ulm university universität ulm

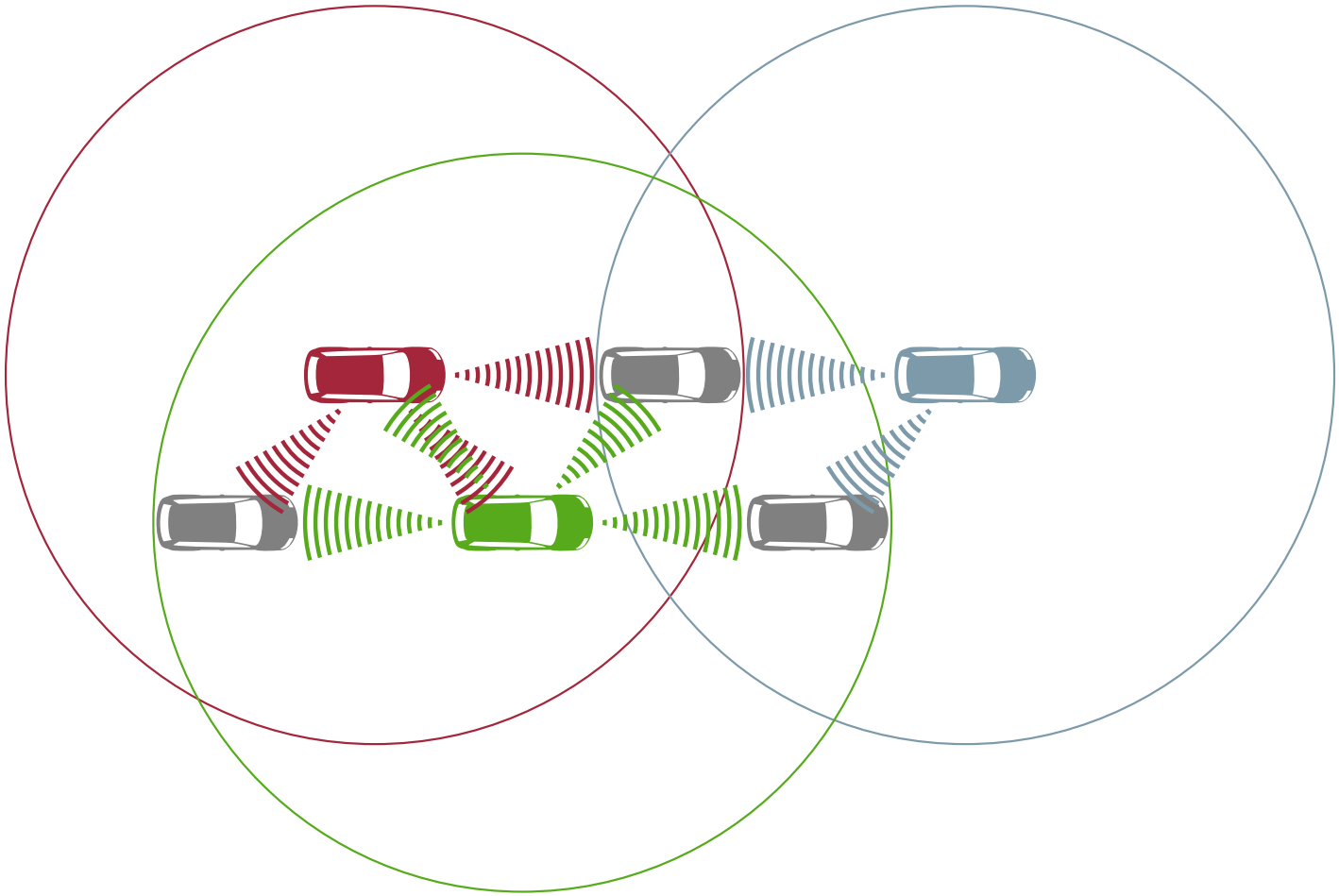
Rens W. van der Heijden, Stefan Dietzel, Frank Kargl

