Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Flexible Misbehavior Detection using Subjective Logic

CAMP V2X Misbehavior Detection Workshop

7 & 8 Nov. 2016, Farmington Hills, USA

Rens van der Heijden

Outline

- Motivation
- Subjective Logic
- Maat: a framework for misbehavior detection
- Advantages of subjective logic
- Wider implications

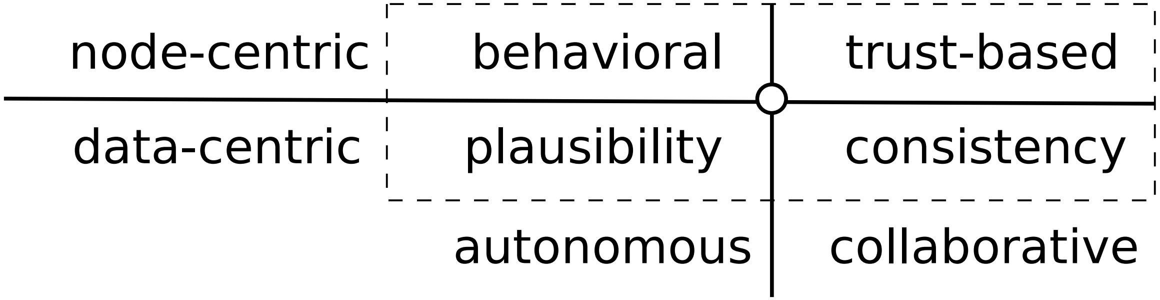
Motivation: Attackers

- Data/application oriented (-> standard IDS fails)
- Cyber-physical systems & attacks
- More accessible (vs. SCADA)

Motivation: Orthogonal Mechanisms

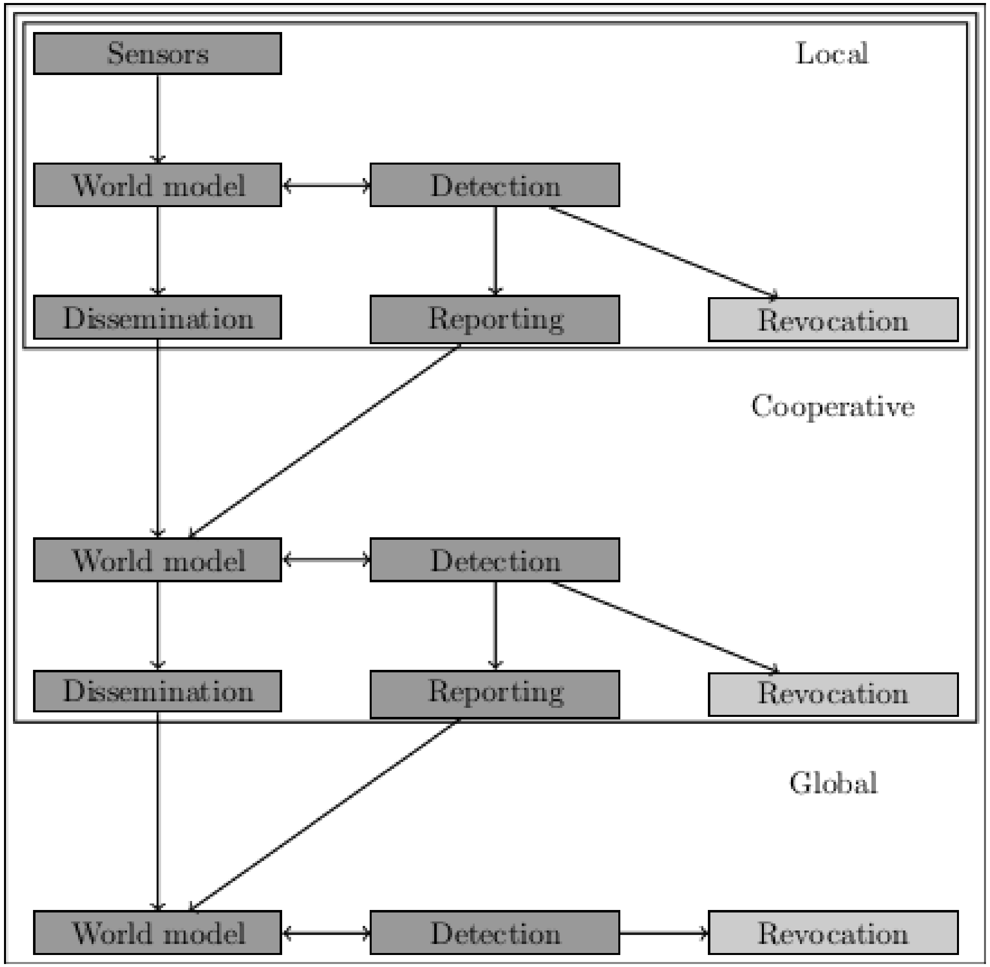
- Variety of attacks
- Variety of detection mechanisms
- Detection mechanisms often designed for specific attacks.

