Secure Vehicle Communication

Intrusion Detection in VANETs

Elmar Schoch ▪ elmar.schoch@uni-ulm.de

SEVECOM Workshop ▪ June 27th, 2006 ▪ Paris

Outline

SEVECOM

- Problem & motivation
  - Proactive vs. reactive security
  - The case in vehicular networks
- Intrusion detection
- Existing work on intrusion detection in
  - … MANETs
  - … WSNs
  - … Vehicular networks
- Architecture ideas
- Conclusion

Proactive vs. reactive security

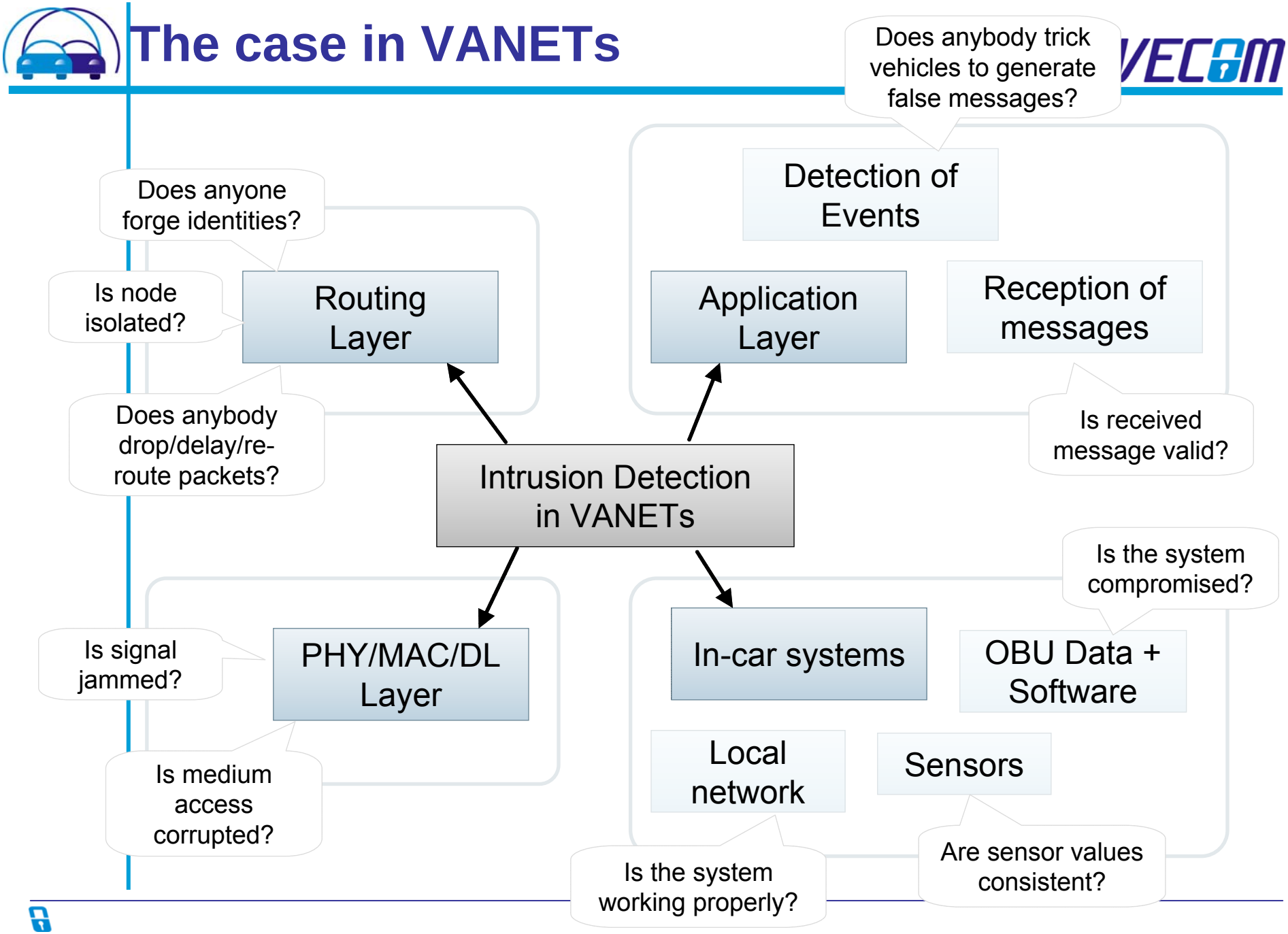
SEVECOM

- Proactive security
  - Prevents illegal operations by appropriate mechanisms, e.g. cryptographic, architectural, …
- Problem: Many illegal operations can hardly be prevented
- Reactive security
  - Tries to detect fraudulent use and
    - Ignore/isolate/exclude originator
    - Minimize impact

