



**1st Public Workshop
IP Daidalos**

**Advanced Mobility and Security
in Heterogeneous Networks**

**Amardeo Sarma
NEC**



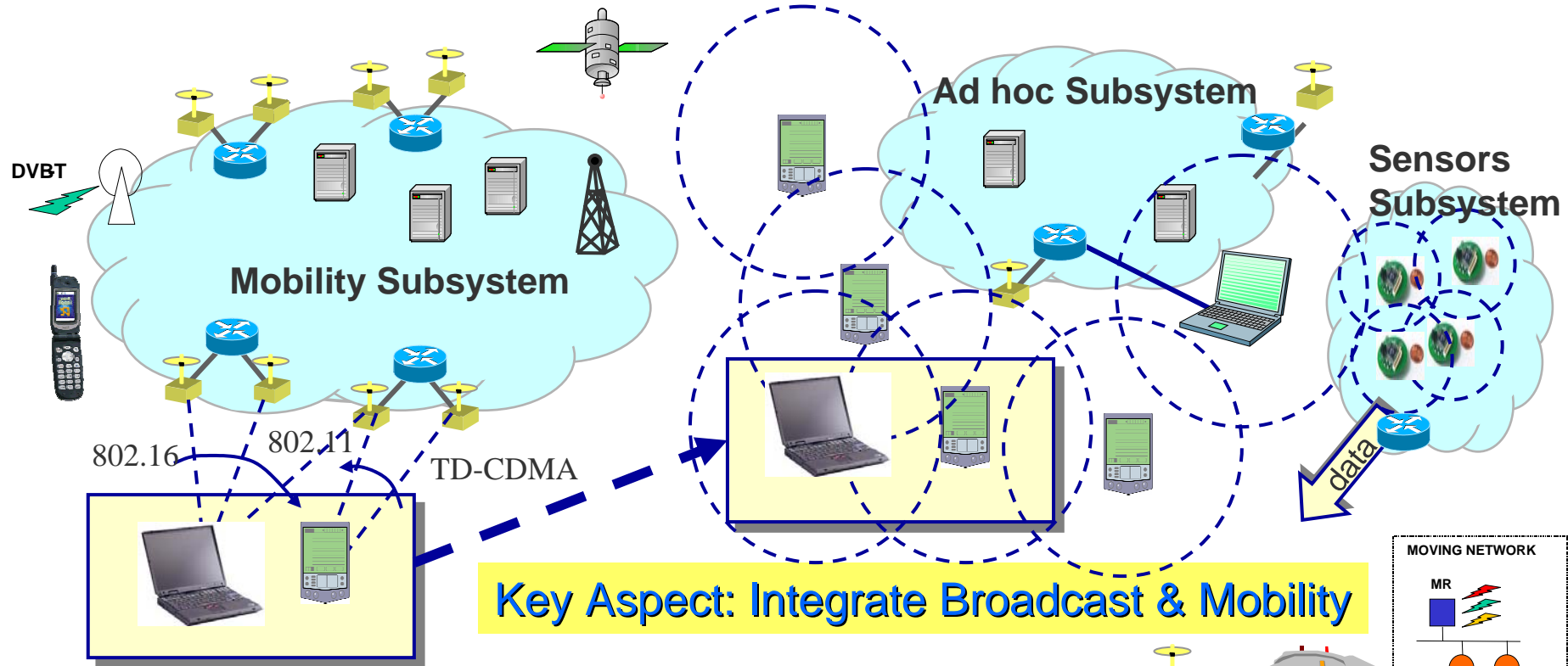
Daidalos – Key Points

- ▶ IPv6 and MIPv6 still the key to integrating heterogeneous technologies, but challenges are looming
- ▶ Integration of Mobility, QoS and A4C – first proof of concept in EU IST Moby Dick – remains centre-stage
- ▶ Integration must span different network types
→ single-hop, ad-hoc / multi-hop, moving **and broadcast**
- ▶ Levels of handling identification in a mobility architecture:
 - Interface (MIP), Device (HIP) **or Identity (Pseudonym/Virtual ID)**
 - Daidalos → Investigate Identity level for phase 2
- ▶ Tomorrow's device will be different → **“Daidalos Personal Assistant” (DPA)**
 - No more 1:1 relationship of owner:device
 - DPA provides time-limited ownership of (part of or multiple) devices

