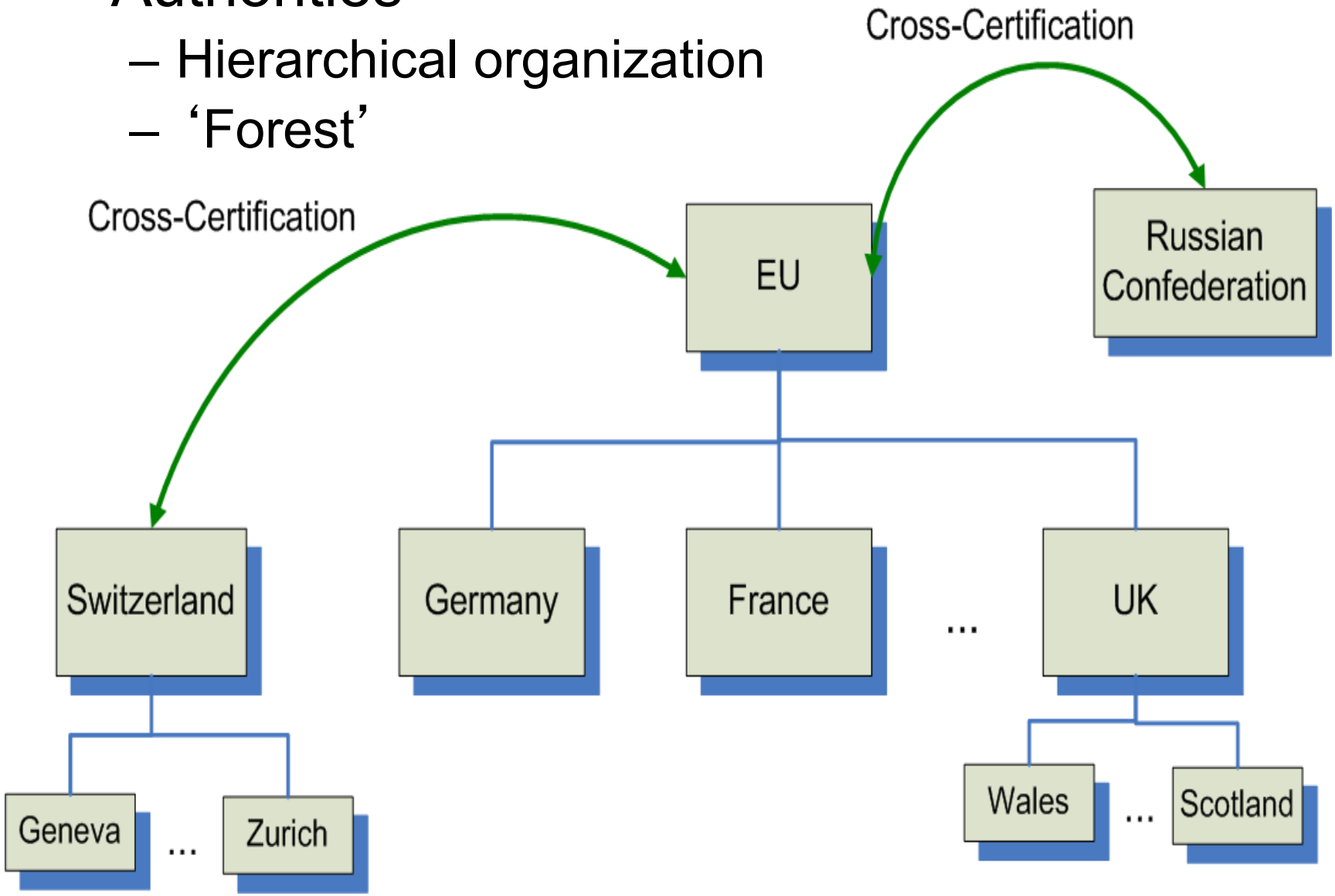
Secure VC Building Blocks



- **Authorities**
  - Trusted entities issuing and managing identities and credentials

