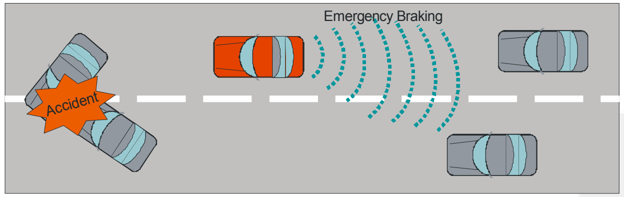
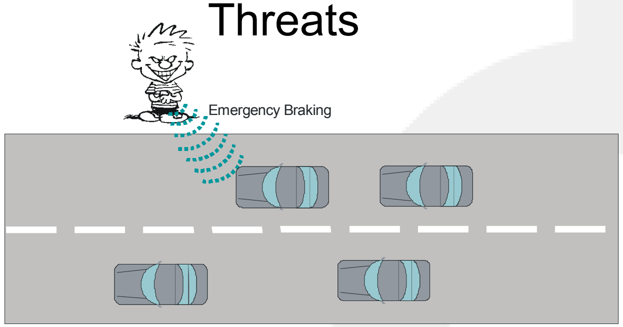
# Intrusion Detection in VANETs

## Scenario



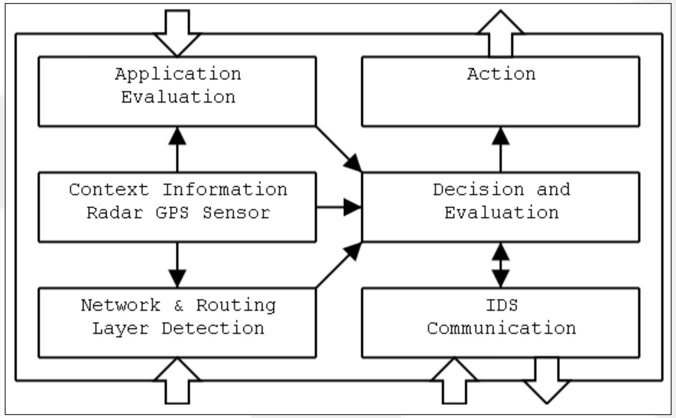
- Wireless ad hoc communication
- High velocity, high rate of topology changes
- Time critical applications
- Position dependent routing and addressing
- Privacy requirements

## Threats



- Falsified warning messages from malicious roadside attackers or malicious VANET nodes
- Common threats for wireless ad hoc networks, such as DoS, node isolation, traffic rerouting, data tampering, spoofing, impersonation, eavesdropping, exploits, viruses and advertisements.

## Intrusion Detection


Application Evaluation
Action
Context Information Radar GPS Sensor
Decision and Evaluation
Network & Routing Layer Detection
IDS Communication

- Modular cross-layer intrusion detection approach
- 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
- Additional usage of temporary available road network infrastructure to exchange audit data

## VANET Applications

- Cooperative driver assistance applications (safety-related or active safety applications)
- Decentralized floating car data applications
- User communication and information services

## Outlook

- Evaluate context supported detection techniques on different layers
- Combine application knowledge and information from location aided routing and addressing
- Detection techniques for position dependent routing (co-operative and non-co-operative)

## Contact Information

- Tim Leinmüller, Albert Held
  Tim.Leinmueller@DaimlerChrysler.com
  Albert.Held@DaimlerChrysler.com
- Günter Schäfer, Adam Wolisz
  Schaefer@tkn.tu-berlin.de
  Wolisz@tkn.tu-berlin.de

DAIMLERCHRYSLER