DAIMLERCHRYSLER

Vehicle IT and Services Research

Berlin · Stuttgart · Ulm · Palo Alto

Security and Geographic Routing

Tim Leinmüller

SEVECOM Kickoff Meeting, Lausanne

February 2, 2006

DaimlerChrysler

Overview

- **Motivation**
  - Geographical Addressing
  - Geographical Forwarding
- **Position Based Routing**
  - Greedy Routing
  - Greedy Versus Topology Based Routing
- **Security of Position Based Routing**
  - Attacks
  - Position Information
- **Summary**

Geographical Addressing

Geo-Broadcast

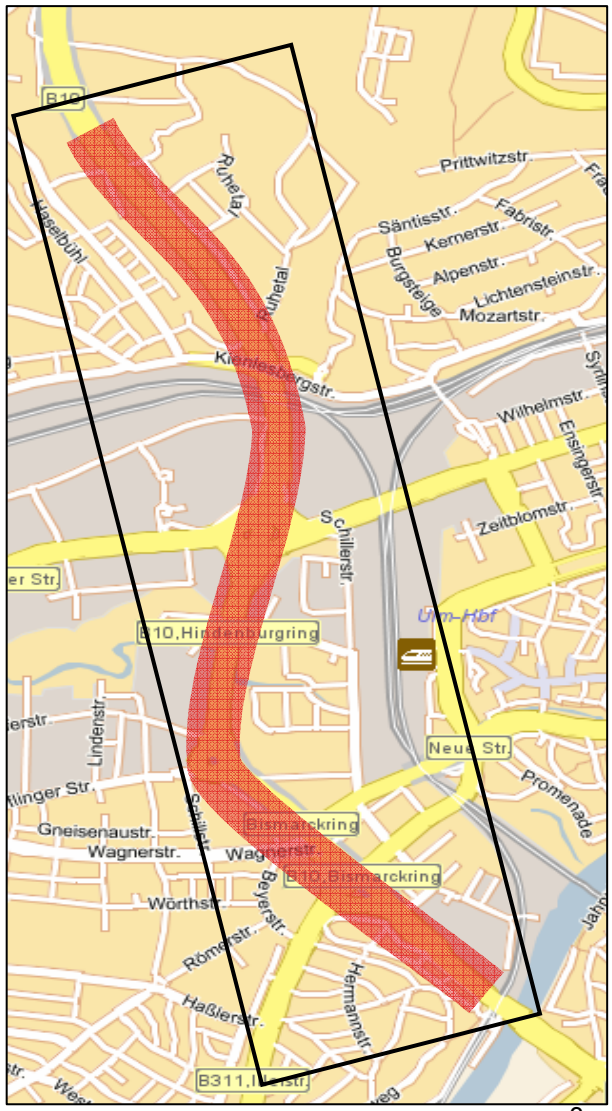
- Distribute a data packet to all vehicles inside the destination area
- Example: traffic jam warning

Geo-Anycast

- Send a data packet to an arbitrary vehicle inside the target area
- Example: request to another vehicle, if the traffic jam has already been resolved

