Security and Cooperation in Wireless Networks

http://secowinet.epfl.ch

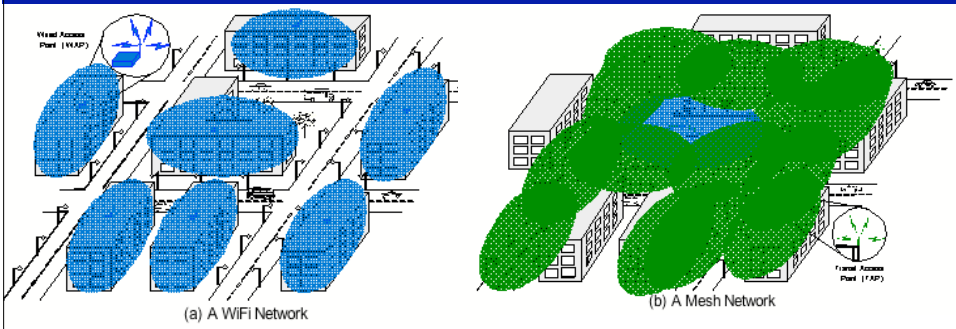
Security of Emerging wireless networks

Generalities
Mesh networks
Vehicular networks

Introduction

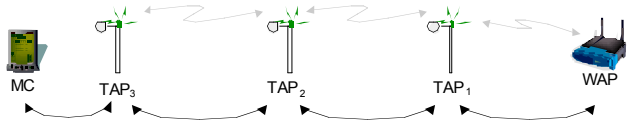
- Emerging wireless networks:
  - Personal communications:
    - Wireless mesh networks
    - Hybrid ad hoc networks
    - Mobile ad hoc networks
  - Vehicular networks
  - Sensor networks
  - RFID
  - Mobility in the Internet

Wireless Mesh Networks



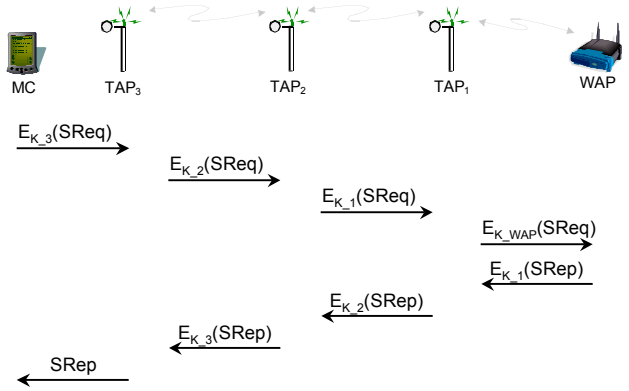
- Wireless Mesh Network (WMN): Same coverage as with WiFi networks but with only one WAP (and several TAPs).
- WMNs allow a fast, easy and inexpensive network deployment.
- However, the lack of security guarantees slows down the deployment of WMNs

A Typical Communication in WMNs



- Several verifications need to be performed:
  - WAP has to authenticate the MC.
  - 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: Example



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

Characteristics of WMNs

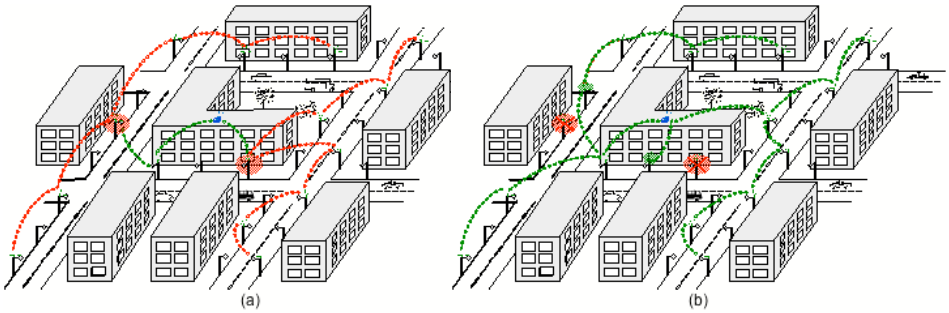
- Multi-hop communications:
  - Delayed detection and treatment of attacks
  - Routing becomes critical
  - Unfairness
- The TAPs are not physically protected:
  - Capture
  - Cloning
  - Tampering

Three fundamental security operations:

