DAIMLERCHRYSLER

ulm university universität uulm

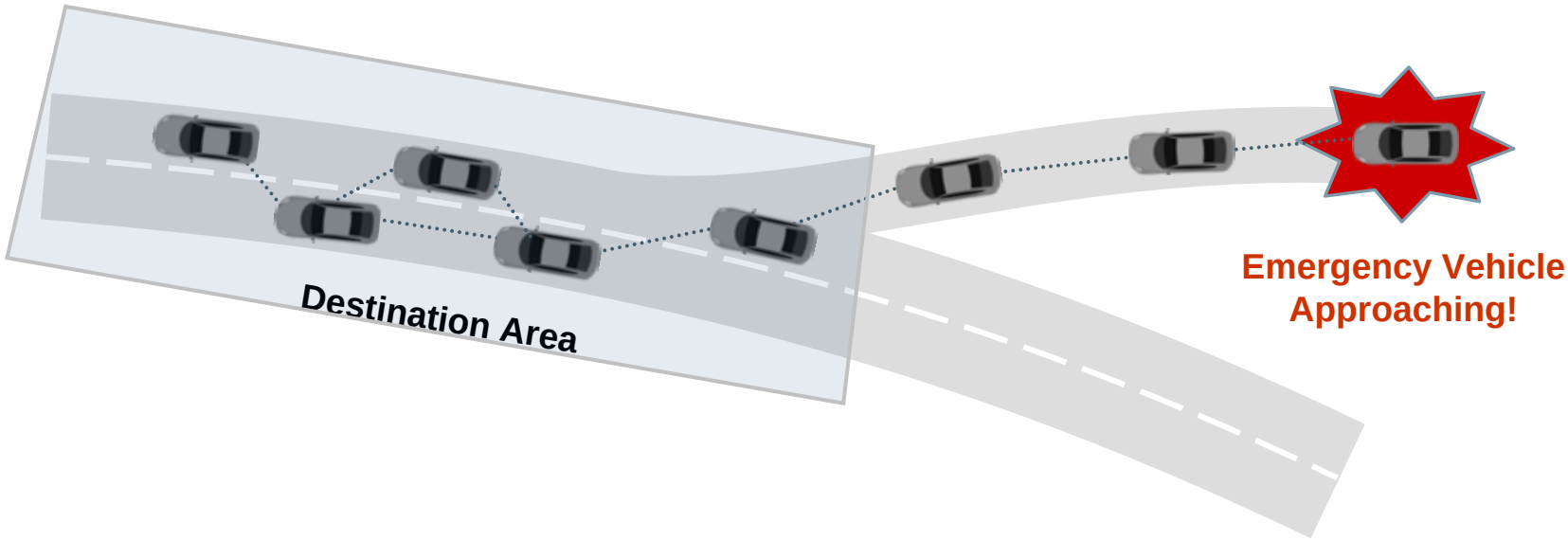
# Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification

Tim Leinmüller • **Elmar Schoch** • Frank Kargl • Christian Maihöfer

# Overview

- Introduction and Motivation
  - Example Scenario
  - Security of Position-based Greedy Routing
- Position Verification
  - Trust-based Approach
  - Autonomous Sensors
  - Simulation Results
- Conclusion and Outlook