Signatures:
- Allow to prove authenticity of sender
- Impersonation of sender not possible

CSMA/CA in IEEE 802.11:
If stations disregard interframe spaces, they can control the channel in their wireless transmission range

The case in VANETs



The case in VANETs

- Proactive security can help
  - To manage identities
  - To protect data integrity and authenticity
  - To avoid eavesdropping
  - …
- In numerous cases, only detection and reaction seems possible
  - Forged & induced messages
  - Disturbed information flow
  - Tricked vehicle sensors

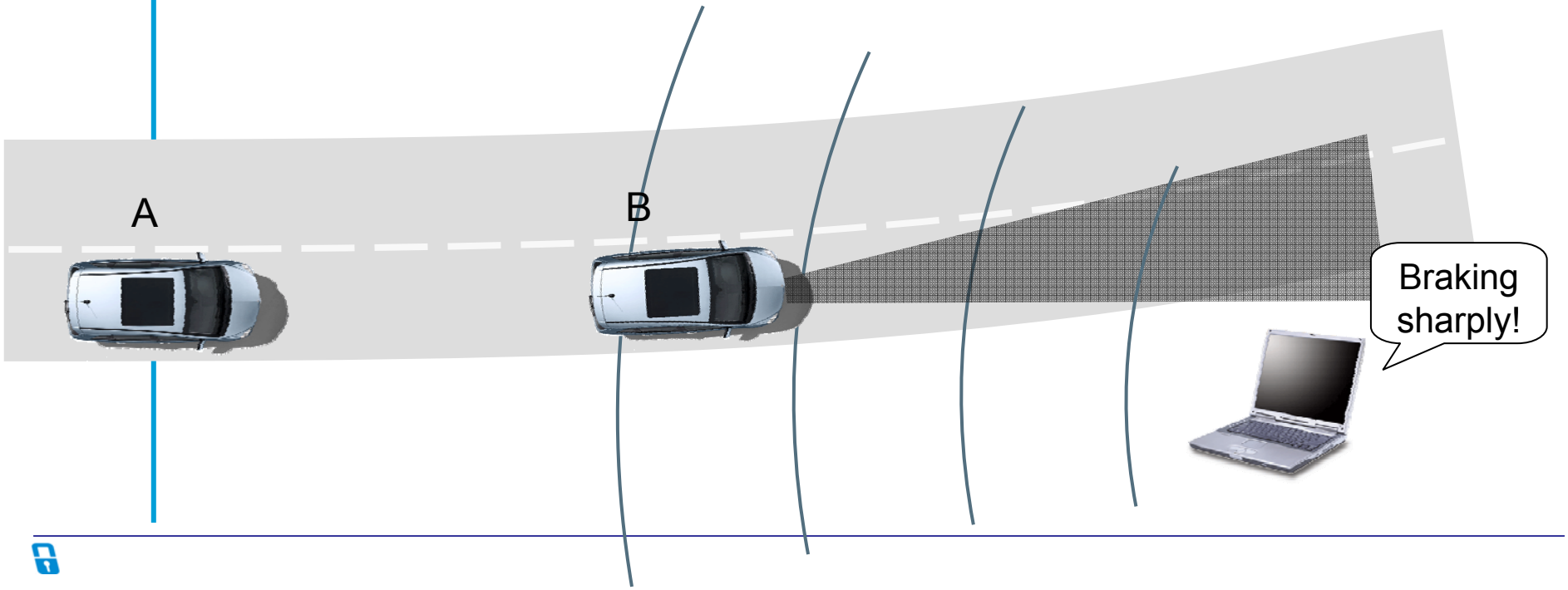
Moreover

- Unknown attacks have to be considered
  - Long vehicle life cycle
  - Rare system updates
- Cryptography tends to be expensive (Computational, organizational)