Geo-Unicast

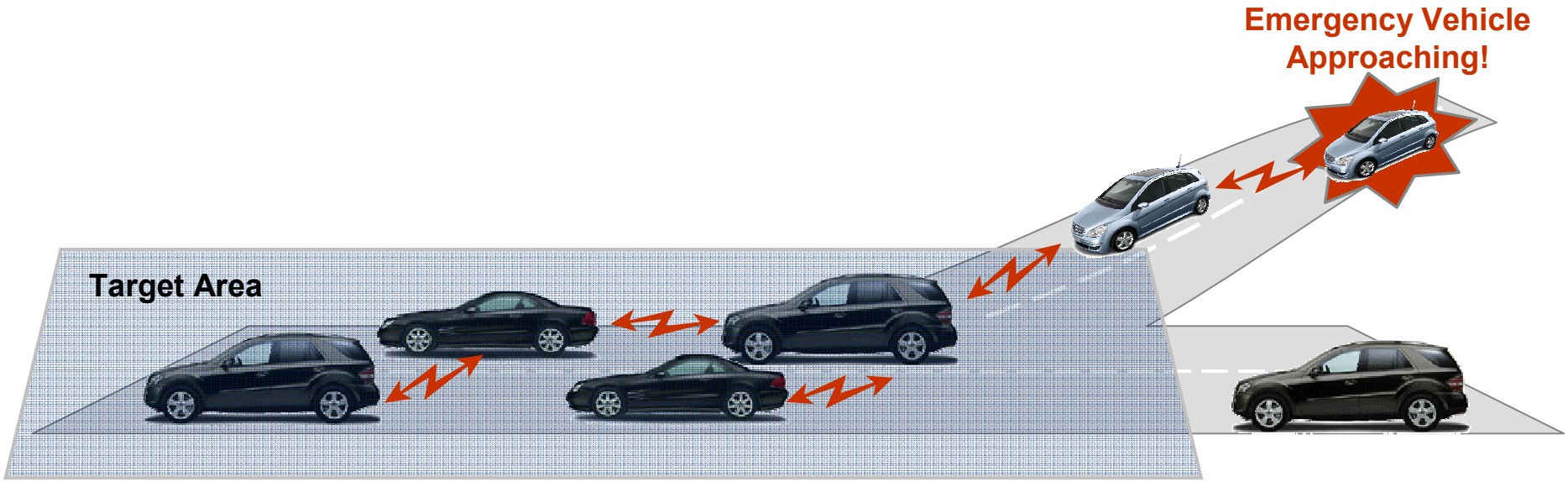
- To send a data packet in unicast mode to an addressed other vehicle. The position information is used to optimize efficiency of the ad hoc network
- Example: virtual caravan driving



Geographical Forwarding: Line Forwarding, Area Forwarding

Example: Emergency Vehicle

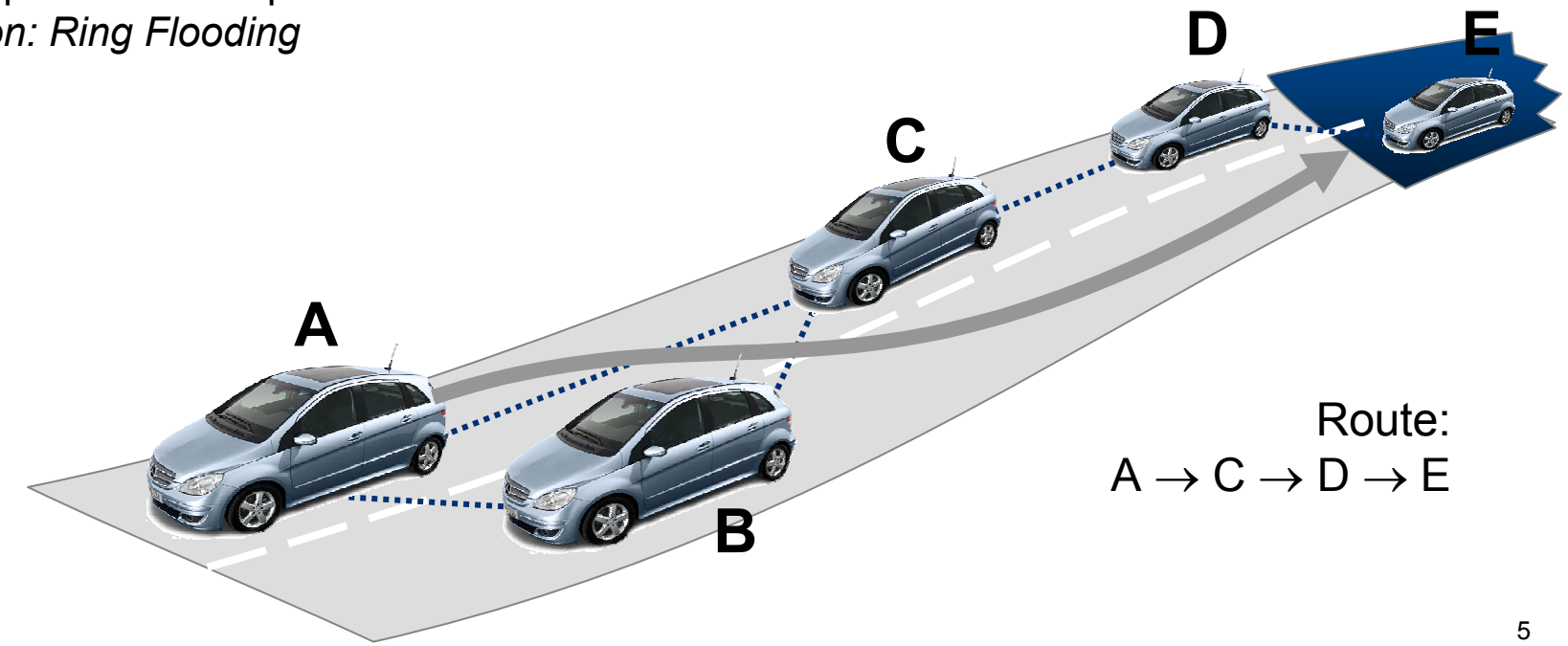
- Line forwarding: transfer data packet to target area
- Area forwarding: distribute data packet inside target area