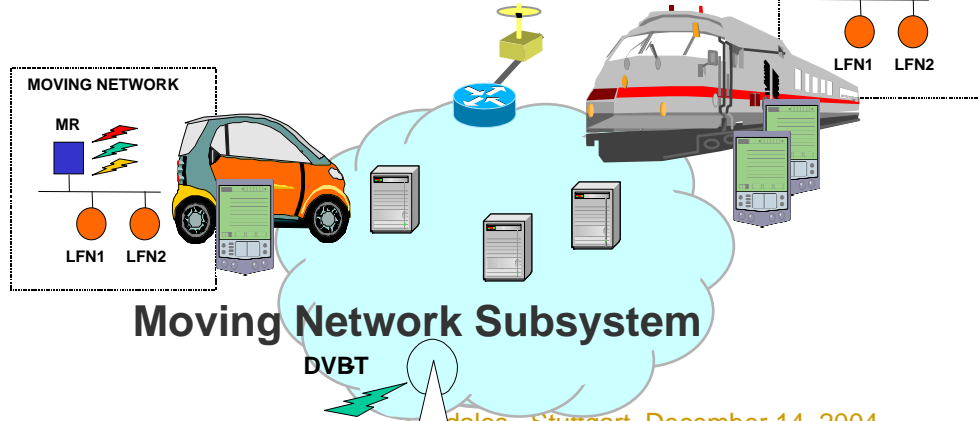




Overall Network Architecture

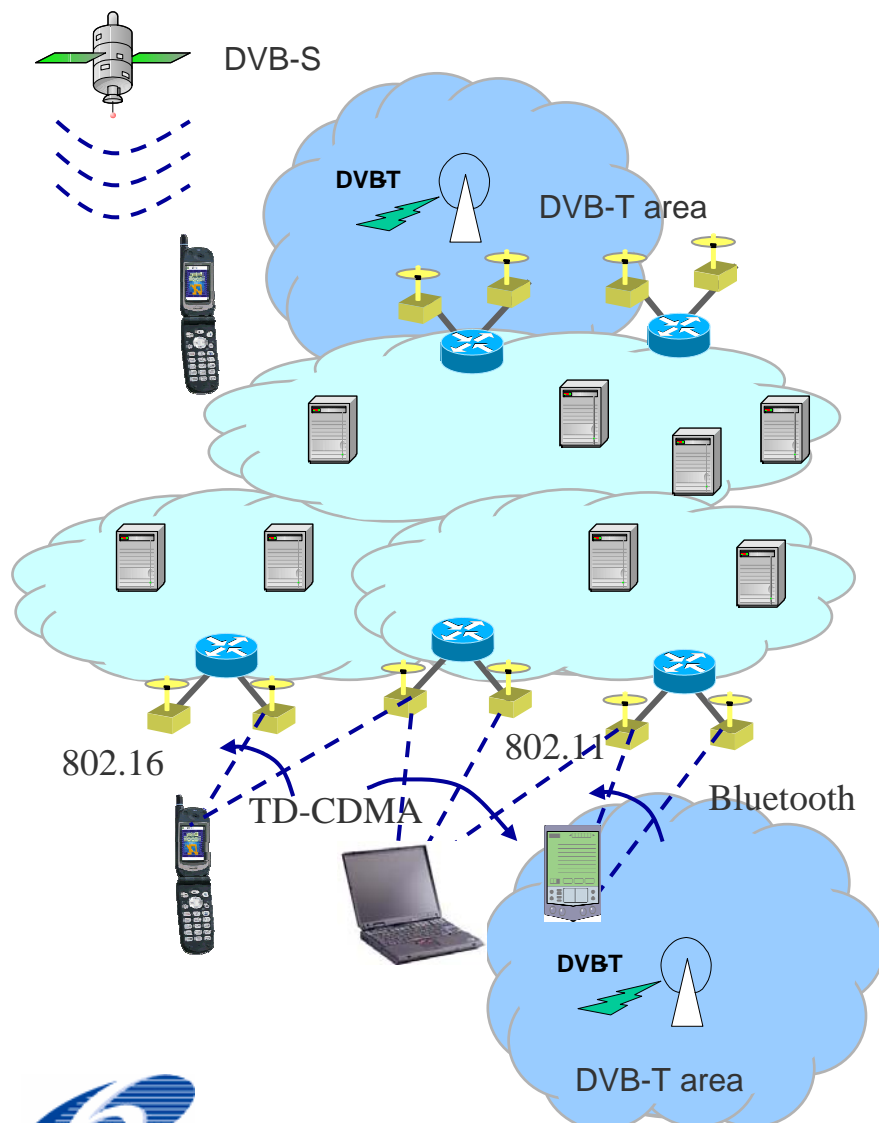


Integrate WLAN (802.11), 802.16, DVB-T/S/H, TD-CDMA, Ethernet (802.3), Bluetooth





Terminal Mobility Scenario



- ▶ Support seamless terminal mobility while supporting choice of:
 - Access routers / access points
 - Suitable technology
 - Interface selection
 - Various domains
- ▶ Seamless Handover
 - Flexible handover preparation
 - Intra and inter-domain
 - Intra- and inter-technology
 - Mobile Terminal Initiated
 - Network Initiated
 - However not for inter-domain case because of competing operators
 - Performance optimisation
- ▶ Paging
 - integrated NIC Power Saving for efficient location management





Mobility Terminal Components

- ▶ Handover preparation
 - Handover Candidate Discovery
 - Intelligent Interface Selection
- ▶ Handover execution
 - Fast Handover Control (Control-Plane)
 - Duplicating and Merging function (User-Plane)
- ▶ Power saving & location tracking
 - Paging Control function
 - Network technology integration
- ▶ Local balancing
 - Multi-Homing
- ▶ Control and technology integration
 - Mobile Terminal Controller
 - Network Interface Abstraction
- ▶ Network Technologies
 - TD-CDMA
 - IEEE802.11
 - DVB-T/H
 - IEEE802.3



Key Functions

- ▶ Co-existing Mobile and Network Initiated Handover
- ▶ CARD mechanism to support Intelligent Interface Selection and Link-Layer handover (IEEE802.11)
- ▶ Fast Handover plus Duplication and Merging for seamless handover support
- ▶ Context Transfer for fast QoS support (VoIP) and network authentication
- ▶ IP paging integration with terminal NIC power save modes
- ▶ Performance Management for capacity optimization and network control
- ▶ Multi-Homing supports load balancing

