DAIMLERCHRYSLER

Vehicle IT and Services Research

Berlin · Stuttgart · Ulm · Palo Alto

Concepts for V2X Intrusion Detection Systems

Tim Leinmüller

SEVECOM Kickoff Meeting, Lausanne

February 2, 2006

DaimlerChrysler

Overview

- **Motivation**
- **Intrusion Detection for V2X communication**
  - Active Safety Applications
  - Position Dependent Routing
  - Concepts
- **Intrusion Detection for Intra-Vehicular Networks**
- **Conclusions**

DaimlerChrysler

Intrusion Detection in V2X Communication - Why?

- V2X communication systems are open systems
  - One lesson learned: every system has flaws that can be used by an attacker
- Updating a deployed system won't be that easy
  - Time between discovery of an exploit and the corresponding update is longer than in other networks
  - Systems might even never be updated
- Combination of two different systems that are well separated until now
  - V2X communication systems: open
  - Intra-vehicular communication systems: closed
- Reactive mechanism to increase security seem easier to realize than preventive security mechanisms
  - Intrusion detection is cheap - asymmetric crypto, identification, certification is expensive

DaimlerChrysler

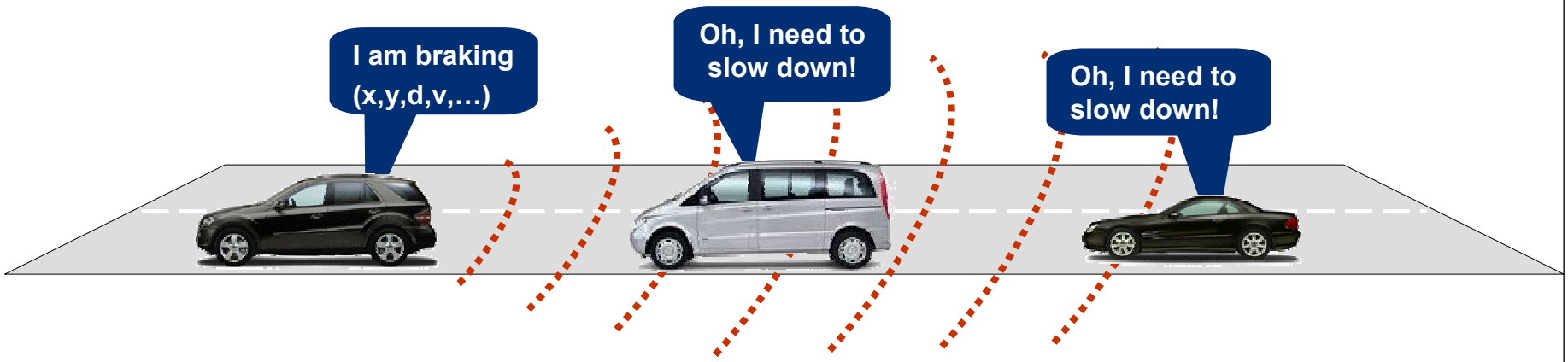
Intrusion Detection in V2X Communication - Aspects

- High mobility
  - Frequent rate of topology changes and connectivity to unknown nodes
- Services are safety-critical and time-critical (alert messages, warnings)
- Services are related to personal data (current location, customized preferences)
- Side channel information are available (sensors, GPS, maps, ...)