Survey: Taxonomy



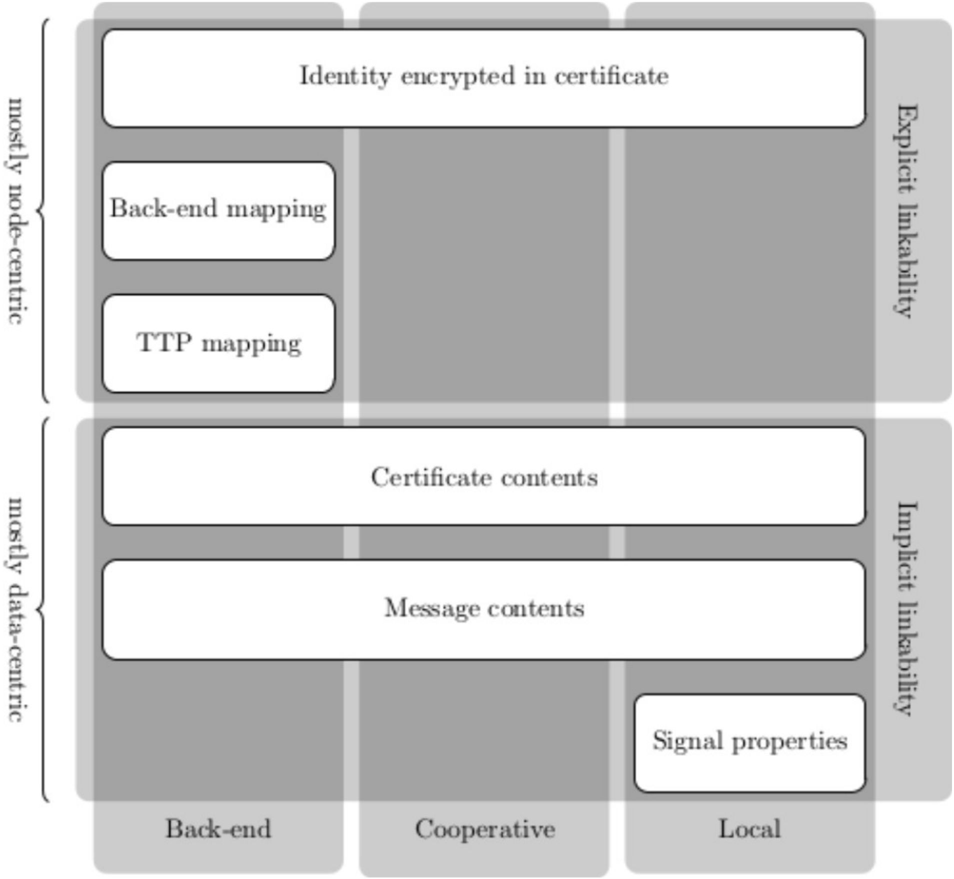
https://arxiv.org/abs/1610.06810

Survey: Local, Cooperative & Global Detection



https://arxiv.org/abs/1610.06810

Survey: Pseudonym Linkability



https://arxiv.org/abs/1610.06810

Motivation: Potential of Fusion

- Exploit orthogonality
- Filtering false negatives
- Combine tenative evidence
- Extensibility

http://ieeexplore.ieee.org/document/6918989/

Motivation: Situational Dependencies

- Mechanisms designed for traffic scenarios

- Example: urban vs. highway traffic

- Traffic jam vs. empty road

http://namnatulco.eu/work/kuvsfg2014-paper.pdf

Motivation: Evidence

- Important for SCMS
- Important for pseudonym resolution
- Useful for legal defence (..?)