↔ Inter Access Router communication: CARD and Context Transfer Protocol

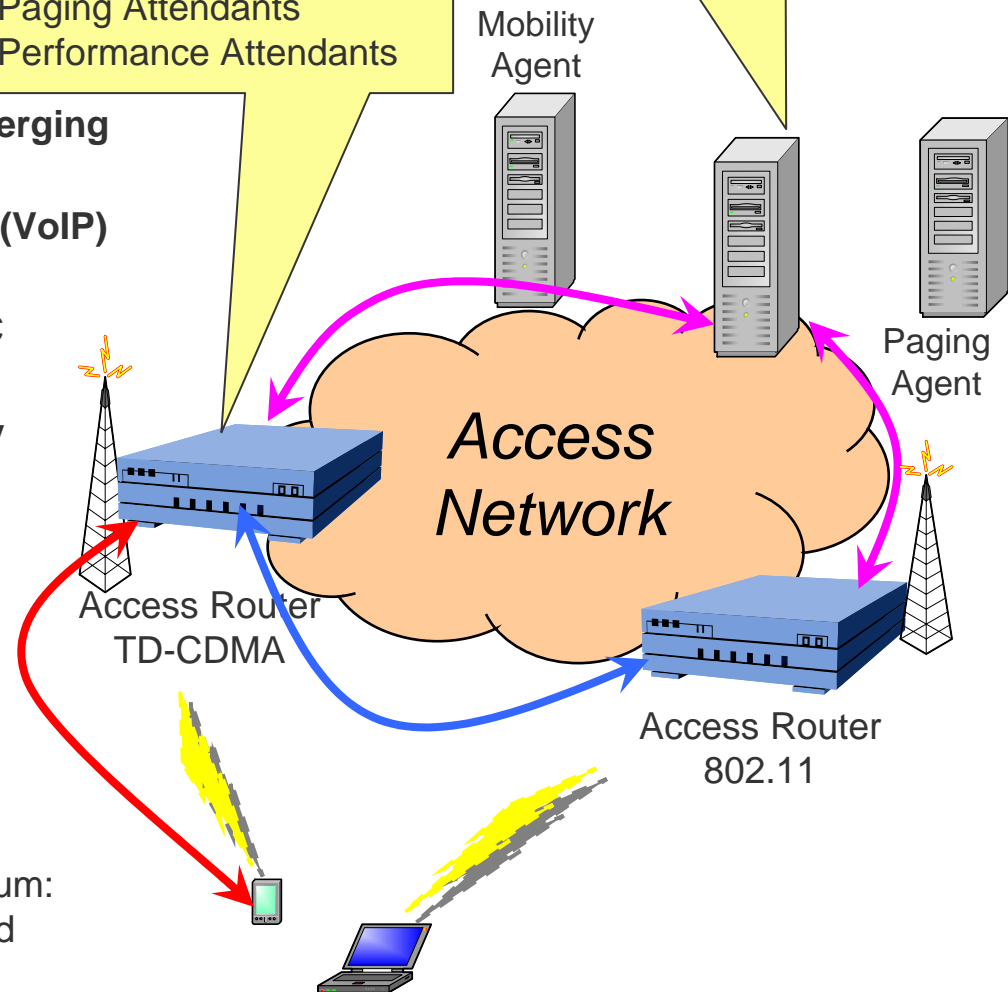
↔ Communication between Access Routers and QoS Broker for mobility reasons

↔ Communication on the Wireless Medium: FHO and CARD messages exchanged

Functional Components:

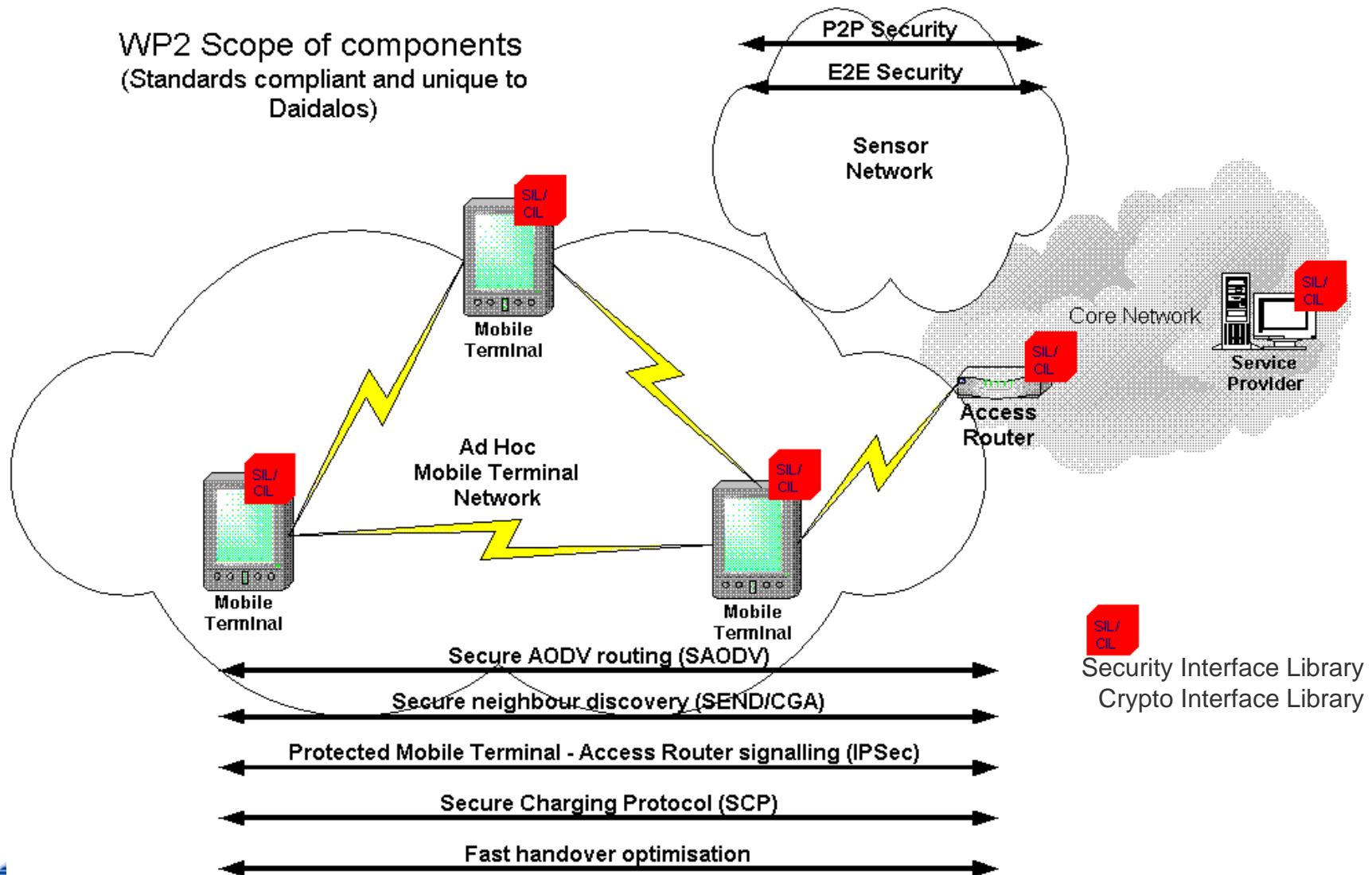
- Candidate AR Discovery
- Fast Handover
- Duplication & Merging
- Context Transfer
- Paging Attendants
- Performance Attendants

Driving Entity for Mobility Decisions and Performance Management





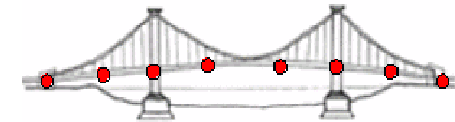
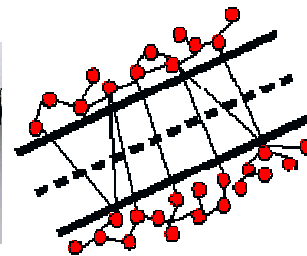
Scope of security in the access network