- Detection of corrupt nodes
- Secure routing
- Fairness

Three Fundamental Security Operations

- Detection of corrupt nodes



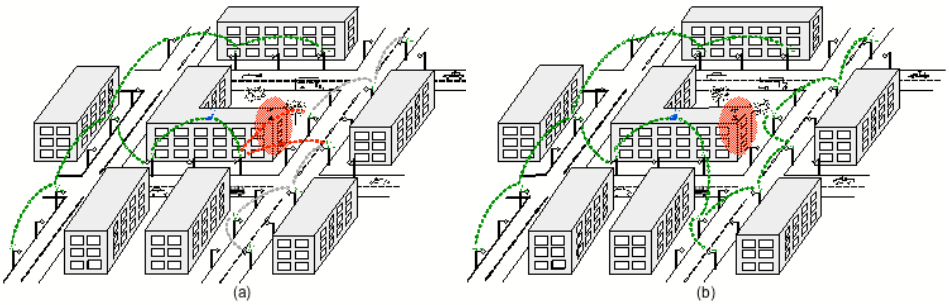
(a) An attacker compromises two TAPs

- Accessing the internal state
- Modifying the internal state

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

Three Fundamental Security Operations

- Routing

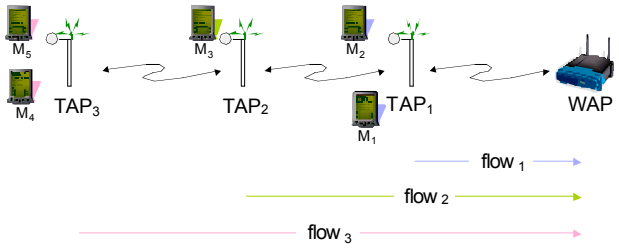


(a) Dos attack

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

Three Fundamental Security Operations

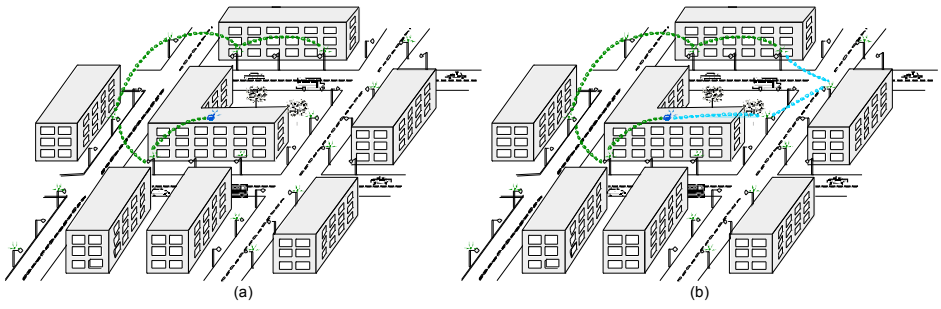
- Fairness: Starvation problem



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

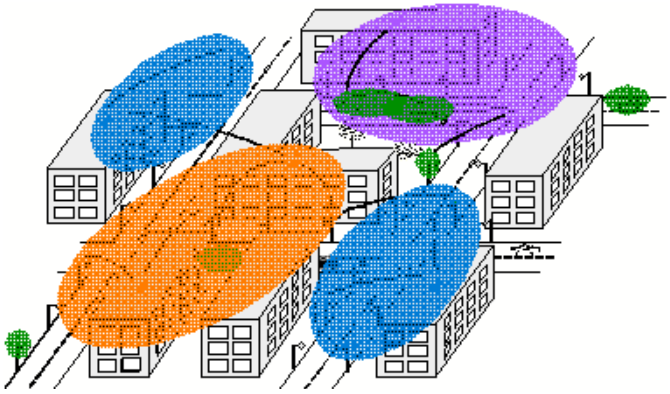
Three Fundamental Security Operations

- Fairness: Example



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

Multi-operator WMNs

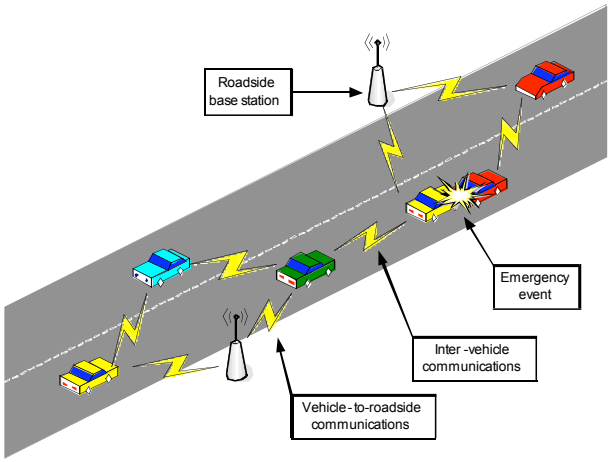


- New challenges:
  - Mutual authentication of nodes belonging to different "operating domains"
  - Competition for the channel (shared spectrum)

Outline

- 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)

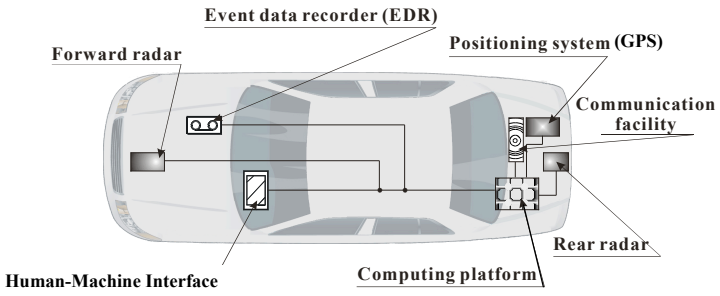
Vehicular communications: why?

