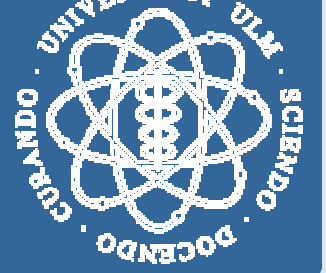
Sensors for Detection of Misbehaving Nodes in MANETs

Frank Kargl
A. Klenk, S. Schlott, M. Weber
Dep. Of Media Informatics
University of Ulm

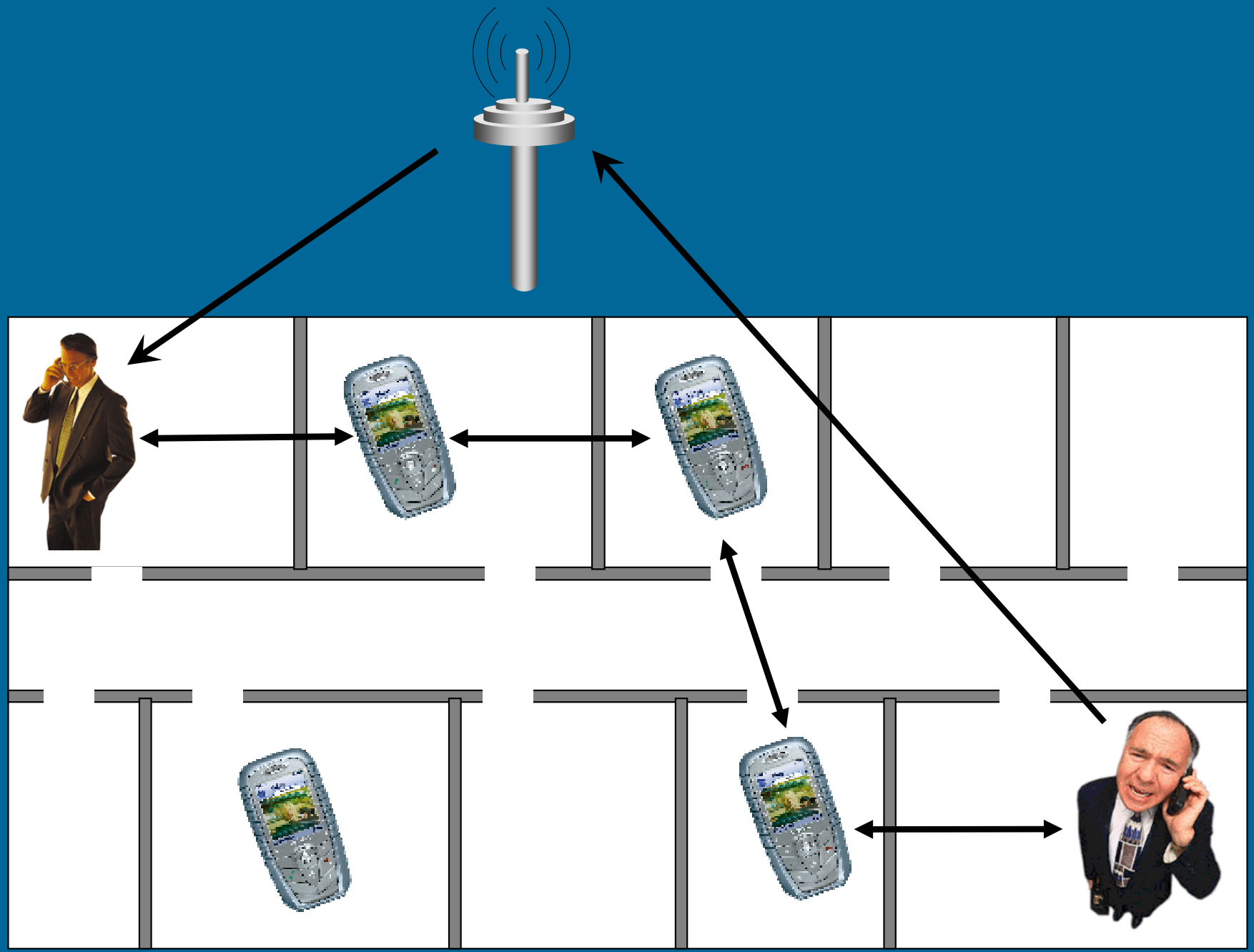
DIMVA 2004
Dortmund, 06.07.2004



Outline

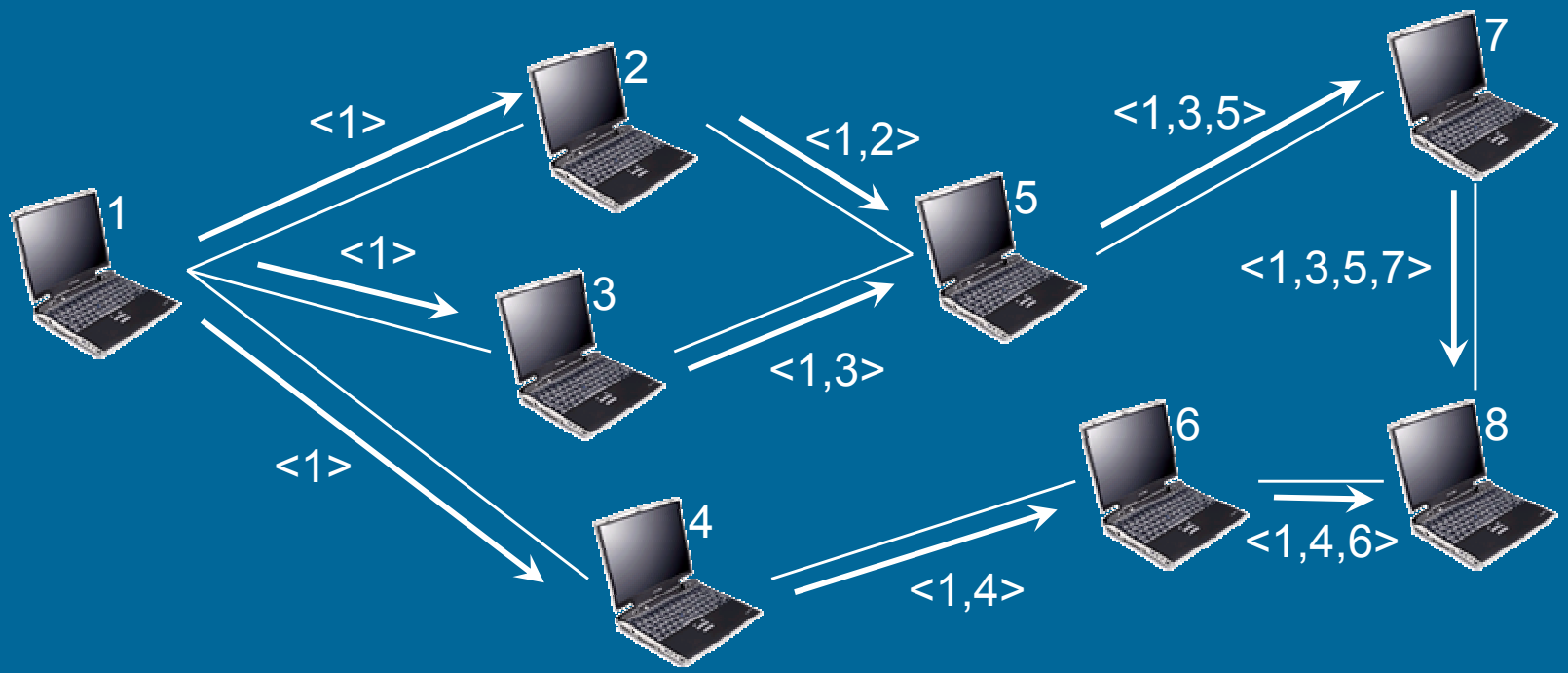
1. What are Mobile Ad-hoc Networks?
2. Security Problems
3. Security Architecture SAM
4. Mobile Intrusion Detection System MobIDS
5. Sensors
6. Summary