Intrusion detection-like mechanisms integral part of security architecture for V2V communication system

Example: Bogus brake message

- Vehicle B receives message of braking vehicle in front
- Intrusion detection could find:
  - Radar/Ultrasound does not indicate a vehicle in front
  - Communication system has never received any beacons from the sender before



Reactive security / Intrusion detection

What should be detected?
- Manipulated information
- Unauthorized access
- Attacks on system reliability

What is needed for detection?
- Store audit data
- Send probes
- Monitor system behavior
- Analyze system status

What to look for?
- Anomalies – extract behavior different to normal
- Attack signature – targets specific, known attacks
- Specification discrepancy – only allow formally specified procedures

What output?
- Malicious node identifier
- Information tagged invalid
- Compromised module

What reaction?
- Ignore/isolate/exclude malicious nodes
- Discard invalid information
- Trigger action like restoring secure system state

Outline

SEVECOM

- Problem & motivation
  - Proactive vs. reactive security
  - The case in vehicular networks
- Intrusion detection
- Existing work on intrusion detection in
  - … MANETs
  - … WSNs
  - … Vehicular networks
- Architecture ideas
- Conclusion

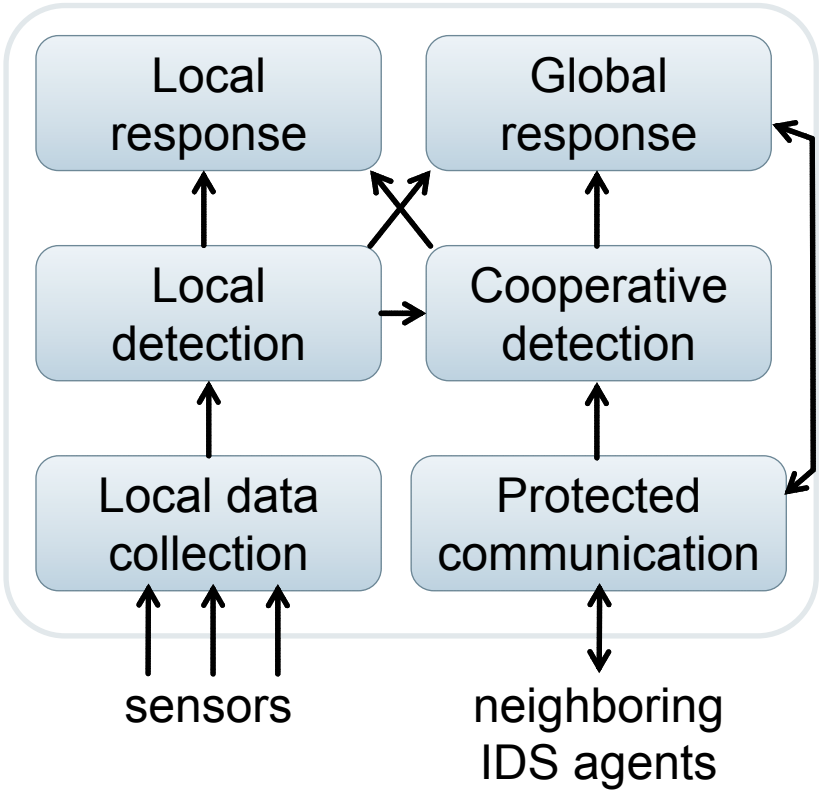
Intrusion detection in MANETs

SEVECOM

- Main focus on routing
  - Particularly detection & correction of selfish behavior
- Watchdog/Pathrater (Marti, Giuli, Lai, Baker)
  - Detects denied forwarding, rating of routes to bypass mal. nodes
- CORE (Michiardi, Molva)
  - Collaborative reputation mechanism, differentiates between observations, e.g. subjective, indirect
- CONFIDANT (Buchegger, Le Boudec)
  - Reputation-based, introduces trust to other nodes
- MobIDS (Kargl)
  - Trust-based, cooperative, integrated with identification and secure communication mechanisms (SDSR), multiple sensors