- 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
  - Very few papers

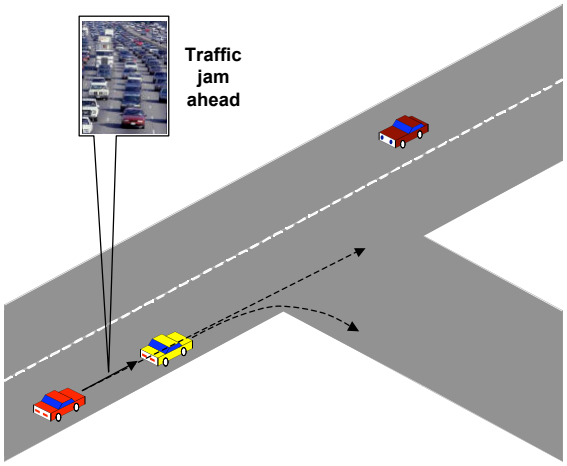
A smart vehicle



Threat model

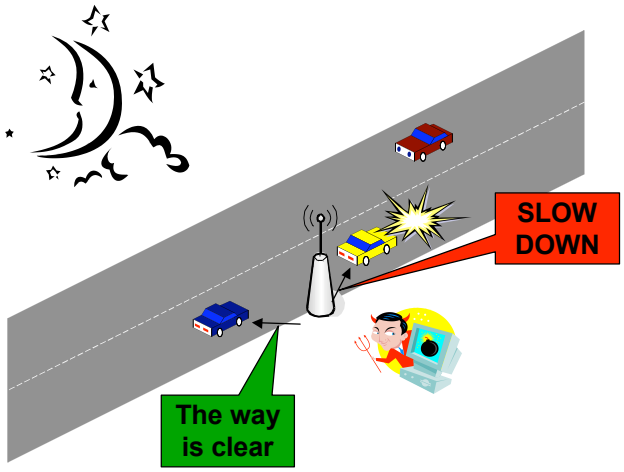
- An attacker can be:
  - Insider / Outsider
  - Malicious / Rational
  - Active / Passive
  - Local / Extended
- Attacks can be mounted on:
  - Safety-related applications
  - Traffic optimization applications
  - Payment-based applications
  - Privacy

Attack 1 : Bogus traffic information



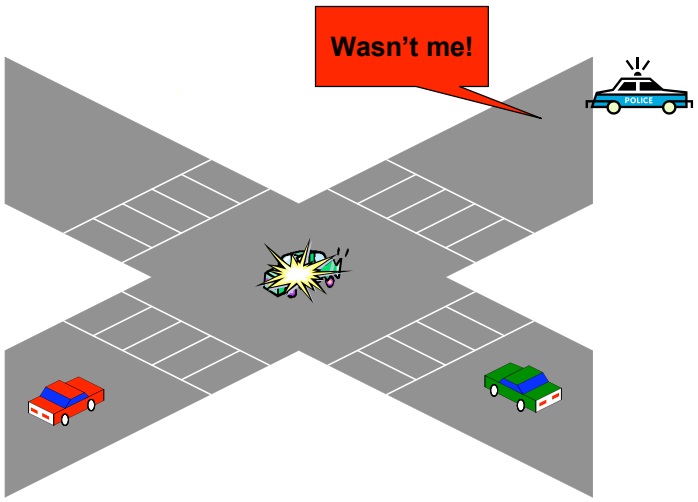
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