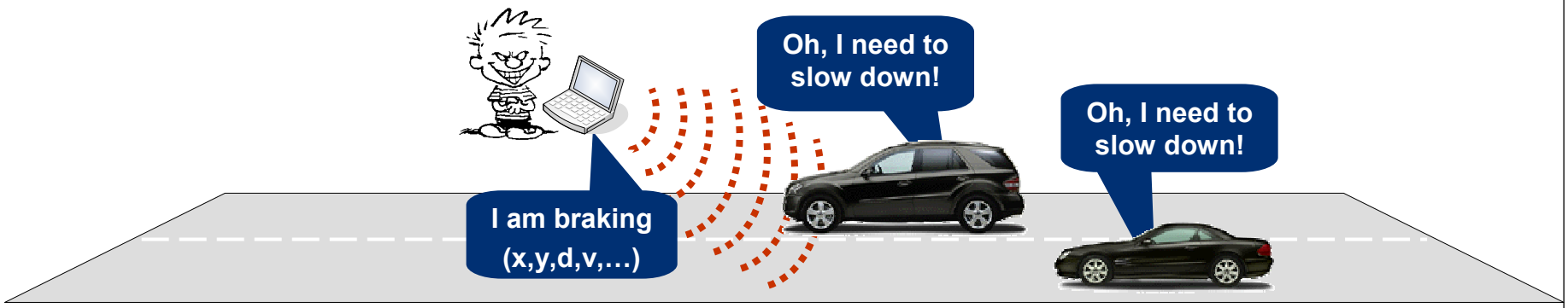
- **Intrusion detection in VANETs**
  - Identify and handle bogus/wrong information, not necessarily the source (e.g. malicious or defective node)
  - Plausibility checks, comparable with anomaly detection
  - IDS in VANET has to work without user interaction
    - Cars are not computers - drivers are not administrators
    - Contribute to an overall self-healing security system for the VANET

What Proactive Security Mechanisms Won't Prevent…

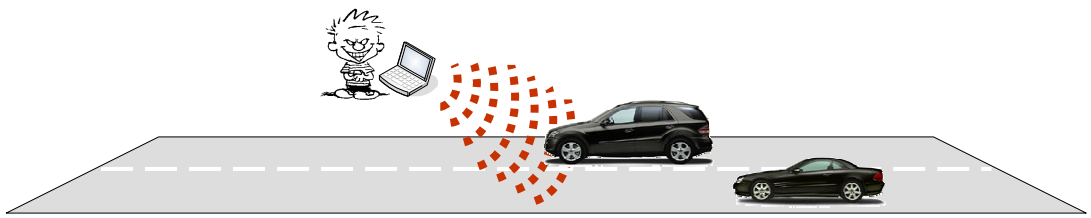
Sharing information among vehicles helps to improve safety