Mobile Ad hoc Netzwerke (MANET)



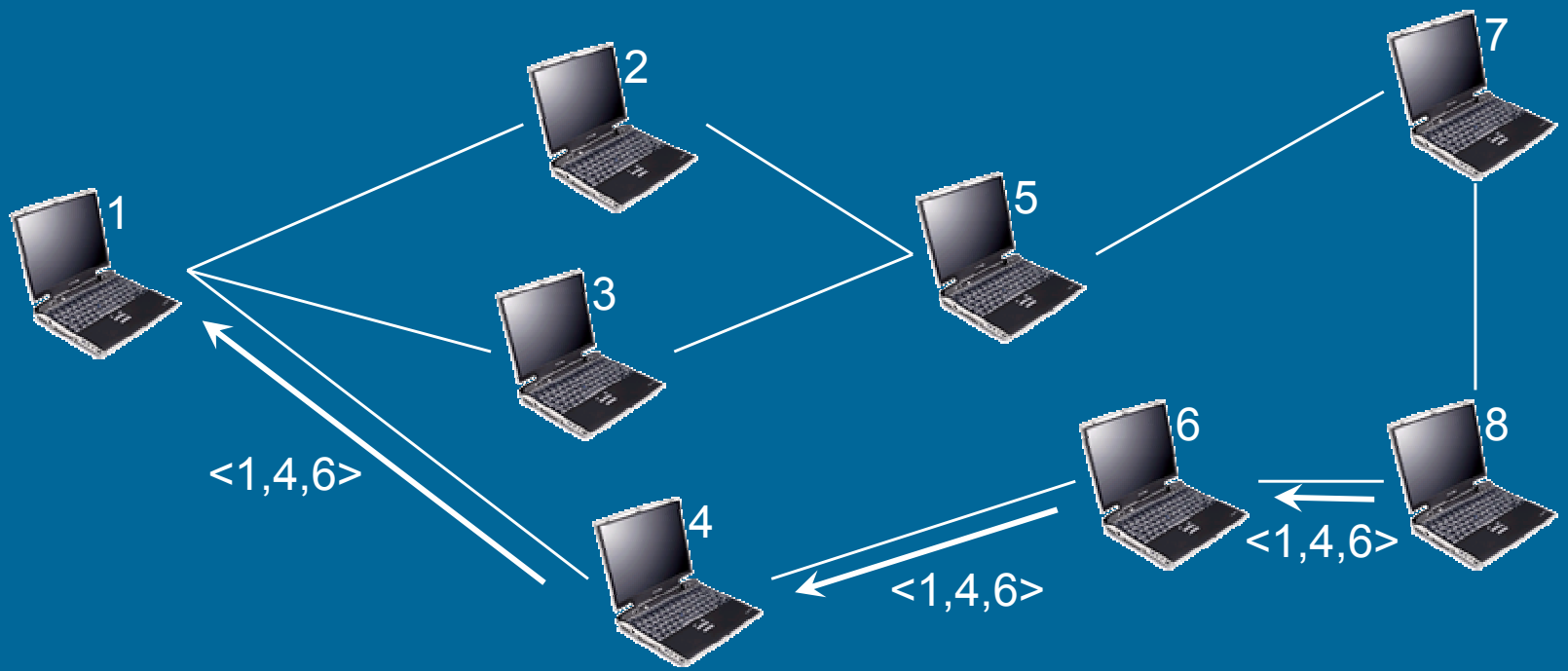
DSR Route Discovery

- Route Request (RREQ)



DSR Route Discovery

- Route Request (RREQ)
- Route Reply (RREP)



MANET Security

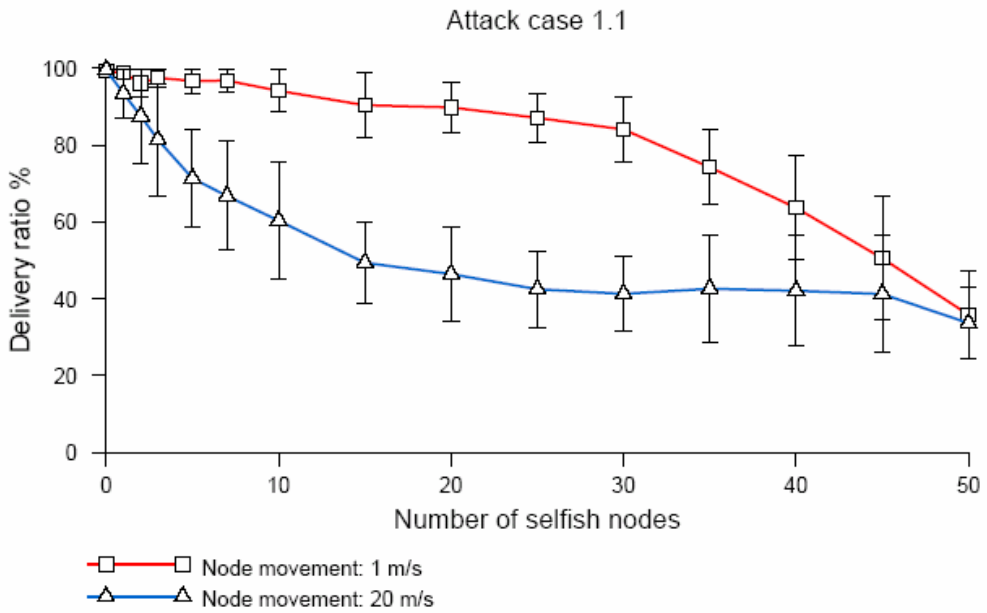
- Very easy to mount attacks
  - eavesdrop on traffic
  - modify traffic
  - DoS network (e.g. disturb routing)
  - localize and track nodes
  - …
- Plus: very limited resources
- Plus: problem of selfish nodes