Position Based Routing: Greedy (Perimeter State) Routing, GPSR

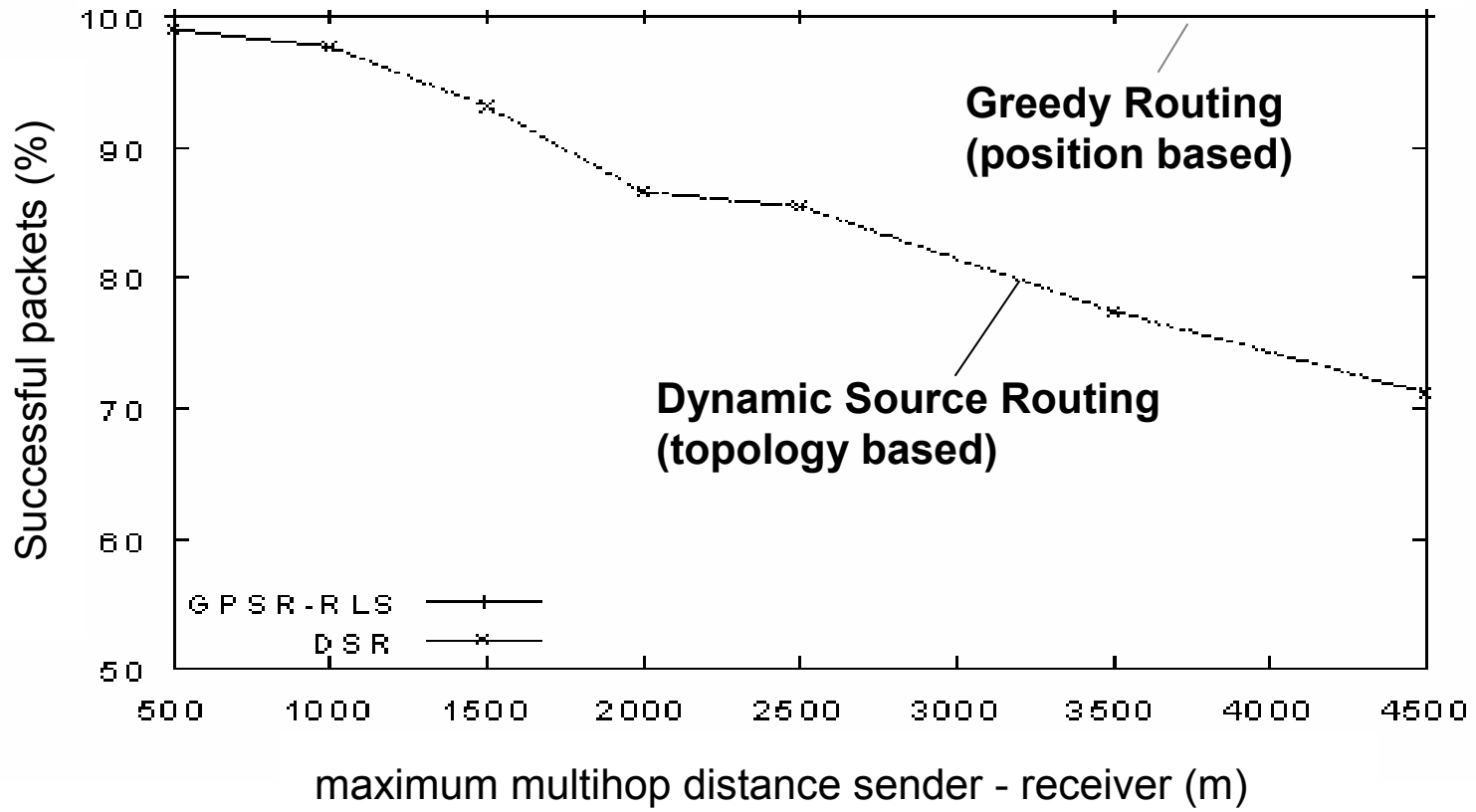
- Beacons: send ID and position to neighbors → neighbor table
- Greedy routing: transmit packet to neighbor closest to the addressed position