April 18, 2013

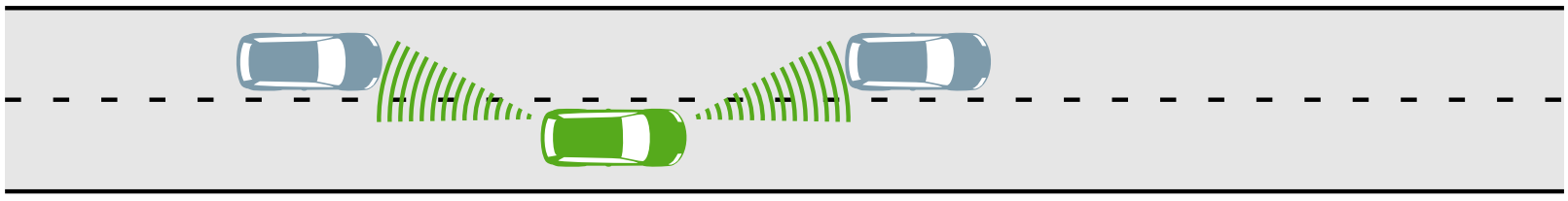
SeDyA

Secure Dynamic Aggregation in VANETs

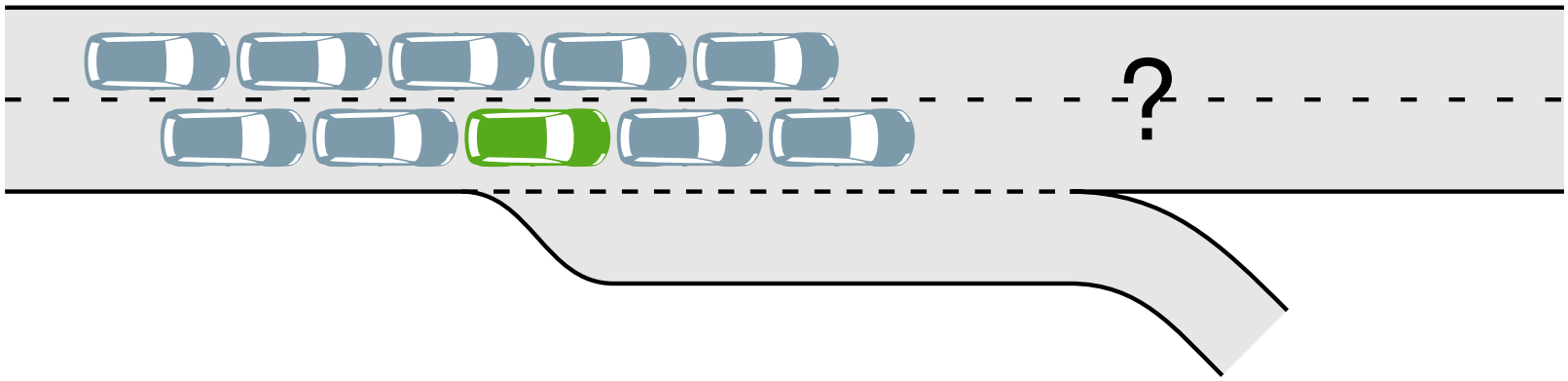
VANETs- a brief introduction



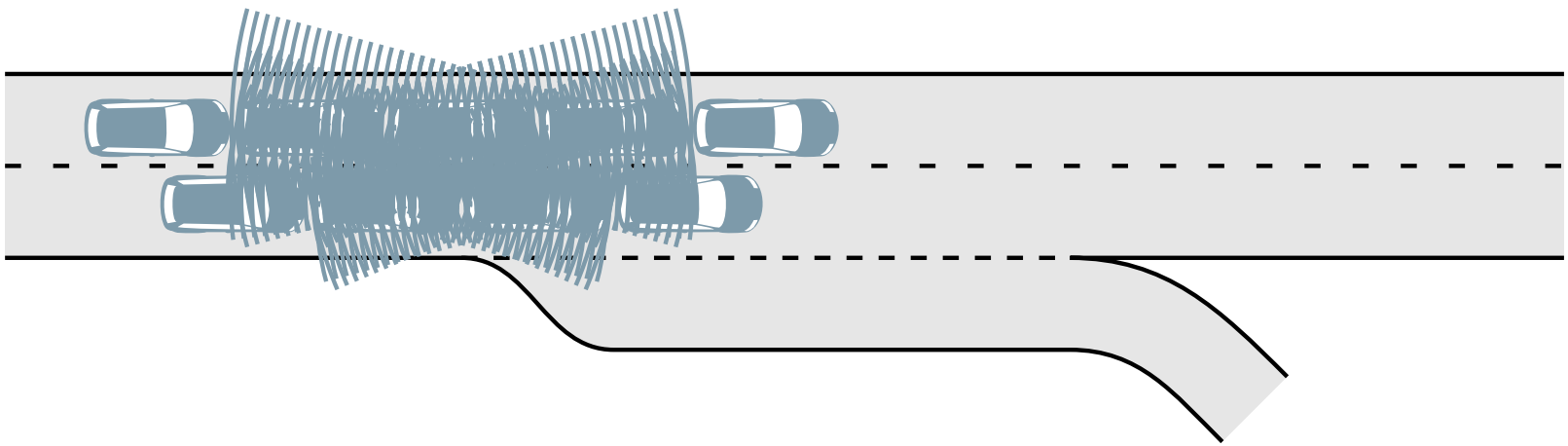
VANETs- a brief introduction



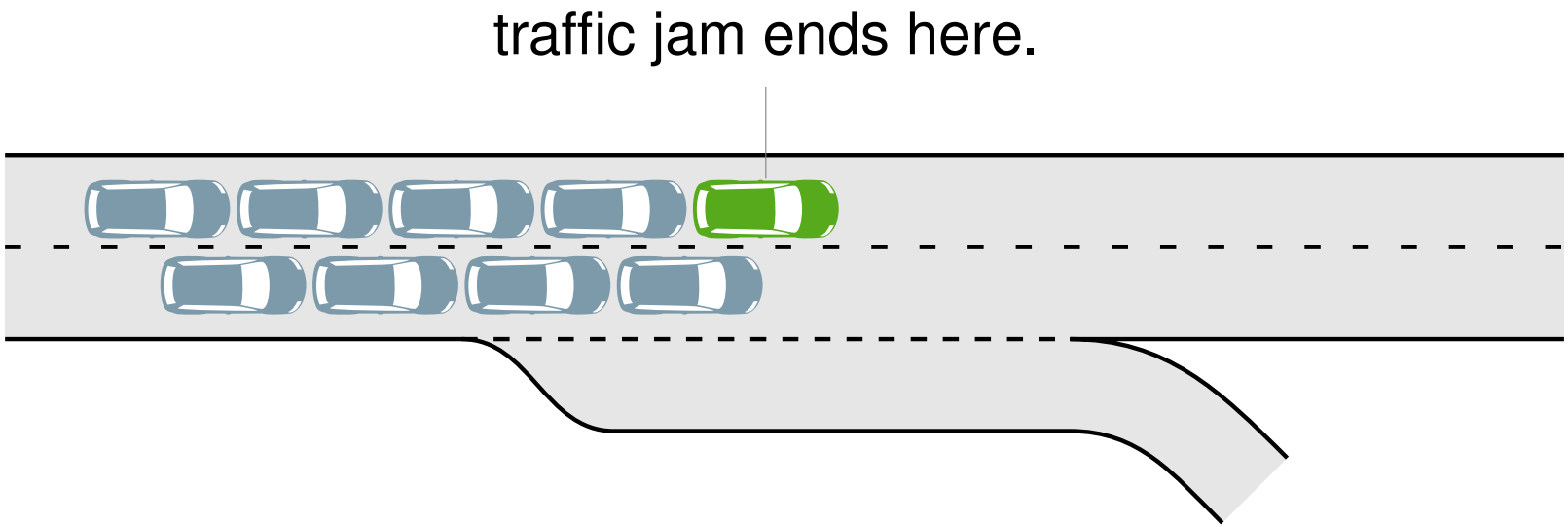
Example use case: traffic jam length



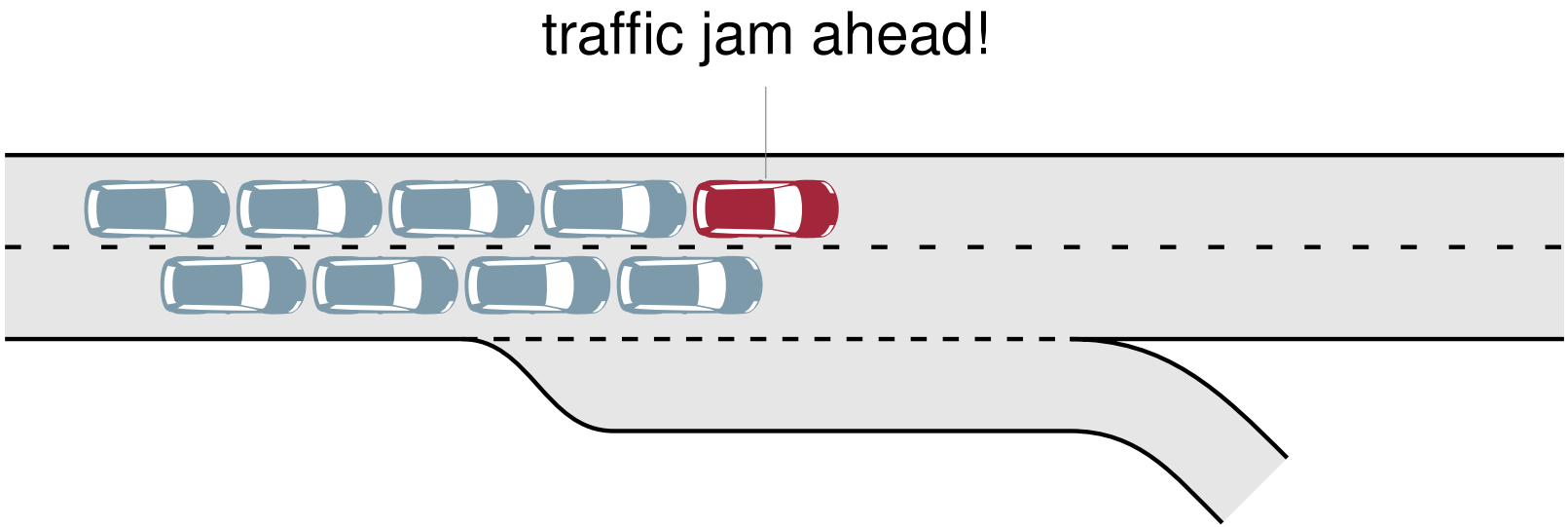
Broadcast Storm!



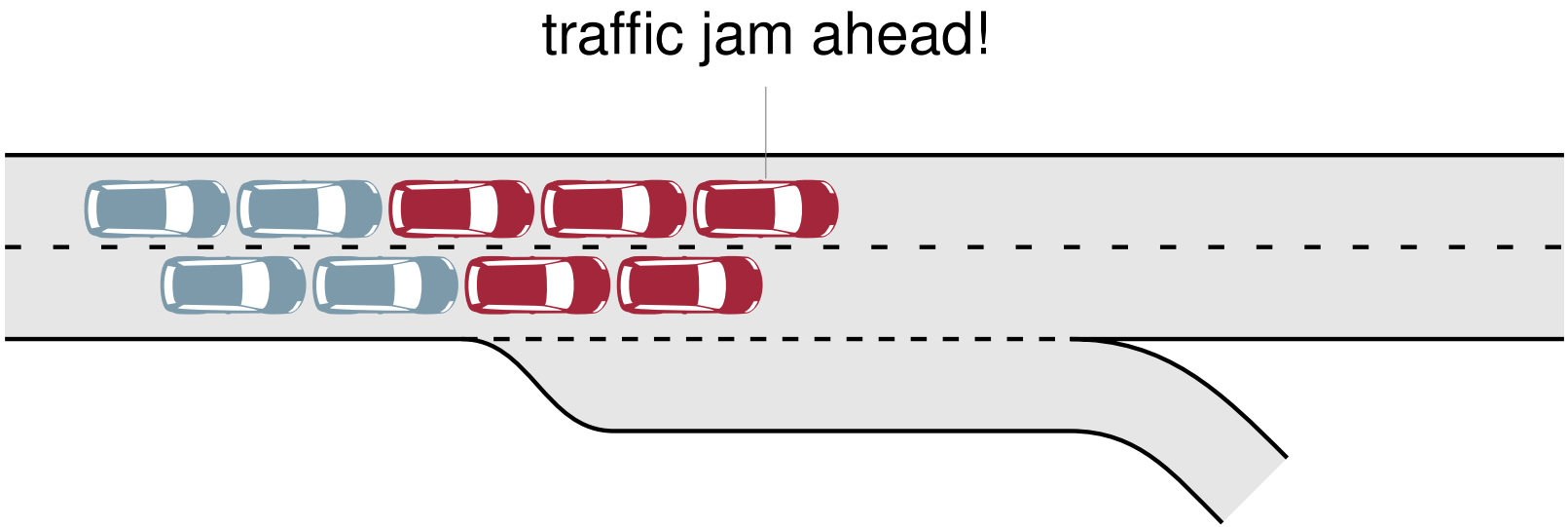
Aggregation- summarizing messages



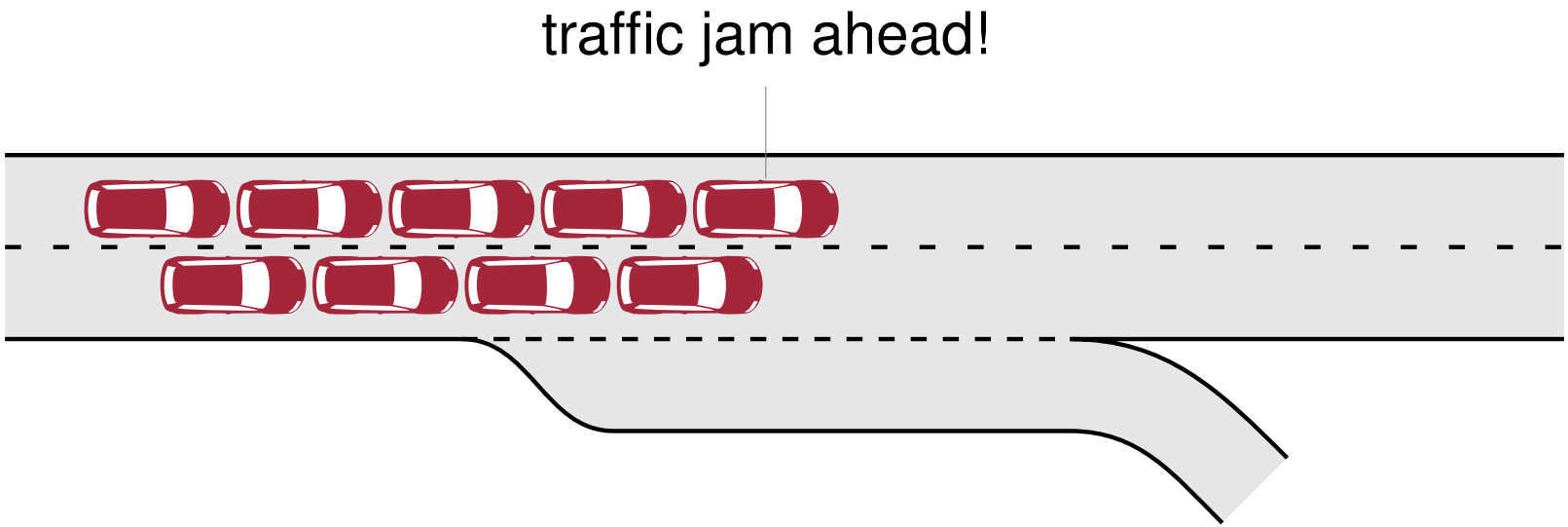
Security- what can go wrong?



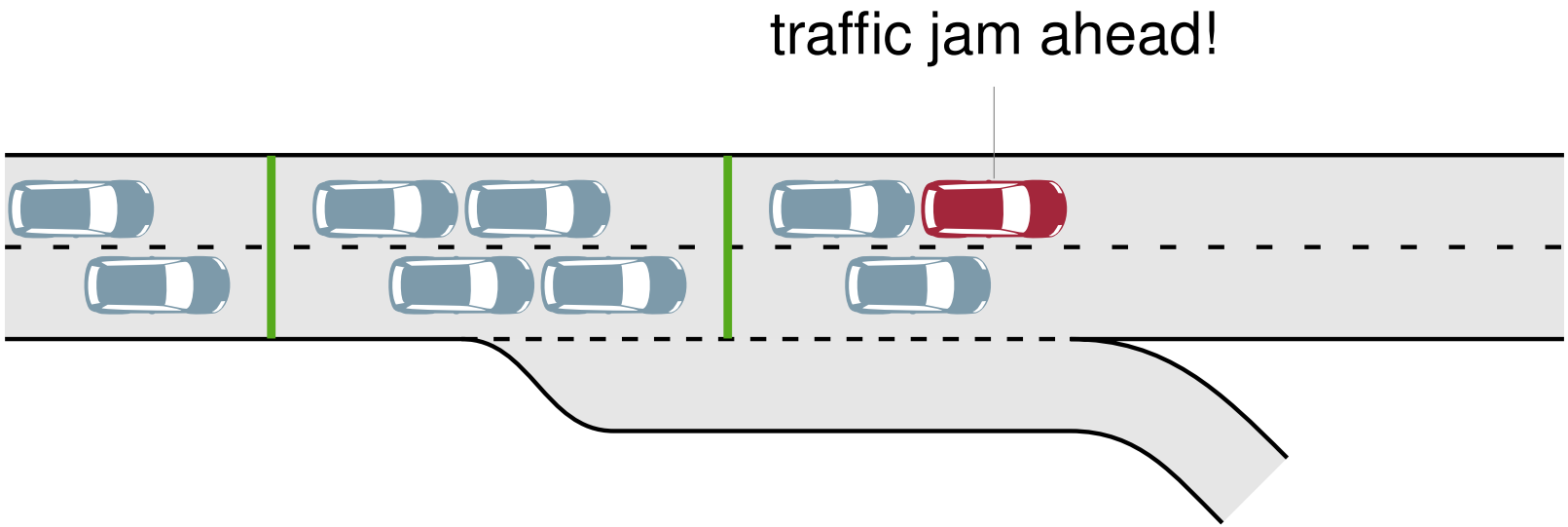
Security- what can go wrong?



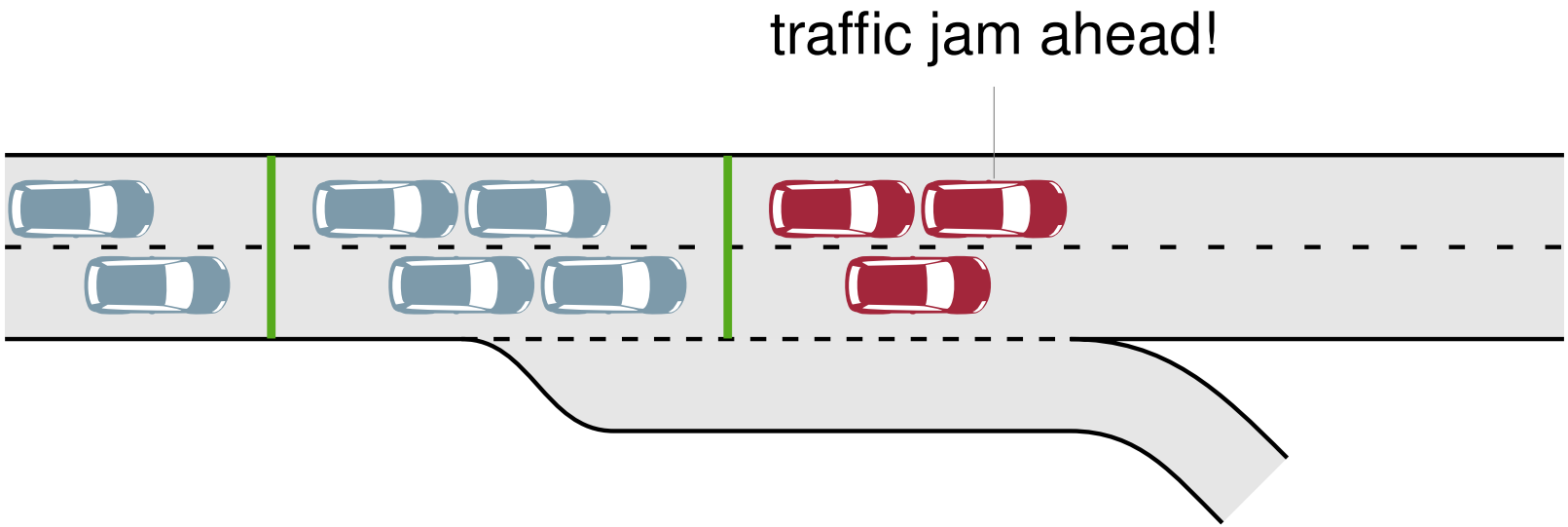
Security- what can go wrong?