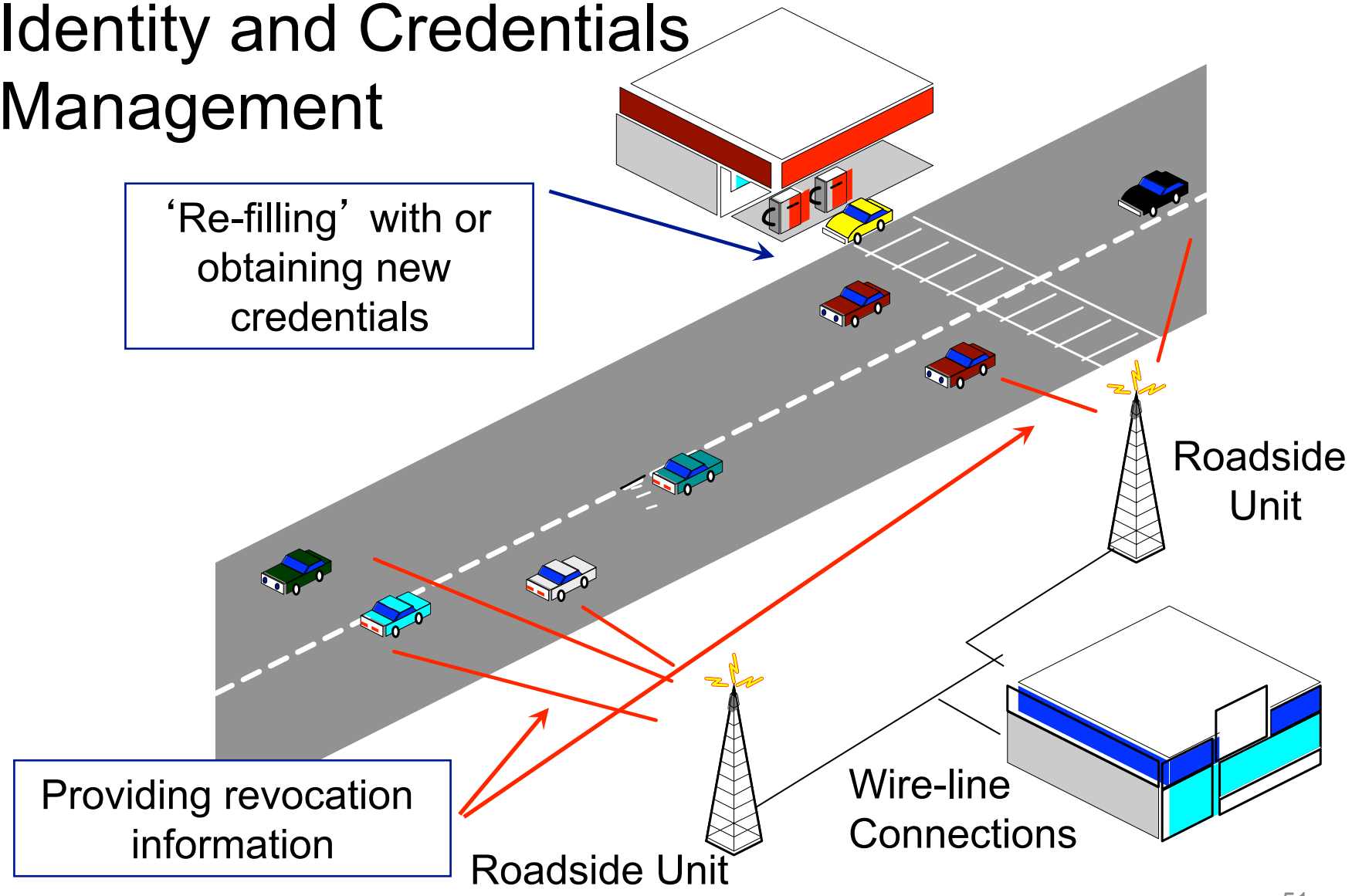
Secure VC Building Blocks

- Authorities
  - Hierarchical organization
  - 'Forest'



Secure VC Building Blocks
(cont' d)