- **Problems:**
- Alternative routes: in case no node closer to destination is found
  Solution: Physical data transport of packets (caching)
- Look-up service: find position of a destination addresses
  Solution: Ring Flooding



Simulation Results: Greedy versus Topology Based Routing

Maximum communication range (1 hop): 250 m

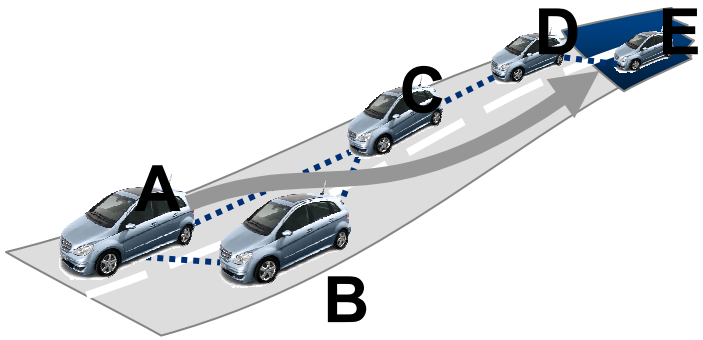


D. Vollmer (DC), M. Mauve (Uni Düsseldorf), H. Füssler, Käsemann (Uni Mannheim), H. Hartenstein (Uni Larlsruhe)

Security of Position Based Routing

Attacking position based routing means to attack the beaconing mechanism

- (Beacons: send ID and position to neighbors)