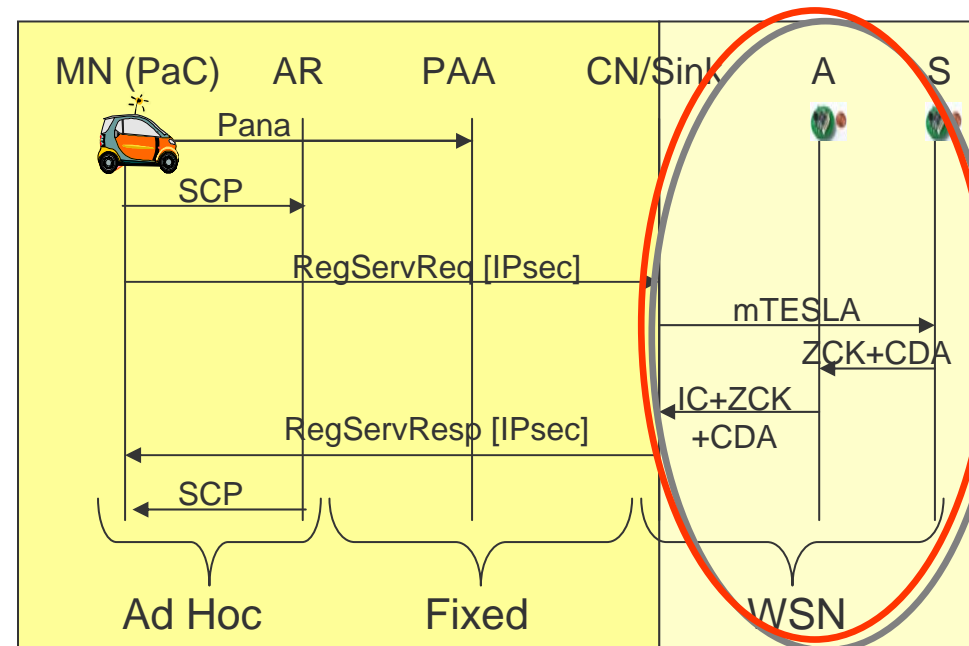


Wireless Sensor Networks in Daidalos

Wireless Sensor Network Automobile Scenario



- ▶ information on road status
- ▶ push or pull modes
- ▶ Useful where
 - temperature of the paving abruptly changes
 - animals are crossing
 - at the edge to bridges, tunnels, shadowed regions, curves, etc.
 - other sensed data is available





Concealed Data Aggregation in WSNs

Problem to be solved...

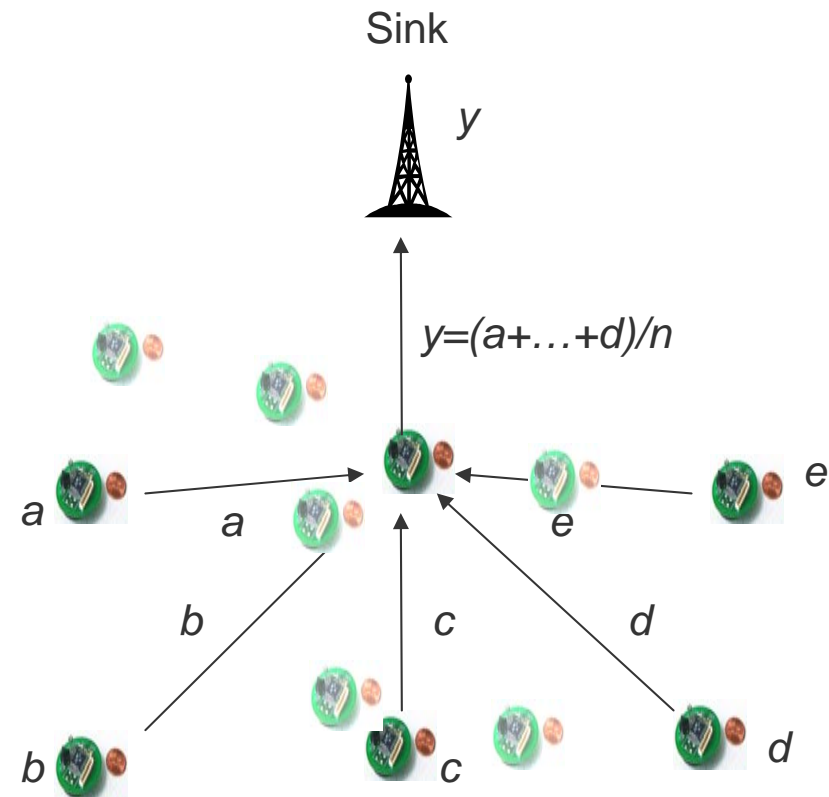
- ▶ ...Merging data aggregation and end-to-end encryption
- ▶ data need to be aggregated on its way to the sink node -> saves energy
- ▶ data aggregation function is context sensitive