Motivation: Summary

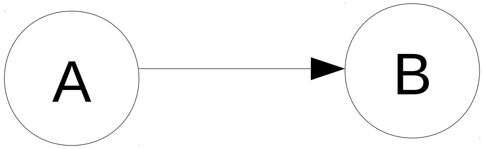
- Literature survey

- Attacker Complexity & Types
- Fusion
- Variations due to Traffic Situation
- Evidence

Subjective Logic: Opinions

- Express probability and uncertainty separately
- Data structure: (subjective) opinion, $o_B^A = (b, d, u, a)$
- Constraints: $(b, d, u, a) \in 0..1$ $b + d + u = 1$

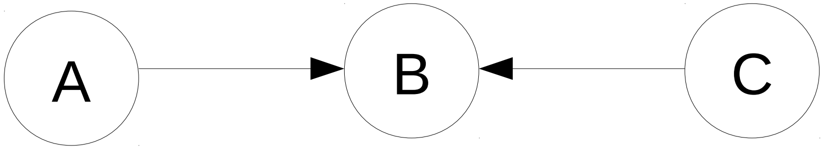
- Event (B) in domain {true, false} and opinion holder (A)
- Graphical representation:



http://www.springer.com/gp/book/9783319423357

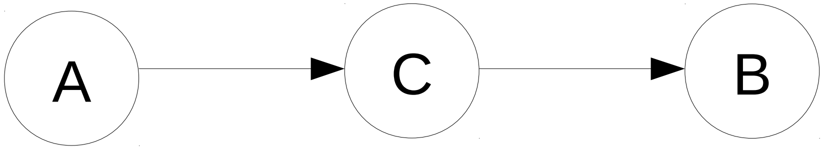
Subjective Logic: Fusion & Transitivity

- Fusion



$$o_B^A \circ o_B^C = o_B^{A,C}$$

- Transitivity



$$o_B^A \circ o_B^C = o_B^A$$

Subjective Logic: Logical Operators

- Boolean logic operators extend to SL

- Useful for expressing relations between (binary) events

Subjective Logic: Multinomial & Continuous Opinions

- Extends the domain of events
- Represents traffic density class (multinomial) or speed (continuous)

$$o_B^A = (b_1, b_2, \dots, u) \qquad u + \sum_i b_i = 1$$

$$o_B^A = (B, u) \qquad u + \int B = 1$$

Subjective Logic: Summary

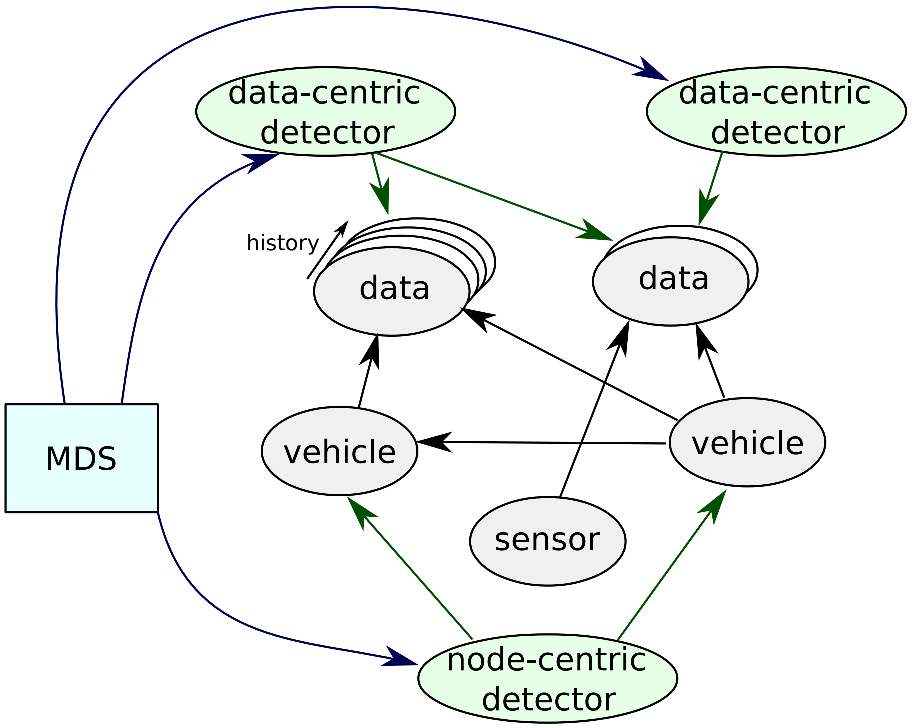
- (Subjective) Opinions
- Fusion Operators
- Transitivity
- Logical Operators
- Mutlinomial & Continuous Opinions