However, proactive security support can not prevent…



Plausibility Checks for Active Safety Applications

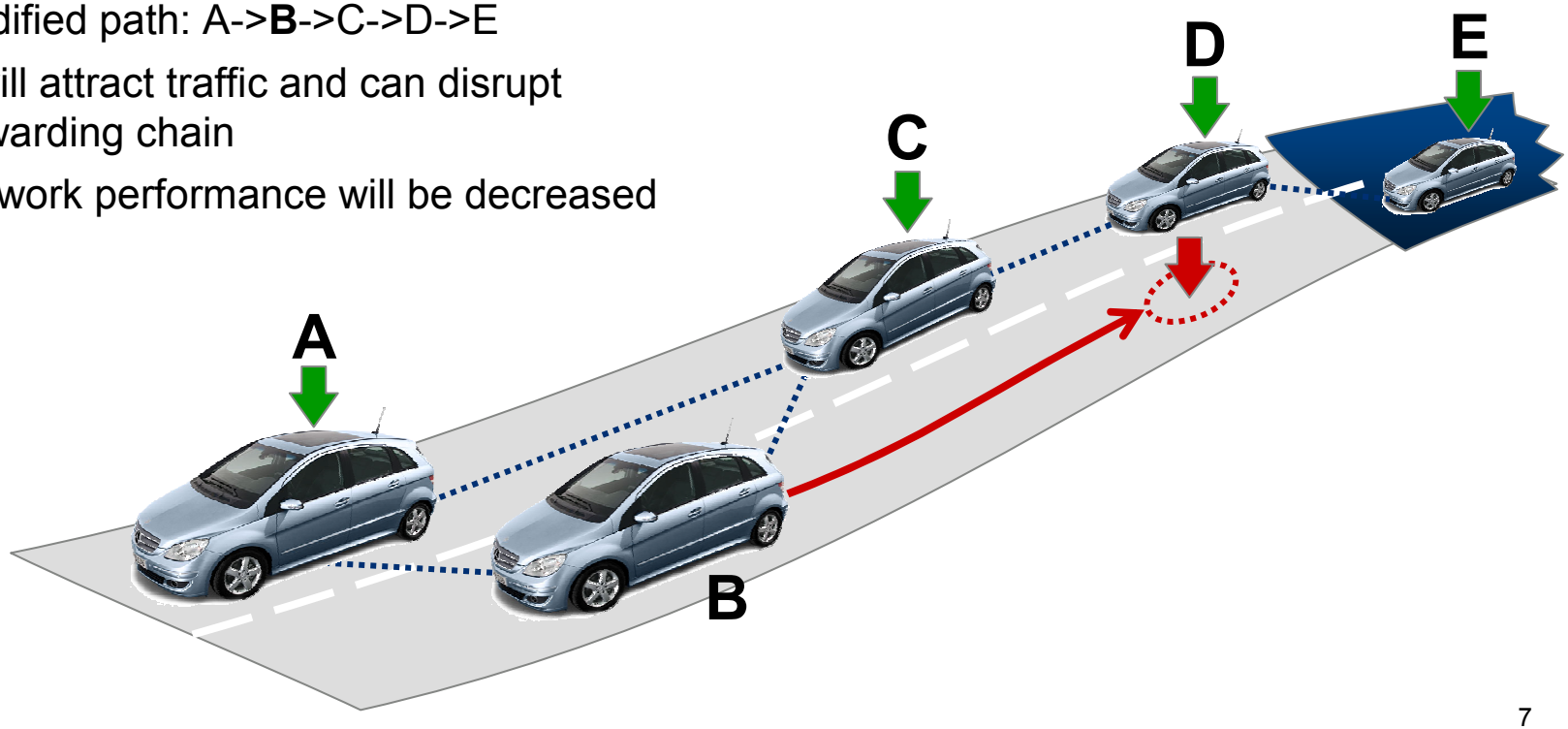


- Vehicles should be able to trust safety messages they receive over the air
- Which means
  - Message was created by valid sender
  - Message has valid content
  - Message content was not tampered in transit
  - Message has not been replayed
- Even if in the worst case only one broadcast message was received!

Plausibility checks will help to evaluate the contents of safety messages

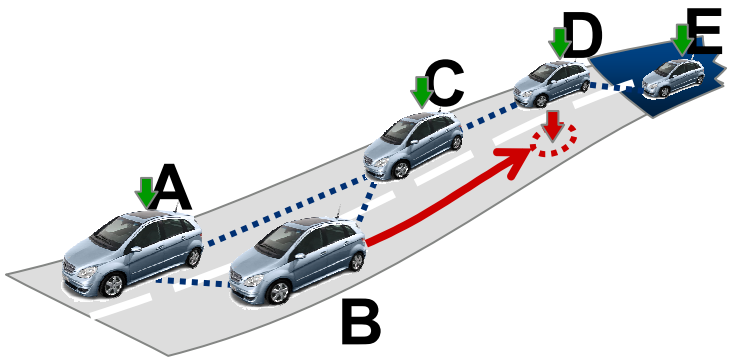
Position Dependent Routing

- Malicious nodes use properties of the communication system to decrease network performance
- Example: Fake position of own car
  - Correct path from vehicle A to vehicle E: A->C->D->E
  - B broadcasts wrong position
    - Modified path: A->**B**->C->D->E
    - B will attract traffic and can disrupt forwarding chain
    - Network performance will be decreased



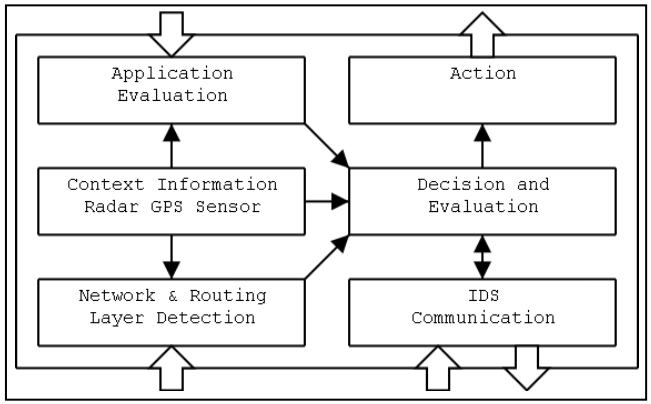
Position Faking: Detection Techniques

- Non cooperative
  - Maximum acceptance range
  - Maximum speed boundary
  - Overhearing
  - Combinations