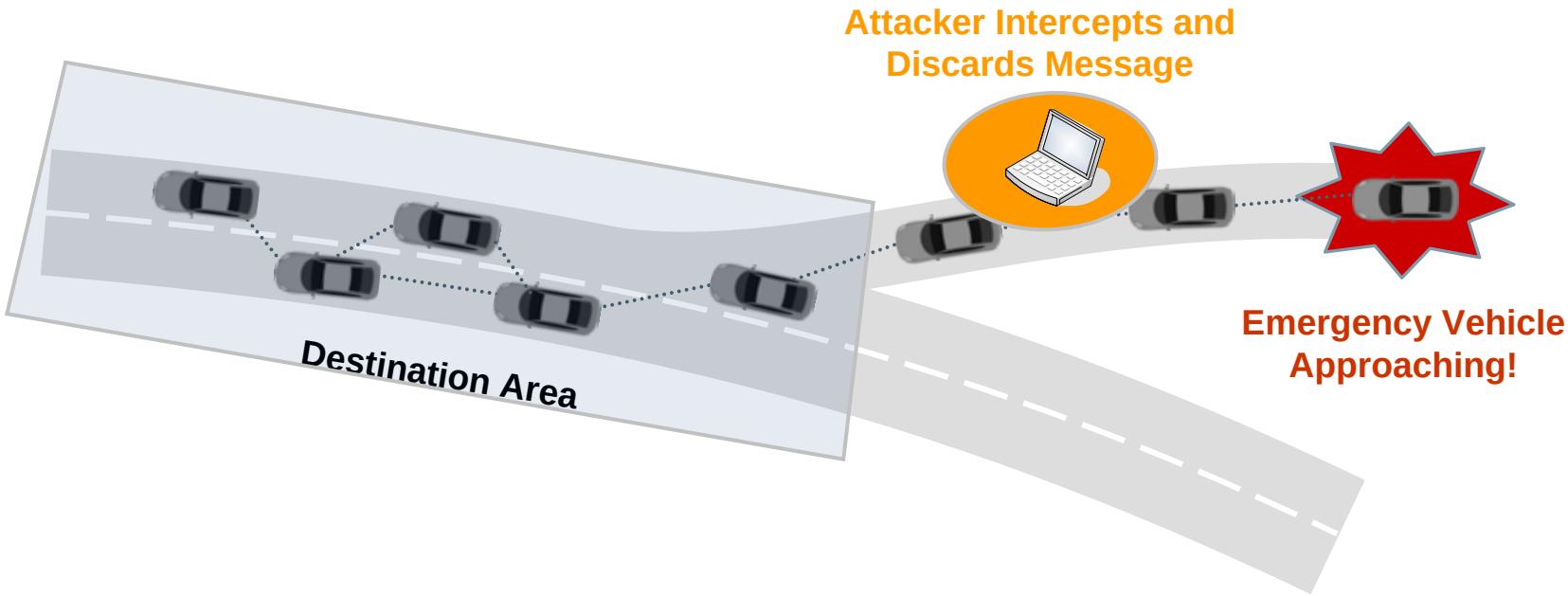
# Motivation




**Example: Emergency Vehicle Approaching**

- Message is forwarded to destination area
- Message is broadcasted in the destination area

# Motivation



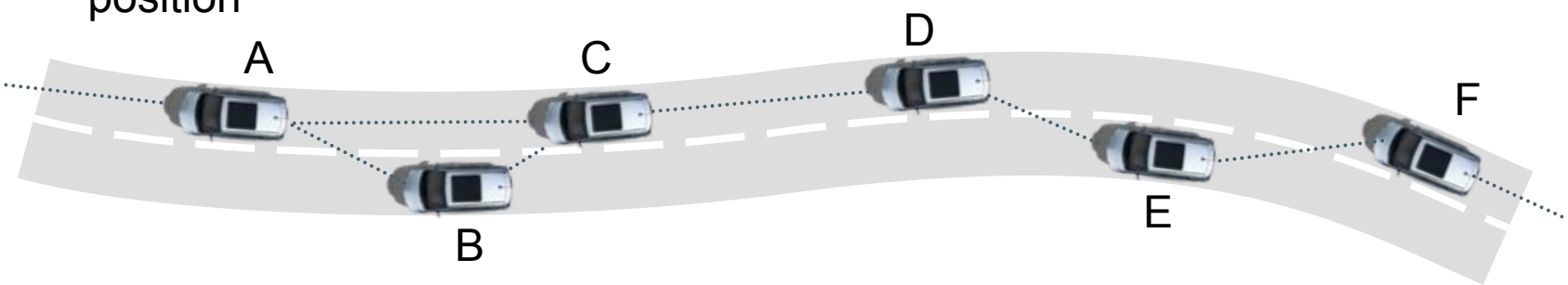

**Example: Emergency Vehicle Approaching**

- Message is forwarded to destination area
- Attacker intercepts message and discards it
- Message is not broadcasted in the destination area