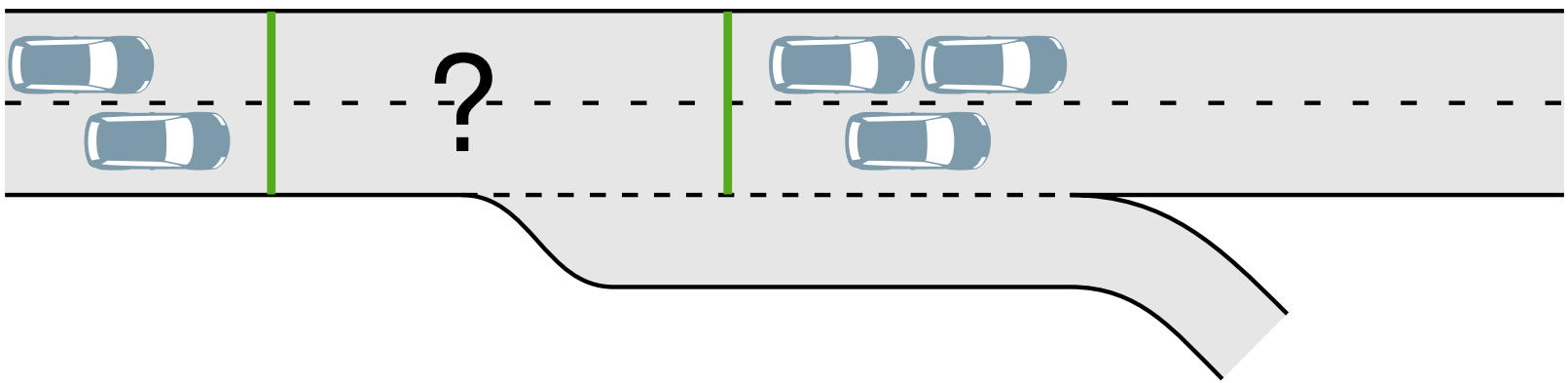
Possible solution- fixed segements



Possible solution- fixed segements



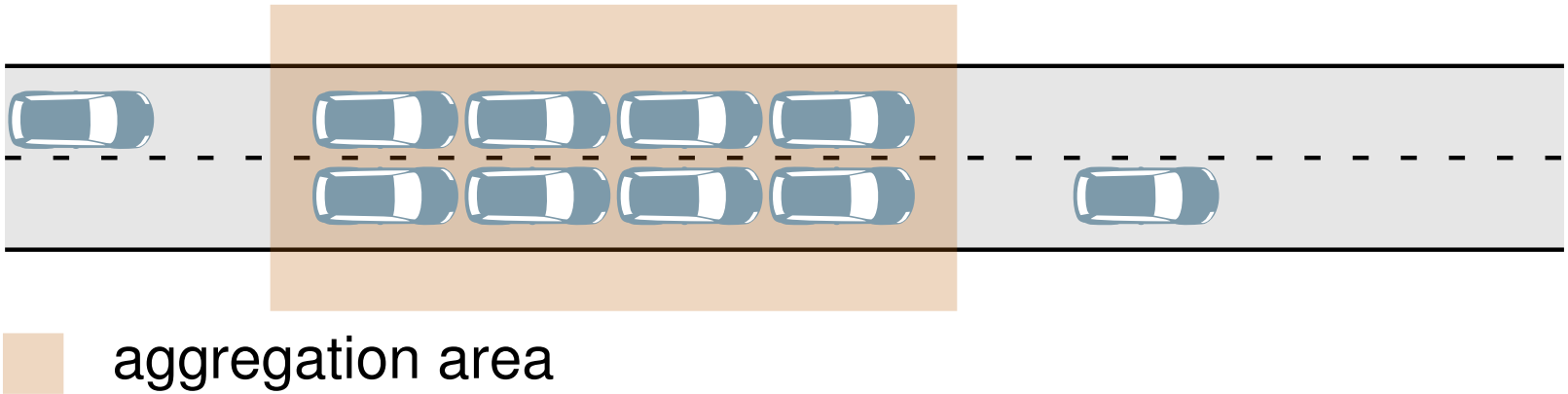
Possible solution- fixed segements



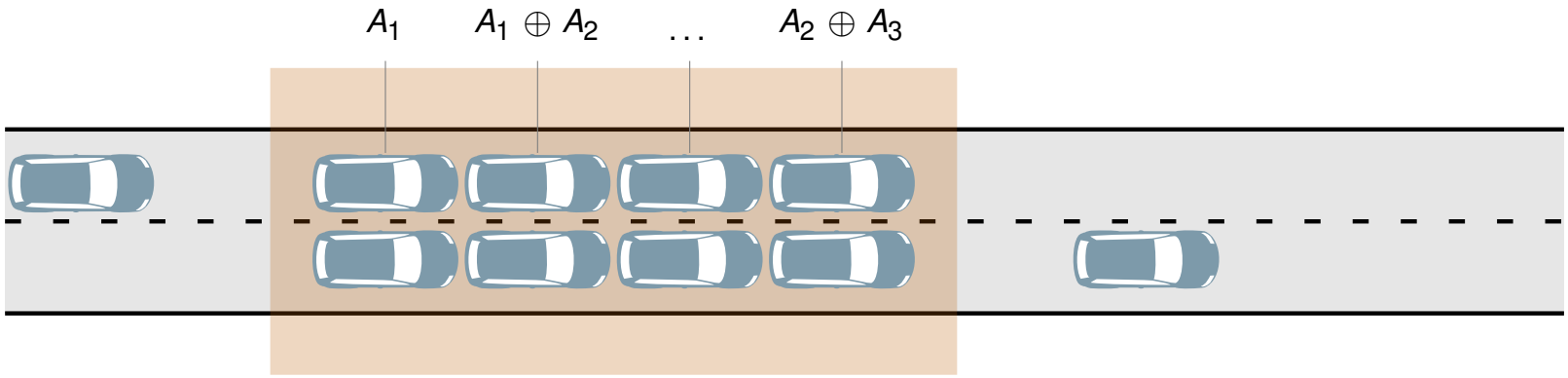
SeDyA

Secure Dynamic Aggregation

Overview

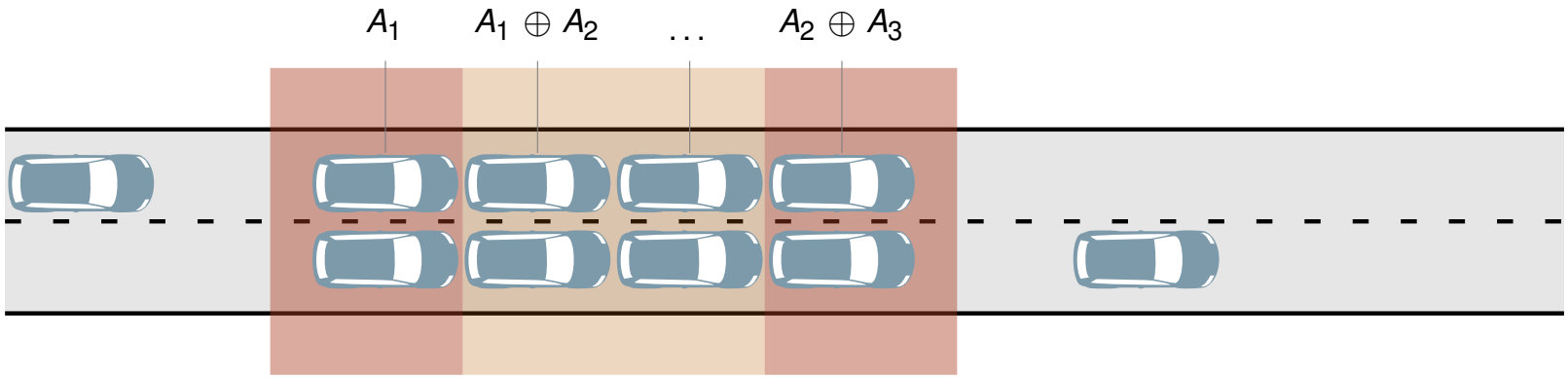


Overview

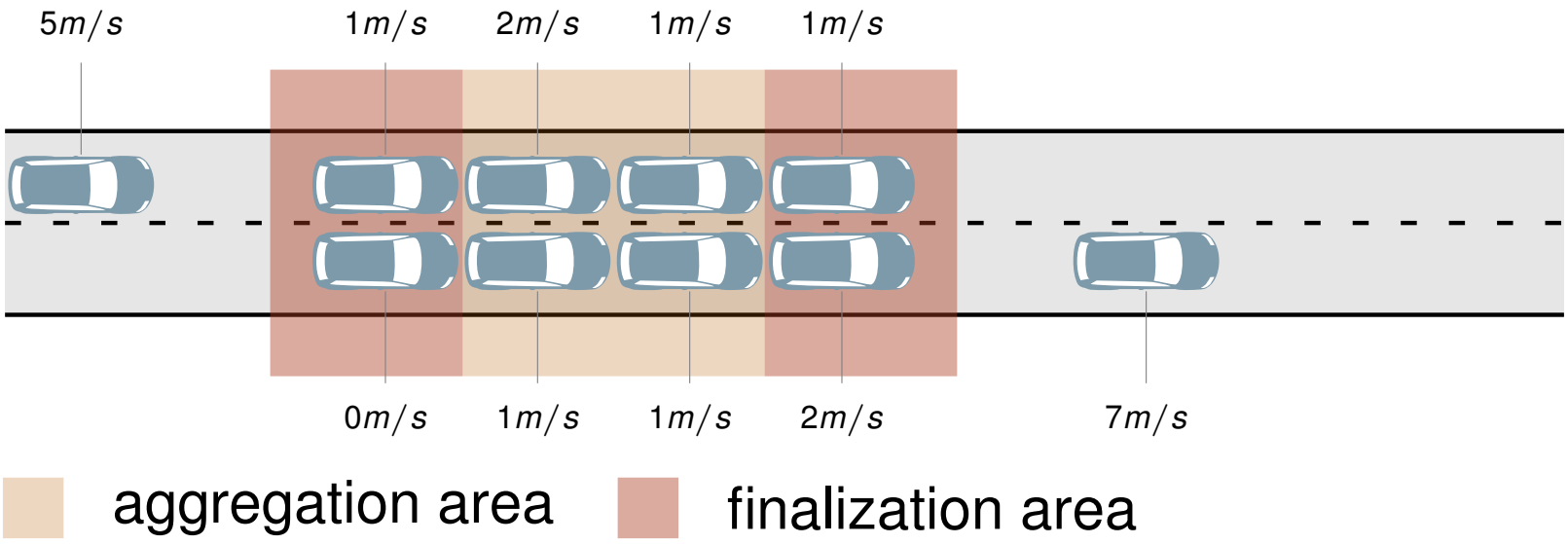


aggregation area

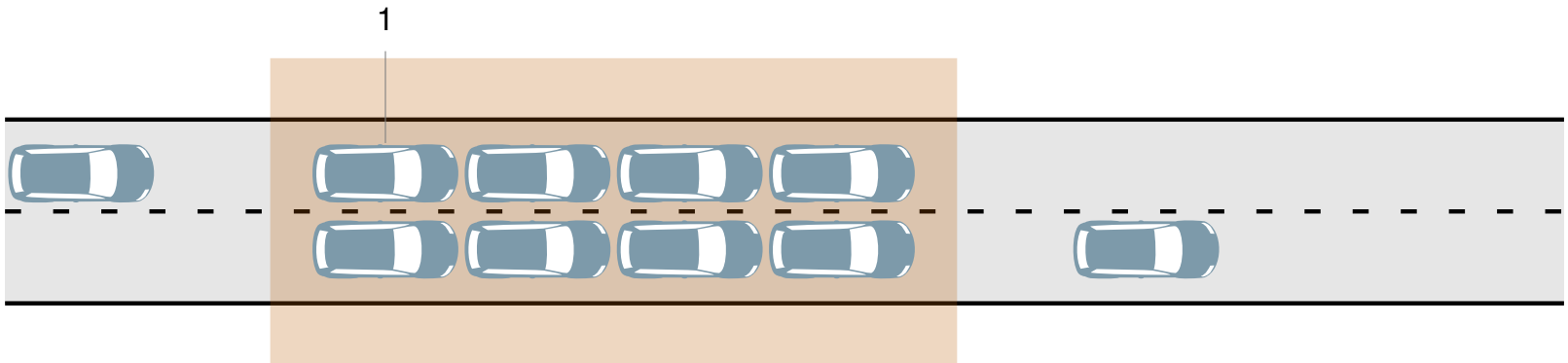
Overview


A_1
$A_1 \oplus A_2$
...
$A_2 \oplus A_3$
aggregation area
finalization area

Scenario

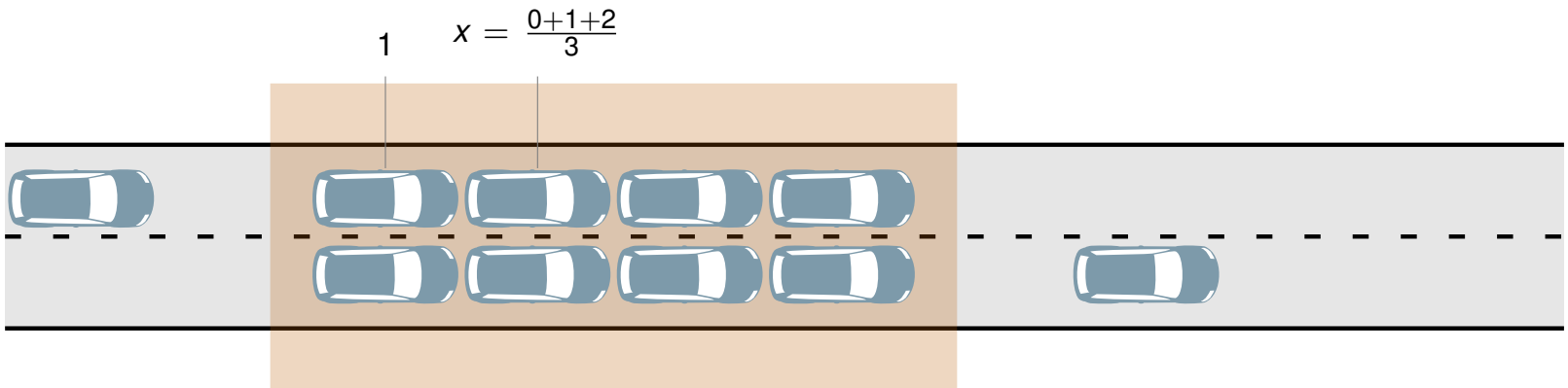

5m/s
1m/s
2m/s
1m/s
1m/s
0m/s
1m/s
1m/s
2m/s
7m/s
