

Towards a Security Architecture for VANETs ARES 2006

# Towards a Security Architecture for Vehicular Ad Hoc Networks

Klaus Plössl  
Thomas Nowey  
Christian Mletzko


University of Regensburg

1

Towards a Security Architecture for VANETs ARES 2006

## Outline

- What is a Vehicular Ad Hoc Network?
- Goals and Application Categories
- Typical Attacks and Security Requirements
- Security Architecture
- Discussion

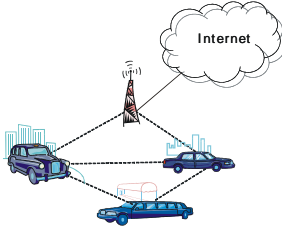


2

Towards a Security Architecture for VANETs ARES 2006

## Vehicular Ad Hoc Network (VANET)

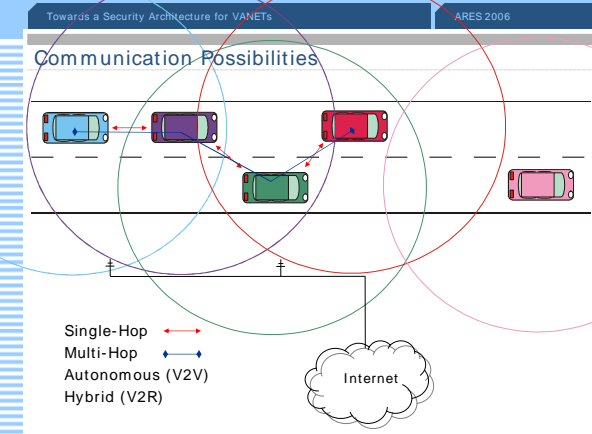
- Subgroup of MANETs
- Main difference
  - Router = Vehicle
- Particularities
  - High speed
  - High computing power
  - Hardly any problems with energy supply
  - Nearly no space restrictions
  - Restricted movement
- Includes
  - Vehicle-to-vehicle communications (V2V)
  - Vehicle-to-roadside communications (V2R)



3

Towards a Security Architecture for VANETs ARES 2006

## Communication Possibilities




4

Towards a Security Architecture for VANETs ARES 2006

## Goals

- Traffic Safety
  - Prevent accidents
  - Reduce accidental damage
- Traffic conditions
  - Increase transportation efficiency
  - Observe volume of traffic
- Environment
  - Avoid congestion
  - Reduce pollution
- Comfort
  - Increase information and entertainment possibilities
  - Develop driving assistance systems

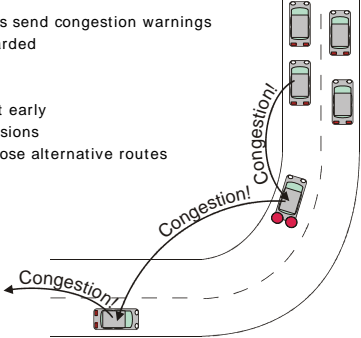


5

Towards a Security Architecture for VANETs ARES 2006

## Example: Congestion Warning

- Mode of operation
  - Standing vehicles send congestion warnings
  - Warning is forwarded
- Advantages
  - Drivers can react early
  - No rear-end collisions
  - Vehicles can choose alternative routes

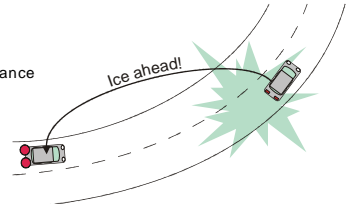


6

Towards a Security Architecture for VANETs ARES 2006

### More Examples

- Main Goal Safety
  - Accident warnings
  - Weather warnings
  - Intersection assistance
  - ...
- Other
  - Navigation
  - Toll collection
  - Finding parking space
  - Broadband Internet access
  - Traffic surveillance
  - ...



7

Towards a Security Architecture for VANETs ARES 2006


### Exchange of Telematics Messages

- Vehicles act as sensors
- Exchange of information like
  - Position, current speed, acceleration or deceleration
  - In-car sensor data from airbag, ABS, ESP, etc.
- Two possibilities
  - Active: A vehicle only sends messages if it recognizes a problem or has to forward a message
  - Passive: Each vehicle periodically broadcasts status messages (beacons)


8

Towards a Security Architecture for VANETs ARES 2006

### Chances and Risks



- Participating in road traffic gets safer
- Roads are used more efficiently
- Environment is protected
- Driving gets more comfortable



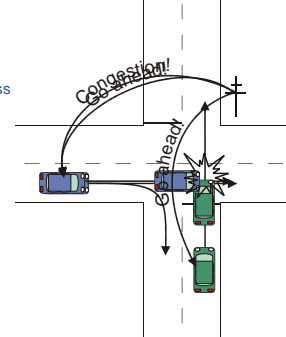
- Road traffic may be manipulated
- Privacy problems may occur
- Congestion may decrease

9

Towards a Security Architecture for VANETs ARES 2006

### Injection of Bogus Information

- Attacker could be
  - Outsider
  - Insider
- Selfish, but relatively harmless
  - Get a free road
  - No traffic noise
  - Additional gains
  - ...
- Malicious
  - Provoke accidents
  - Cause damage
  - ...