- Cooperative
  - Position verification by active neighbor query
  - Position history exchange (tracing)

Concepts for V2X Intrusion Detection



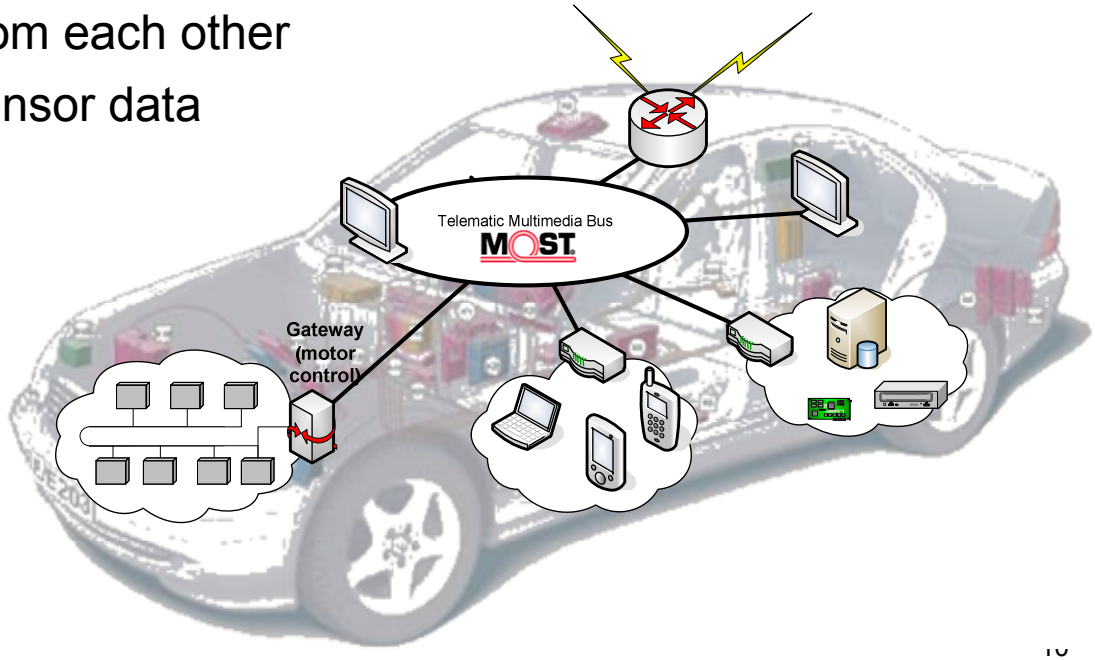
- Modular cross-layer intrusion detection
- Audit data collection on all nodes on multiple layers
- Neighborhood and network topology monitoring
- Message content evaluation on the application layer
- Context awareness (e.g. vehicle sensor data)
- Local evaluation and local decision in combination with co-operative exchange of audit data
- Near-real-time reaction
- Additional usage of temporary available road network infrastructure to exchange for example audit data
- Combine application knowledge and information from location aided routing and addressing
- Detection techniques for position dependent routing (co-operative and non-co-operative)

In-vehicle Communication Protection

Active safety applications rely on trusted usage of car sensor data

Protection against outside and inside attacks on vehicle sensor data

- Integration of tamper-proof devices (SW and HW) in an in-vehicle architecture
- In-vehicle firewalls mechanisms (e.g. CALM vehicle architecture)
- **Development of intrusion detection and prevention system (in-vehicle IDS combined with VANET IDS)**
  - Protect both network parts from each other
  - Detect wrong/manipulated sensor data
  - Prevent intrusions from the VANET part of the network



DaimlerChrysler

Conclusions

There is a need for “automatic intrusion detection systems” to observe and analyze the current status of the network. The goal of the system has to be to detect attacks, both from inside and outside, to the system and its resources.

- Identify bogus/wrong information, not necessarily the source (malicious node)
- Handling of messages from defective nodes
- Plausibility checks
- IDS in VANET has to work without user interaction
  - Cars are not computers - drivers are not administrators
  - Contribute to an overall self-healing security system for the VANET