Mobile Device and Wireless Network Security

Vehicular Network Security

VANET Applications;

Security and Privacy Requirements;

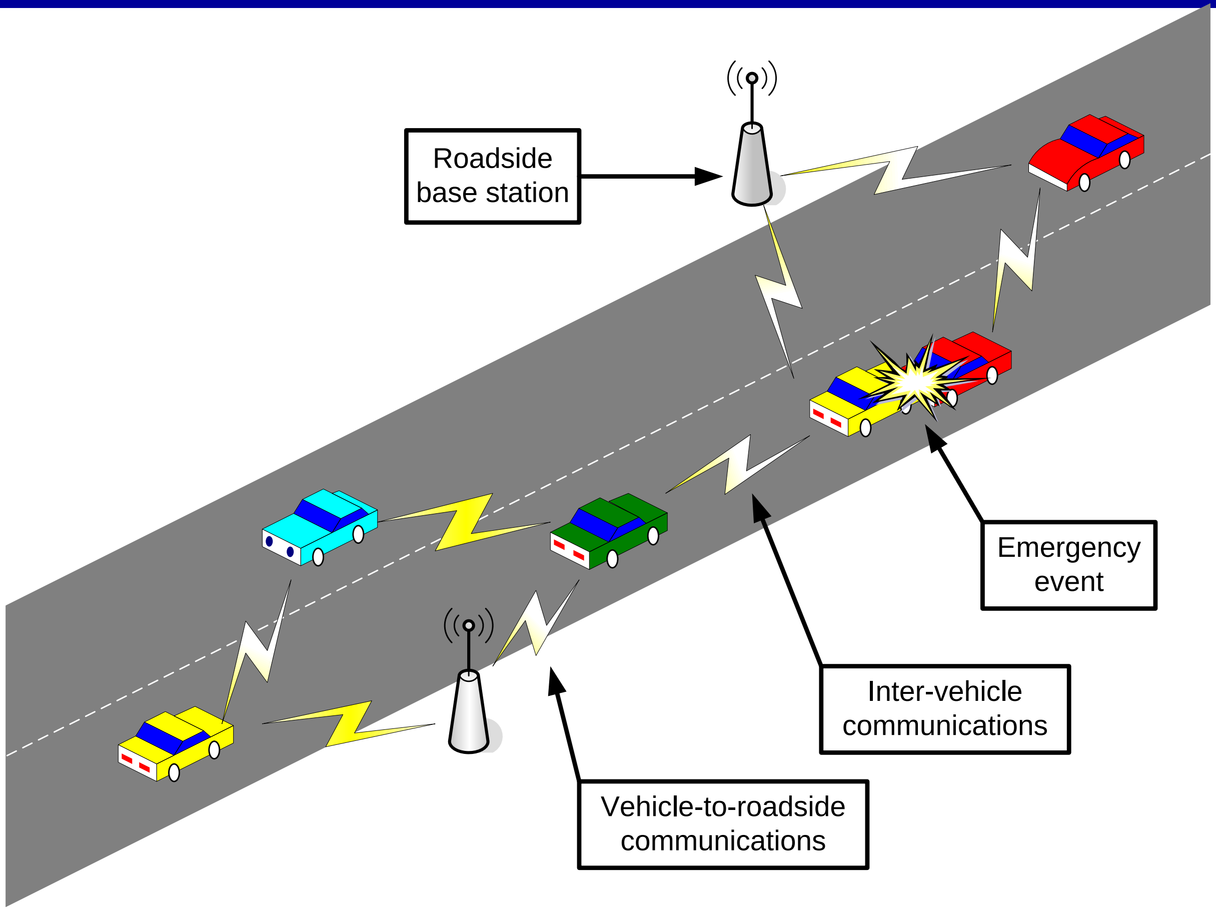
TACK

Di Ma

Outline

- VNAET and its Applications
- VANET security and privacy requirements
- TACK

What is a VANET (Vehicular Ad hoc NETwork)?

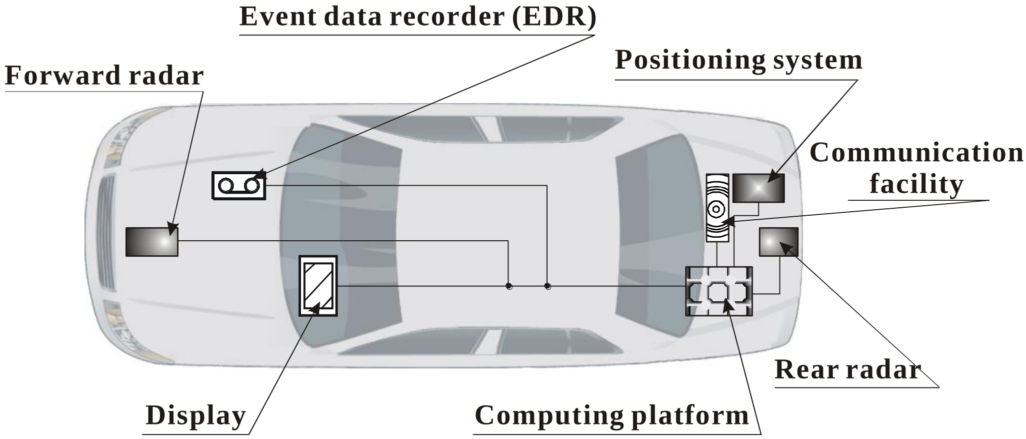

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

- Vehicle to Vehicle communication (V2V), Vehicle to Infrastructure communication (V2I), Vehicle to Pedestrian communication (V2P)

The Enabling Standard: DSRC / IEEE 802.11p

Dedicated Short Range Communications

- Car-Car communications at 5.9Ghz (FCC)
- Derived from 802.11a
- three types of channels:
  - Vehicle-Vehicle *service*
  - a Vehicle-Gateway *service*
  - a *control broadcast* channel
- Ad hoc mode and infrastructure mode
- 802.11p: IEEE Task Group for Car-Car communications



V2V Applications

- Safe Navigation
- Efficient Navigation/Commuting (ITS)
- Urban Sensing
- Location Relevant Content Distribution
- Advertising
- Commerce
- Entertainment/Games

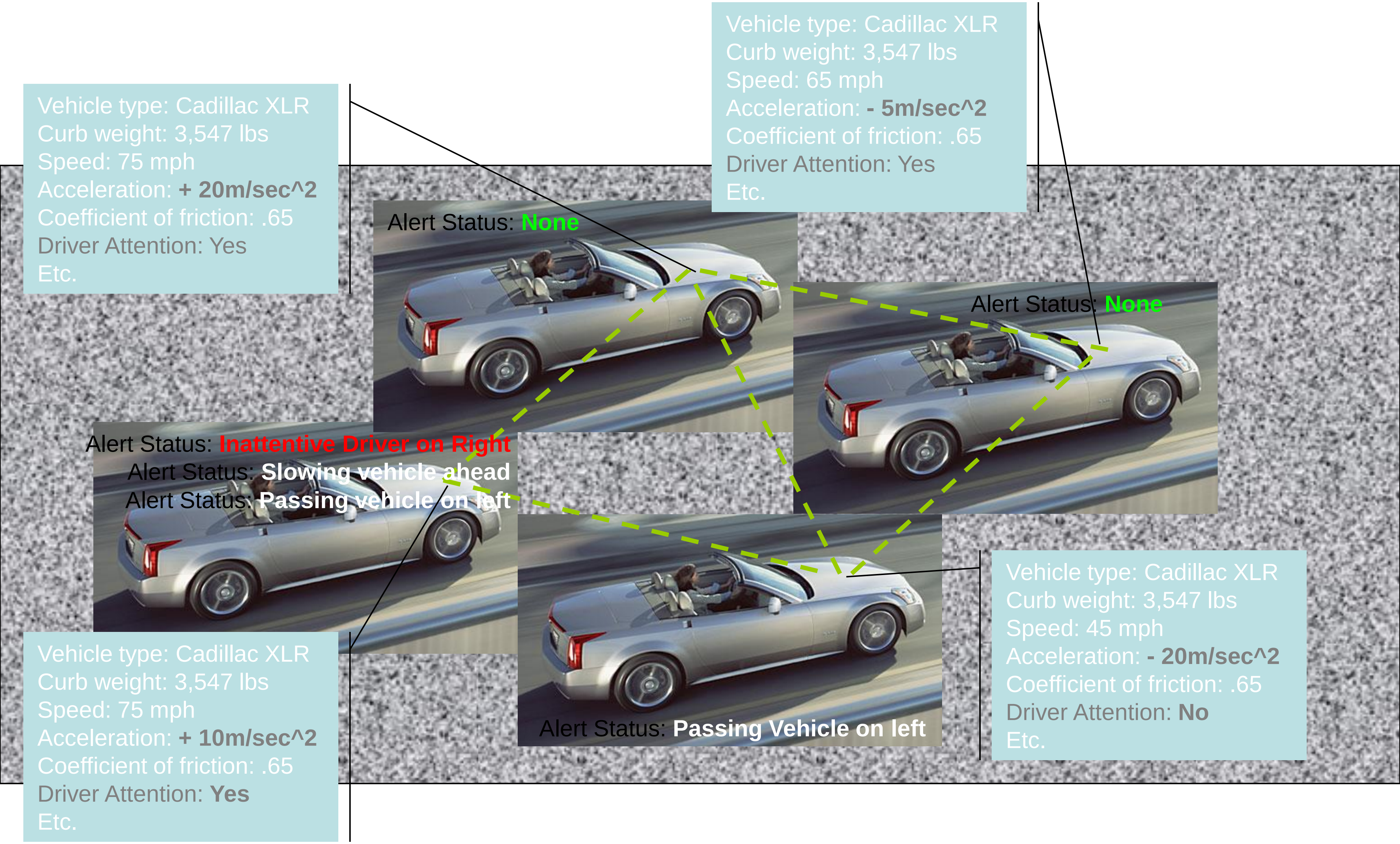
Vehicular communications: why?