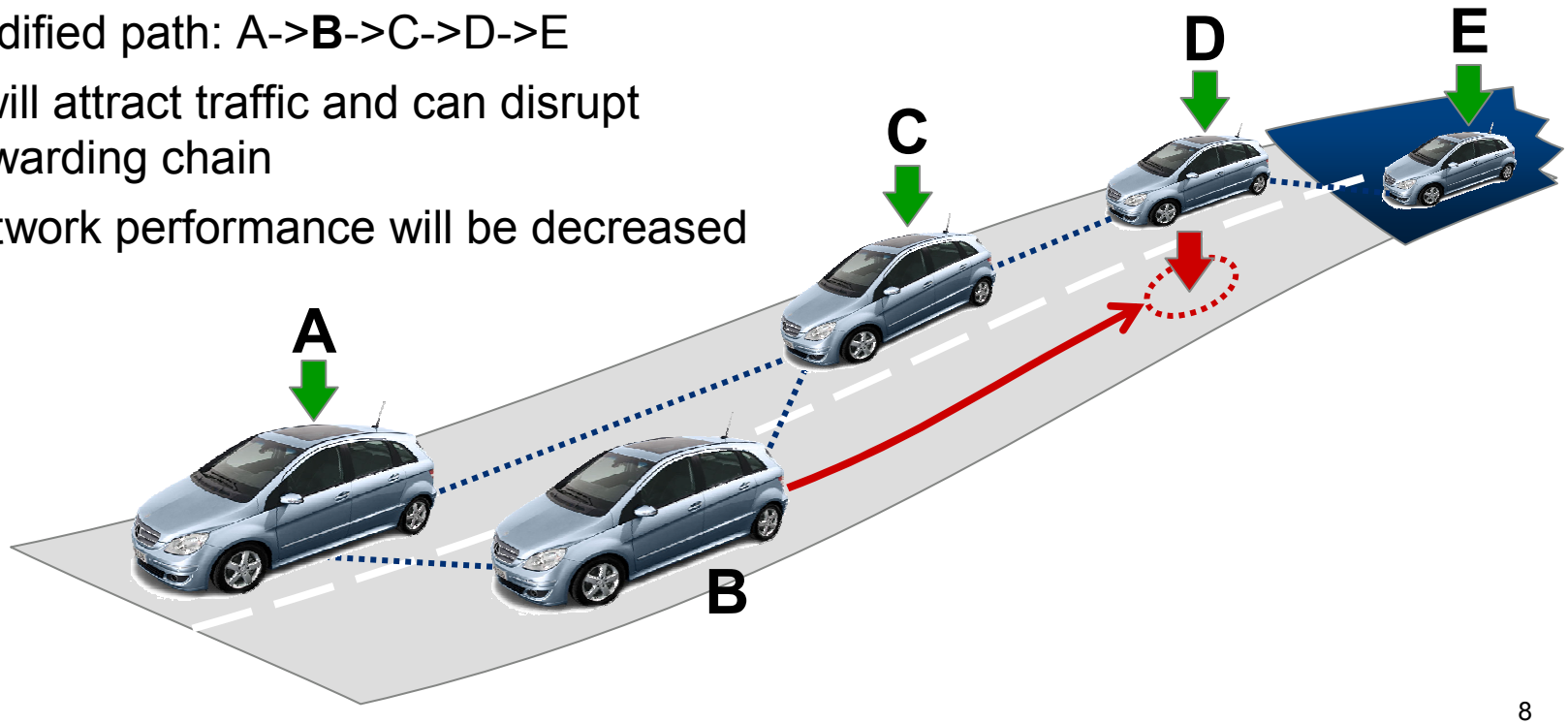


Attacks

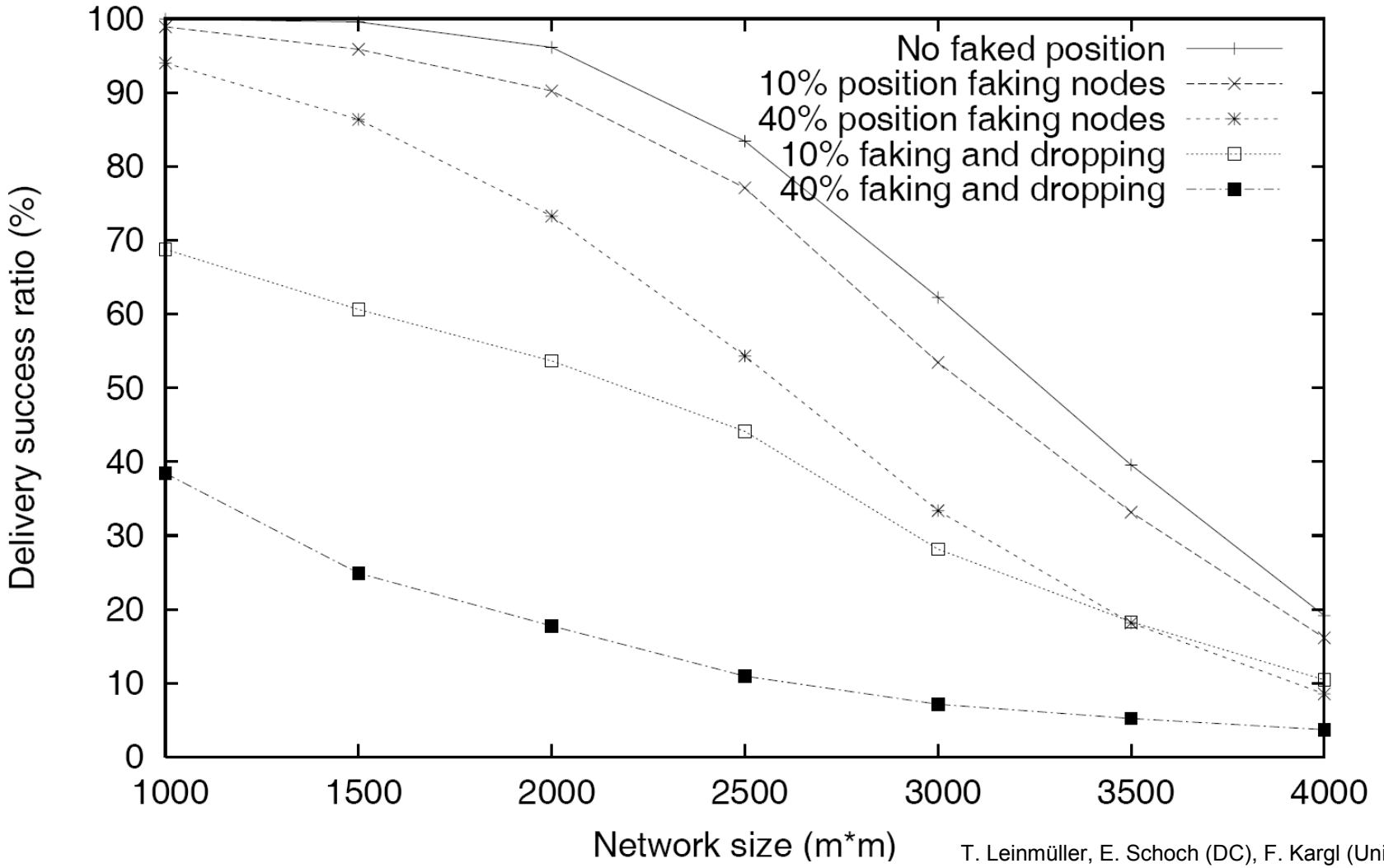
- Node identifiers
  - Create (additional) node identifiers
    - Sybil Attack
  - Impersonate other nodes
    - Discredit other nodes
- Position information
  - Modify / falsify position information in beacons
    - Reroute data
    - Intercept data