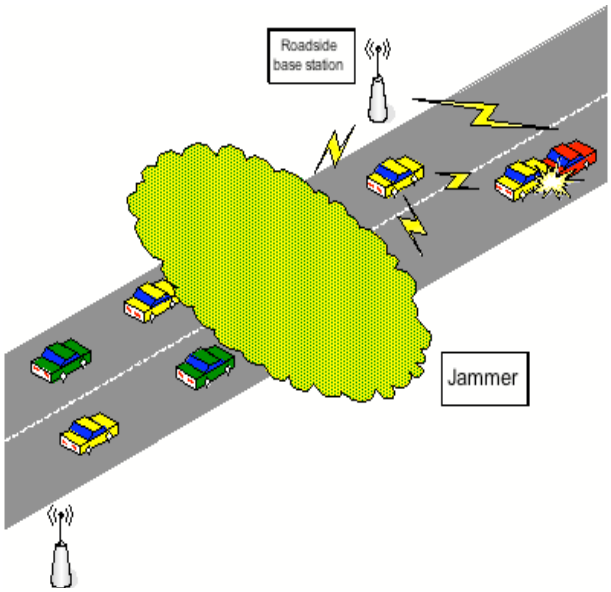
- Attacker: insider, malicious, active

Attack 3: Cheating with identity, speed, or position

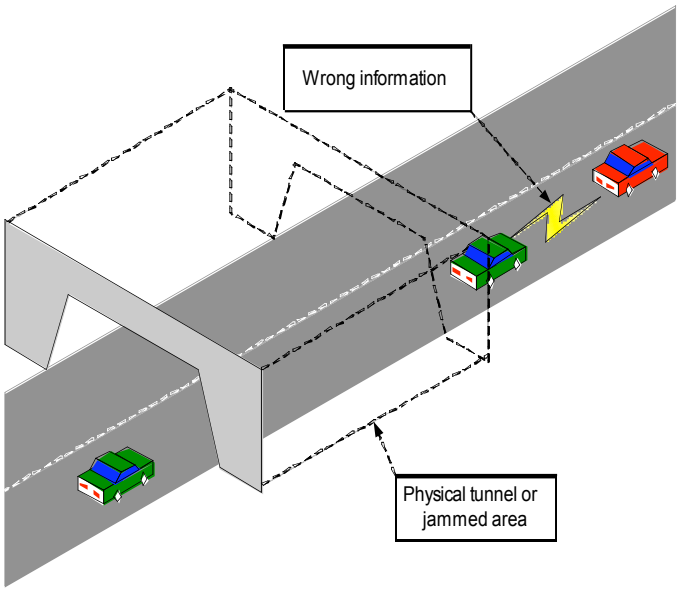


- Attacker: insider, rational, active

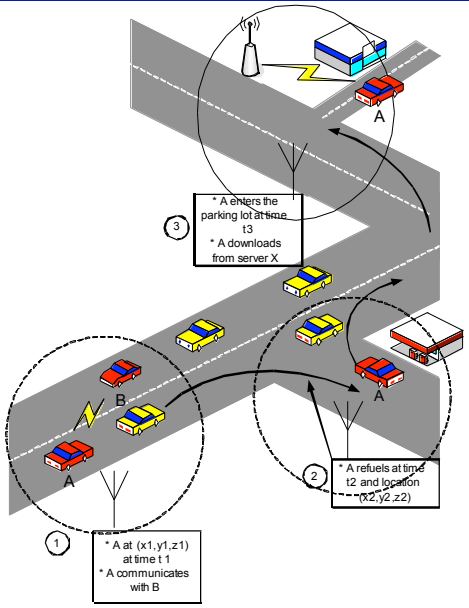
Attack 4: Jamming



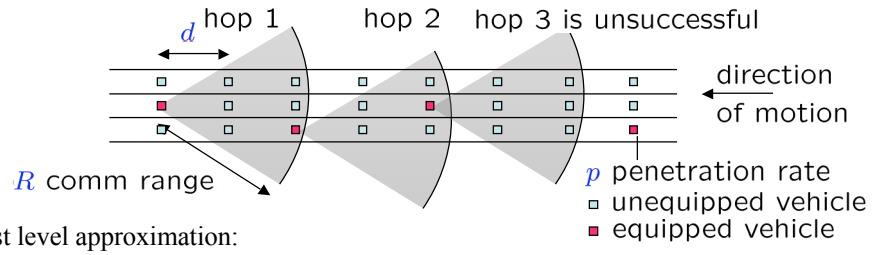
Attack 5: Tunnel



Attack 6: Tracking



Penetration and connectivity



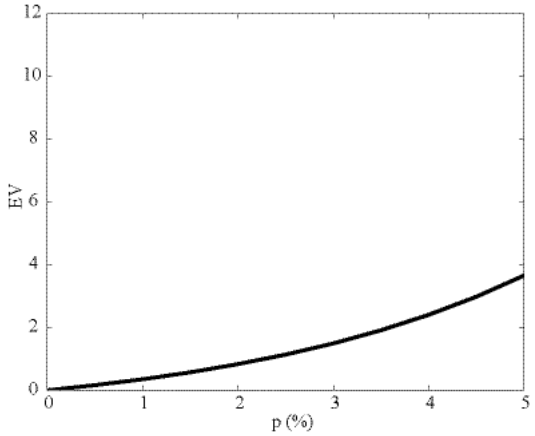
First level approximation:

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

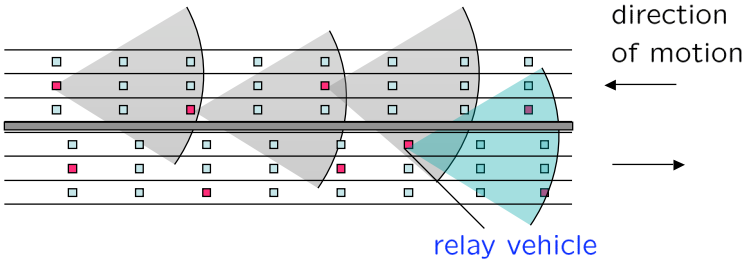
Courtesy of Pravin Varaiya

Number of hops Vs penetration (1/2)