- Combat the awful side-effects of road traffic
  - In the US and Europe, 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 (or mitigated) by providing appropriate ***information*** to the driver or to the vehicle

V2V Applications

- Safe navigation:
  - Forward Collision Warning
  - Intersection Collision Warning
  - Weather and road hazard alerts
    - “Ice on bridge”, “Congestion ahead”,…

Car to Car communications for Safe Driving



Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 75 mph
Acceleration: **+ 20m/sec^2**
Coefficient of friction: .65
Driver Attention: Yes
Etc.

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 65 mph
Acceleration: **- 5m/sec^2**
Coefficient of friction: .65
Driver Attention: Yes
Etc.

Alert Status: **None**

Alert Status: **None**

Alert Status: **Inattentive Driver on Right**
Alert Status: **Slowing vehicle ahead**
Alert Status: **Passing vehicle on left**

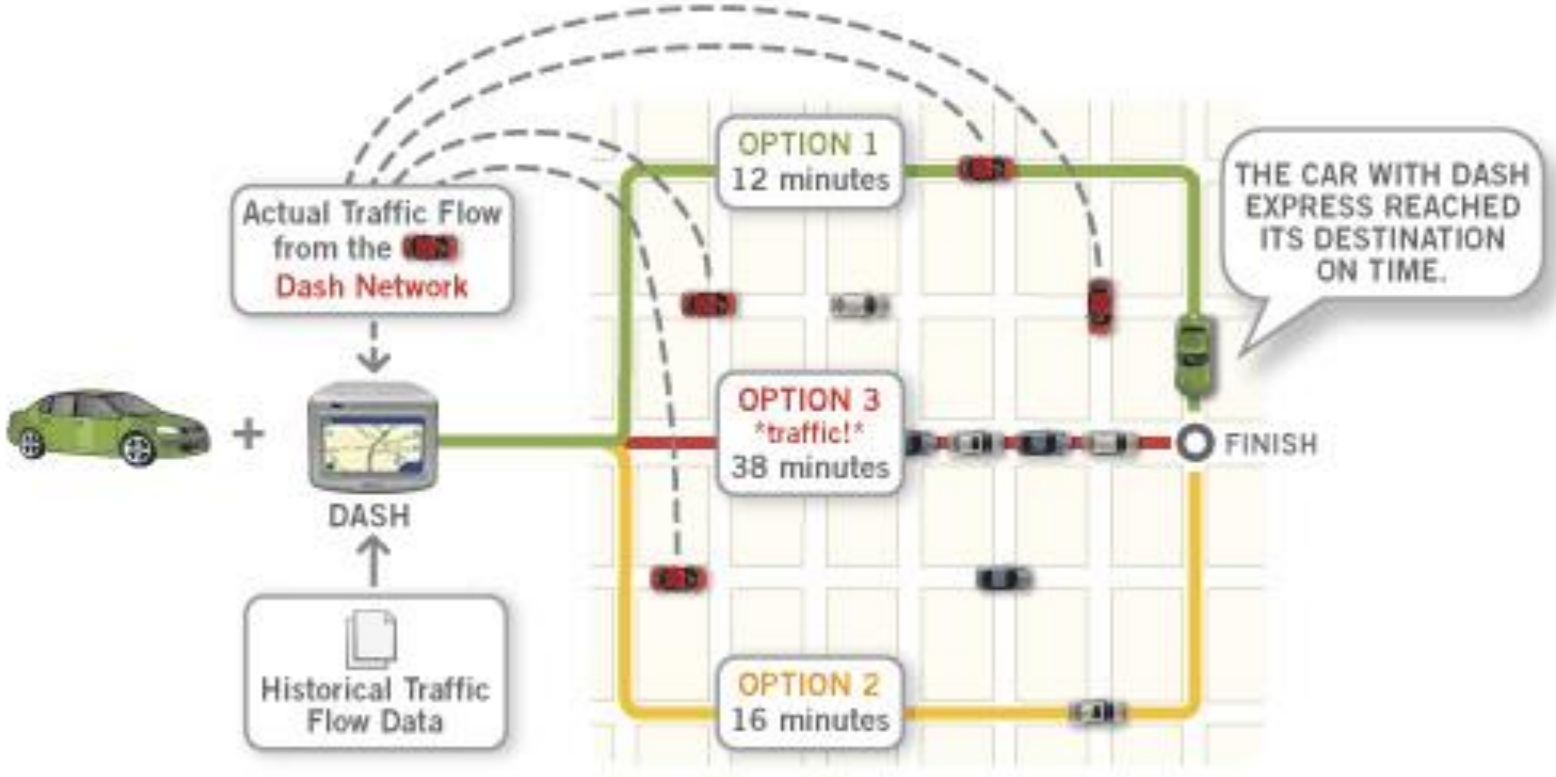
Alert Status: **Passing Vehicle on left**

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 45 mph
Acceleration: **- 20m/sec^2**
Coefficient of friction: .65
Driver Attention: **No**
Etc.

Vehicle type: Cadillac XLR
Curb weight: 3,547 lbs
Speed: 75 mph
Acceleration: **+ 10m/sec^2**
Coefficient of friction: .65
Driver Attention: **Yes**
Etc.

V2V Applications (cont)

- Efficient Navigation
  - GPS Based Navigators
  - Dash Express (Internet-connected GPS):



Incentive to use Ad Hoc vehicular networks

- **Can cover very large area**
- Nodes are not energy-starved
- Infrastructure-less setup

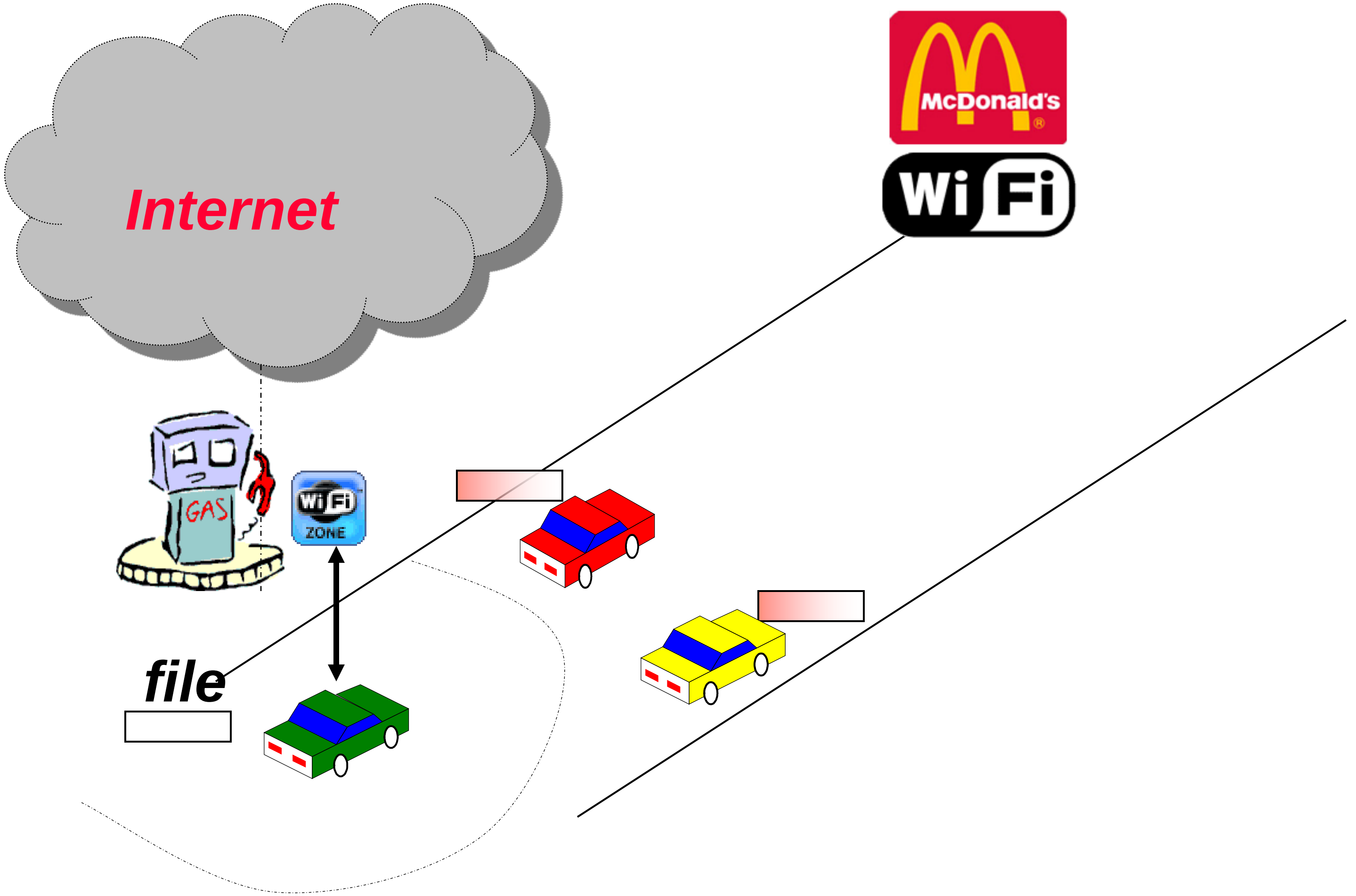
- Vehicular network => *Opportunistic* Ad Hoc Network
  - Access to Internet readily available, but..
  - opportunistically "bypass it" with "ad hoc" if too costly or inadequate
  - Routes are built dynamically
  - Contacts between nodes are viewed as an opportunity to move data closer to the destination

V2V Applications (cont)

- Location related content delivery/sharing:
  - – Traffic information
  - – Local attractions
  - – Tourist information, etc

You are driving to Vegas
You hear of this new show on the radio
Video preview on the web (10MB)

One option: Highway Infostation download



Incentive for opportunistic “ad hoc networking”

Problems:

Stopping at gas station for full download is a nuisance

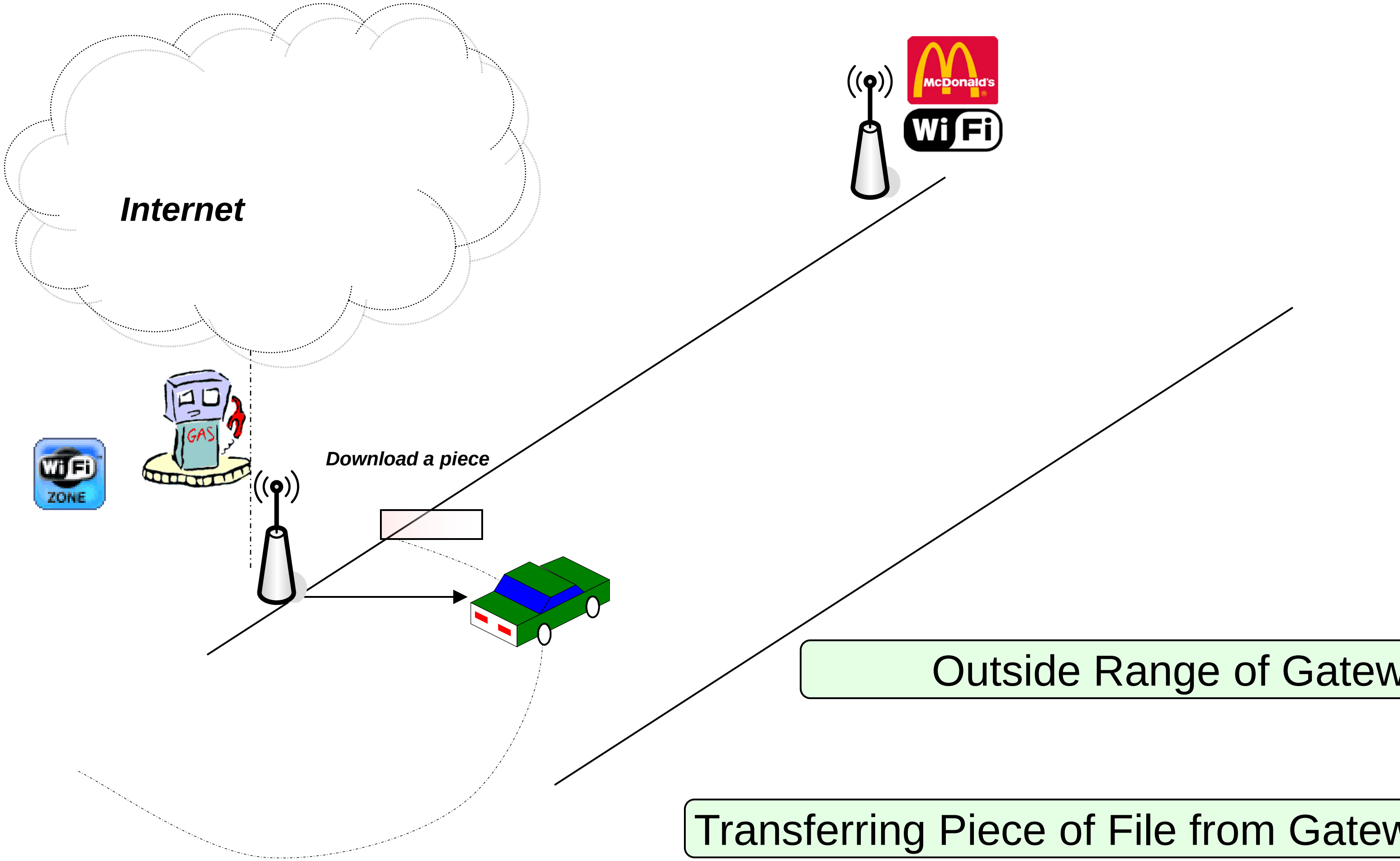
Downloading from GPRS/3G too slow and quite expensive

3G broadcast services only for TV

Observation: many other drivers are interested in download sharing

Solution: Co-operative P2P Downloading via Car-Torrent (like Bit Torrent in the Internet)

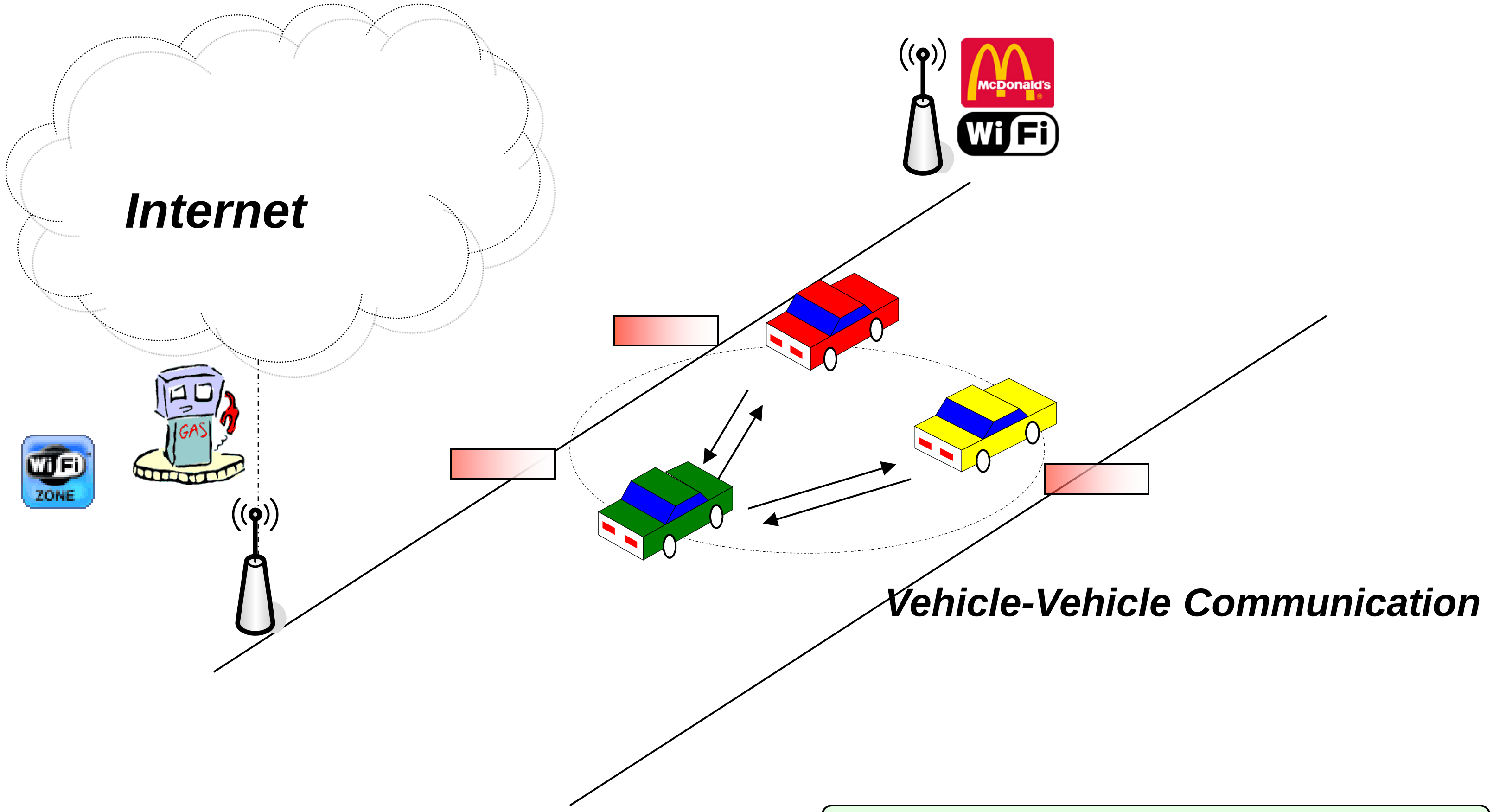
CarTorrent: Basic Idea



Outside Range of Gateway

Transferring Piece of File from Gateway

Co-operative Download: Car Torrent

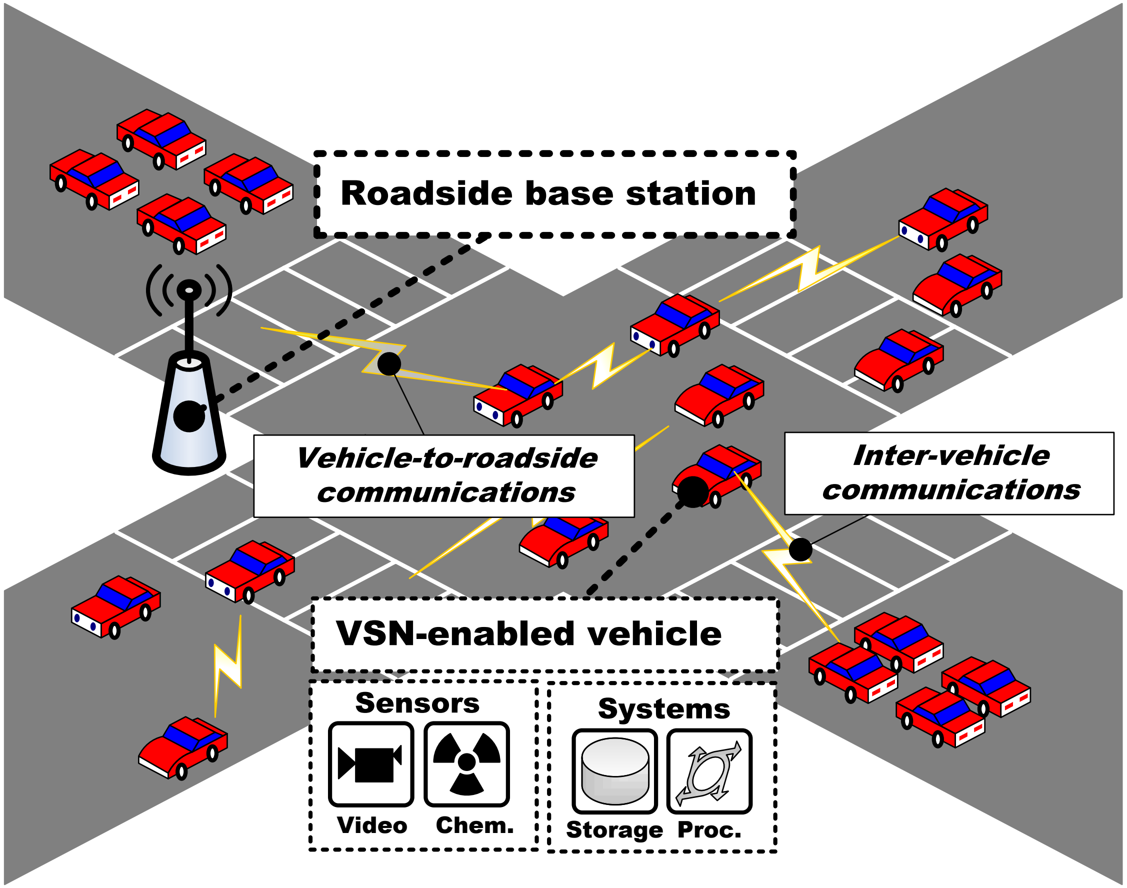


Exchanging Pieces of File Later

V2V Applications (cont)