IDS model according to Zhang/Lee

- Local sensing
  - Collection of data on several communication layers
- Local & global detection
  - Detection of anomalies
  - Cooperative majority voting
- Local & global reaction
  - Re-authentication of nodes
  - Isolation of nodes



Intrusion detection in Wireless Sensor Networks (WSNs)

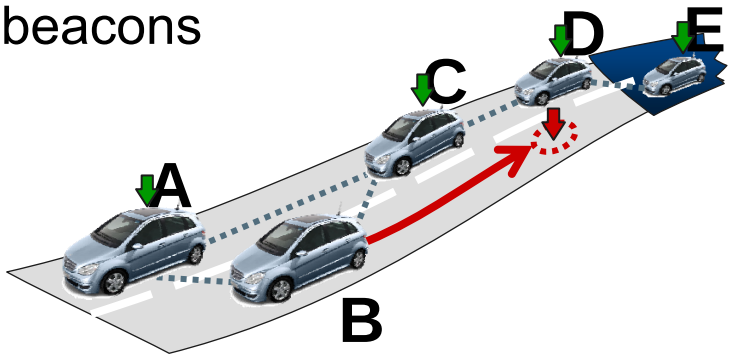
SEVECOM

- Detection of
  - node replication attack (Parno, Perrig, Gligor)
  - node relocation
  - energy drain attack
  - wormholes
  - …
- But: mechanisms are usually designed for typical requirements of wireless sensor networks
  - no/slow node movement, low energy consumption, sensing applications, …