# Position-based Routing

Position-based routing

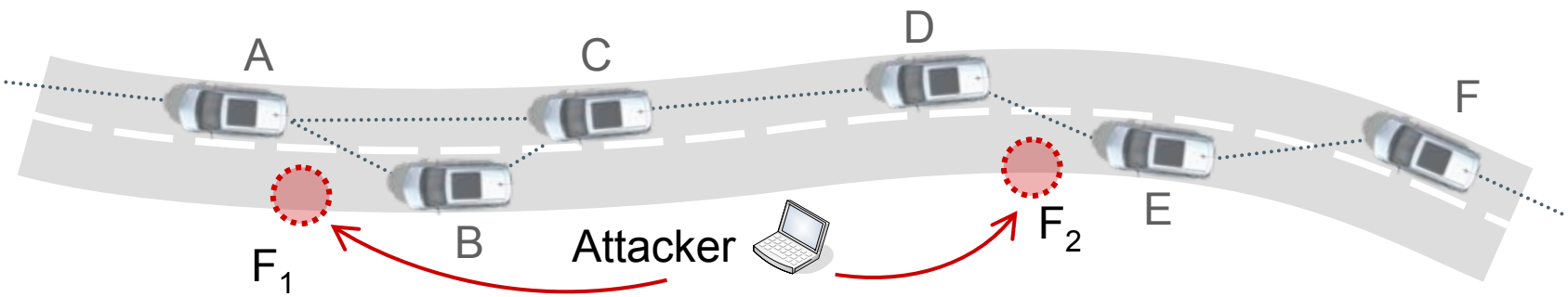
- Beacons: broadcast ID and position to neighbors → neighbor tables
- Greedy routing: transmit packet to neighbor closest to the addressed position




- Selected route from A to F:
  A → C → D → E → F

# Security of Position-based Routing

- Attacking position based routing actively means to attack the beaconing mechanism
  - Beacons: broadcast ID and position to neighbors

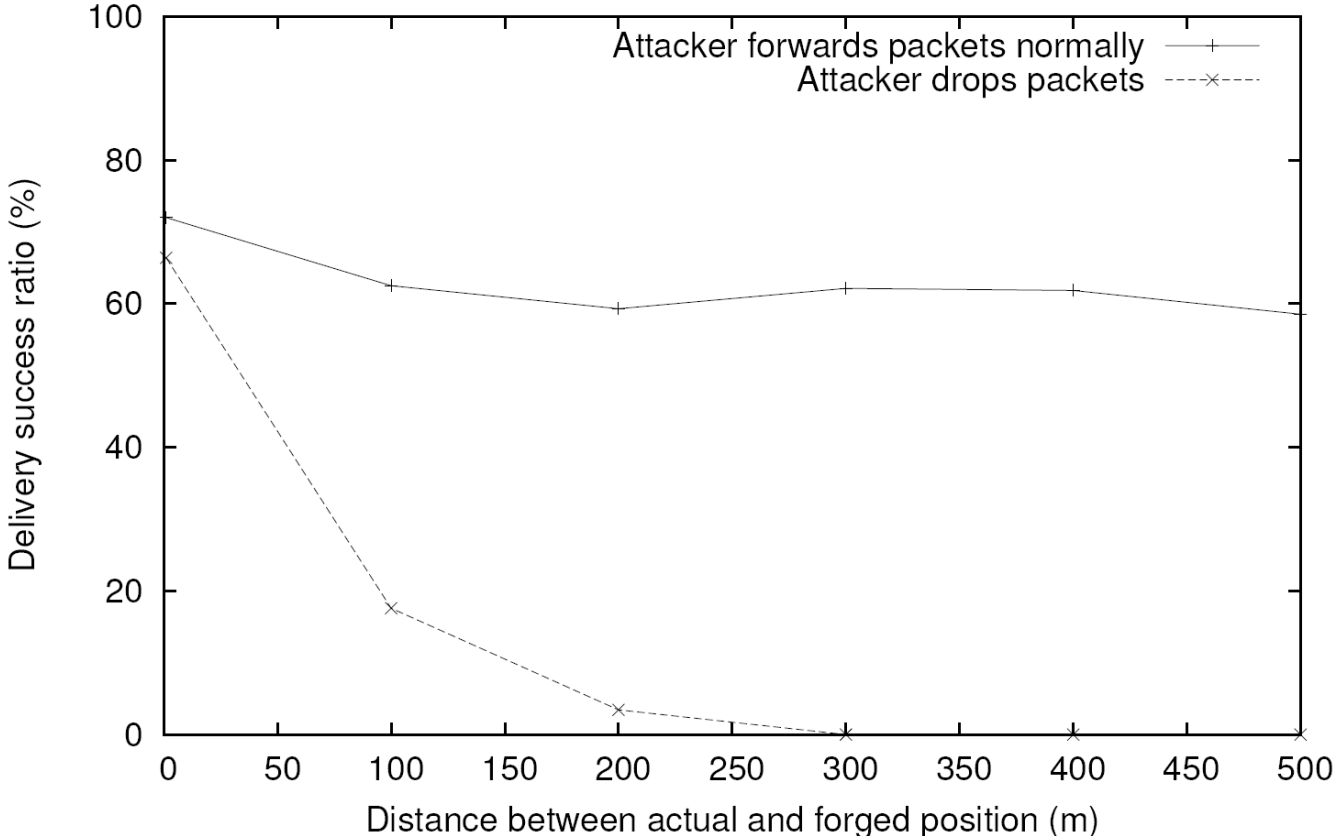



Using position information
- Modify/falsify own position

Using node identifiers
- Create (additional) node identifiers
- Impersonate other nodes