R = 500m; d = 50m [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

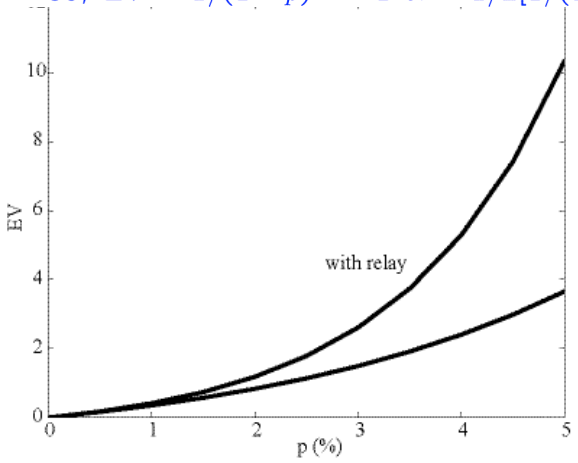


Equipped vehicles in other direction serve as relays. So $d \rightarrow d/2, N \rightarrow 2N$. However, only half the number of successful hops are useful on average, so $EV \rightarrow EV/2$,

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

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 $= 1/2[1/(1-p)^{60} - 1]$



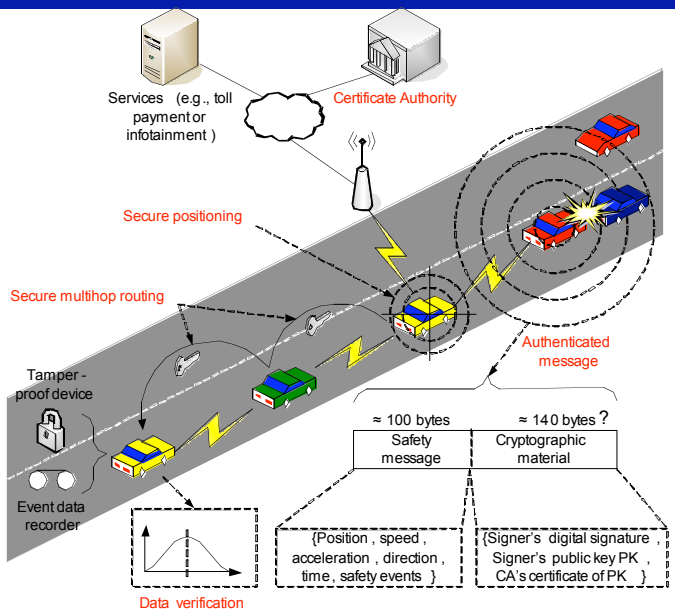
Our scope

- 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

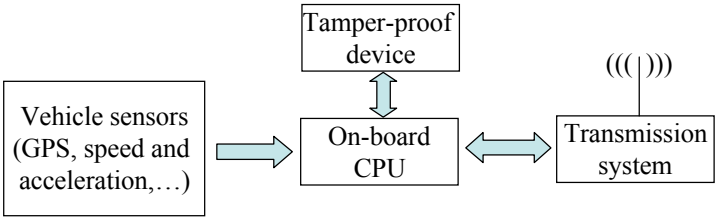
- Sender authentication
- Verification of data consistency
- Availability
- Non-repudiation
- Privacy
- Real-time constraints