Maat: A Framework for Misbehavior Detection

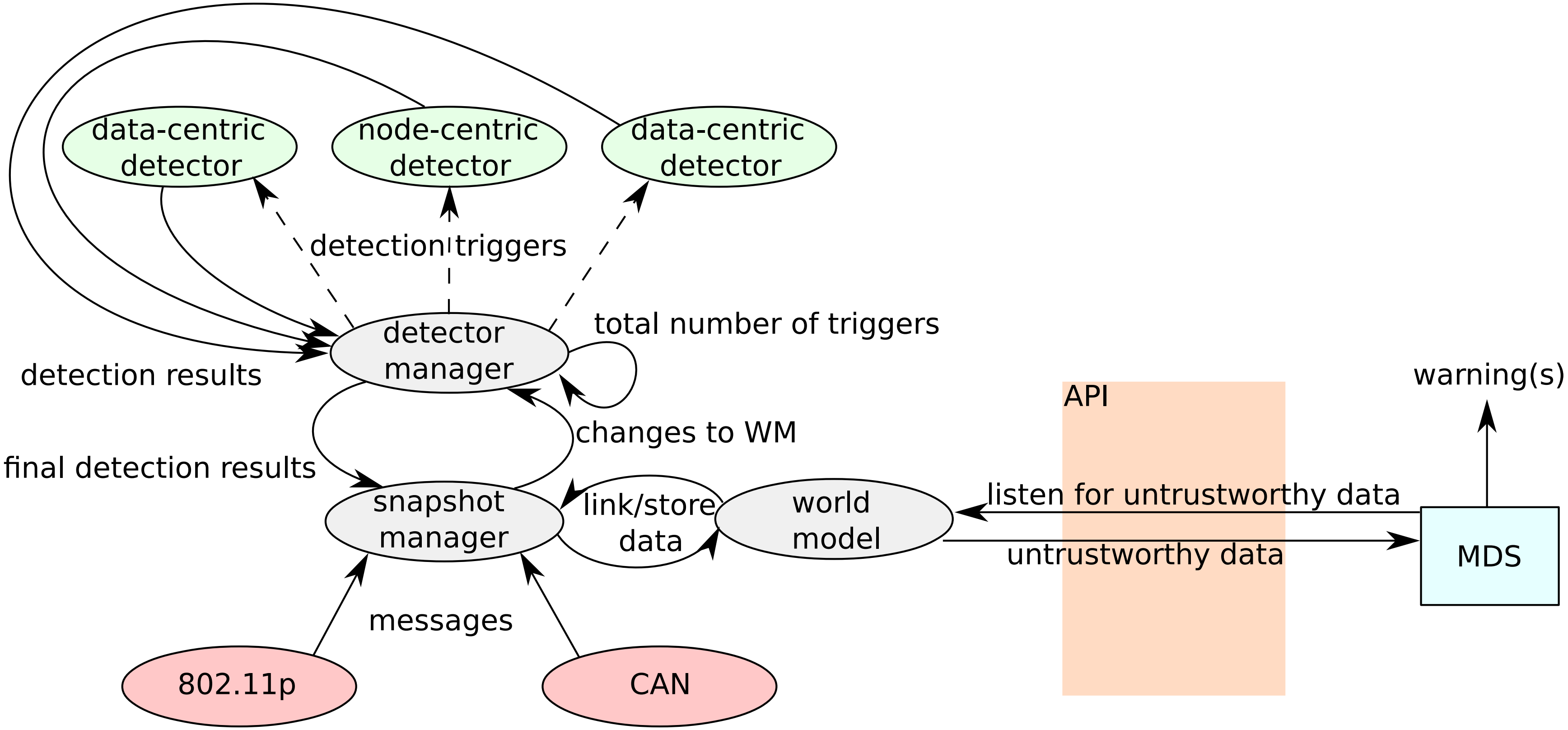
- Use subjective logic to maximize detector performance
- Based on graphical representation
- Exploit detector orthogonality
- Base idea: express data correctness, not attack probability
- Store data to use as evidence

http://ieeexplore.ieee.org/document/6918989/

Maat: Graphical Data Model



Maat: Computational Model & Detector Integration



Maat: Data access

- API for data access (please note: concept is WIP...)
- Graph traversal to determine trust
- Database indices for range queries & caching results
- Optionally: “historical queries”

Maat: Reconfiguration

- Adding new detectors is easy

- Several approaches for dealing with configuration:
  - Repeated computation
  - Parallel execution & subjective logic

Maat: Evidence Exchange

- Idea: send subsets of the model to other nodes
- Requires ‘evidence storage’ (EDR or record of messages)
- Potentially large data volumes
- Reproduce results

Maat: Summary

- Data Model
- Integration of Existing Detectors
- Reconfiguration
- Evidence Exchange