- Environment sensing/monitoring:
  - Traffic monitoring
  - Pollution probing
  - Pavement conditions (e.g., potholes)
  - Urban surveillance (e.g., disturbance)
  - Witnessing of accidents/crimes

Vehicular Sensor Network

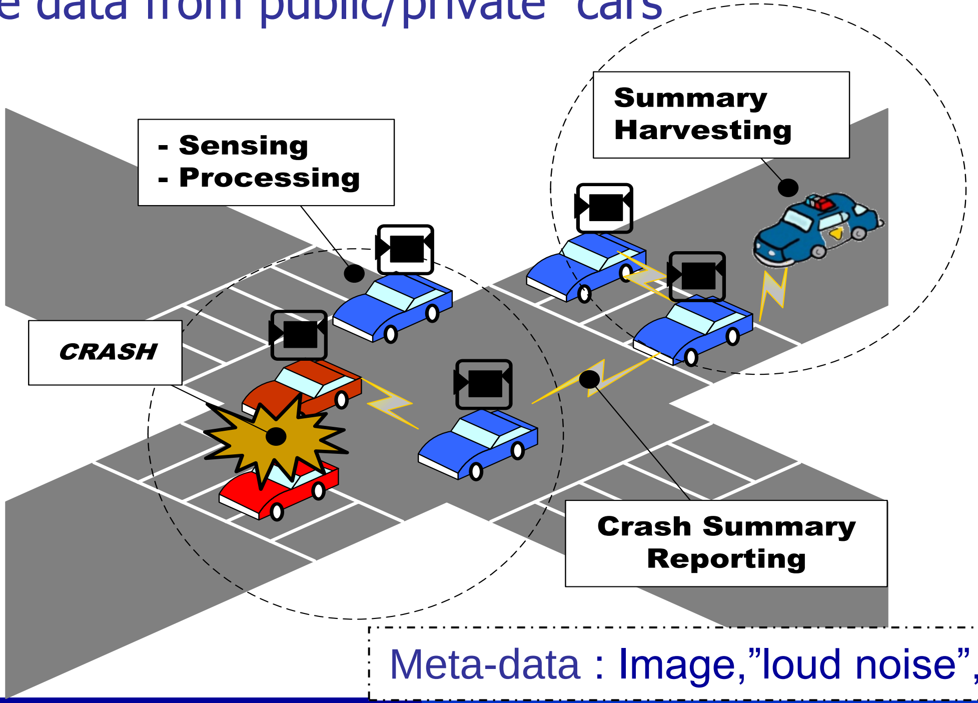


Vehicular Sensor Applications

- Environment
  - Traffic density/congestion monitoring
  - Urban pollution monitoring
  - Pavement, visibility conditions
- Civic and Homeland security
  - Bomb threat alerts
  - Terrorist alerts
  - Forensic accident or crime site investigations

Accident Scenario: storage and retrieval

- Public/Private Cars (eg, busses, taxicabs, police, commuters, etc):
  - Continuously **collect** images on the street (store data locally)
  - Process the data and **detect** an event
  - **Classify the event as Meta-data** (Type, Option, Loc, time,Vehicle ID)
  - **Distribute Metadata to neighbors probabilistically (ie, "gossip")**
- Police retrieve data from public/private cars



Meta-data : Image,"loud noise",(10,10), 3:15PM, V1710

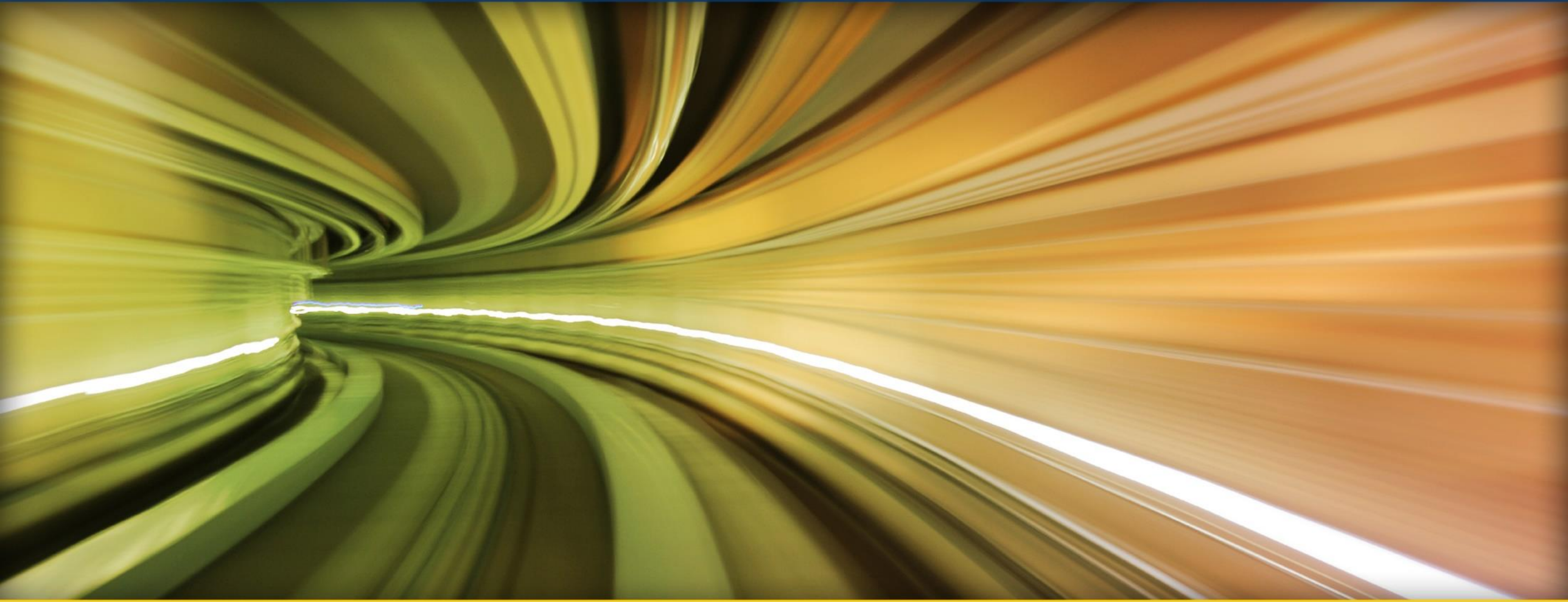
V2V Applications (cont)

Advertising (AdTorrent):

- Access Points push Ads to passing cars
- Advertisement: multimedia file (data, image, video)
- Movie trailer; restaurant ad; club; local merchant..

Commerce (FleaNet):

- virtual market (bazaar) concept in VANET
- A mix of mobile and stationary users buy/sell goods using the vehicular network



The Mobility Transformation Center (MTC)

A public/private partnership for connected and automated vehicle R&D

Founding Leadership Circle Members

Ford

GM

TOYOTA

HONDA

DELPHI

BOSCH

NISSAN

ECONOLITE Group, Inc.

QUALCOMM®

DENSO

verizon

ITERIS®

M

MOBILITY TRANSFORMATION CENTER

UNIVERSITY OF MICHIGAN

With Support From

MDOT
Michigan Department of Transportation

PURE MICHIGAN®
Michigan Economic Development Corporation

StateFarm®

xerox®

Automated and Connected Vehicles

- A very exciting topic with many recent developments
  - Google—possible plan to implement “robo-taxi”
  - GM: Super Cruise
  - Mercedes: Stop&Go Pilot, Fully autonomous vehicles by 2020
  - Volvo: Self-parking valet, pedestrian detection and braking
  - Honda: intersection safety by V2P/V2M
  - Nissan: Fully autonomous vehicles by 2020
  - Audi: a large suite of safety systems to be commercialized

Transformational Goals

- will demonstrate a mobility system that addresses order-of-magnitude advancements in multiple metrics

What is MTC – three pillar projects

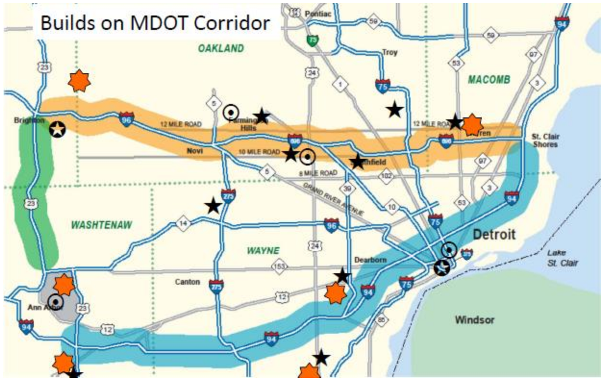
1. Expand the Safety Pilot model deployment from 3,000 vehicles to 9,000 vehicles, and from the Northeast quadrant of Ann Arbor to the entire city, including the surrounding freeways;
2. Working with MDOT to connect the freeway systems in Southeast Michigan, and recruit at least 30,000 corporate and government owned fleets, including heavy trucks, to test selected V2V and V2V functions; and
3. To design, build and operate an integrated network of 2,000 connected, coordinated, driverless, and shared vehicles serving 10% of the trips in Ann Arbor.