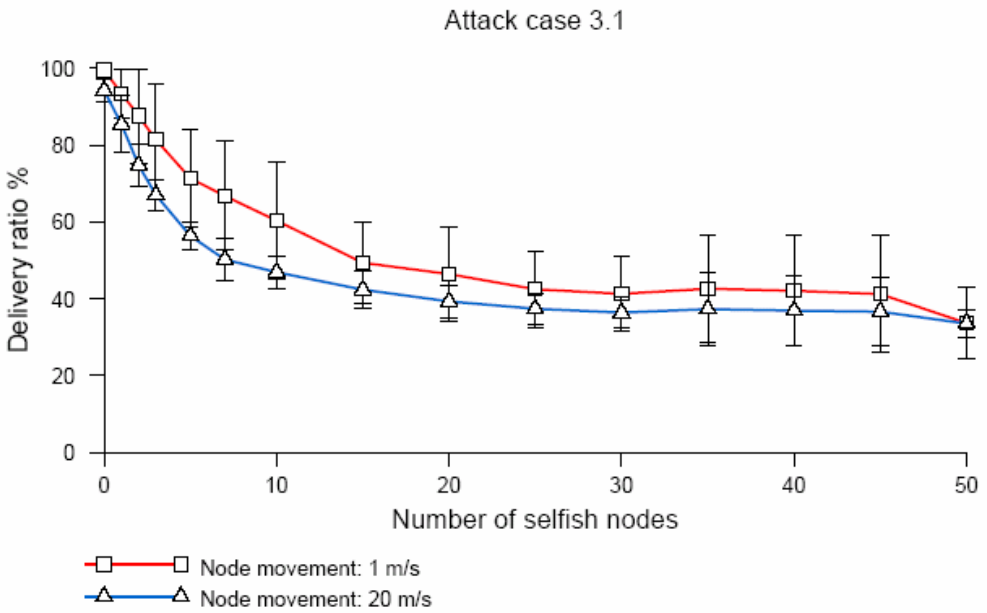
Problem of Selfish Nodes

- Devices have limited resources
  - CPU, energy, bandwidth
- Why “waste” resources on supporting other nodes in the network?
- Lot of possibilities to “safe”
  - do not participate in route discovery
  - deny forwarding of packets
  - pretend you cannot “hear” a neighbor

Simulations

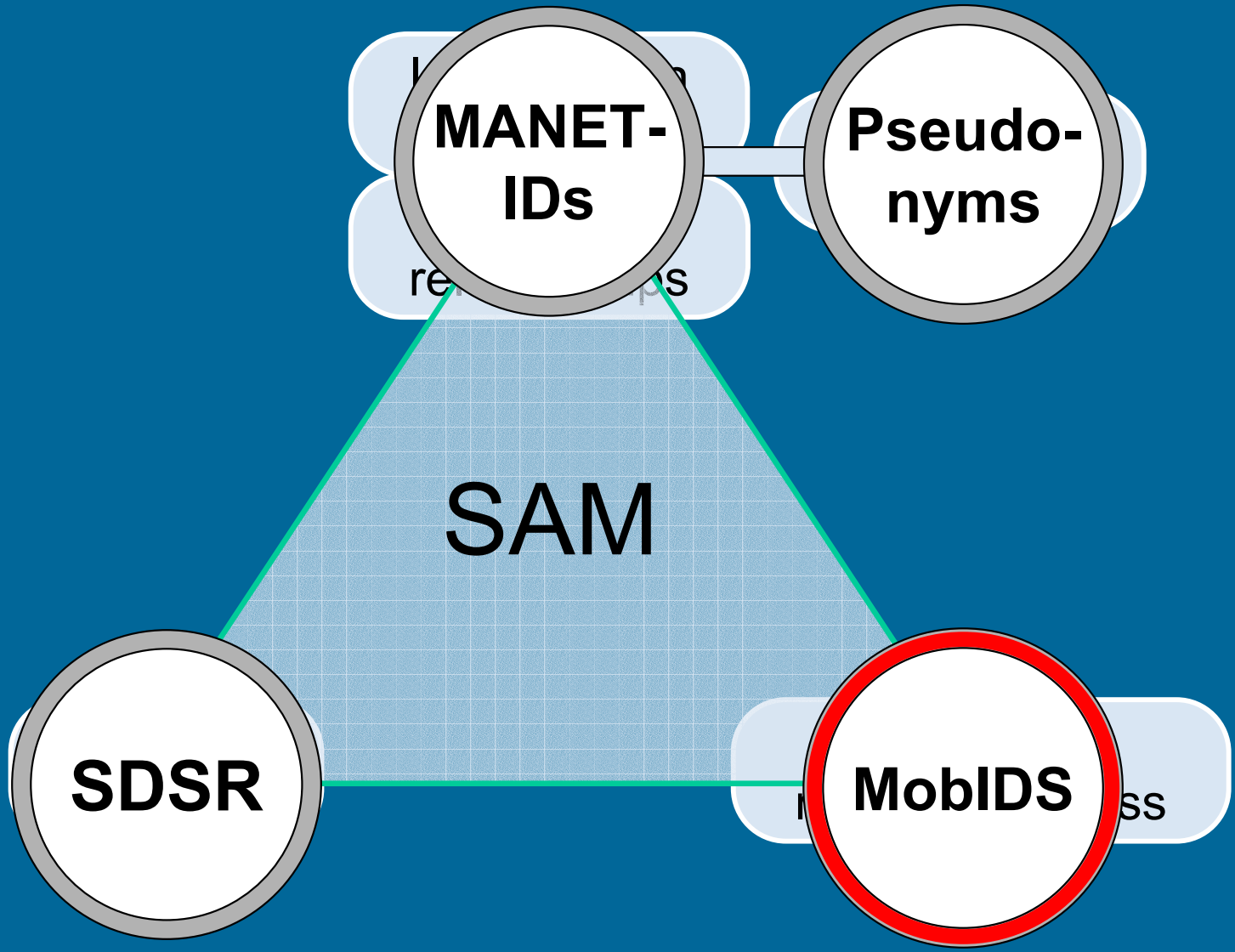
- Selfish nodes cause tremendous decrease in network performance