aggregation area
finalization area

Phase 1: Aggregation phase



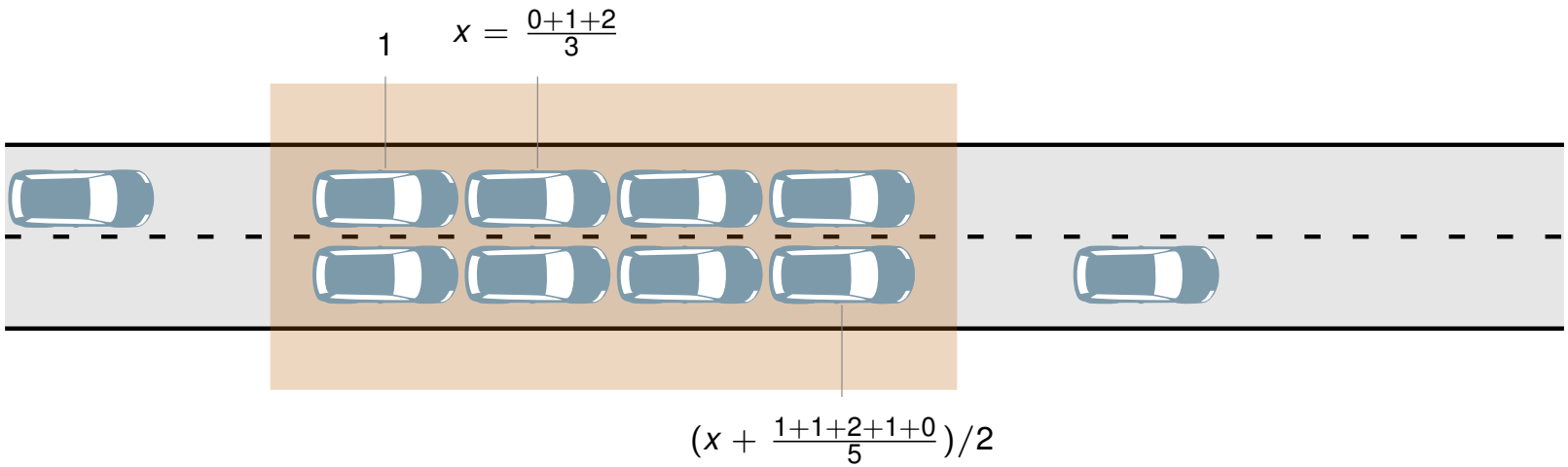
aggregation area

Phase 1: Aggregation phase



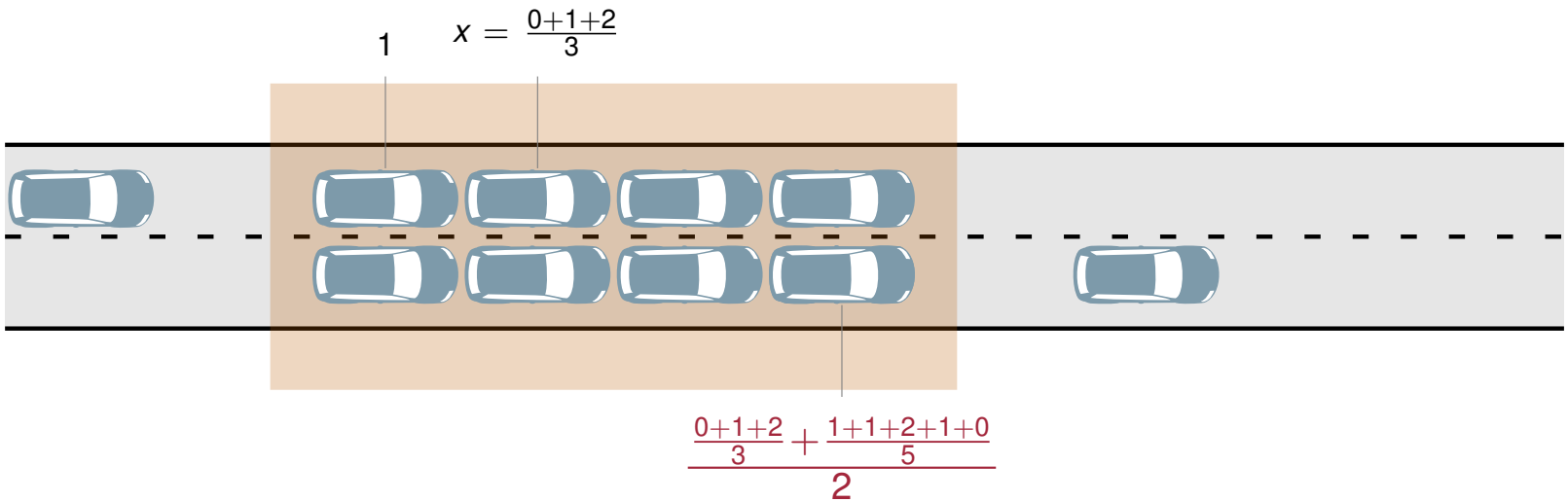
aggregation area

Phase 1: Aggregation phase



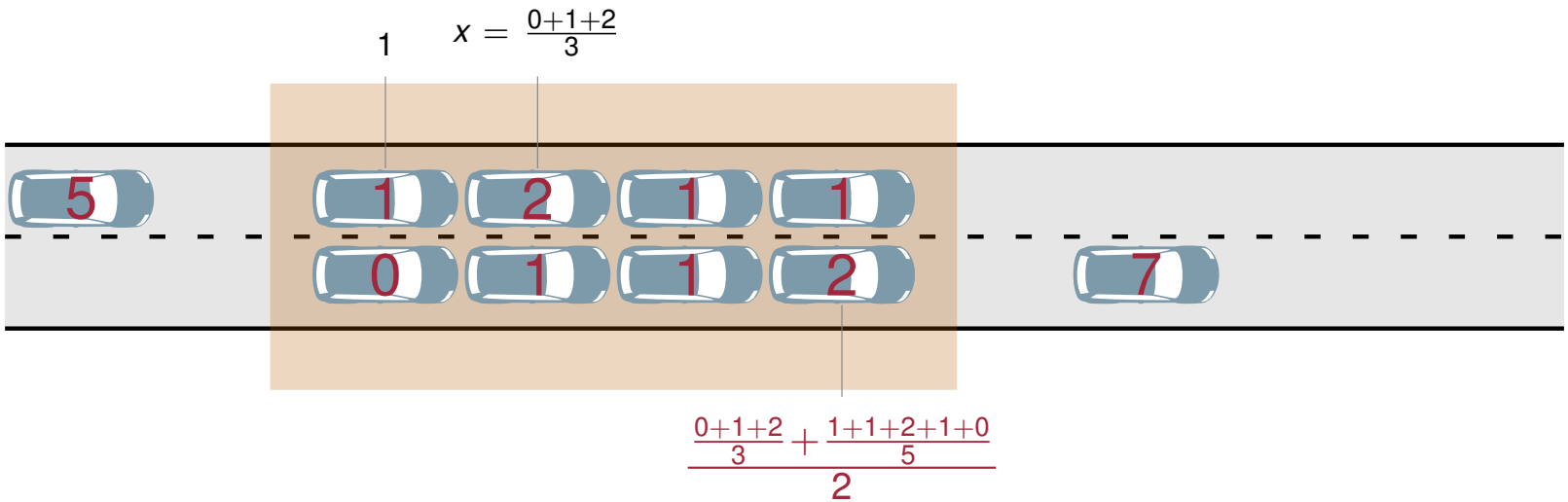
aggregation area

Phase 1: Aggregation phase



aggregation area

Phase 1: Aggregation phase



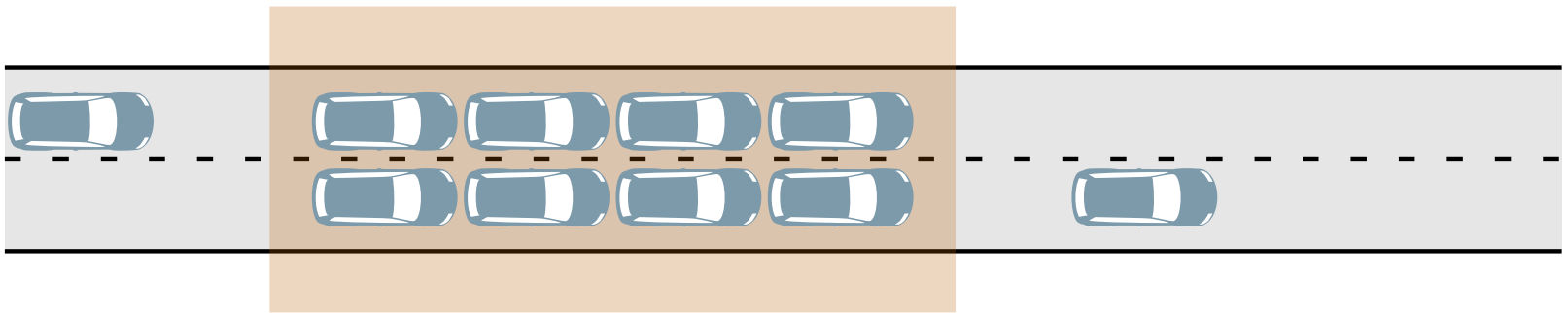
aggregation area

$\rightarrow$ FM sketches

$\rightarrow$ FM sketches $\rightarrow$ duplicate insensitivity

Phase 1: Aggregation phase

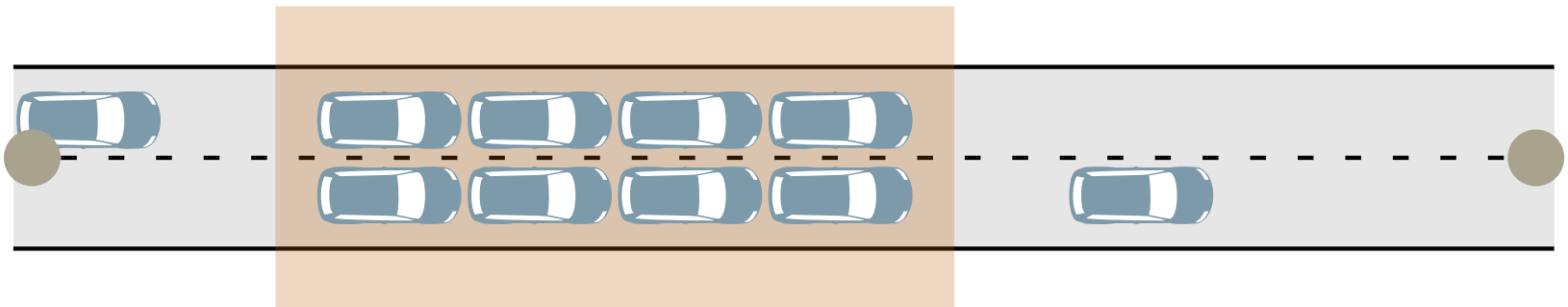
making it ‘dynamic’