MTC @ University of Michigan

- Major research themes
  - Technology
  - Risk management
  - Customer value
  - Societal impact

Source: U.S.DOT

Photo provided by UM Architecture, E



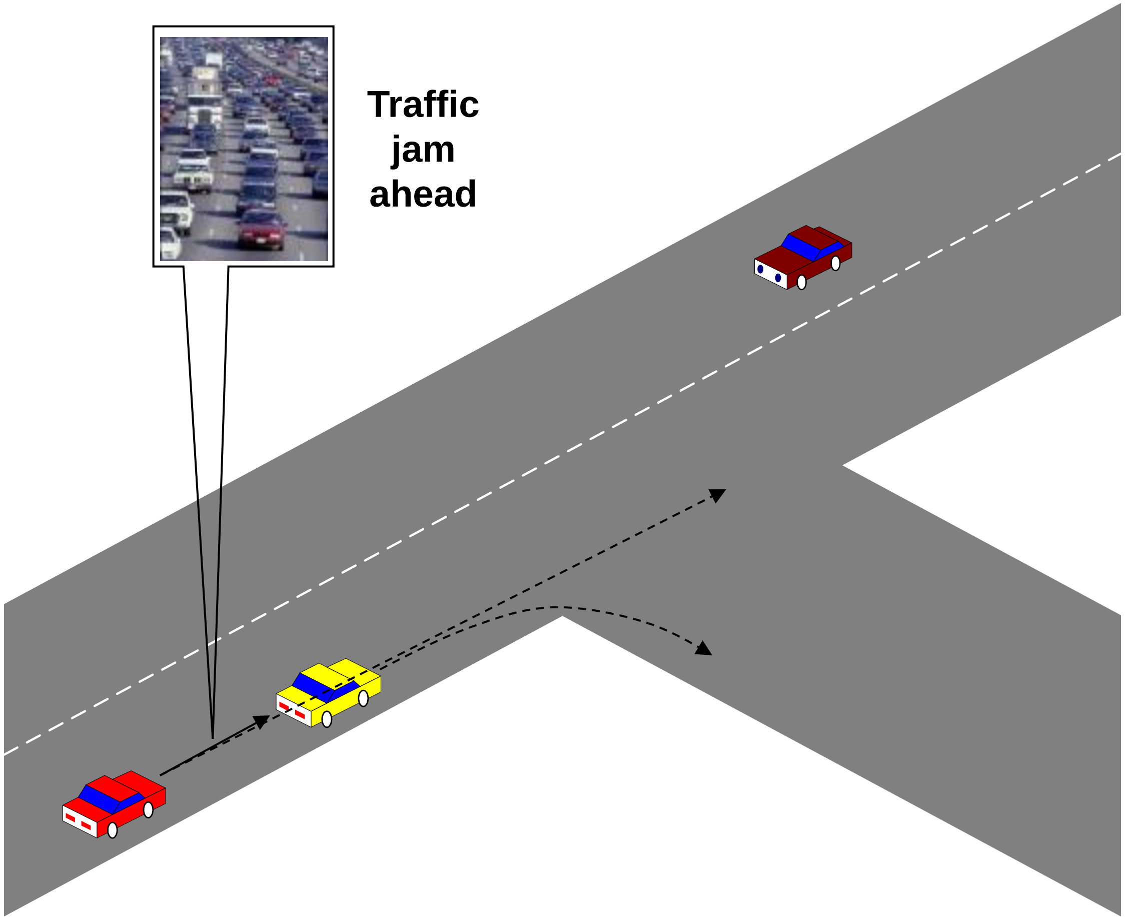
Outline

- VNAET and its Applications
- VANET security and privacy requirements
- TACK

Why is VANET security important?

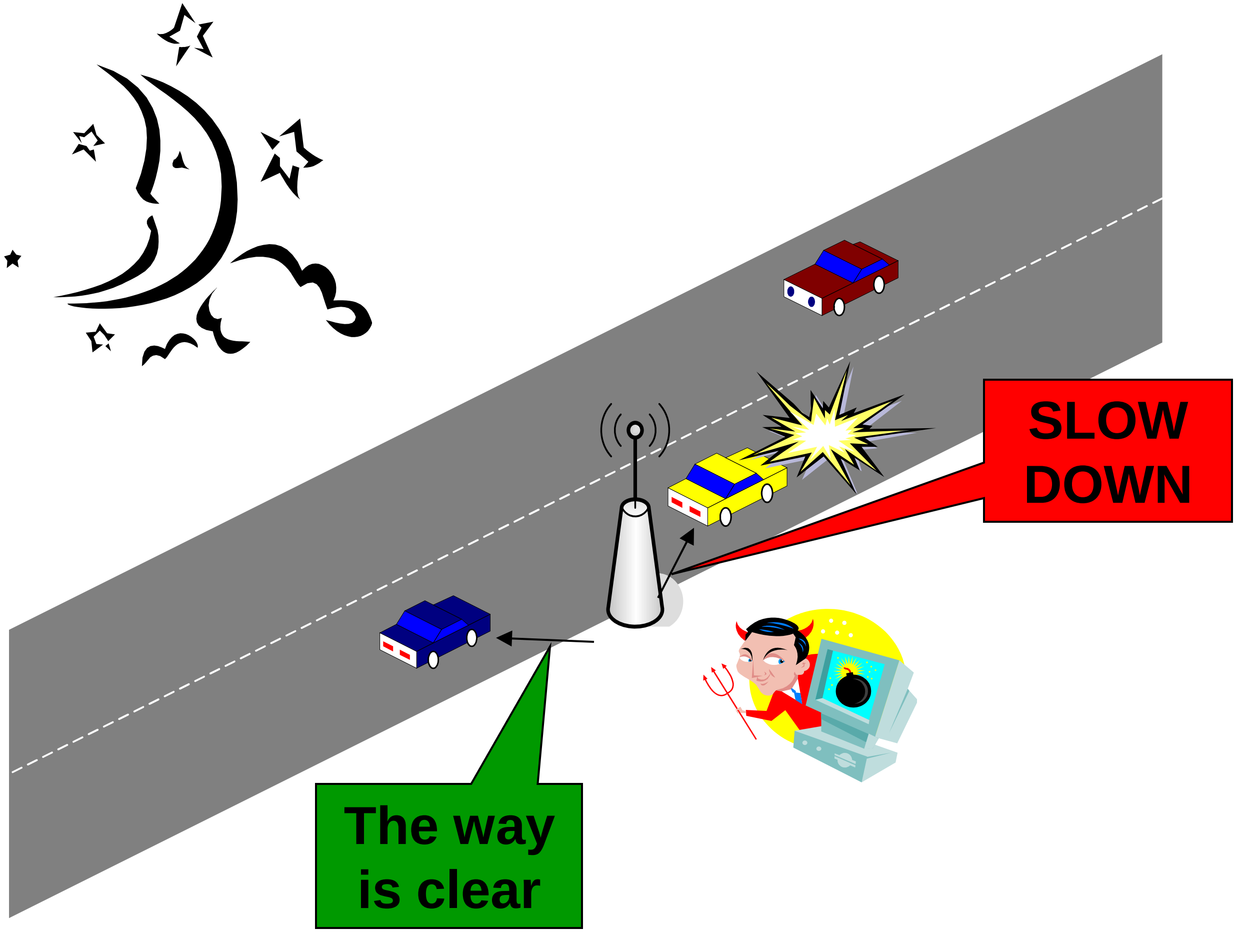
- Large projects have explored vehicular communications: Fleetnet, PATH (UC Berkeley),…
- No solution can be deployed if not properly secured
- The problem is non-trivial
  - Specific requirements (speed, real-time constraints)
  - Contradictory expectations
- Industry front: standards are still under 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 good papers

Attack 1 : Bogus traffic information



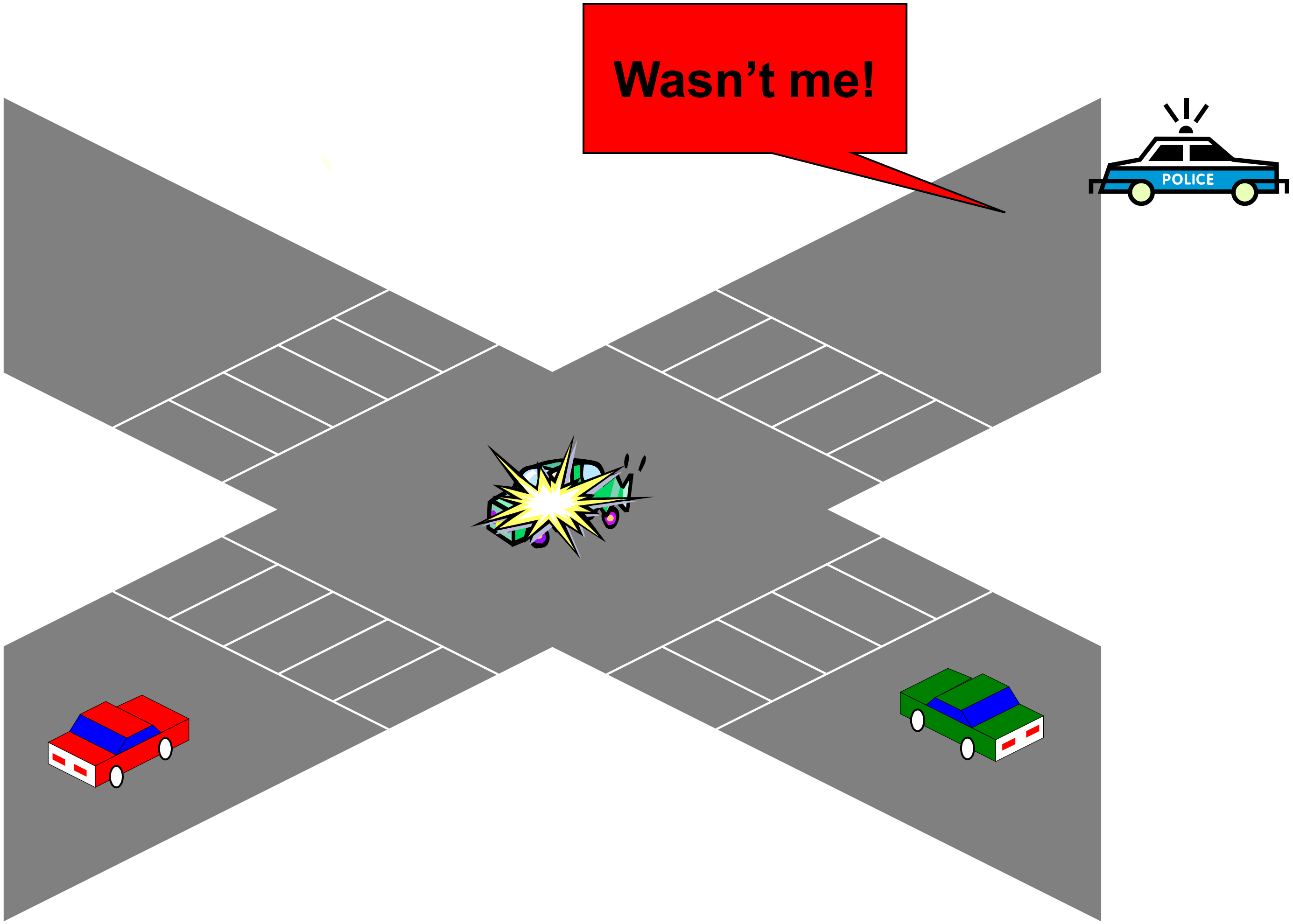
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