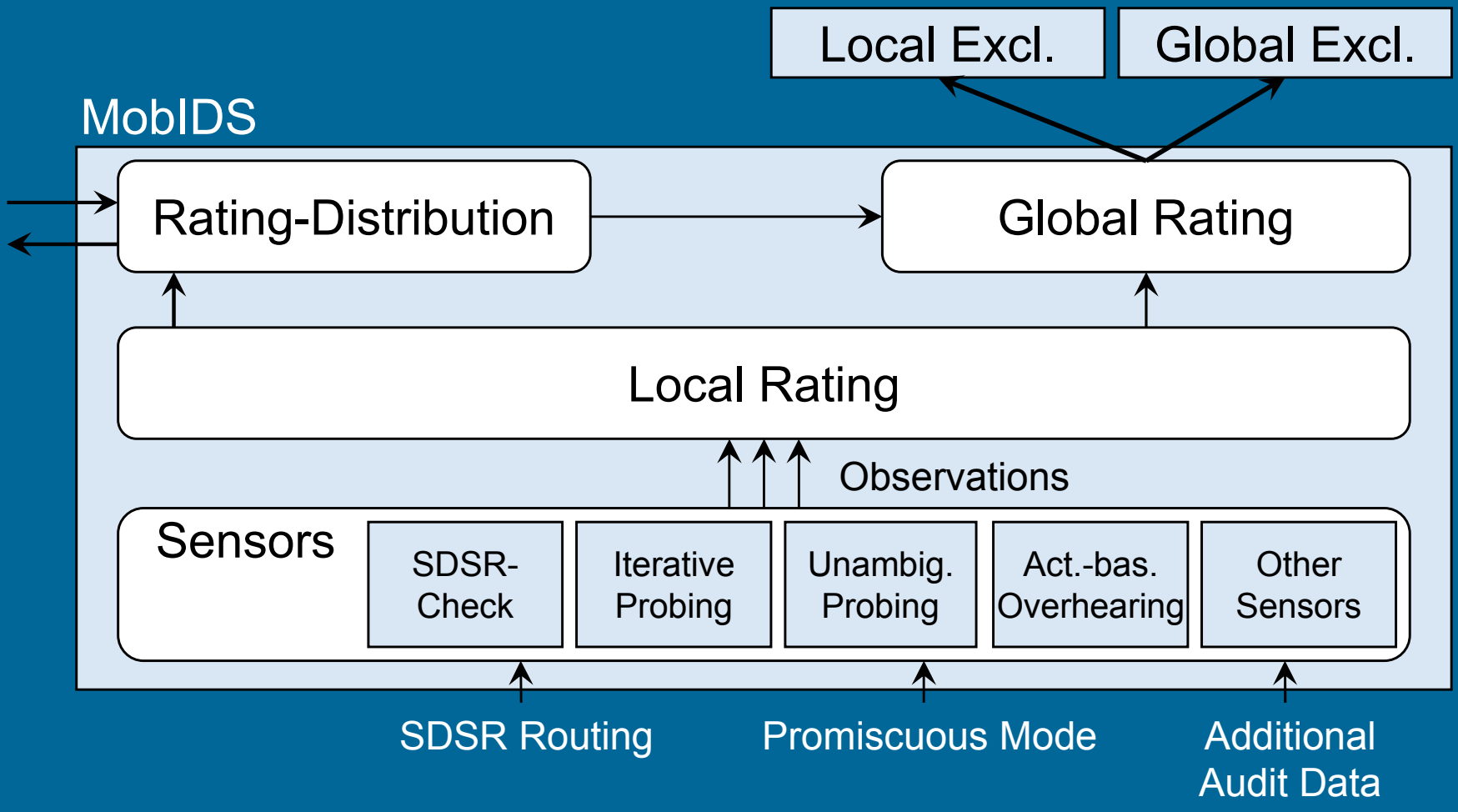
Security Architecture for Mobile Ad hoc Networks

MANET Security Problems



Mobile Intrusion Detection System

Detect and exclude selfish nodes
which do not participate in routing



Local Rating

- Sensor rating:

$$r_{k_i}^t(k_j|s) = \left(\sum_{\forall n} \rho(t, t_n) \cdot \sigma_n \right) / n$$

- Weighting function:

$$\rho(t, t_n) = 1 - \left(\frac{t - t_n}{T} \right)^x$$

- Local rating:

$$r_{k_i}^t(k_j) = \sum_{\forall s} w_s \cdot r_{k_i}^t(k_j|s)$$

Global Rating

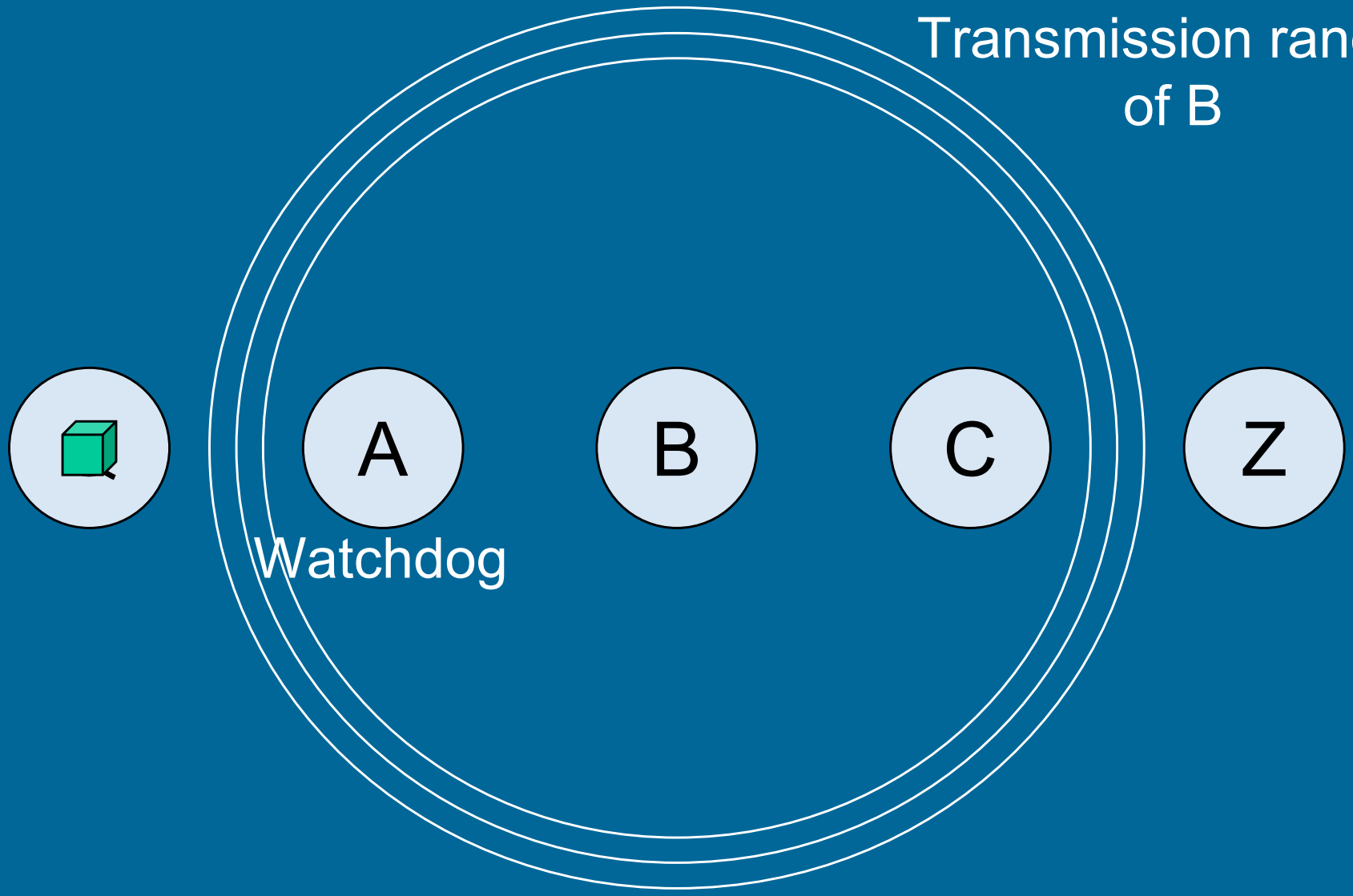
- Distribute (signed) local ratings in neighborhood
- Global rating is average of all local ratings
- At least *n* local ratings necessary, to make global rating valid