Security Architecture



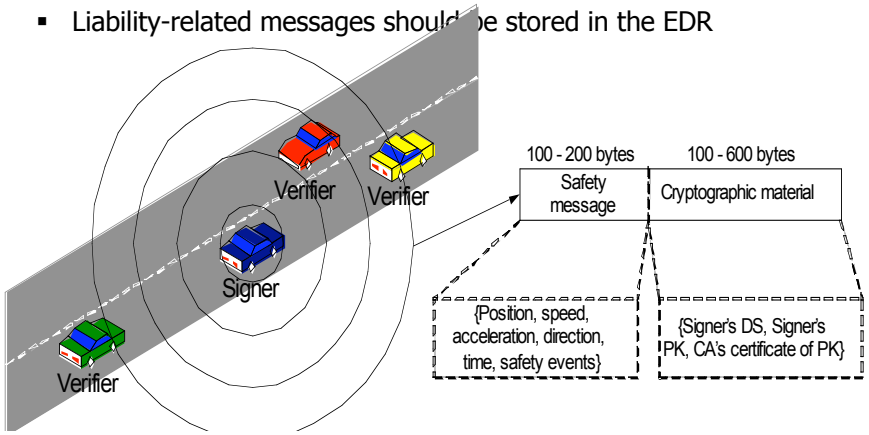
Tamper-proof device

- 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

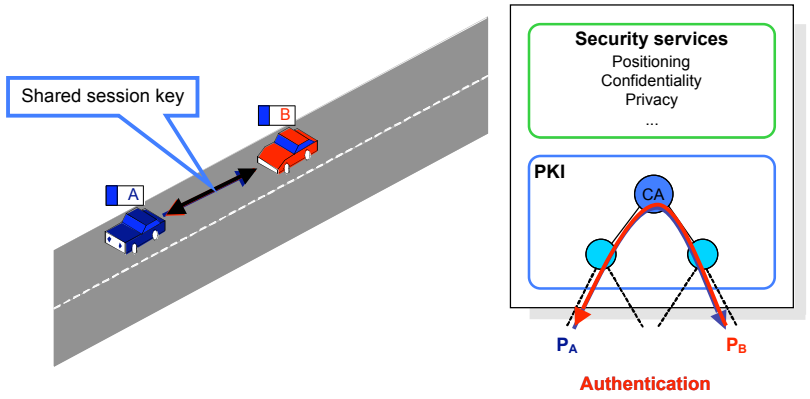


Digital signatures

- 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



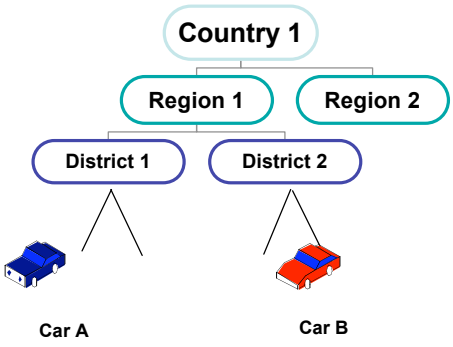
VPKI (Vehicular PKI)



- Each vehicle carries in its **T**amper-**P**roof **D**evice (**TPD**):
  - A unique and certified identity: **E**lectronic **L**icense **P**late (**ELP**)
  - A set of certified anonymous public/private key pairs
- Mutual authentication can be done without involving a server
- Authorities (national or regional) are cross-certified