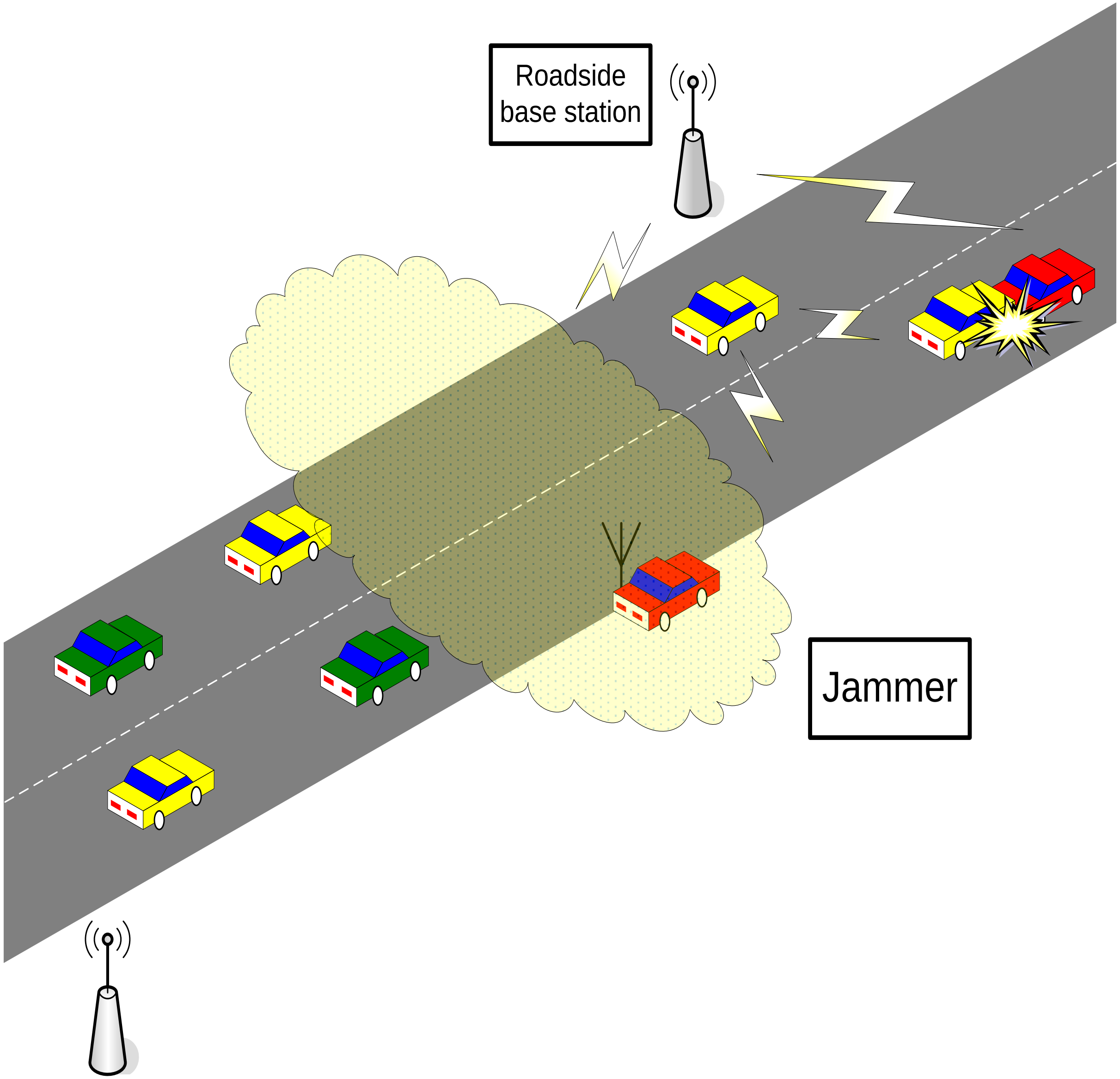
- Attacker: insider, malicious, active

Attack 3: Cheating with identity, speed, or position

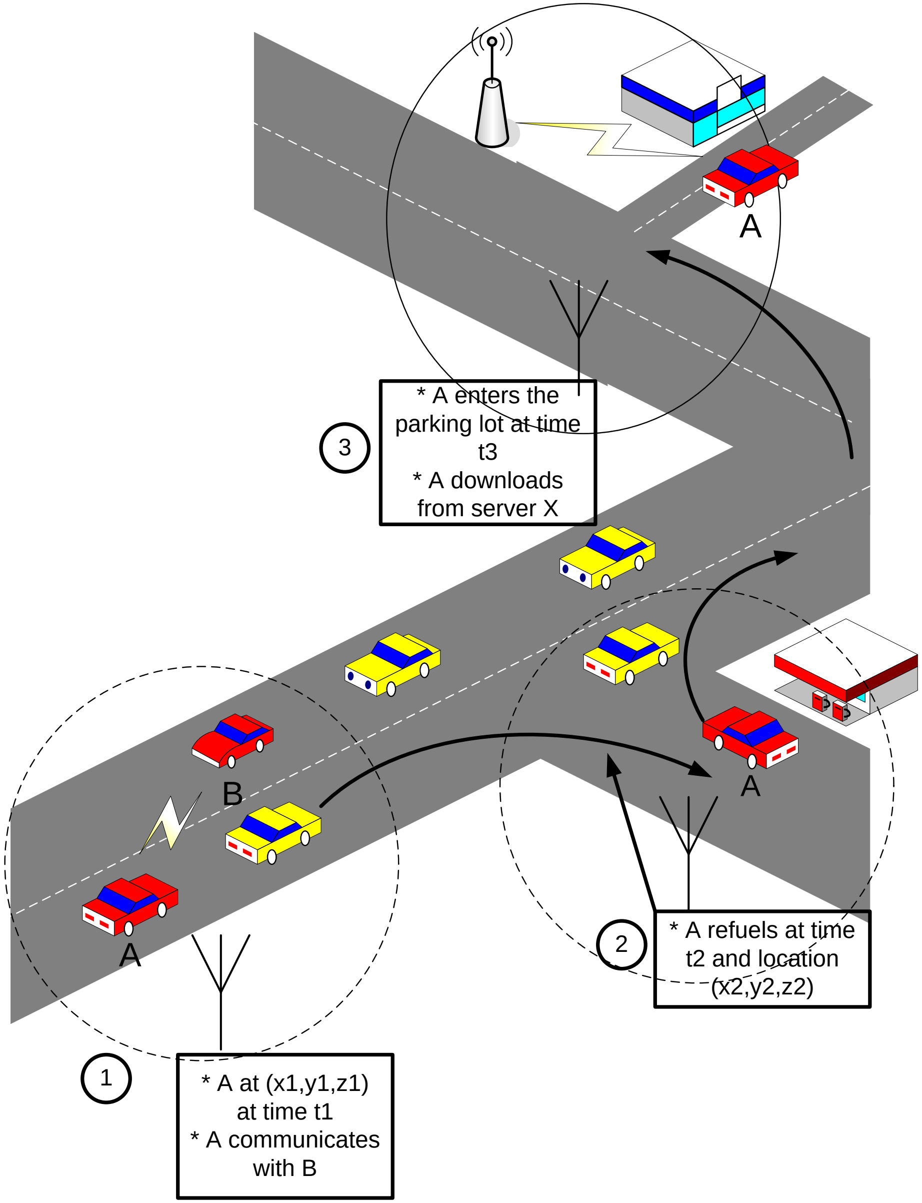


- Attacker: insider, rational, active

Attack 4: Jamming



Attack 5: Tracking



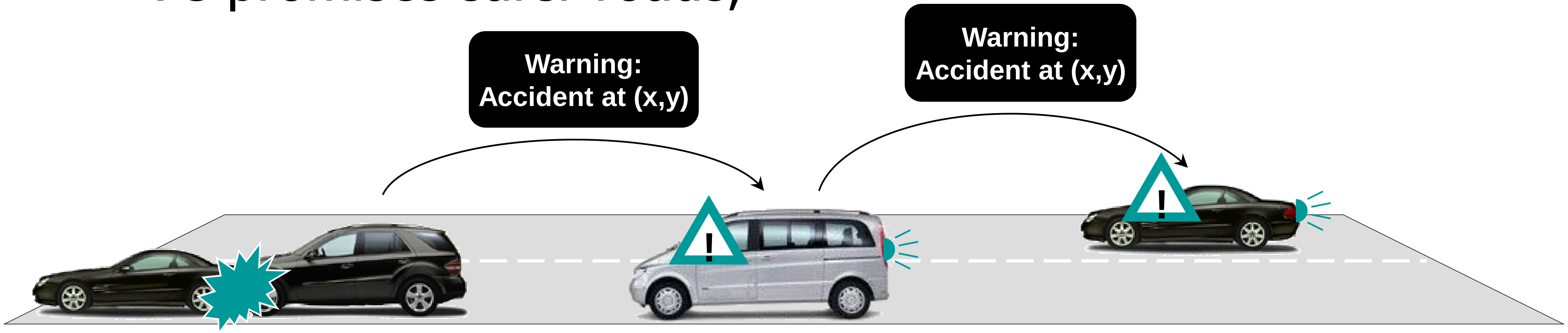
* A enters the parking lot at time t3
* A downloads from server X