- NO validation of ratings! Only authentication
- Different thresholds prevent false accusations

Exclusion

- Local exclusion
  - Other nodes deny routing packets for locally excluded nodes
  - Rehabilitation as old observations time out
- Global exclusion
  - In case of continued selfish behavior, invalidation of ID “certificates”
  - Permanent exclusion

Simple Overhearing

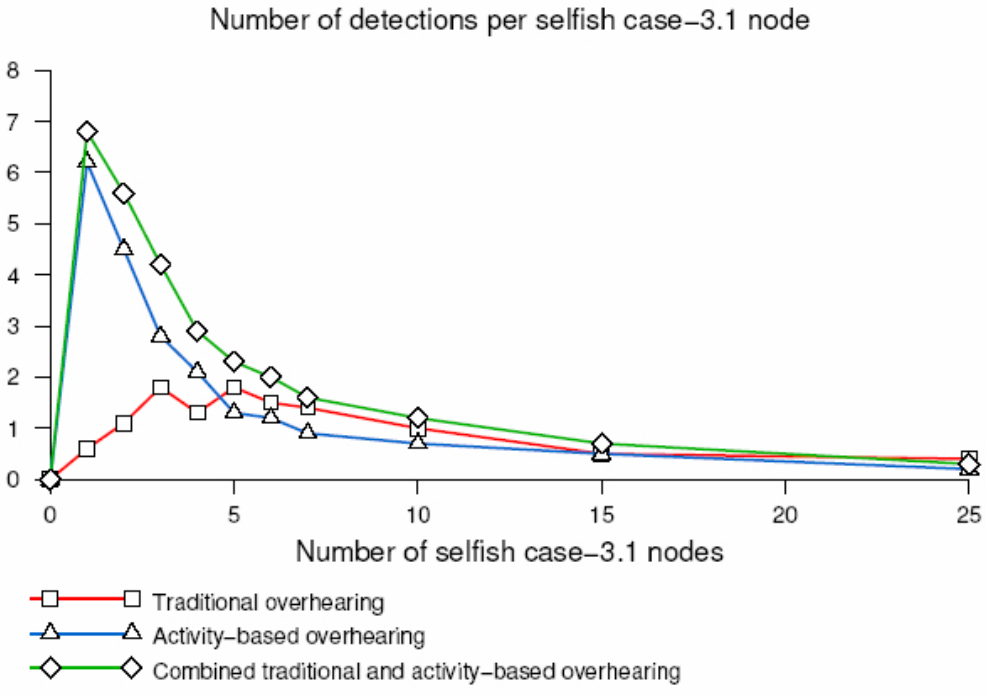


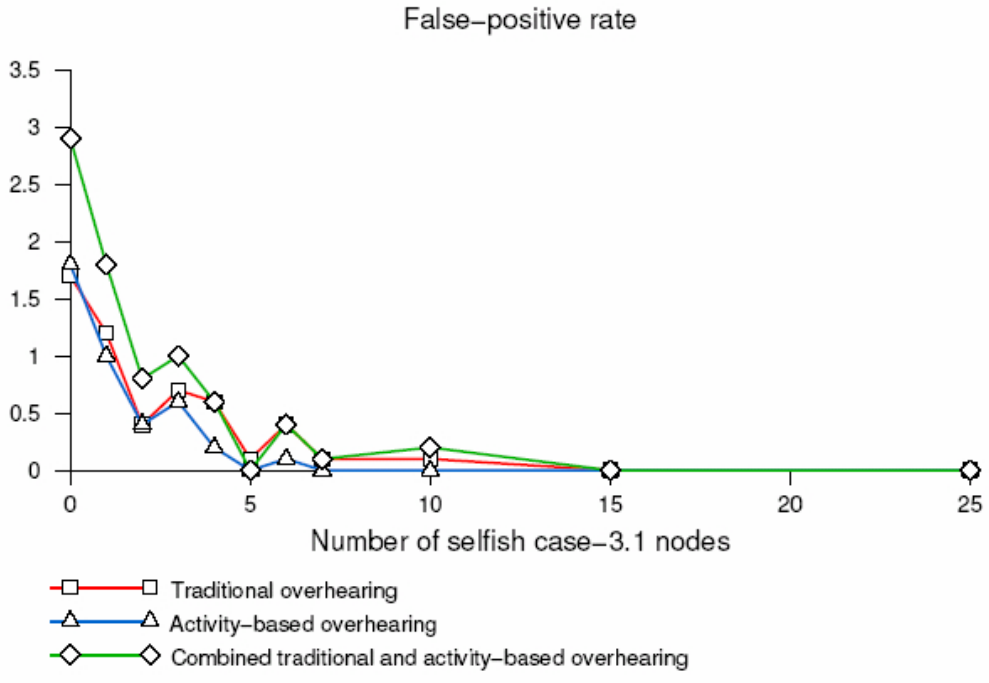
Simple Overhearing

- Watchdog originally proposed by Marti e.a. 2000
- Very unreliable (esp. false-positives):
  - node movement
  - collisions
  - different speeds (1/2/5.5/11 mbps)
  - …
- Nevertheless base of most MANET IDS to prevent selfishness
- Idea: improve overhearing sensor

Act.-based Overhearing

- Consider observations by overhearing sensor only when seeing recent regular activity by observed host
  - opt. consider signal strength of recent activities