# Impact of Falsified Position Information

- Dedicated falsifying allows to intercept entire traffic along the road




Source: „Greedy Routing in Highway Scenarios: The Impact of Position Faking Nodes“, WIT 2006

# Overview

- Introduction and Motivation
  - Example Scenario
  - Security of Position-based Greedy Routing
- Position Verification
  - Trust-based Approach
  - Autonomous Sensors
  - Simulation Results
- Conclusion and Outlook

# Position Verification

**Position cheating detection system**

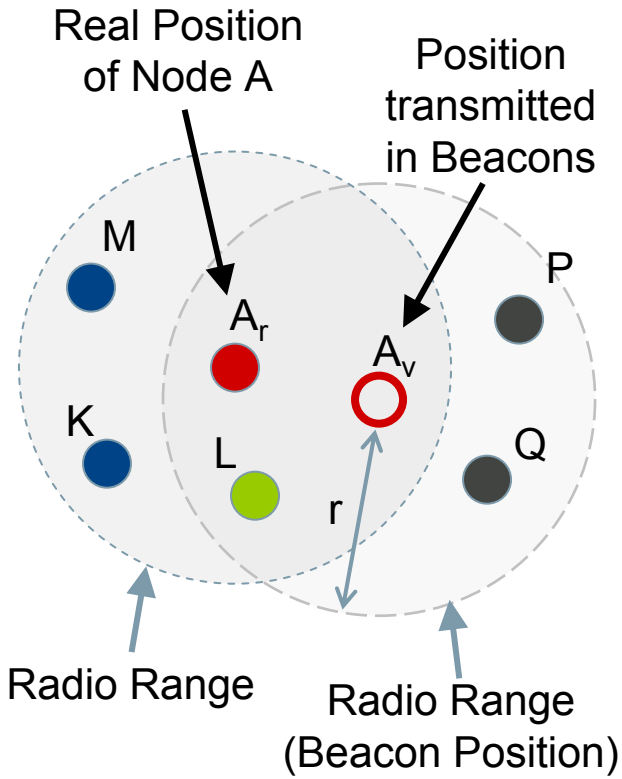
- Similar to intrusion detection systems (IDSs) in MANETs
  - Every node uses multiple (software) sensors to detect position cheating
  - Each node calculates a trust value for its neighbors
- Quick estimation of trustworthiness of distributed position information

**Adapted to VANET environment**

- Relies on information from beacons and from GPS
- No specific hardware requirements
- No dedicated infrastructure requirements
- Adapted to different node movement patterns of VANETs
  - City scenarios
  - Highway scenarios

# Sensor: Acceptance Range Threshold

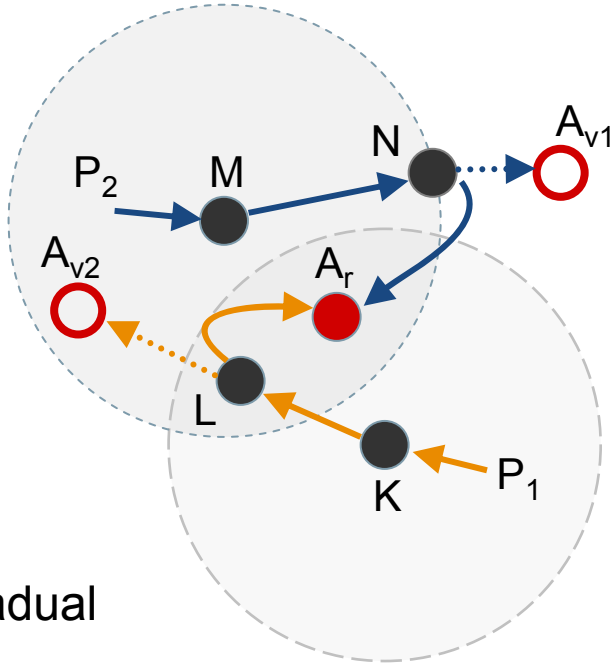
- Based on the limited radio range
- Maximum ART := $\Delta_{max}$
- Accept neighbors N where distance(Pos($N_i$),Pos($N_j$)) ≤ $\Delta_{max}$, otherwise decrease trust
- The bigger the distance between $A_r$ und $A_v$, the more nodes will detect the falsified position
- Issues
  - Fixed threshold is not flexible enough
  - False positions within reasonable distance will not be detected by some neighbors