- Identity and Credentials Management



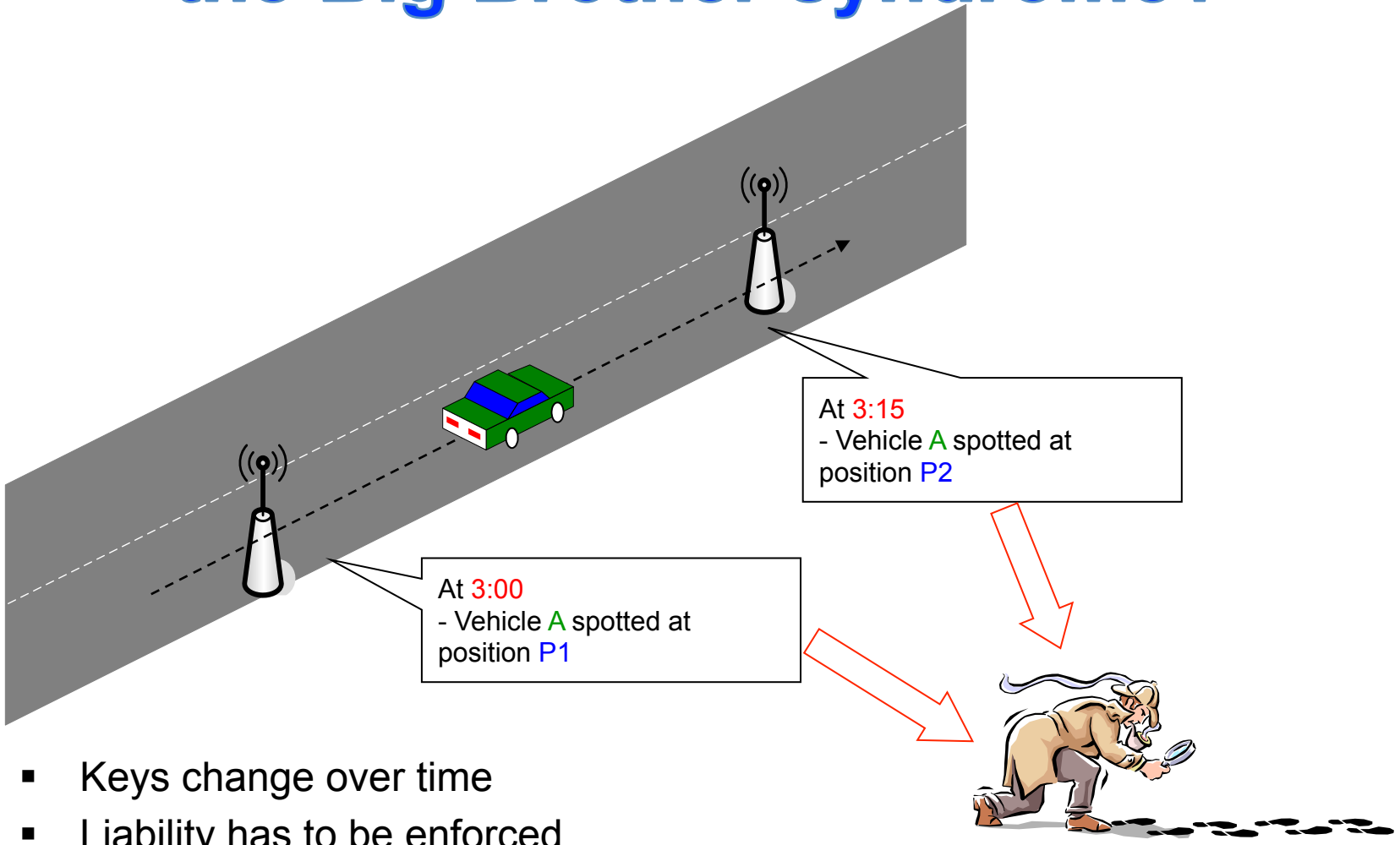
Anonymous keys

- Preserve identity and location privacy
- Keys can be preloaded at periodic checkups
- The certificate of *V*'s i^{th} key:

$$Cert_V[PuK_i] = PuK_i \mid Sig_{SK_{CA}}[PuK_i \mid ID_{CA}]$$

- Keys renewal algorithm according to vehicle speed (e.g., ≈ 1 min at 100 km/h)
- Anonymity is conditional on the scenario
- The authorization to link keys with ELPs is distributed

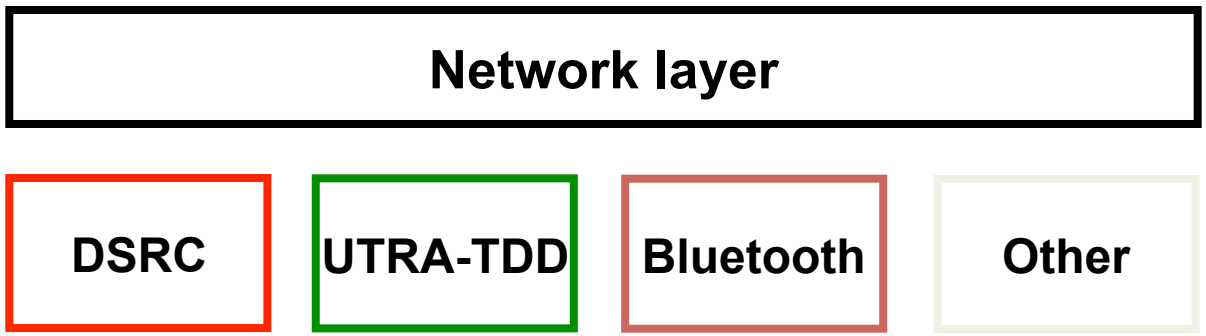
What about privacy: how to avoid the Big Brother syndrome?