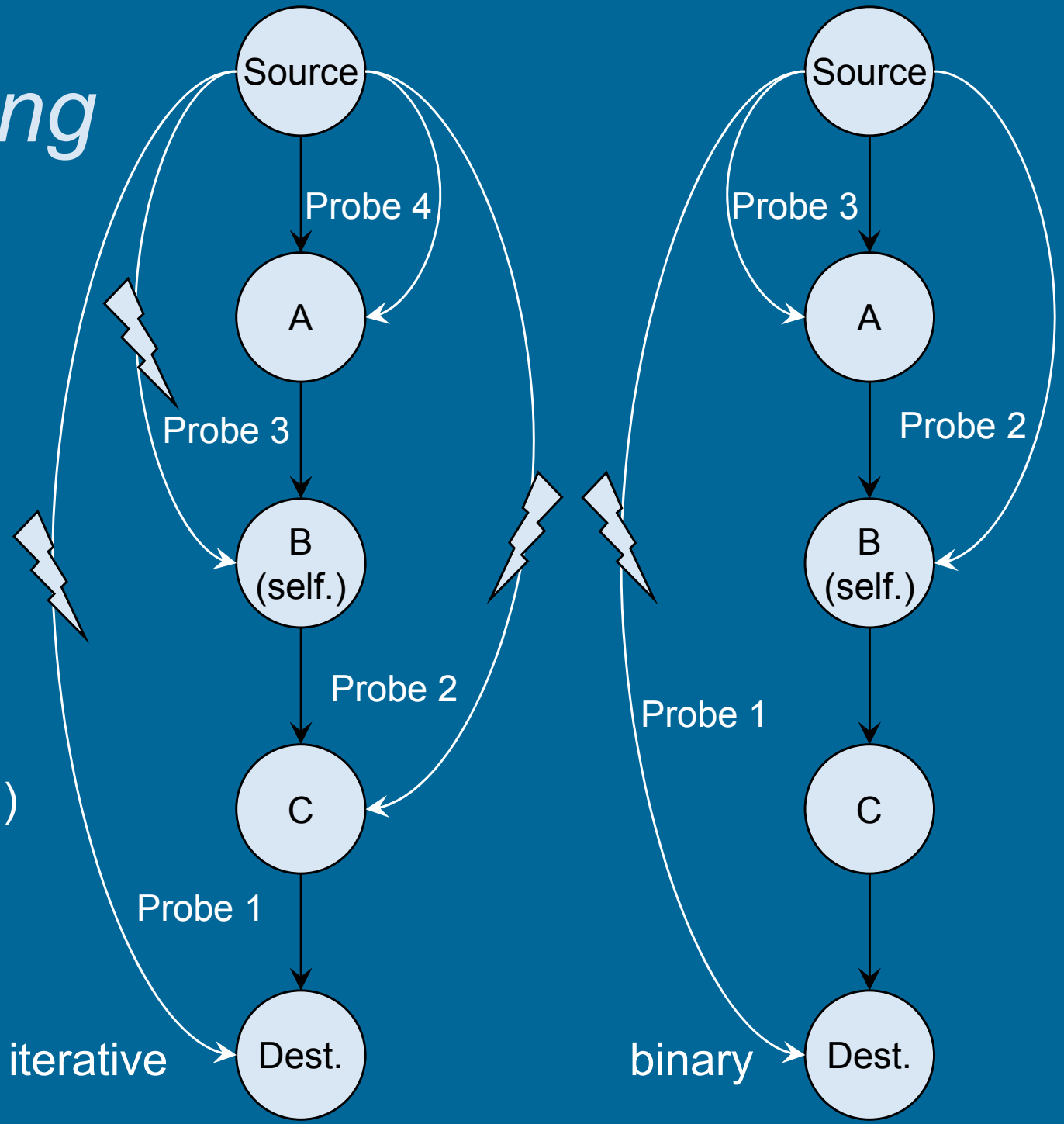




Probing

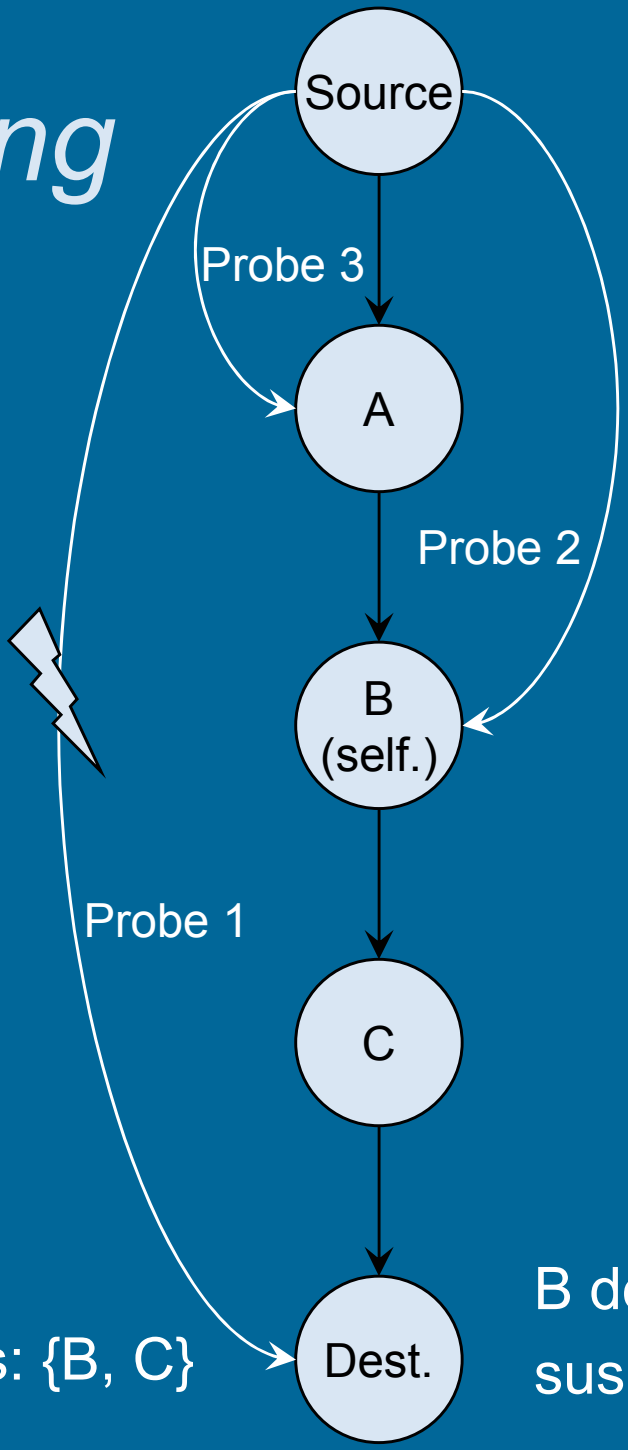
check if path is functional

sent (encrypted) probe packets

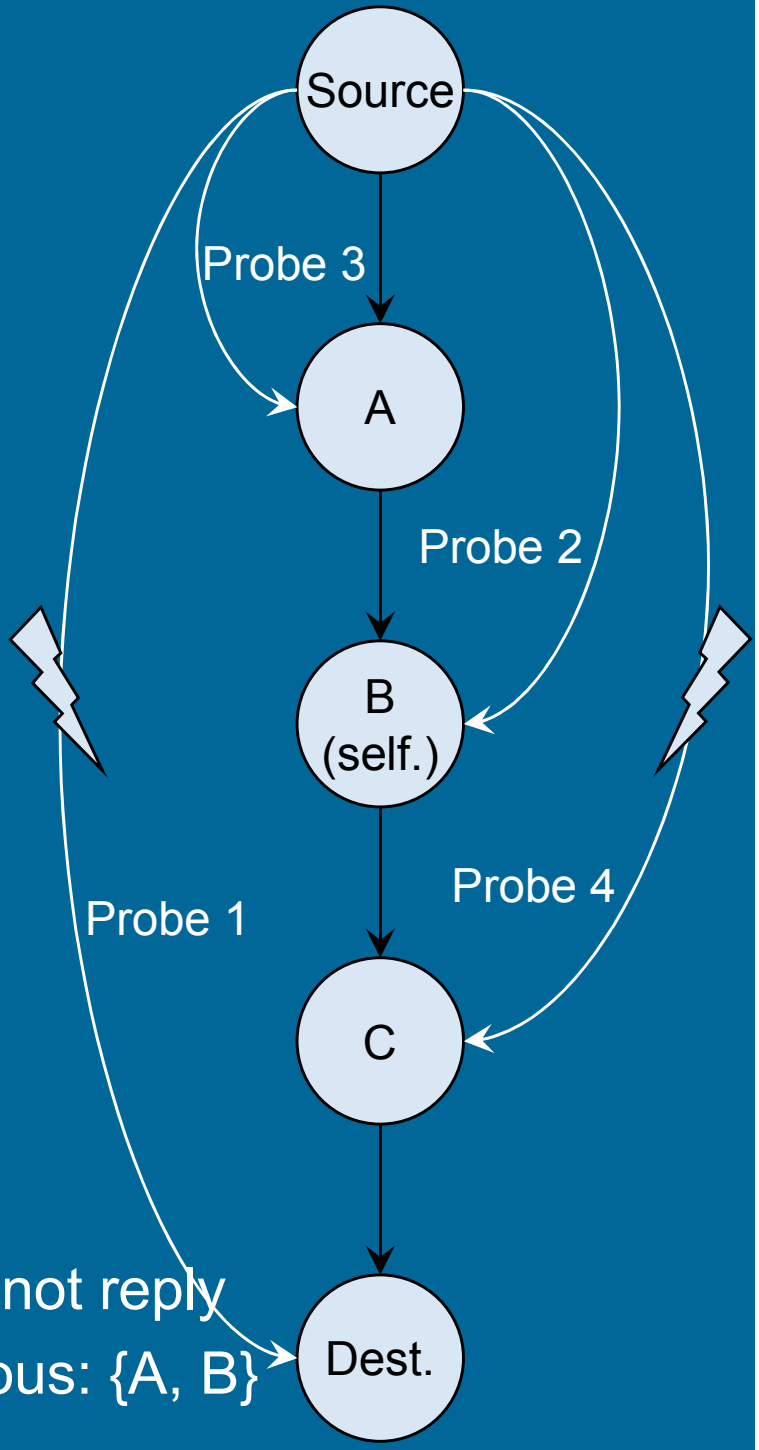


Probing

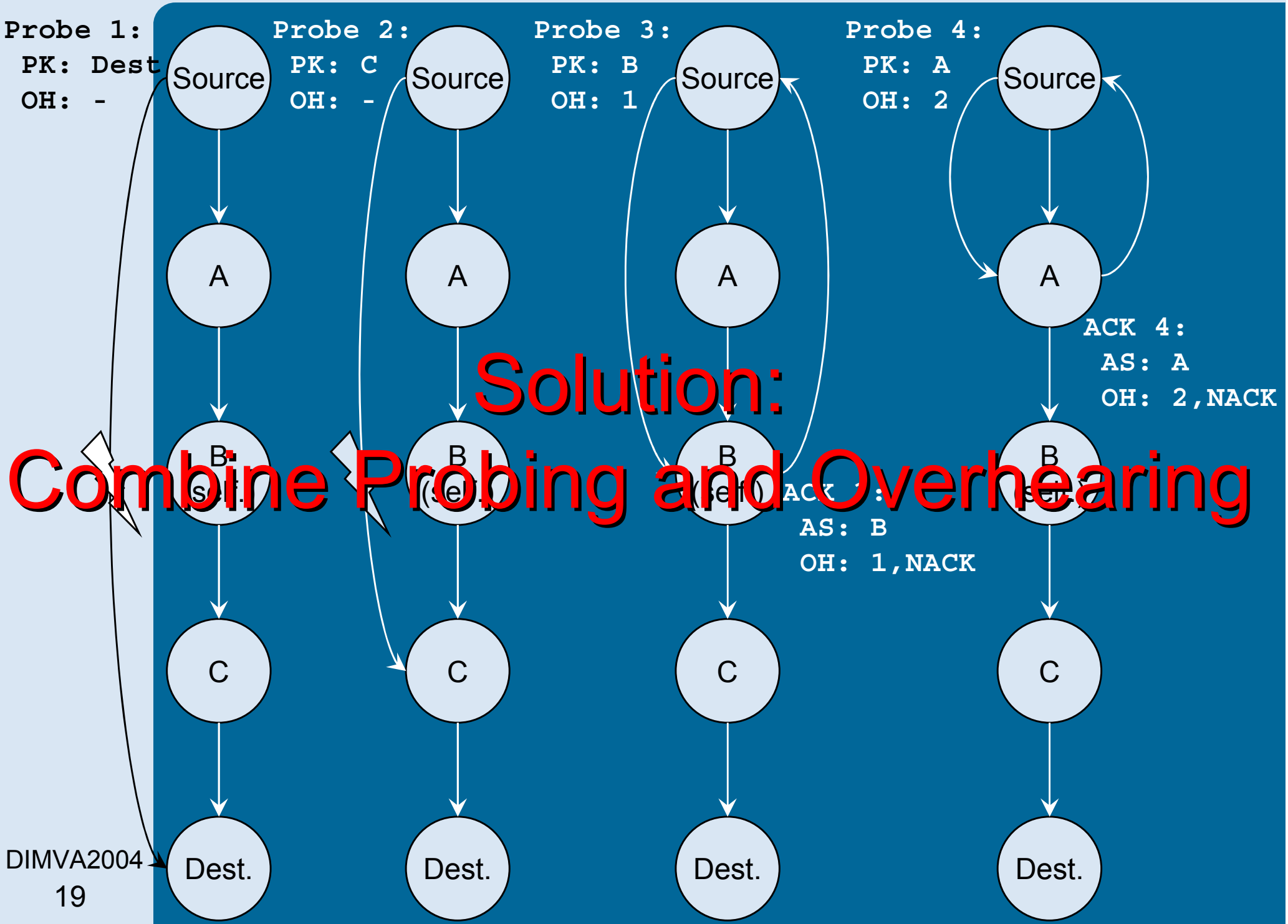
Probing-Dilemma

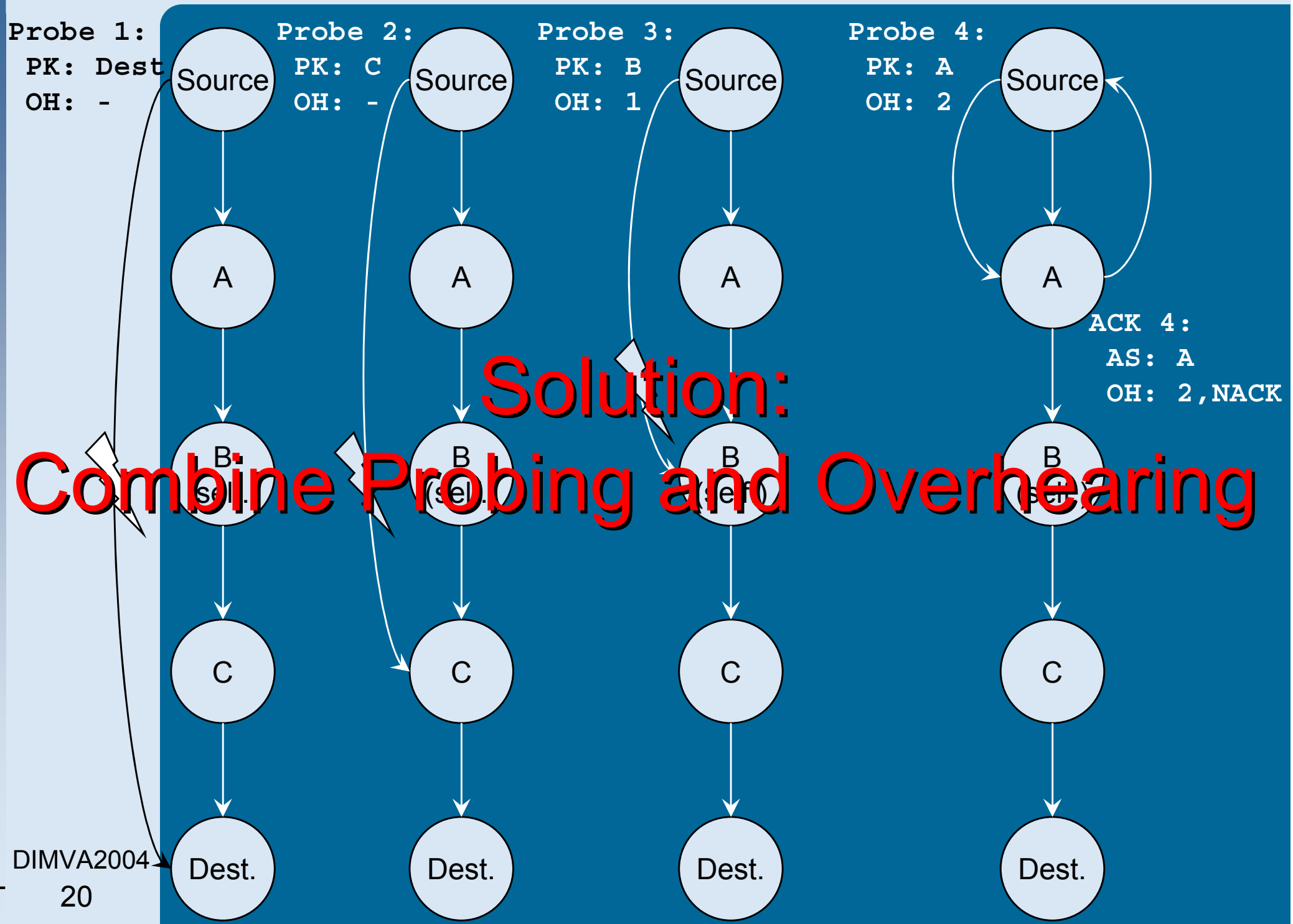