M,K: distance([M|K],$A_v$) > $\Delta_{max}$ → ignore
L: distance([M|K],$A_v$) > $\Delta_{max}$ → accept
Q,P: no beacon received

# Sensor: Mobility Grade Threshold (MGT)

- Based on limited velocity of nodes
- Maximum node velocity := $V_{max}$
- Accept neighbors N where distance(Pos($N_i$[t]), Pos($N_i$[t+x])) / x ≤ $V_{max}$, otherwise ignore them
- Issues
  - Varying velocities in different scenarios
  - Only rapid changes are detected, not gradual



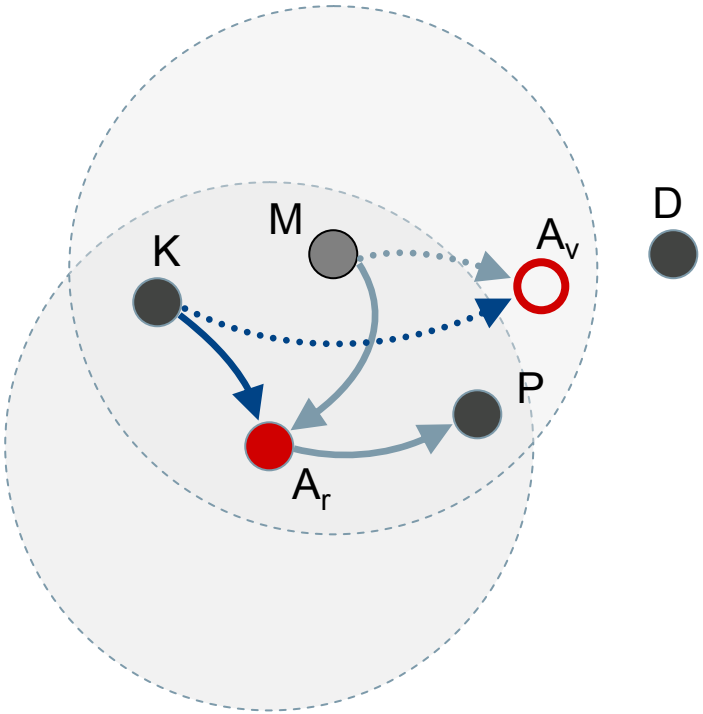

$A_r$ – Real Position Node A

$A_{vi}$ – Virtual Positions Node A

- Attacker A listens to transmissions to selectively intercept packets
- A sends beacon with a position $A_{vi}$ in routing path
- N,L: distance(Pos($A_r$), Pos($A_{vi}$)) / x > $V_{max}$
  → ignore

# Sensor: Overhearing

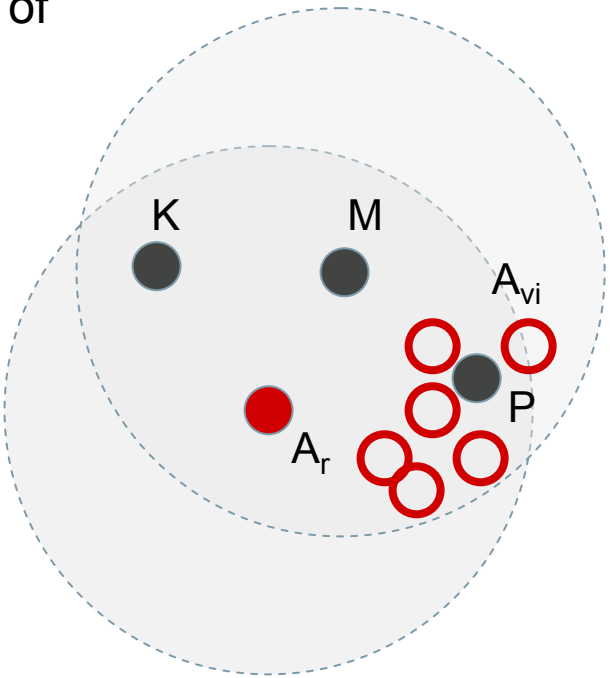
- Nodes monitor data traffic of neighboring nodes and try to identify irregularities
  - Own packet is routed to a less suitable neighbor at the next hop
  - Other nodes forward packets to a node that normally should not be able to receive the packet
- Issues
  - Identification of cheating nodes
  - False positives caused by node mobility
  - Load for processing entire data traffic in neighborhood