Position Faking Malicious Node

- 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



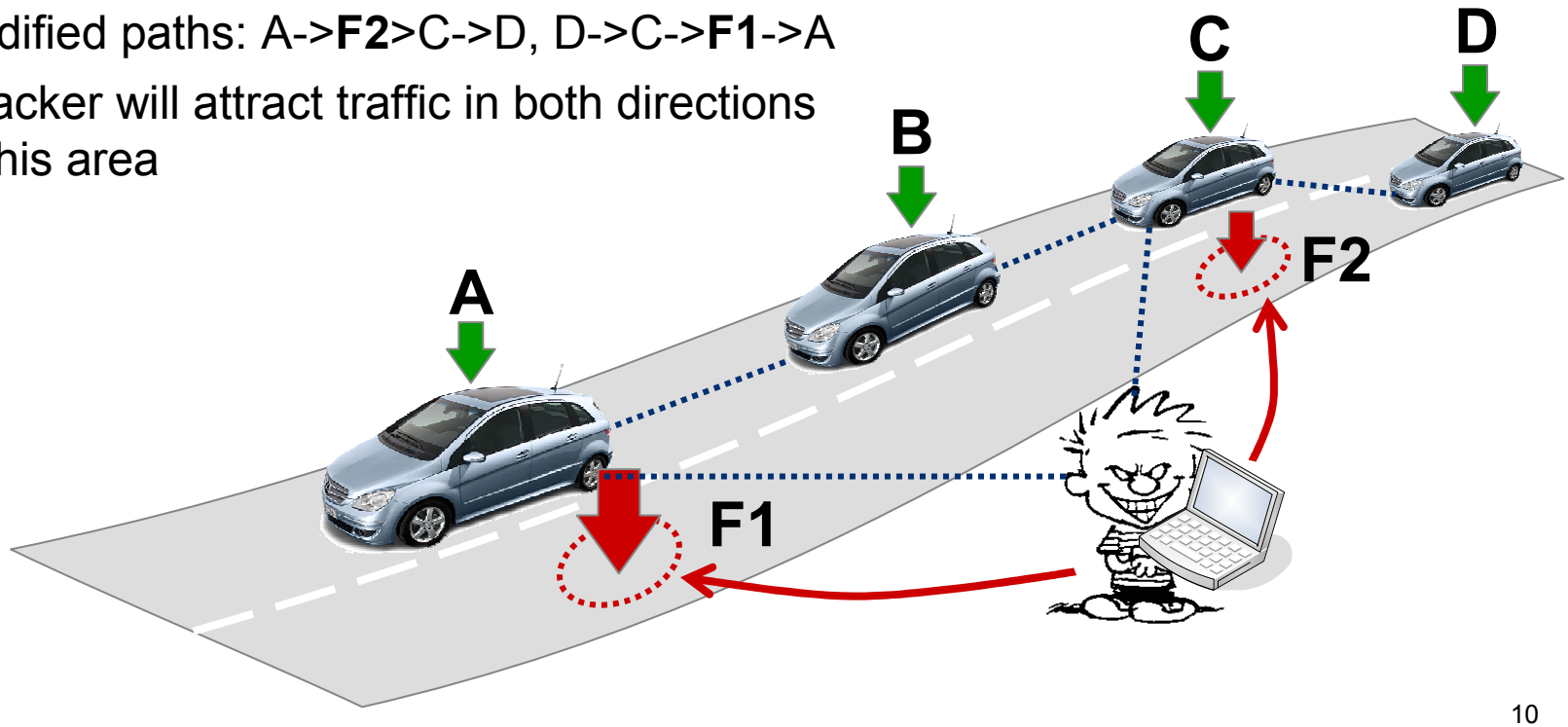
Simulation Results: Impact of Wrong Positions



T. Leinmüller, E. Schoch (DC), F. Kargl (Uni Ulm)

Roadside Attacker

- Roadside Attacker pretends to be part of the network and use properties of the communication system to decrease network performance
- Example: Create attacker creates two fake nodes
  - Correct path between vehicle A and vehicle D: A->B->C->D, D->C->B->A
  - Attacker broadcasts positions for two fake identities
    - Modified paths: A->**F2**>C->D, D->C->**F1**->A
    - Attacker will attract traffic in both directions in this area



DaimlerChrysler

Summary

Origin of false position data

- “Defective” nodes (receiving or misinterpreting position data)
- Malicious nodes

Position based routing is vulnerable to attacks on beacon information

- Identifier
- Position Information

Effects

- Performance degradation
  - Formation of routing loops: loops are detected, packets dropped
  - No suitable next hop: packets cannot be routed, remain in cache
  - Packets maliciously dropped: position faking nodes drop intercepted packets
- ► Impact on safety related applications