aggregation area

Phase 1: Aggregation phase

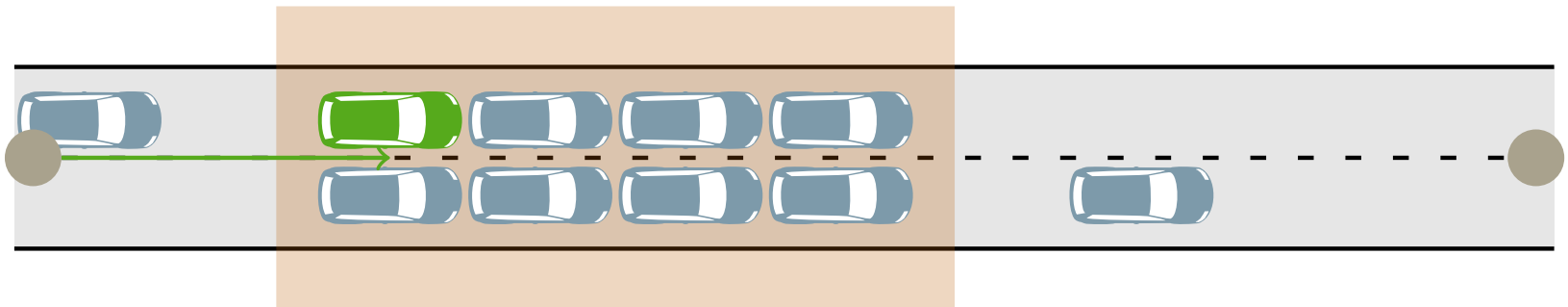
making it ‘dynamic’



aggregation area

Phase 1: Aggregation phase

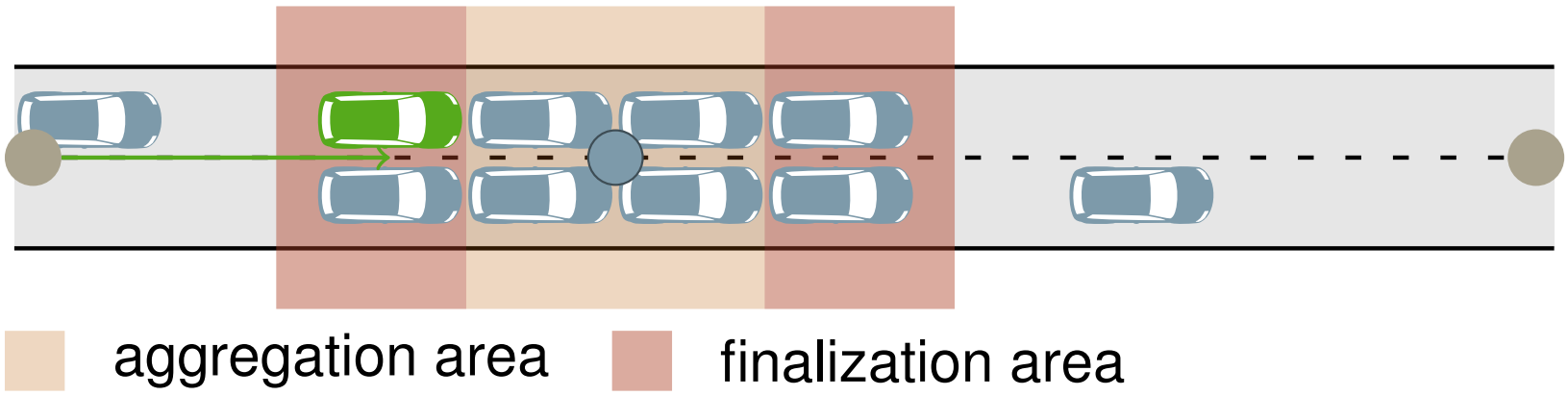
making it ‘dynamic’



aggregation area

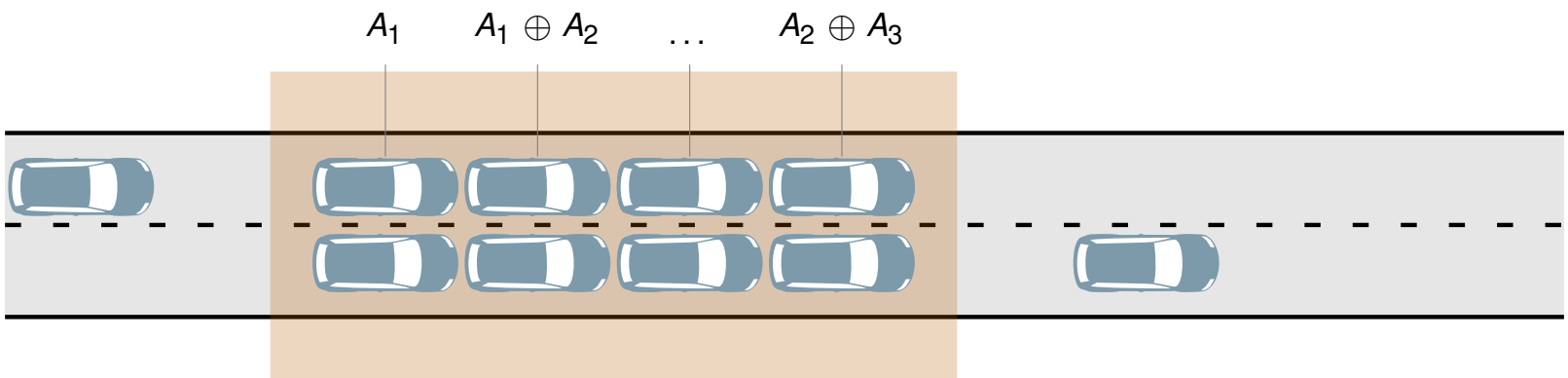
Phase 1: Aggregation phase

making it ‘dynamic’