P1: A → P detected by M
(P is “inferior” than $A_v$)
P2: K → Av detected by M
($A_v$ is too far away from K)

# Sensor: Maximum Density Threshold (MDT)

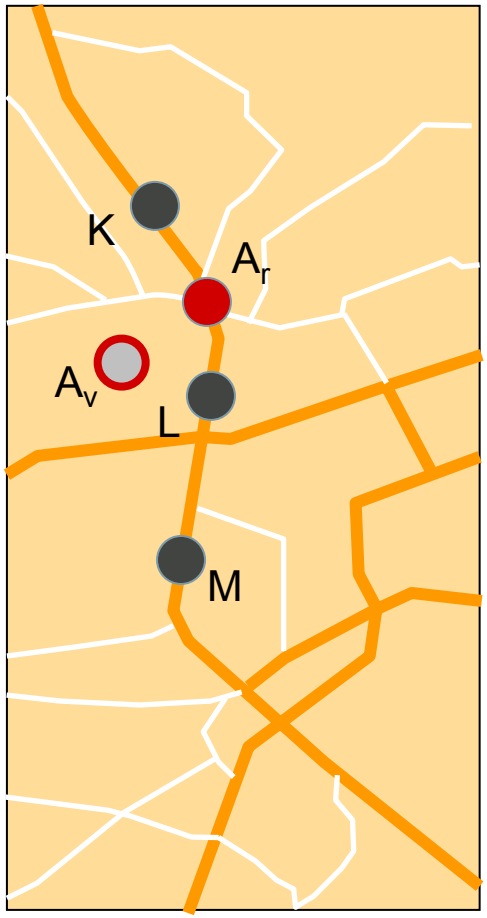
- Based on the fact that only a restricted number of physical entities can reside in a certain area
- Maximum node density $\rho_{max}$
- Accept beacons from regions where number of nodes / size of region ≤ $\rho_{max}$, otherwise ignore them
- Prevents having several identities at the same position (e.g. aims at detecting Sybil attacks)
- Issues
  - Node density depends on node velocity
  - Nodes in the surroundings of attackers could get assigned bad ratings




A distributes multiple beacons
M ignores beacons from region around P

# Sensor: Map-based Verification

- Based on the assumption that vehicles move mainly on roads
- Nodes with navigation systems can cross-check other nodes' positions with roads on digital maps
- Issues
  - Map accuracy
  - GPS accuracy