Current proposals: data aggregation + hop-by-hop encryption, e.g. RC5 (single group key)

Our proposal: data aggregation + end-to-end encryption

PROS:

- saves energy consuming encryption operations in the backbone...
- no lack of security at aggregating backbone nodes...
- most flexible for aggregator node election process over different epochs



aggregation function “average” of n sensor nodes





Concealed Data Aggregation in WSNs

CDA – Concealed Data Aggregation

- ▶ additive and multiplicative PH

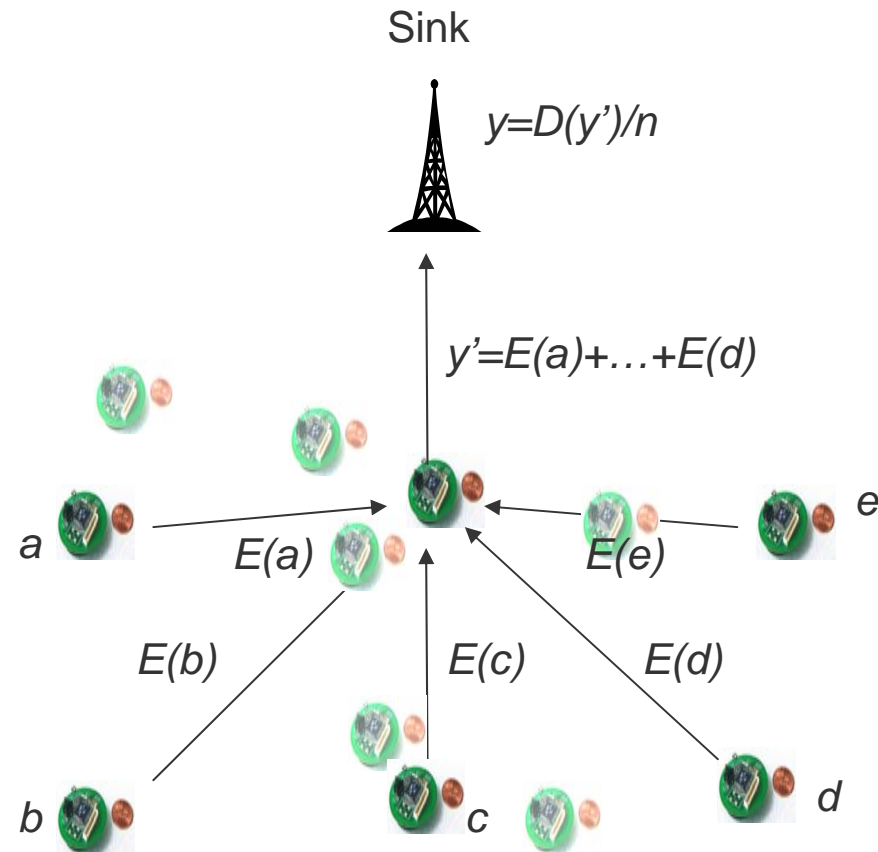
$$a+b=D_k(E_k(a)+E_k(b))$$
$$a*b=D_k(E_k(a)*E_k(b))$$

with rings $(Q,+,x)$ and $(R,+,x)$ and

$$E: K \times Q \rightarrow R$$
$$D: K \times R \rightarrow Q$$

a, b from Q , k from K

- ▶ E.g. by PH from Domingo-Ferrer
- ▶ aggregation functions
 - **average** and **movement detection**
 - no min/max
- ▶ suits also for aggregator hierarchies



aggregation function “average” of n sensor nodes





Workshop Demonstrations & Posters

Implementations

- ▶ Broadcast
- ▶ Ad-hoc Network Integration
- ▶ Multi-homing

Simulations

- ▶ Paging

Posters

- ▶ Quality of Service
- ▶ Moving Networks