Overview

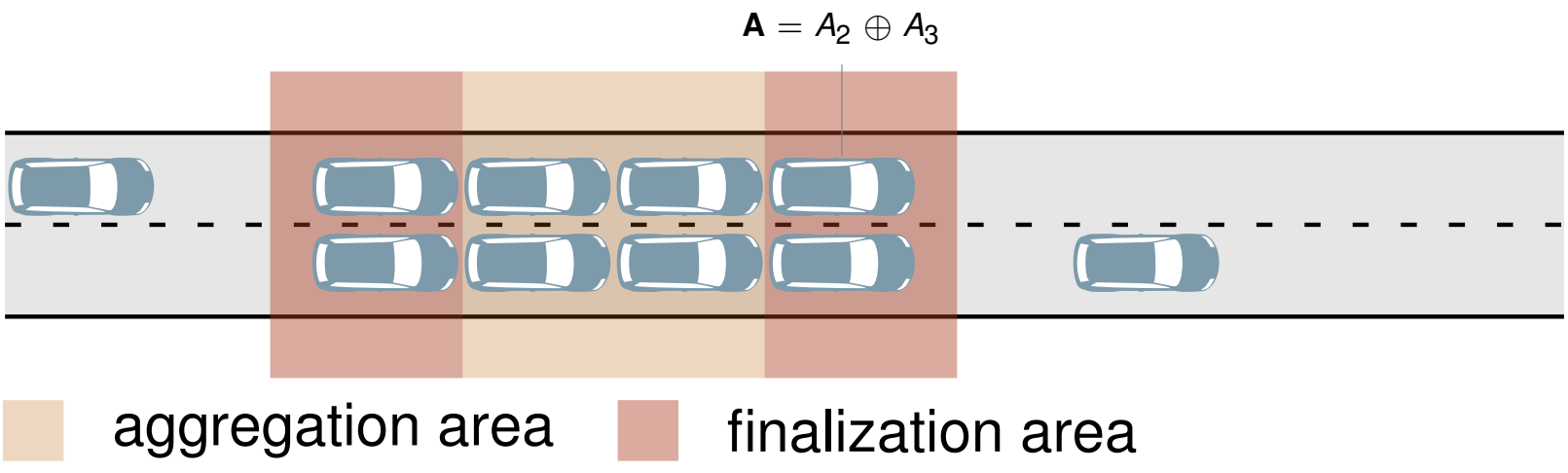
Phase 2: Finalization Phase



aggregation area finalization area

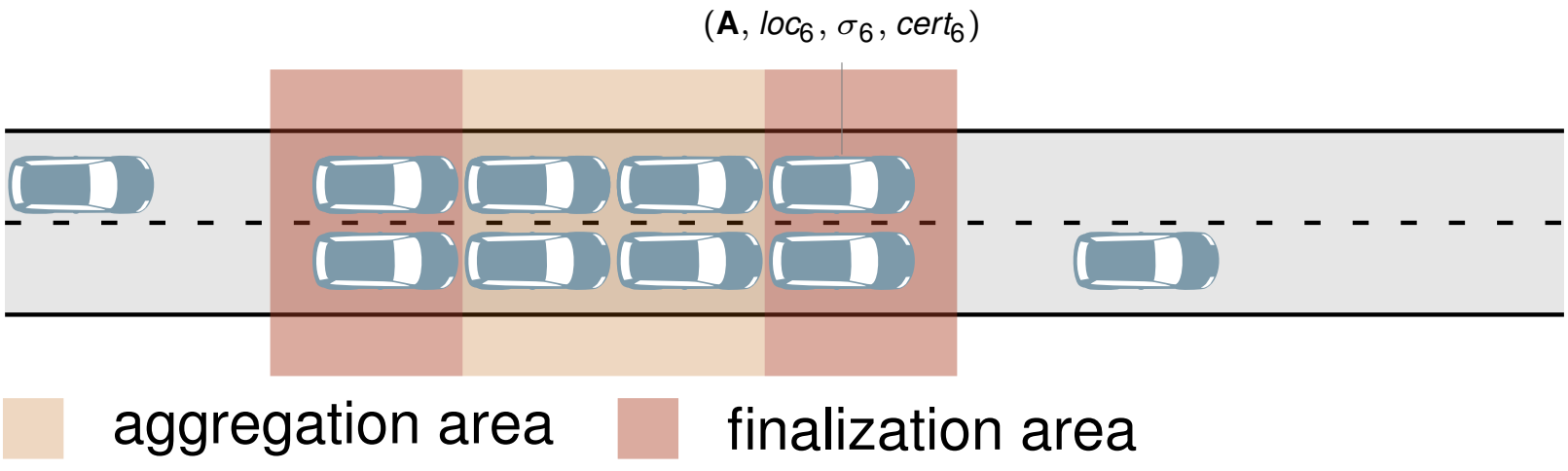
Overview

Phase 2: Finalization Phase



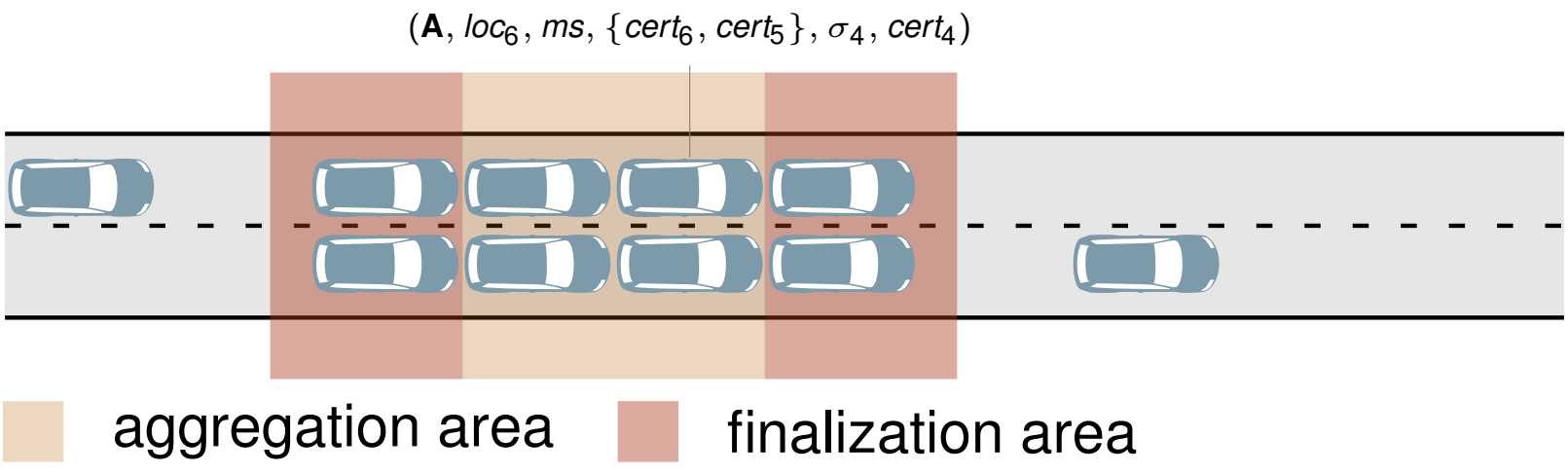
Overview

Phase 2: Finalization Phase



Overview

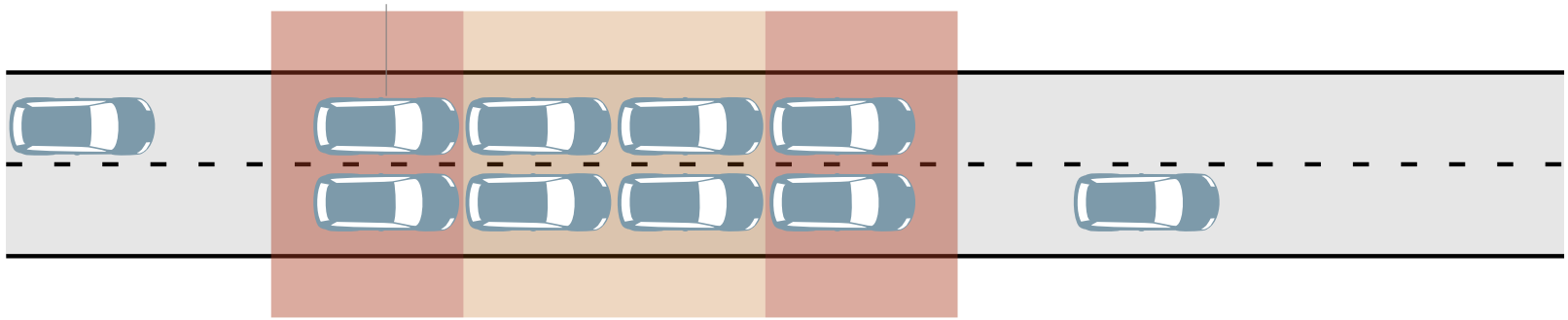
Phase 2: Finalization Phase



Overview

Phase 3: Dissemination Phase

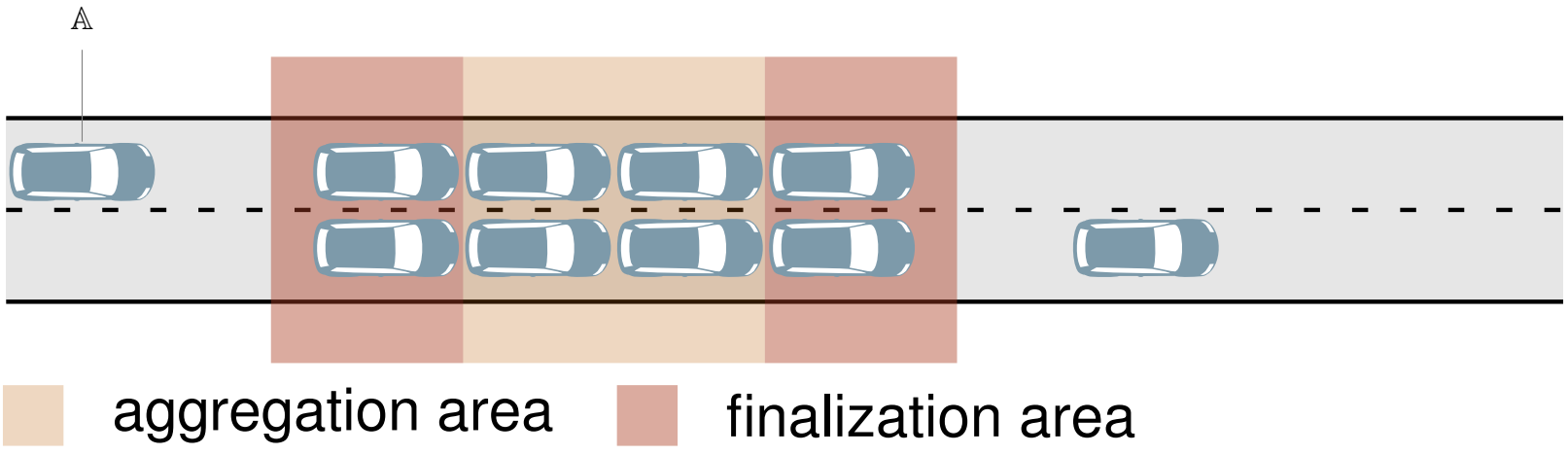
$\mathbb{A} = (\mathbf{A}, loc_6, ms, \{cert_6, cert_5, cert_4\}, \sigma_1, cert_1)$



aggregation area finalization area

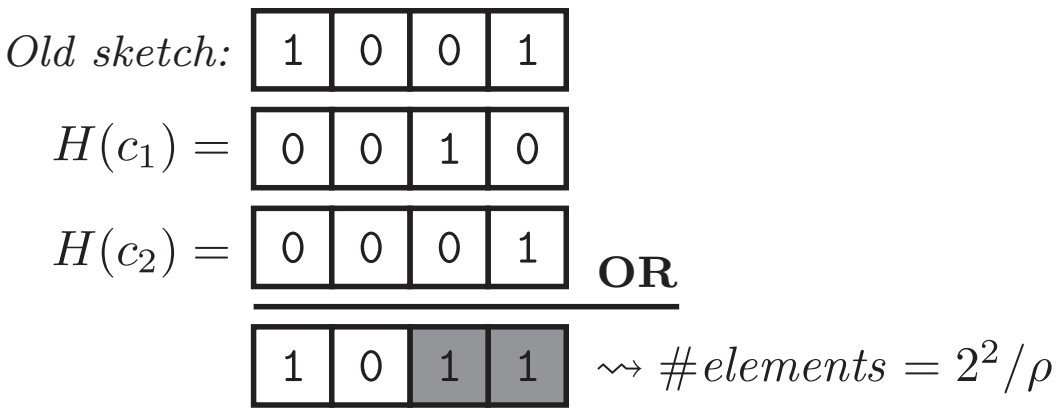
Overview

Phase 3: Dissemination Phase



Aggregation: FM Sketches

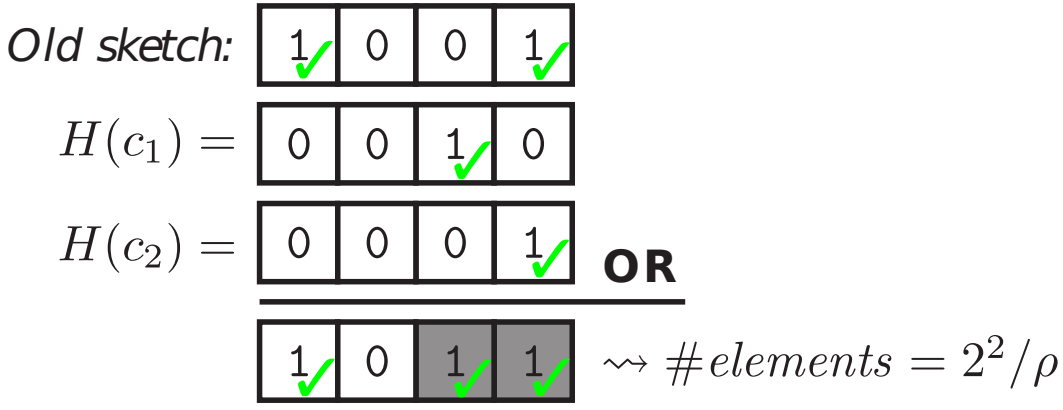
Probabilistic but duplicate-insensitive counting



P. Flajolet and G. Nigel Martin, Probabilistic counting algorithms for data base applications, Journal of Computer and System Sciences, vol. 31, no. 2, pp. 182–209, Oct. 1985.

Related work

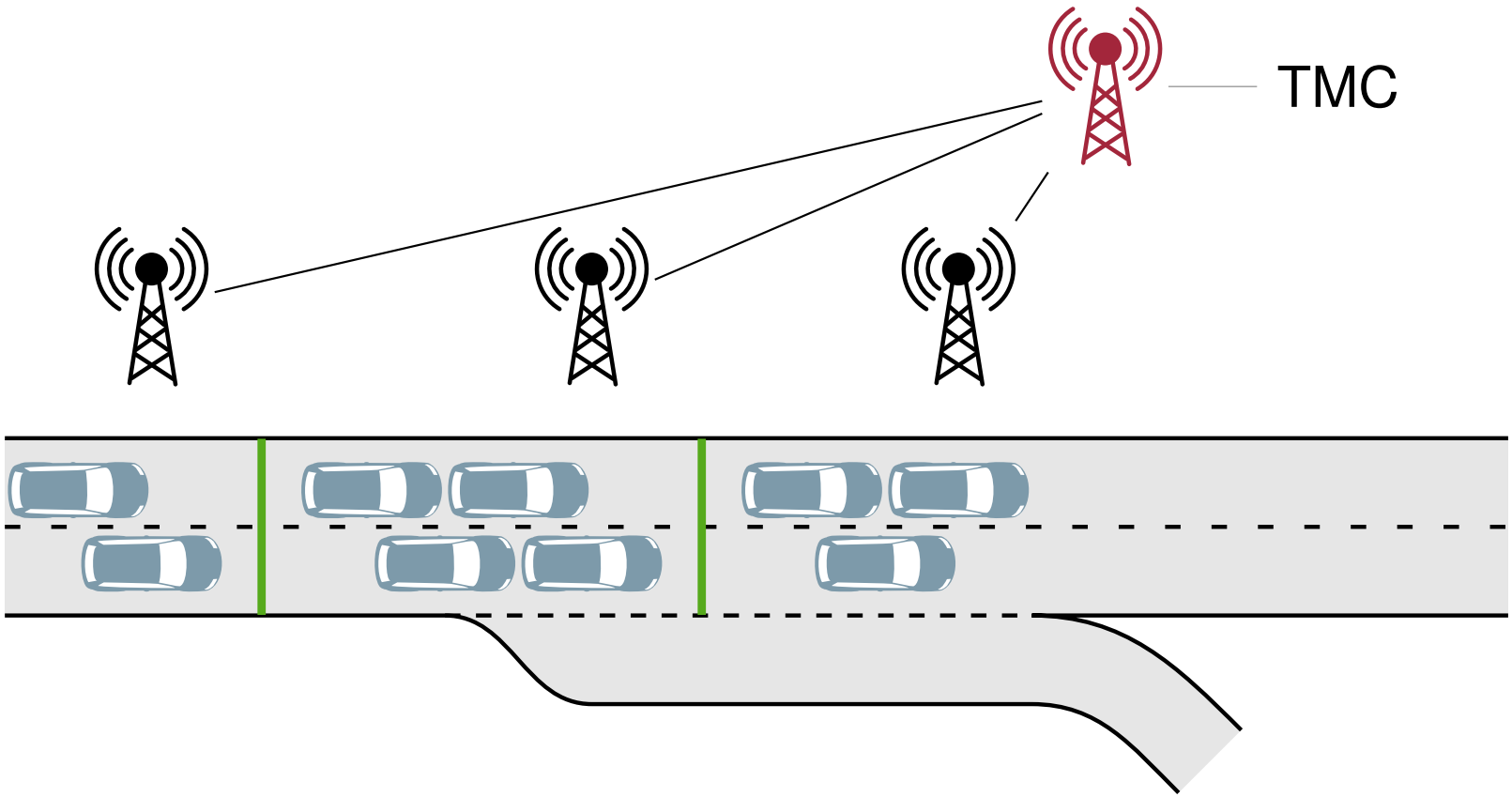
AM-FM sketches



M. Garofalakis, J. M. Hellerstein, and P. Maniatis, Proof sketches: Verifiable in-network aggregation, in 2007 IEEE 23rd International Conference on Data Engineering, page 996-1005, 2007.