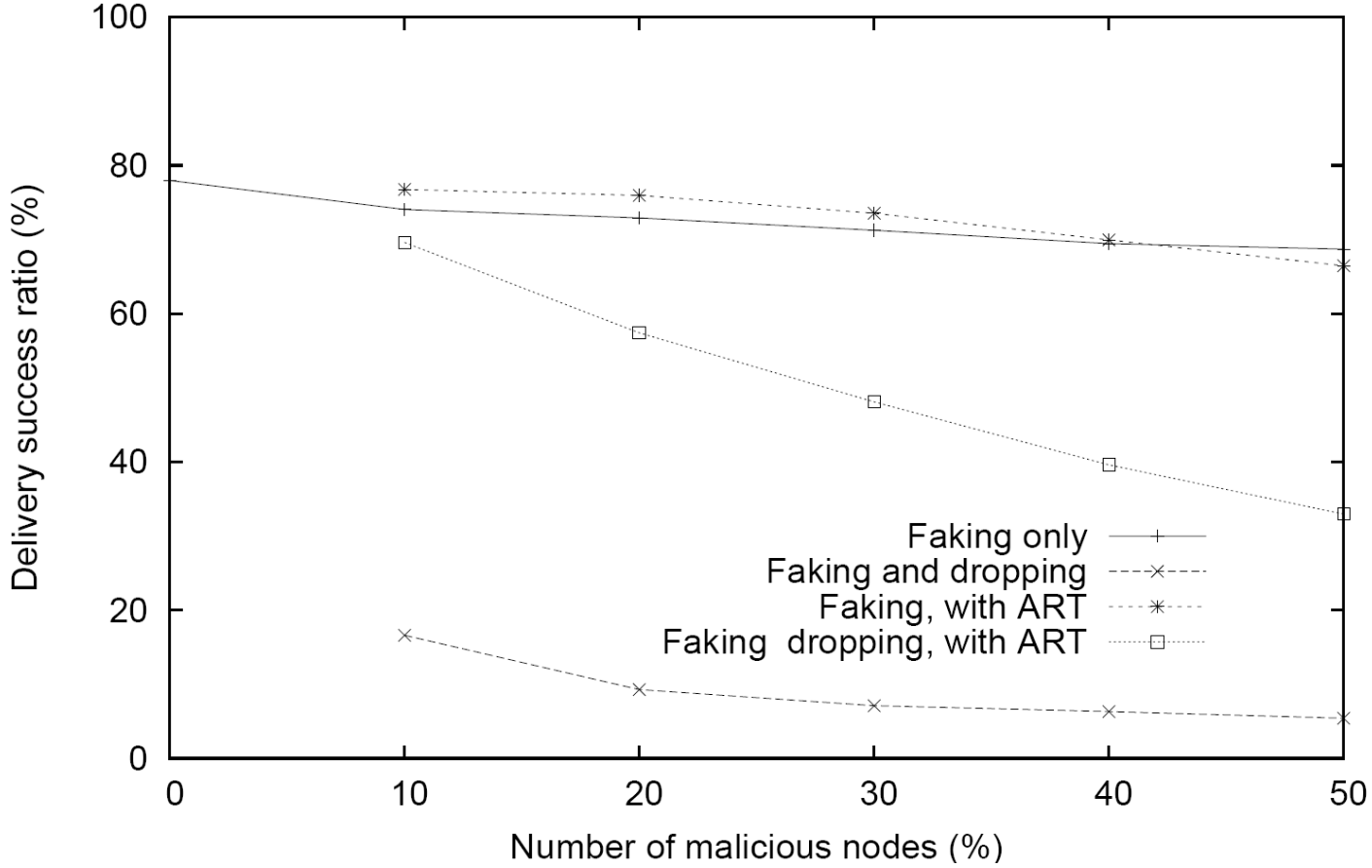

Node L and Node K detect that the announced position $A_v$ is off-road

# Simulation Environment

- Detailed simulation study using ns-2
- City and highway scenario
- Effectiveness of the positon verification system
- Influences of several parameters like distance between real and false position of attacker