Intrusion detection in VANETs

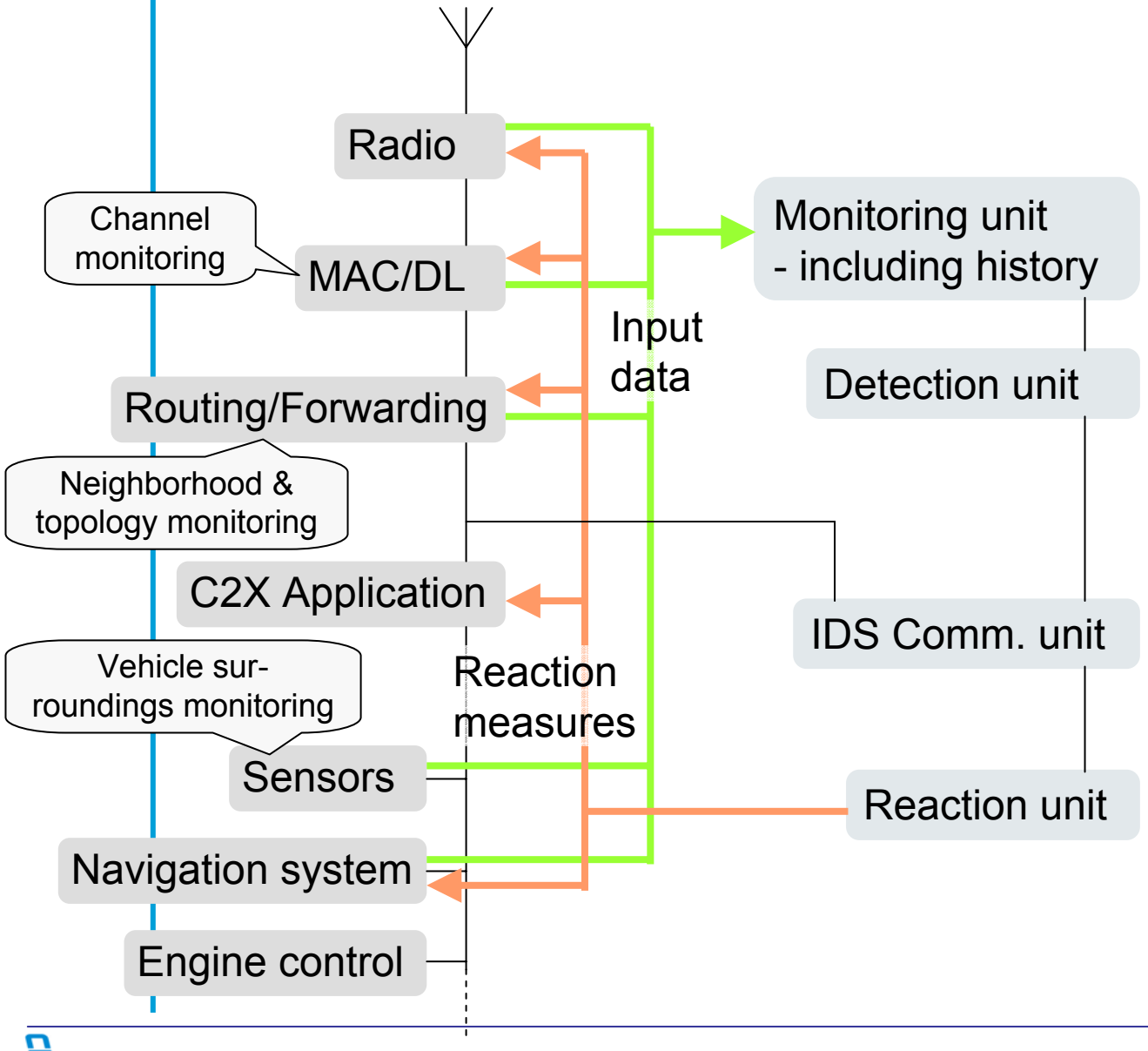
SEVECOM

- Work on location cheating (Tim Leinmüller and myself)
  - Detection of false position claims in beacons
  - Up to now, mainly focuses on position dependent routing



- Using sensor aggregation to detect malicious behavior (Golle, Green, Staddon)
- VARS (Dötzer, Fischer, Magiera)
  - Nodes piggyback their opinion on the message when forwarding
  - Different behavior of forwarders, depending on zones (event, decision, distribution area)

IDS architectural approach



- Monitoring per module
- Continuous detection vs. evaluation on event
- Evaluation depends on module and wanted output
- Local, regional, global detection
- Reaction totally depends on detected action
- May include several parts of the system

Particular questions in VANETs

SEVECOM

- Extreme topological diversity (time and space)
  - Fast changing scenarios due to high node mobility
  - Number of nodes in wireless transmission range may vary from zero to dozens or even hundreds
  - → Hard to make assumptions, IDS mechanisms may have to be continuously adapted to context
  - → Too much communication does not make sense
- V2V applications
  - Some messages need to be validated almost in real-time
  - Receivers may have completely different context as sender
- In-Vehicle systems
  - Depending on function, need strong protection

Particular questions in VANETs

SEVECOM

- Autonomous system action
  - No administrator, no user interaction
- Dependability of vehicles
  - “False positives” need to be minimized as well
    (do not accuse regular vehicles including detection of attempts to maliciously modify the reputation of vehicles)
- Privacy of drivers
  - Monitoring collects data that might be abused

Conclusion

- Proactive security is important – but is also limited
- Intrusion detection is indispensable as a complement to prevention
  - Maybe IDS will also need some support by proactive security

Network intrusion detection
- Validate application messages
- Detect communication disturbance/misuse including forwarding, medium access and physical layer

In-vehicle intrusion detection
- Validate sensor readings
- Detect corrupted system state/operation

- Existing work is mostly generic or adapted to special scenario
  - Useful, but does not solve many specific requirements in VANETs

Questions?

SEVECOM