* A refuels at time t2 and location (x2,y2,z2)

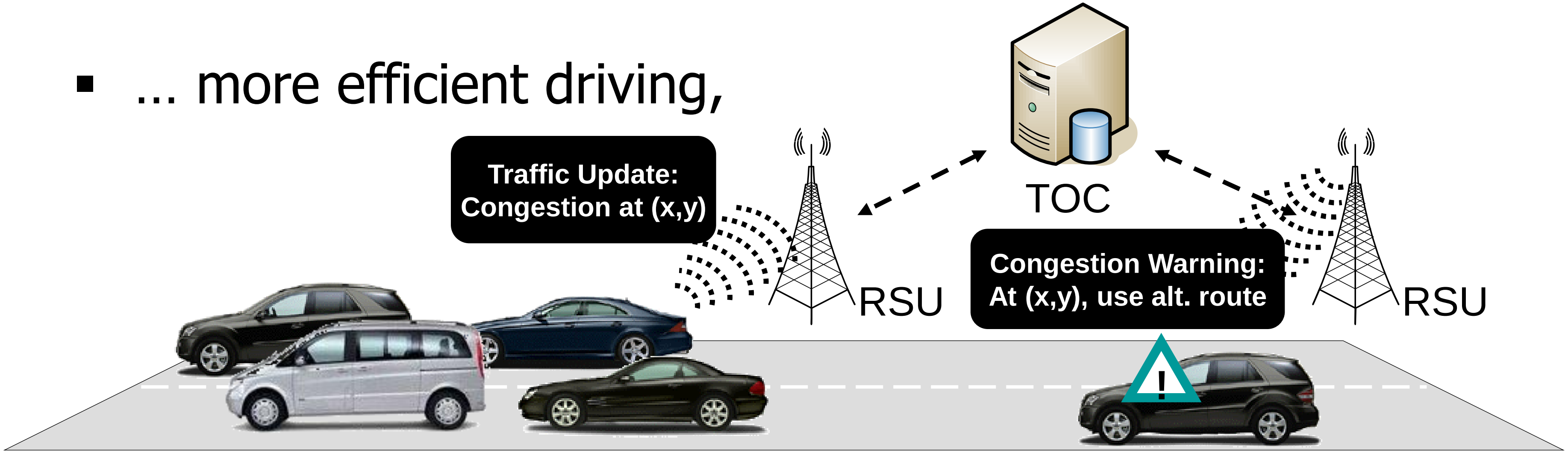
* A at (x1,y1,z1) at time t1
* A communicates with B

Vehicle Communication (VC)

- VC promises safer roads,

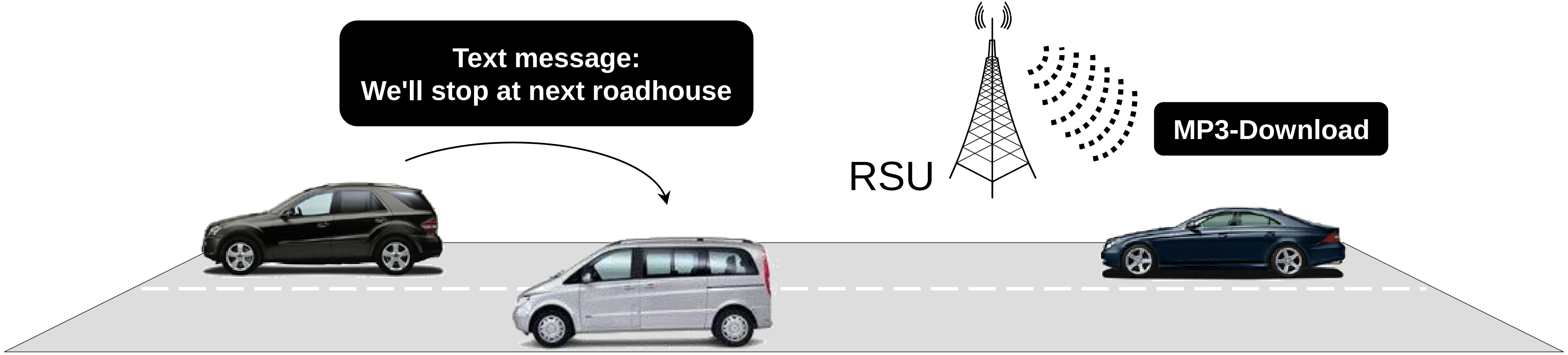


- … more efficient driving,



Vehicle Communication (VC)

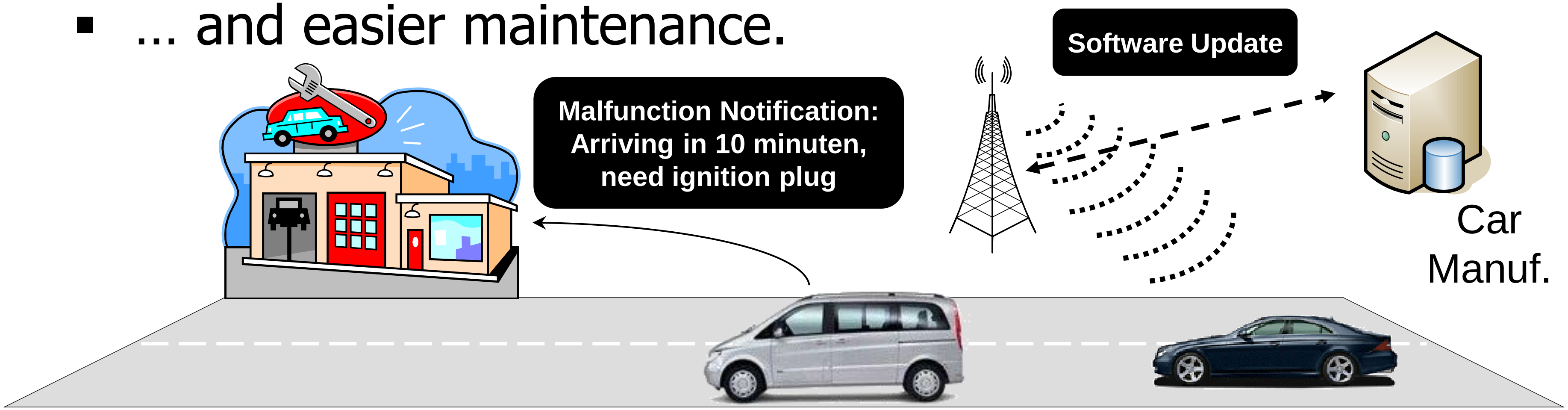
- … more fun,



Text message:
We'll stop at next roadhouse

MP3-Download

- … and easier maintenance.

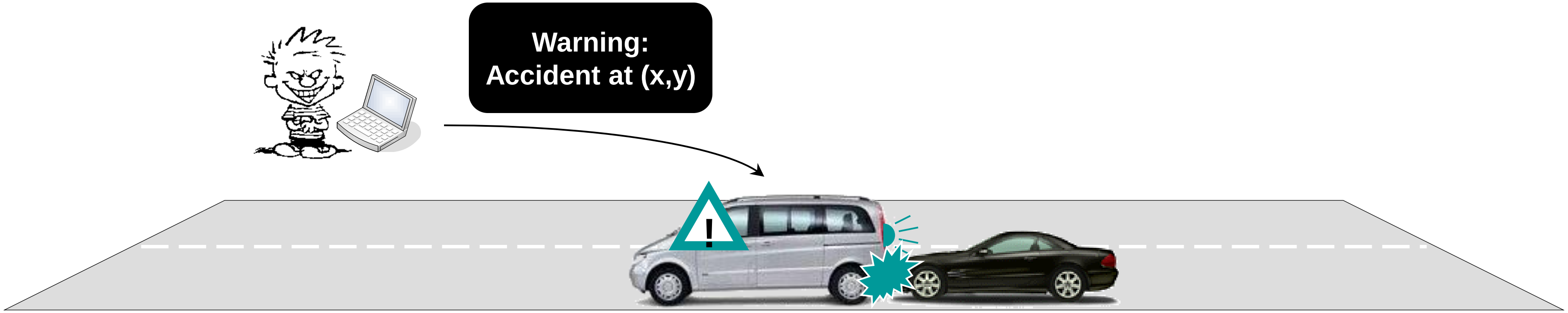


Malfunction Notification:
Arriving in 10 minuten,
need ignition plug

Software Update

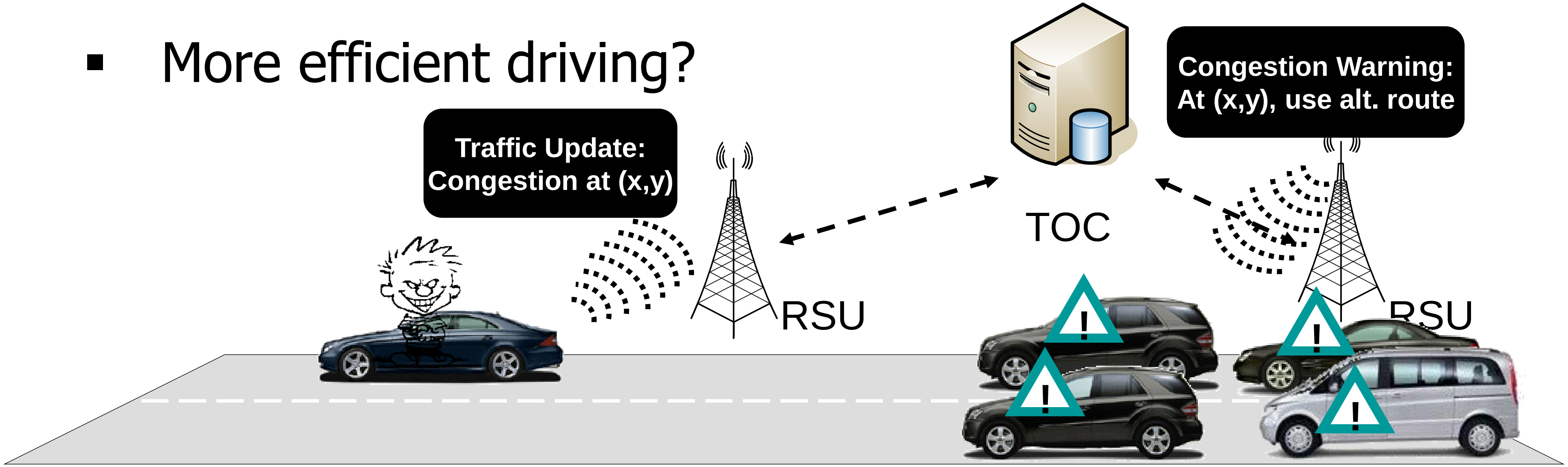
Security and Privacy???