Related work

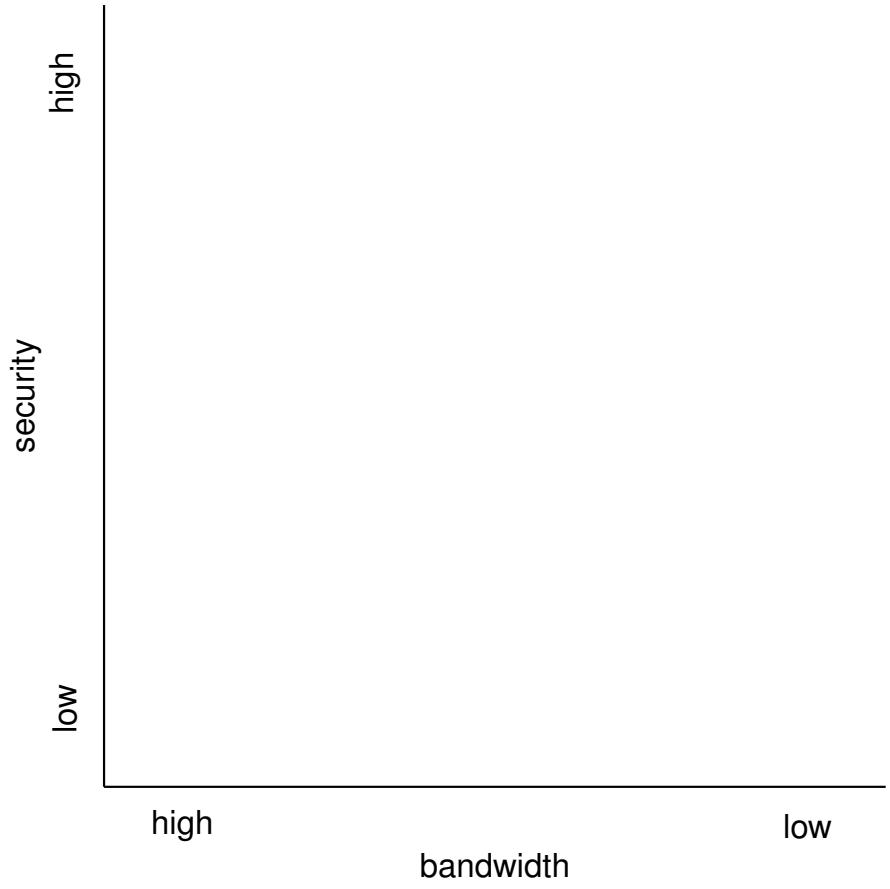
SAS



Q. Han, S. Du, D. Ren, and H. Zhu. SAS: A secure data aggregation scheme in vehicular sensing networks, in 2010 IEEE International Conference on Communications, 2010.

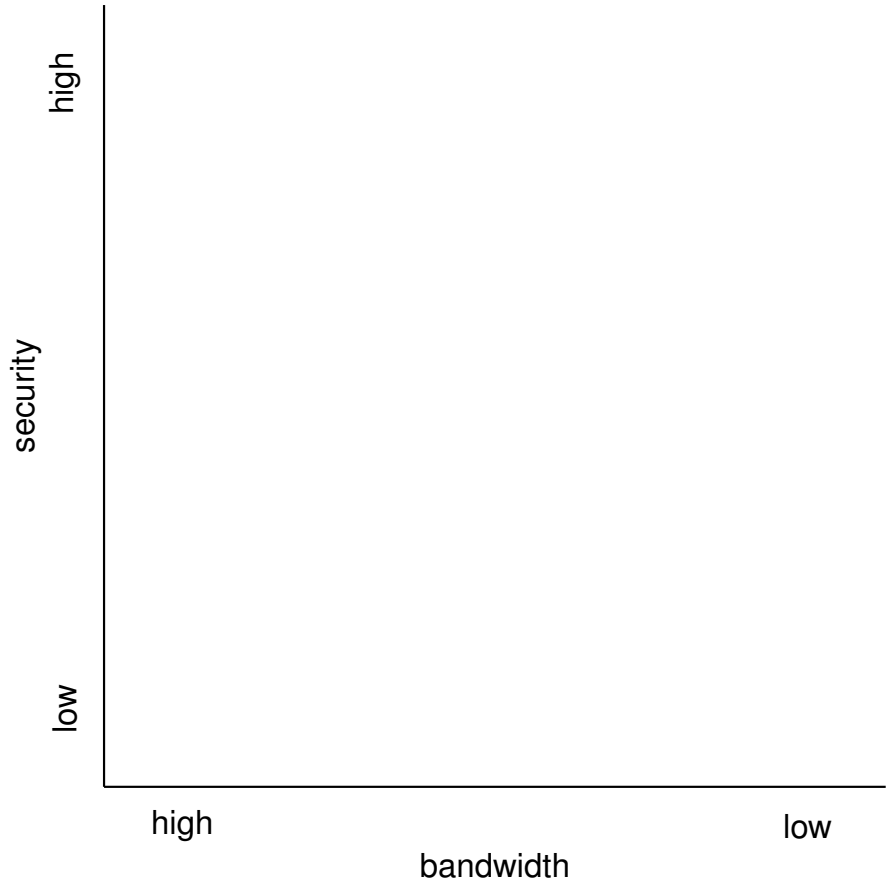
Conclusion

- SeDyA trades-off:



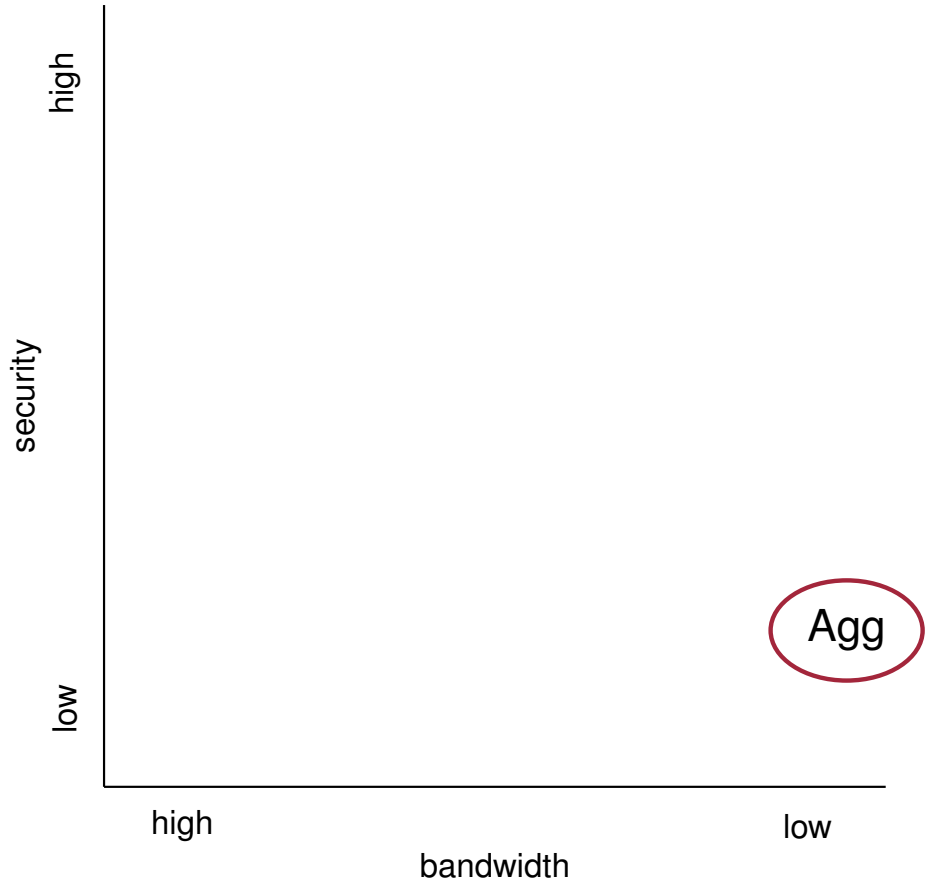
Conclusion

- SeDyA trades-off:
  - Efficiency
  - Security



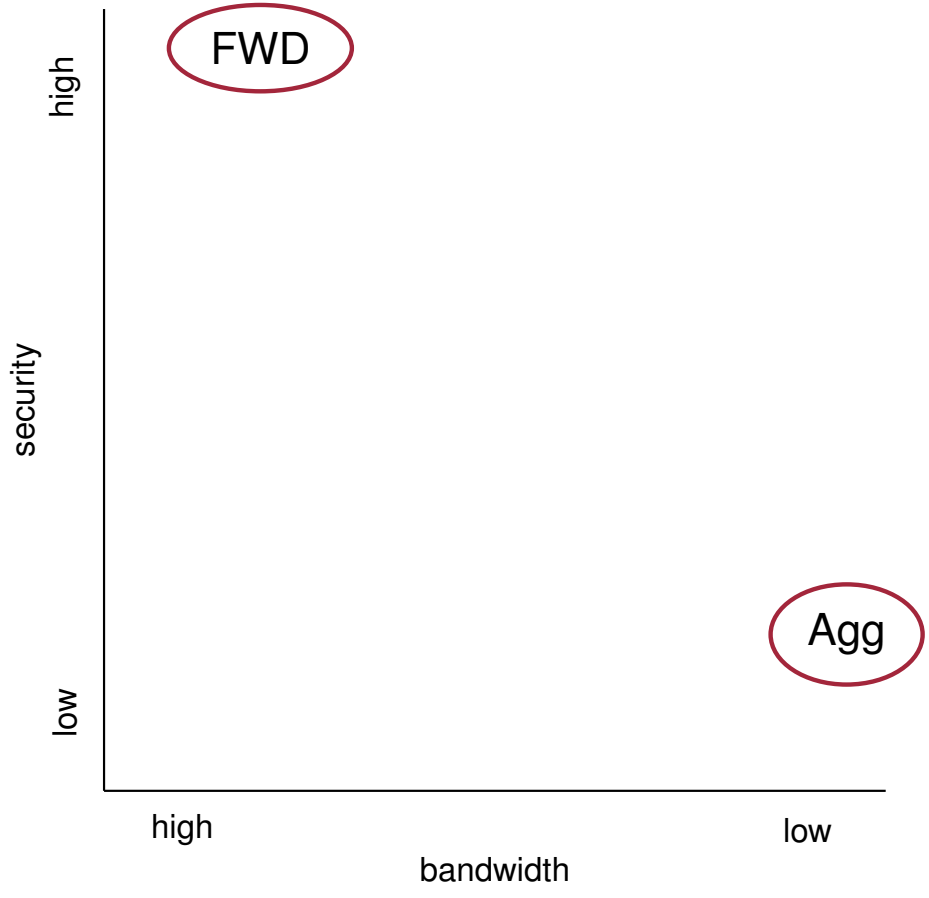
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security



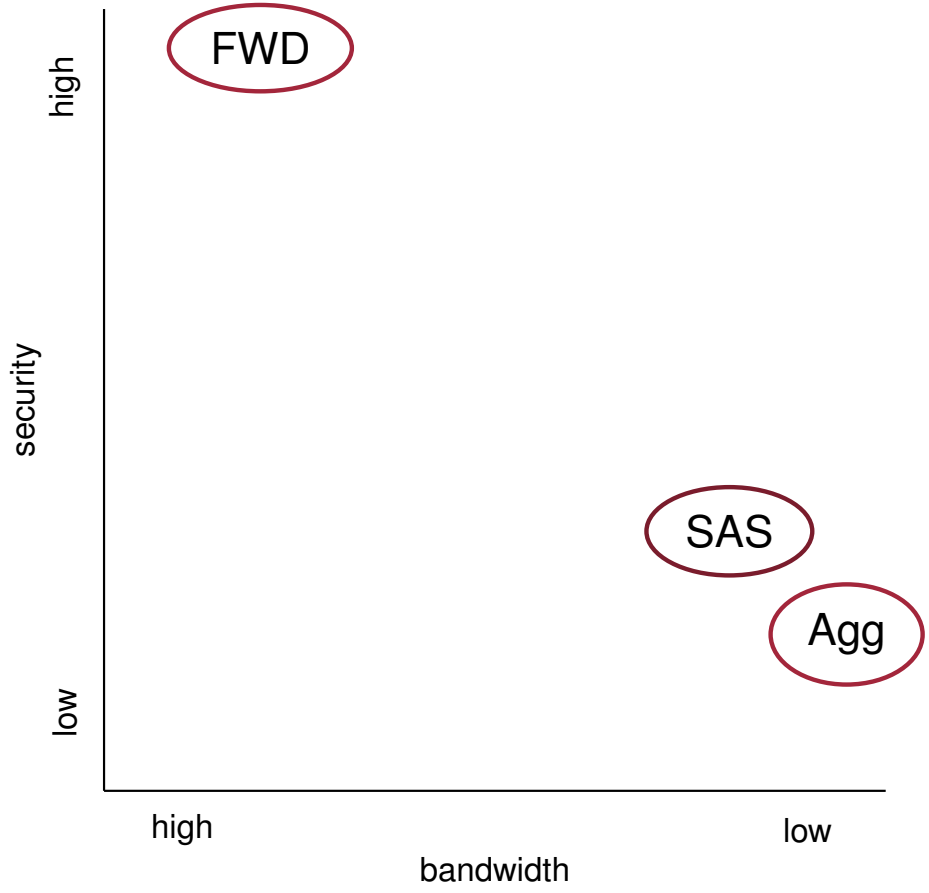
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)