- Keys change over time
- Liability has to be enforced
- Only law enforcement agencies should be allowed to retrieve the real identities of vehicles (and drivers)

DoS Resilience

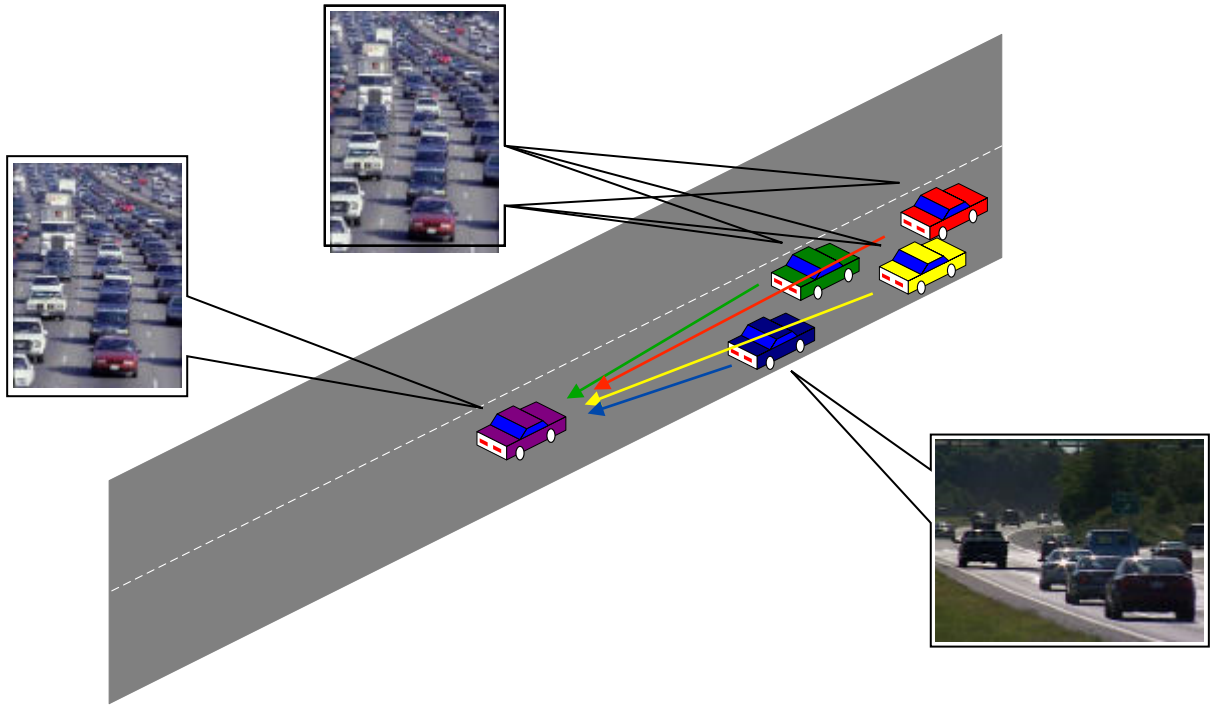
- Vehicles will probably have several wireless technologies onboard
- In most of them, several channels can be used
- To thwart DoS, vehicles can switch channels or communication technologies



- In the worst case, the system can be deactivated

Data Verification by Correlation (plausibility)

- Bogus info attack relies on false data
- Authenticated vehicles can also send wrong data (on purpose or not)
- The correctness of the data should be verified
- Correlation can help



Security Analysis

- How much can we secure VANETs?
- Messages are authenticated by their signatures
- Authentication protects the network from outsiders
- Correlation and fast revocation reinforce correctness
- Availability remains a problem that can be alleviated
- Non-repudiation is achieved because:
  - ELP and anonymous keys are specific to one vehicle
  - Position is correct if secure positioning is in place

Conclusion on the Security of Vehicular Communications

- The security of vehicular communications is a difficult and highly relevant problem
- Car manufacturers seem to be poised to massively invest in this area
- Slow penetration makes connectivity more difficult
- Security leads to a substantial overhead and must be taken into account from the beginning of the design process
- The field offers plenty of novel research challenges
- Pitfalls
  - Defer the design of security
  - Security by obscurity