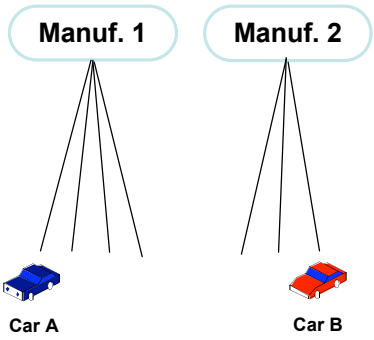
The CA hierarchy: two options

1. Governmental Transportation Authorities



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

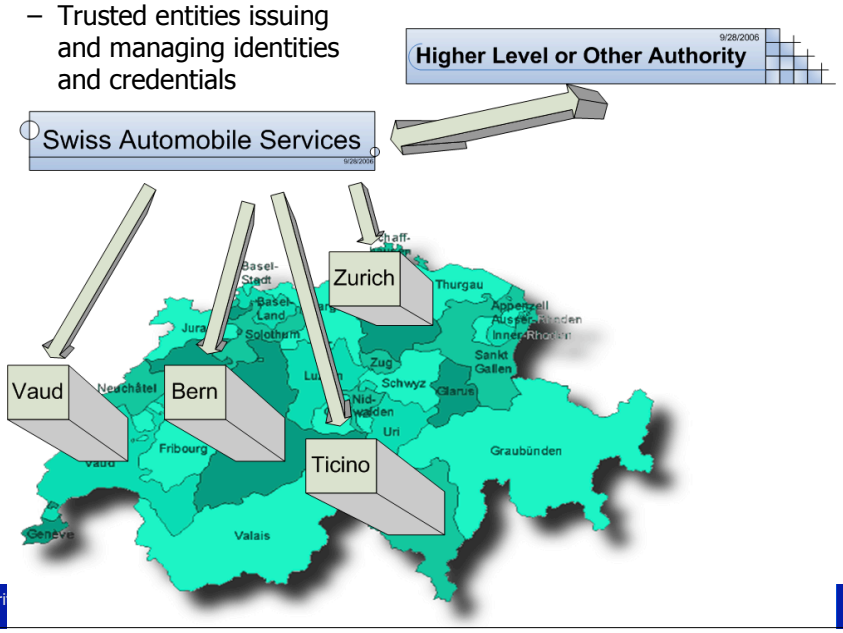
2. Manufacturers



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

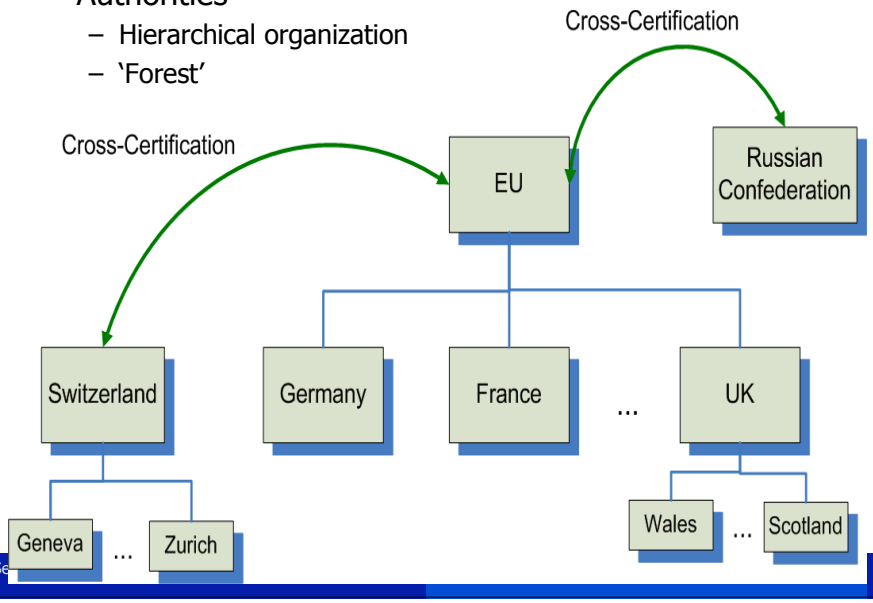
Secure VC Building Blocks

- Authorities
  - Trusted entities issuing and managing identities and credentials



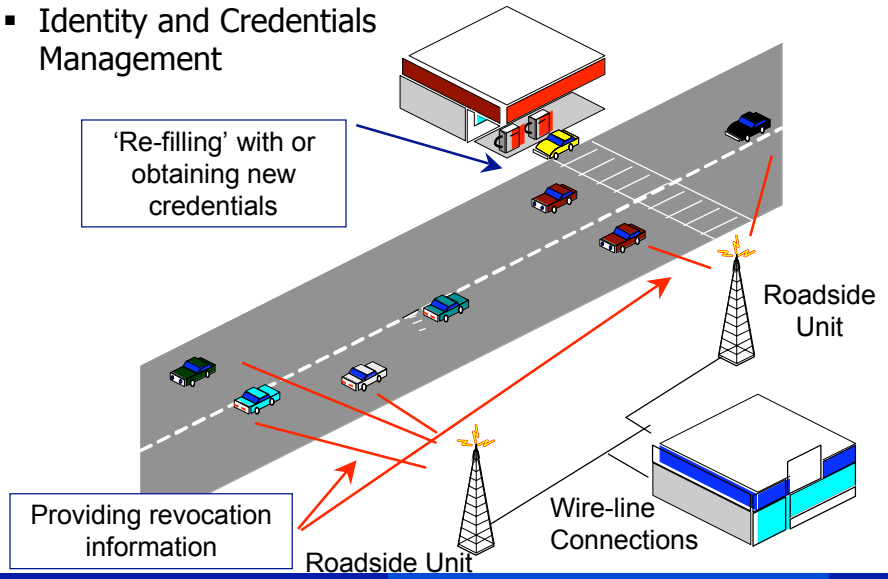
Secure VC Building Blocks

- Authorities
  - Hierarchical organization
  - 'Forest'



Secure VC Building Blocks (cont'd)

- Identity and Credentials Management



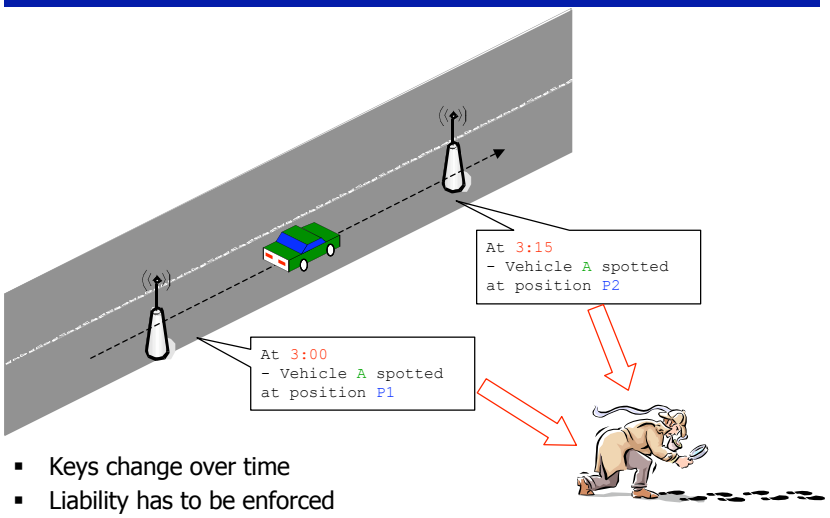
Anonymous keys

- 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

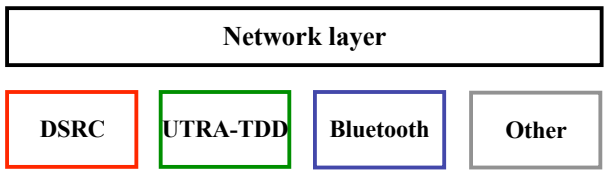
What about privacy: how to avoid the Big Brother syndrome?