B replies
suspicious: {B, C}



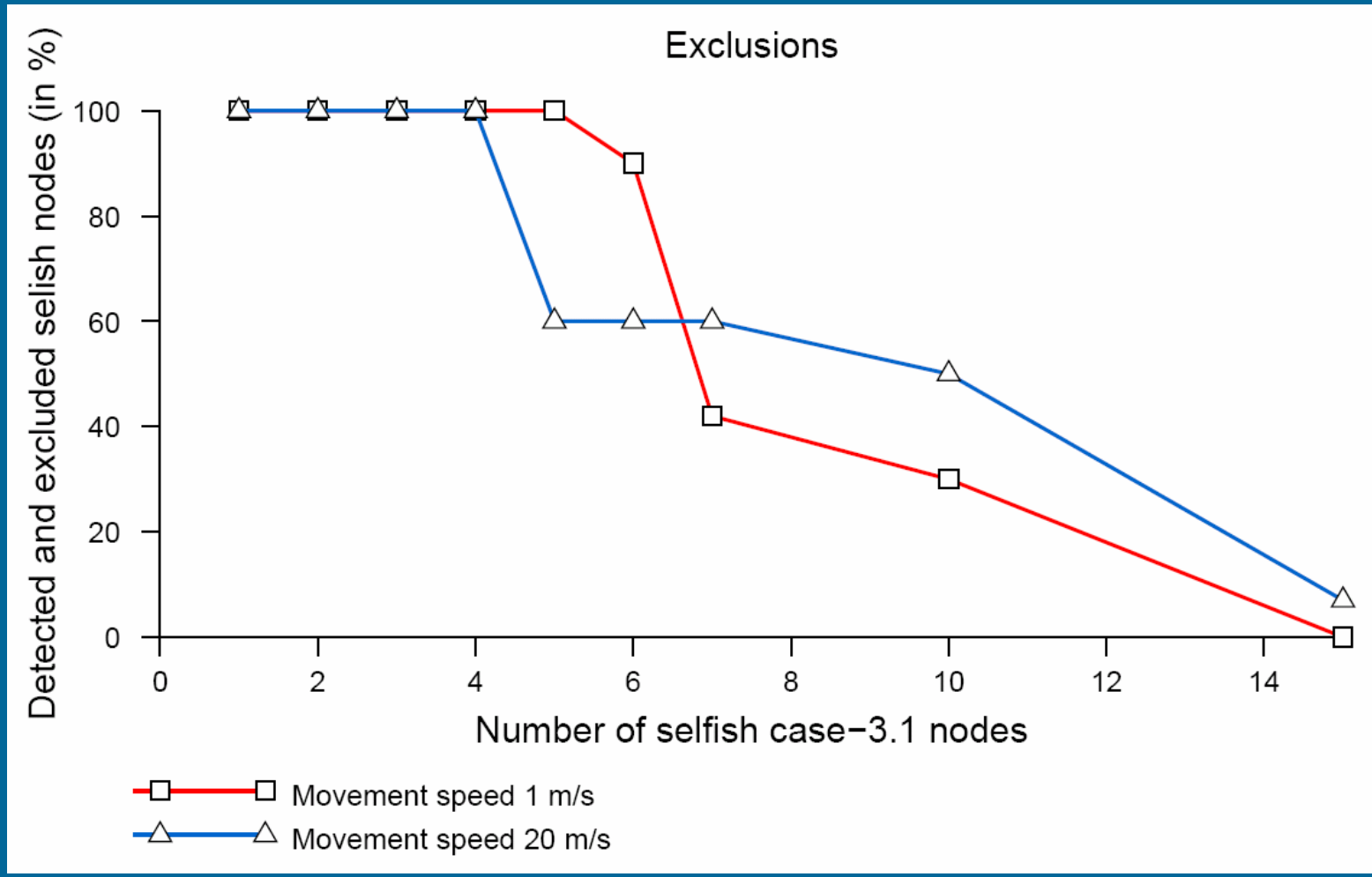
B does not reply
suspicious: {A, B}


Probe 1:
PK: Dest
OH: -
Probe 2:
PK: C
OH: -
Probe 3:
PK: B
OH: 1
Probe 4:
PK: A
OH: 2
Source
A
B
C
Dest.
ACK 4:
AS: A
OH: 2,NACK
ACK 1:
AS: B
OH: 1,NACK
Solution:
Combine Probing and Overhearing


Probe 1:
PK: Dest
OH: -
Probe 2:
PK: C
OH: -
Probe 3:
PK: B
OH: 1
Probe 4:
PK: A
OH: 2
Source
A
B
C
Dest.
ACK 4:
AS: A
OH: 2,NACK
Solution:
Combine Probing and Overhearing

Total Results MobIDS

Total detection and exclusion



Thank you for your attention

Questions?

Ad-Hoc
Networking