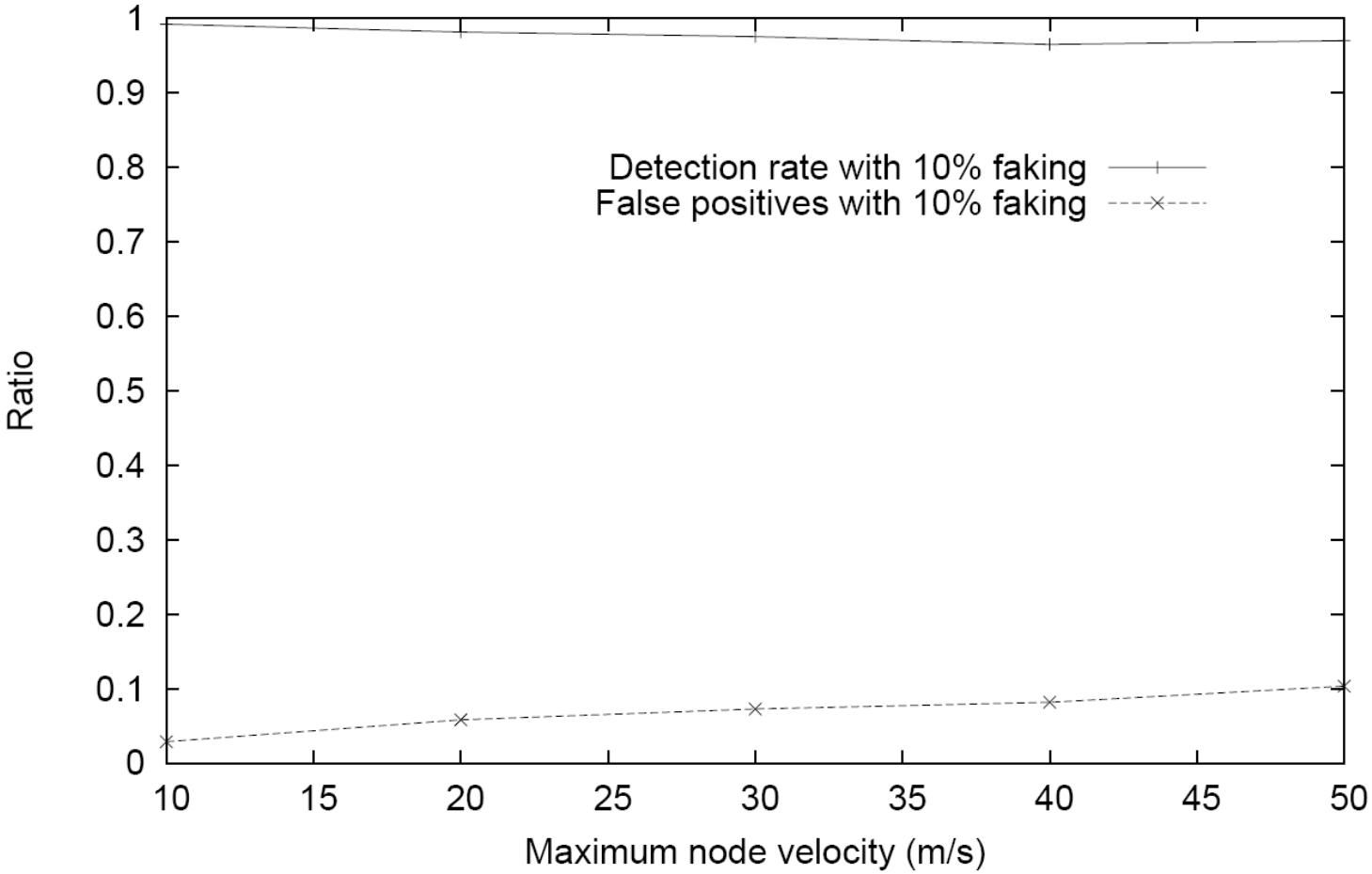
| | | |
|---|---|---|
| | Link-/MAC-Layer | IEEE 802.11b |
| | Wireless transmission range | 250m |
| | Sent messages | 100 |
| | Simulation per parameter set | 20 |
| City | Number of nodes | 100 |
| City | Field length (square) | 1000-4000m |
| City | Mobility model | RWP |
| City | Max. node velocity | 50 m/s |
| City | Pause times | 0 s |
| City | Simulation time | 40s |
| Highway | Number of nodes | ~ 350 |
| Highway | Lanes per direction | 2 |
| Highway | Road length | ~ 12 km |
| Highway | Simulation time | 120s |

# Simulation Results I




- Performance degradation reduces when applying the position verification system

# Simulation Results II




- Detection rates larger than 96%
- False Positives between ~ 2% and 10%

# Overview

- Introduction and Motivation
  - Example Scenario
  - Security of Position-based Greedy Routing
- Position Verification
  - Trust-based Approach
  - Autonomous Sensors
  - Simulation Results
- Conclusion and Outlook

# Conclusions

- Position based routing is vulnerable to attacks on beacon information
- Impact of position faking ranges between
  - Routing performance degradation and
  - Attackers control over entire traffic along a highway

    ►Impact on safety related applications

- Position verification is an effective countermeasure
- Concept of a reactive, IDS-like approach where
  - no specific hardware is required
  - no dedicated infrastructure required
- ►Presented mechanisms will not entirely prevent malicious nodes from using falsified position information, however, they will significantly limit the options of position faking nodes (i.e. fake positions must meet all criteria as opposed by the deployed sensors)

# Outlook

**Combination of sensor results in the rating system**

- Current implementation considers time of observation and sensor weight
- In addition, it should consider
  - Scenarios (highway vs. city)
  - Velocity
  - Node density / traffic situation

**Adaptation of the position verification system for applications**

- Current system is designed for routing
- The aim is to support plausibility checks for applications such as
  - Traffic jam warning
  - Hazard warning

# Questions?

Contacts

Elmar Schoch
Ulm University, Media Informatics
elmar.schoch@uni-ulm.de

Tim Leinmüller
DaimlerChrysler AG, Group Research
tim.leinmueller@daimlerchrysler.com

NOW: Network on Wheels

Information Society Technologies

This work has partly been carried out in contribution to the SEVECOM project that is supported by the European Commission e-Safety initiative.

See http://www.sevecom.org for details

SEVECOM