Opinion Generation

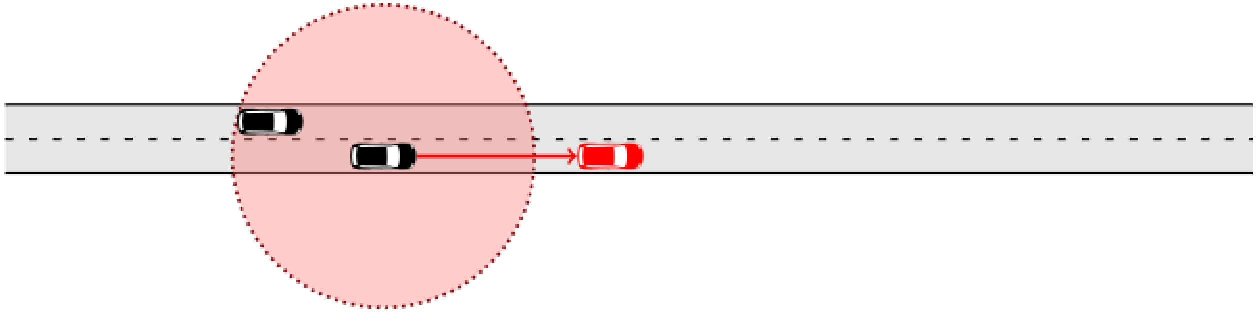
- How do we actually assign belief, disbelief and uncertainty?

- Can we stick with only binary events?

http://namnatulco.eu/work/vanderHeijden2016-VTCFall.pdf

Opinion Generation: Example

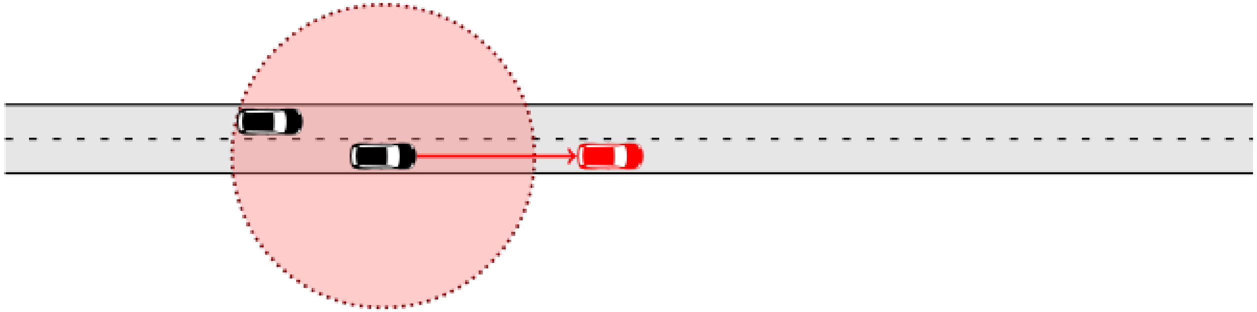
- ART (Leinmüller et al.)



http://namnatulco.eu/work/vanderHeijden2016-VTCFall.pdf

Opinion Generation: Example

- ART (Leinmüller et al.)



$$\omega_{eART} = \left(\frac{\delta}{2\theta} e^{-\frac{|\delta - \theta|^2}{2\sigma}}, \left(1 - \frac{\delta}{2\theta}\right) e^{-\frac{|\delta - \theta|^2}{2\sigma}}, e^{-\frac{|\delta - \theta|^2}{2\sigma}}\right)$$

http://namnatulco.eu/work/vanderHeijden2016-VTCFall.pdf

Fusion

- We examined fusion with a neighbor exchange mechanism

- Conclusion: overall performance higher

http://namnatulco.eu/work/vanderHeijden2016-VTCFall.pdf

Improving Global Misbehavior Detection with Maat

- Evidence Exchange
- Reproducibility
- Large scale graph computation & event sourcing
- Pseudonym resolution
- High detection delay

Improving Local Misbehavior Detection with Maat

- Subjective logic provides increased precision
- Integration with world model approaches
  - Single API for all data
  - Aggregation
  - Include non-V2X data
- Detect misbehaving components

Summary

- Orthogonal detectors
- Subjective logic
- Maat framework
- Opinion generation
- Future possibilities

Thank you for your attention!

How to reach me:

E-mail: rens.vanderheijden@uni-ulm.de

Twitter: @namnatulco

Web: http://namnatulco.eu

ResearchGate

OrcID: http://orcid.org/0000-0003-3280-1825