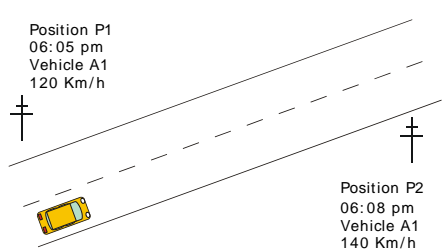


10

Towards a Security Architecture for VANETs ARES 2006

### Violate Privacy

- Create movement patterns
- Track down certain vehicles
- ...



Position P1  
06:05 pm  
Vehicle A1  
120 Km/h

Position P2  
06:08 pm  
Vehicle A1  
140 Km/h

11

Towards a Security Architecture for VANETs ARES 2006

### Requirements

- Integrity
  - Integrity for all messages
  - Authentication for participants
  - Reliable time and position information
- Confidentiality
  - Encryption of message data
  - Privacy protection
- Availability
  - Routing with guaranteed delivery rates
  - Low latency
  - Scalability

12

Towards a Security Architecture for VANETs ARES 2006

### Application Categories

- Alarm signals
  - Mainly geocast
  - Integrity and non-repudiation very important
  - E.g. from police cars, fire engines, ambulances, ...
- Telematics messages and warnings
  - Geocast
  - Integrity and privacy important
  - E.g. full brake application warning, congestion warning, beacons, ...
- Value-added services
  - Mainly unicast
  - Confidentiality very important
  - Not critical for traffic safety
  - E.g. broadband Internet access, information about nearby hotels, restaurants or places of interest, ...

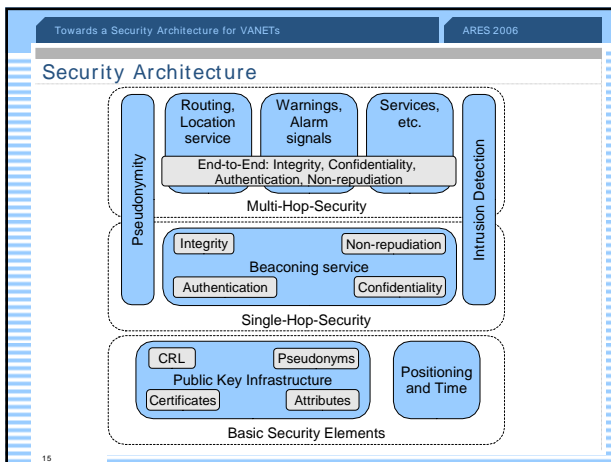
13

Towards a Security Architecture for VANETs ARES 2006

### Communication Model

- Hybrid telematics system
  - Periodically sent beacons (passive, single hop)
  - Warnings (active, multi hop)
- Routing
  - First contact by beacons
- Beacon should include
  - Identity (pseudonym)
  - Current position and time
  - Movement information (direction, speed, acceleration or deceleration)

14



Towards a Security Architecture for VANETs ARES 2006

### Basic Security Elements

- Used in other layers
- Public key infrastructure
  - Centralized approach with trusted third party (TTP)
  - Certificates and pseudonyms are stored in tamper proof hardware
  - Additional attributes for emergency vehicles
  - Sufficient number of pseudonyms for each participant
  - Existing proposals
    - LKN-ASF (LKN Ad hoc Security Framework)
    - MANET-IDs in conjunction with MANET-CRS
- Positioning and time
  - GALILEO
    - 99,8% availability, 4-6m precision
    - Provable integrity and authenticity

16

Towards a Security Architecture for VANETs ARES 2006

### Single-Hop-Security

- Beacons
  - Basis for routing and hybrid telematics system
  - Digitally signed
  - Contain current time
  - Sent in conjunction with certificate
- Possible optimization
  - Exchange symmetric keys after authentication
  - Use message authentication code (MAC)
- Encryption
  - Imposes a lot of overhead
  - Increases reaction time
  - Privacy protection by means of changing pseudonyms

17

Towards a Security Architecture for VANETs ARES 2006

### Multi-Hop-Security

- Warnings and alarm signals
  - Geocast
  - Only asymmetric cryptography
  - Encryption not possible
  - Digital signature provides authenticity and integrity
- Value-added services
  - Uni- or multicast
  - Certificate and key exchange possible
  - Encryption, authenticity, integrity and non-repudiation possible
- Spatial cloaking
  - Use imprecise position information
  - Improves privacy
  - Not applicable for all geocast messages

18

### Further Aspects

- Pseudonym changes
  - Problem with linkability
  - Identifiers on all communication layers must change
- Hybrid telematics system
  - Aggregation of beacons to warnings potentially dangerous
  - Depends on cooperation and trustworthiness of participants
  - Save messages that triggered a warning
  - Use tamper proof hardware
- Intrusion detection system
  - Technical checks
  - Plausibility checks
  - Inform TTP about inconsistencies
- Priority schema

19

### Discussion and Future Work

- Fulfillment of requirements
  - Integrity is ensured for single-hop and multi-hop messages
  - All messages are authenticated
  - Encryption is possible
  - Privacy is protected by pseudonyms
  - Time and position information from external source
  - Problem: secure routing algorithm with geocasting capabilities
- Future work
  - Fill architecture with existing or new mechanisms
  - Test scalability and latency in simulations

#### Contact:

Klaus Ploessl  
University of Regensburg  
Klaus.Ploessl@wiwi.uni-regensburg.de

20