- Safer roads?



Warning:
Accident at (x,y)

- More efficient driving?

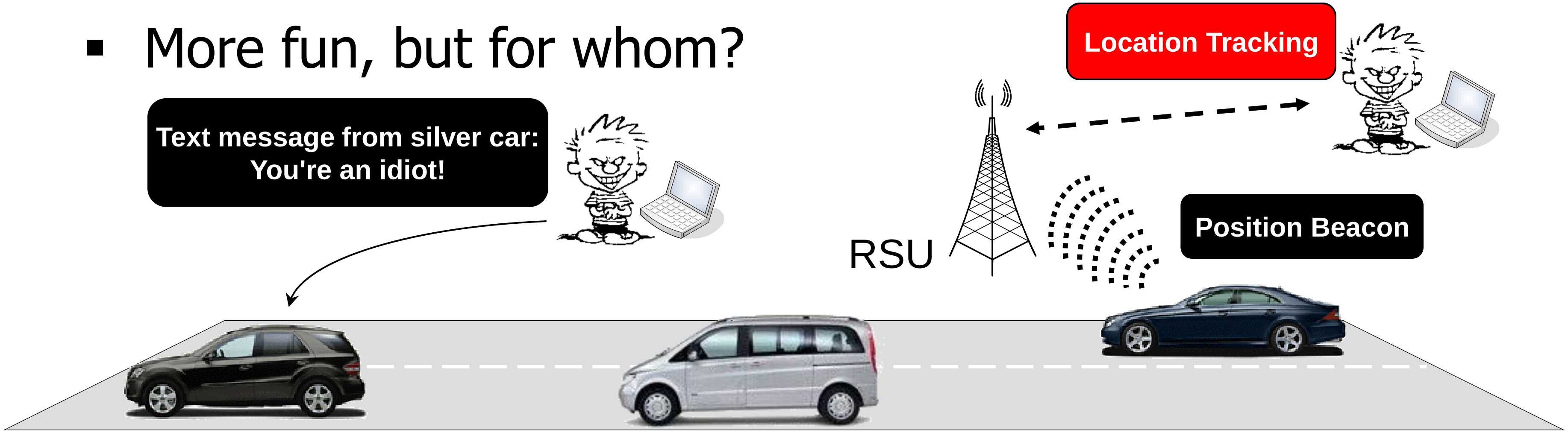


Traffic Update:
Congestion at (x,y)

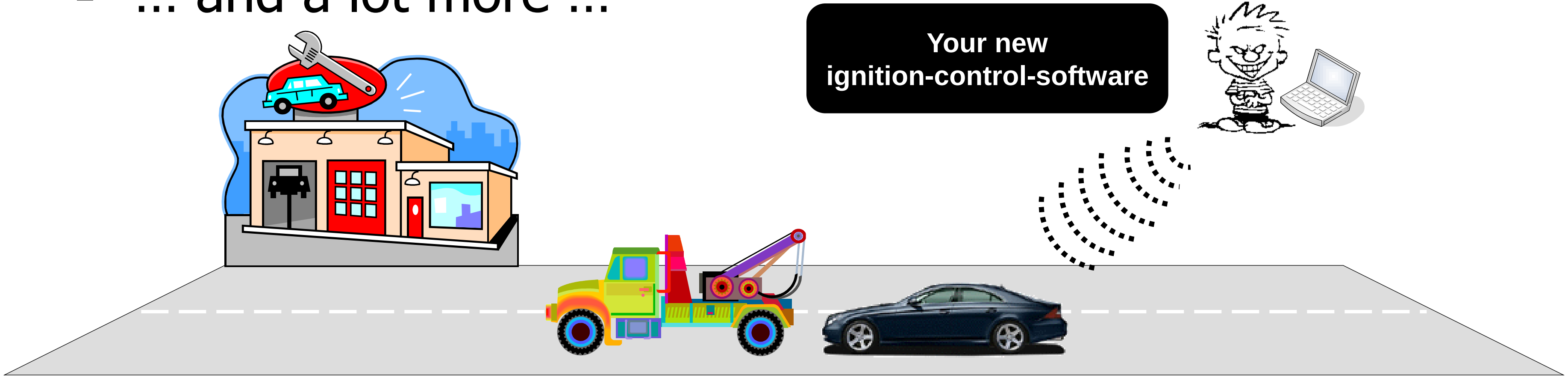
Congestion Warning:
At (x,y), use alt. route

Security and Privacy???

- More fun, but for whom?



- … and a lot more …



Security system requirements

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

How to achieve efficient anonymous authentication?

Outline

- VNAET and its Applications
- VANET security and privacy requirements
- TACK
  - To achieve anonymous authentication

TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs

By Studer et. al.

TACK: Temporary Anonymous Certified Key

Previous work: digital signature

- Trusted authority signs a copy of each OBU’s public key
- Every OBU gets a copy of the authority’s public key
- OBUs sign each message using their private key
- Authority can sign messages saying which OBUs are no longer valid
  - Certificate Revocation List

Public Key Infrastructure Works...Somewhat

- Distributing CRLs is an issue
  - Large list to distribute and keep up to date
  - Millions of vehicles removed from the road annually

- No Long Term Unlinkability
  - Traditionally each vehicle possesses one asymmetric key
  - Like driving down the road with a loudspeaker and shouting your name

Multiple Certificates Per OBU

- Each OBU stores a year’s worth of certificates & keys
- Each key is used for a short period of time

+ Straightforward

+ Limited connectivity to an authority is needed

- Large overhead to revoke 1 OBU

- Malicious OBU can pose as multiple vehicles (Sybil Attack)

Raya and Hubaux “The Security of Vehicular Ad Hoc Networks” ACM Workshop on Security of ad hoc and sensor networks (SASN 05)

Group Signatures to Generate Certificates

- OBU uses a group signature to sign its own certificate
  - Proves signer is a valid OBU (not which OBU)

+ Certificate changes can be frequent

+ One key per OBU to revoke

- Computationally expensive

- OBUs can generate arbitrary number of certificates

  - Fake a traffic jam

Calandriello et al. "Efficient and Robust Pseudonymous Authentication in VANET" VANET workshop 2007

Temporary Anonymous Certified Keys (TACKs)

- A hybrid approach
  - more efficient anonymous authentication than pure group signature based scheme
- Three entities: OBU, RA and MA
  - MA certifies both RA and OBU
  - RA issues TACK upon a valid TACK request
  - TACK is used for V2V communication
- OBUs anonymously request certificates
  - OBU signs the request with a **Group Signature**
    - Only proves an OBU is valid (not revoked)
- Certificates are only valid for a short period of time in a specific region
  - OBUs frequently change keys
  - No long-term linkability

TACKs Assumptions

- OBUs know their current location
  - GPS provides enough accuracy
- OBUs know how to contact an Authority
  - Location of authority is included in map metadata
  - Opportunistic network approach
    - When in range, acquire certificates
  - Or a multi-hop routing protocol helps to enable the communication between authority and OBUs
    - The existence of multi-hop routing protocol is a separate issue (should not be in 1609.2 standard)

TACK Update

- **OBU:** pick new temporary key pair (K^+, K^-)
- **OBU → Authority:** group signature of K^+ to prove that it is a valid OBU
- **Authority:** verify proof

  (wait a little bit)
- **Authority → OBU:** certificate(K^+)

- Temporary keys can be ECDSA, TESLA, …
  - TACK is independent of the authentication schemes specified

TACK Update

- Use Boneh & Shacham’s group signature
  - Verifier can tell who has been revoked
  - Verifier can tell if 1 OBU makes multiple requests in an interval
  - Only the group manager can determine which OBU generated the request

- Group signature is 228B
  - 360ms to sign on a 400MHz processor
  - 36ms to verify on a 3.2GHz processor
  - 149B version is 5x slower

Boneh & Shacham “Group Signatures with Verifier-Local Revocation”
Conference on Computer and Communications Security 2004

TACK Properties

- Authenticate valid OBUs (temporary cert.)
- Authenticate messages (signatures)
- Short Term Linkability (1 cert. per interval)
- Low Overhead
  - Computation (OBU generates 1 group signature per interval)
  - Communication (228B)
  - **OBUs no longer need CRLs for other OBUs**

Identifying the Origin of a Message

- Want to identify misbehaving or malfunctioning OBUs
- In TACKs, the group signature hides which OBU requested a certificate from the RA
- RA must record the request
- Group manager can use the request to find the OBU

Revocation

- OBU’s long term user group key revocation:
  - Communication between RA-MA
  - RA handles TACK requests from abusing OBU to MA
  - MA identifies the abusing OBU and updates the revocation list
  - Future TACK request from the abusing OBU is then rejected by the RA

- OBU’s TACK revocation:
  - Short-lived
  - Implicit revocation

TACK Summary

- TACKs improves key management while providing some privacy
  - A single key pair is associated with each OBU
  - No OBU revocation data sent to OBUs
  - Only an authority can identify the signer of a message
- TACKs requires very few changes to the standard

Conclusion

- 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