- 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

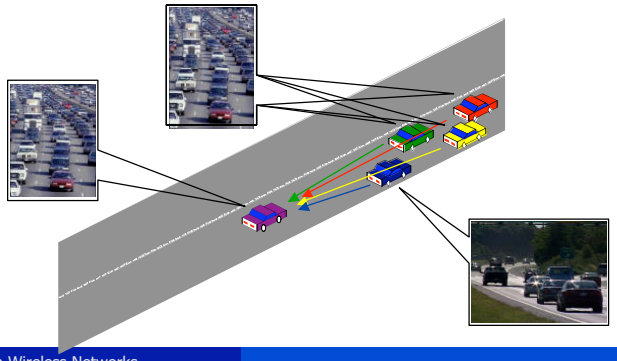
- Vehicles will probably have several wireless technologies onboard
- In most of them, several channels can be used
- To thwart DoS, vehicles can switch channels or communication technologies



- 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 there 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

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

Upcoming networks vs. mechanisms

Upcoming wireless networks \ Rule enforcement mechanisms	Naming and addressing	Security associations	Securing neighbor discovery	Secure routing	Privacy	Enforcing fair MAC	Enforcing PKT FWing	Discouraging greedy op.	Behavior enforc.
Small operators, community networks	X	X			X	X		X	X
Cellular operators in shared spectrum	X				X	X		X	X
Mesh networks	X	X	X	X	X	X		X	?
Hybrid ad hoc networks	X	X	X	X	X	X	X	X	X
Self-organized ad hoc networks	X	X	X	X	X	X	X		X
Vehicular networks	X	X	X	X	X	?	?	?	?
Sensor networks	X	X	X	X	X	?		X	?
RFID networks	X	?	X		X				?

Security ↔ Cooperation

Security and Cooperation in Wireless Networks

http://secowinet.epfl.ch

Chapter 3: Trust assumptions and adversary models

Trust

- the trust model of current wireless networks is rather simple
  - subscriber – service provider model
  - subscribers trust the service provider for providing the service, charging correctly, and not misusing transactional data
  - service providers usually do not trust subscribers, and use security measures to prevent or detect fraud
- in the upcoming wireless networks the trust model will be much more complex
  - entities play multiple roles (users can become service providers)
  - number of service providers will dramatically increase
  - user – service provider relationships will become transient
  - how to build up trust in such a volatile and dynamic environment?
- yet, trust is absolutely fundamental for the future of wireless networks
  - pervasiveness of these technologies means that all of us must rely on them in our everyday life!

Reasons to trust organizations and individuals

- Moral values
  - Culture + education, fear of bad reputation
- Experience about a given party
  - Based on previous interactions

} Will lose relevance ?

- Rule enforcement organization
  - Police or spectrum regulator

→ Scalability challenge

- Usual behavior
  - Based on statistical observation

→ Can be misleading

- Rule enforcement mechanisms
  - Prevent malicious behavior (by appropriate security mechanisms) and encourage cooperative behavior

Trust vs. security and cooperation

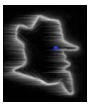
- trust preexists security
  - all security mechanisms require some level of trust in various components of the system
  - security mechanisms can help to *transfer* trust in one component to trust in another component, but they cannot create trust by themselves
- cooperation reinforces trust
  - trust is about the ability to *predict* the behavior of another party
  - cooperation (i.e., adherence to certain rules for the benefit of the entire system) makes predictions more reliable

Malice and selfishness

- malice
  - willingness to do harm no matter what
- selfishness
  - overuse of common resources (network, radio spectrum, etc.) for one's own benefit
- traditionally, security is concerned only with malice
- but in the future, **malice and selfishness must be considered jointly** if we want to seriously protect wireless networks

Who is malicious? Who is selfish?

Harm everyone: viruses,…

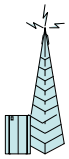


Big brother

Selective harm: DoS,…

Spammer

Cyber-gangster: phishing attacks, trojan horses,…



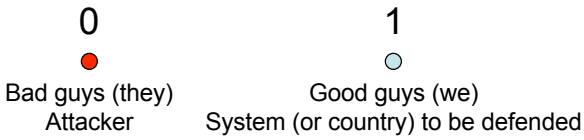
Greedy operator

Selfish mobile station

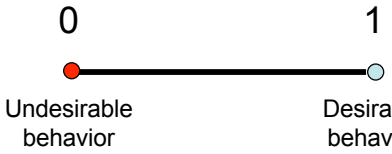
There is no watertight boundary between malice and selfishness
➔ Both security **and** game theory approaches can be useful

From discrete to continuous

Warfare-inspired Manichaeism:



The more subtle case of commercial applications:



- Security often needs incentives
- Incentives usually must be secured

Definitions

- A **misbehavior** consists in deliberately departing from the prescribed behavior in order to reach a specific goal
- A misbehavior is **selfish** (or **greedy**, or **strategic**) if it aims at obtaining an advantage that can be quantitatively expressed in the units (bitrate, joules, or coverage) or in a related incentive system (e.g., micropayments); any other misbehavior is considered to be **malicious**.

Text Book structure