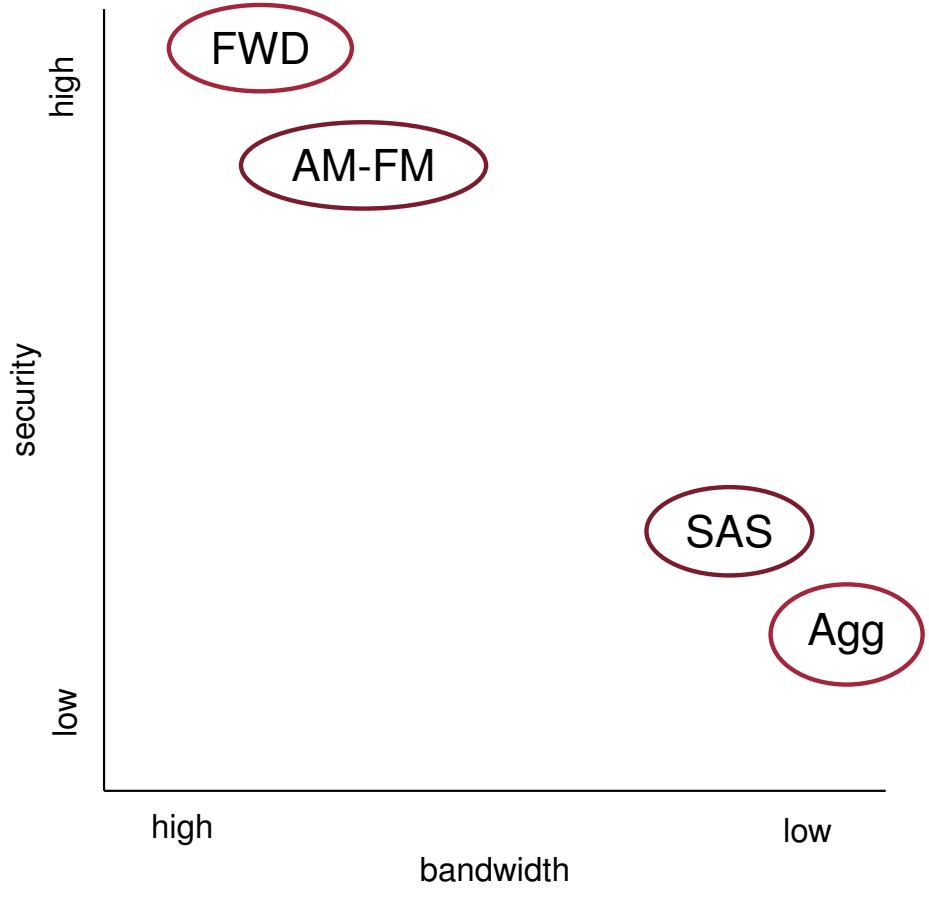
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)



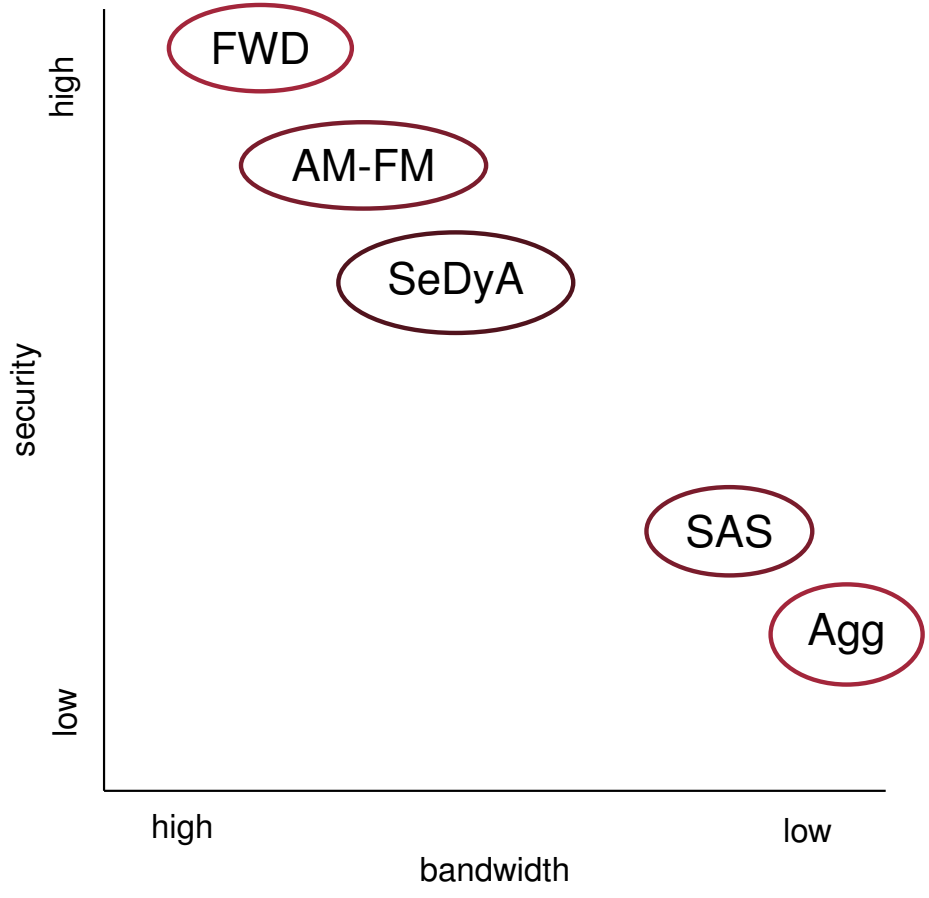
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)



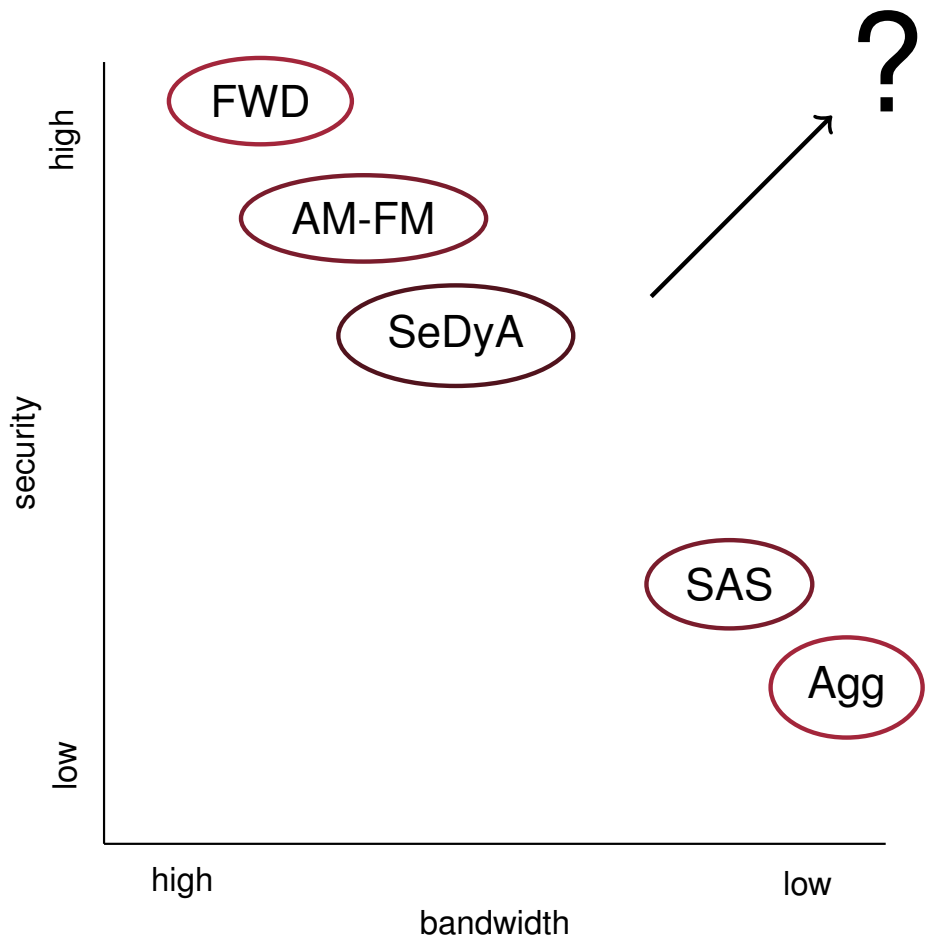
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)



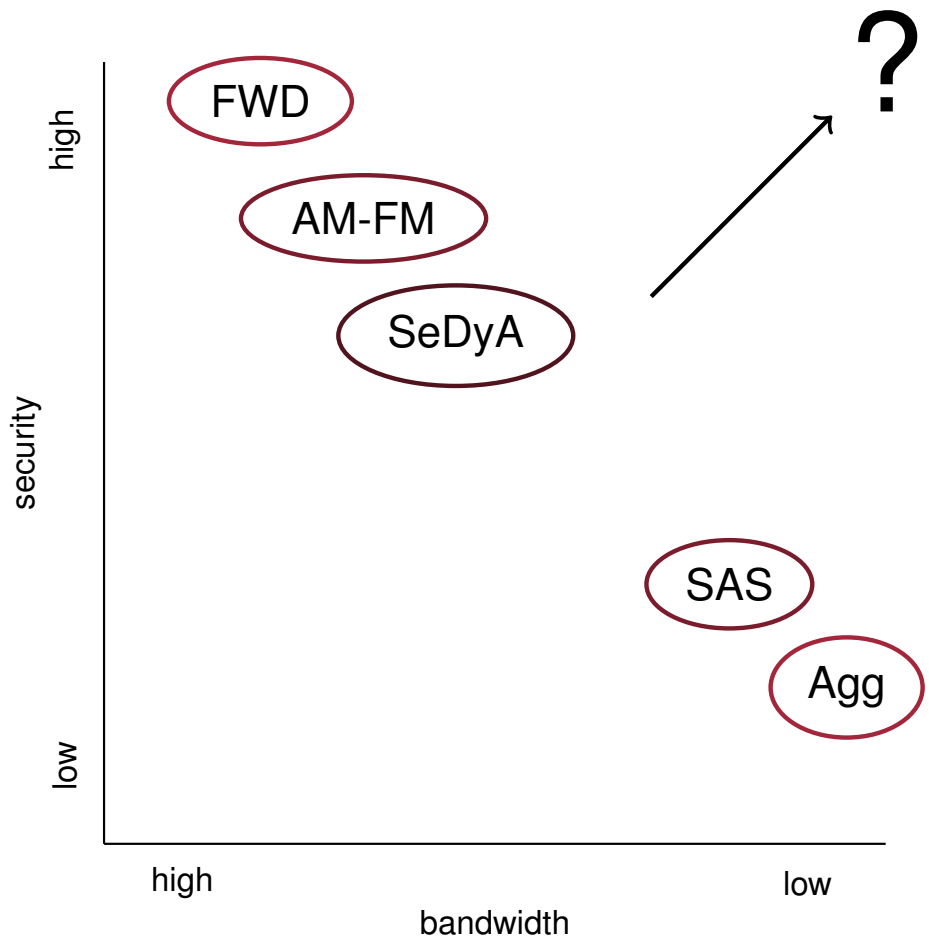
Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)
- Future work:
  - More data on trade-off



Conclusion

- SeDyA trades-off:
  - Efficiency (insecure aggregation: Agg)
  - Security (beacon forwarding: FWD)
- Future work:
  - More data on trade-off
  - Misbehavior detection



Questions?