Balancing Auditability and Privacy in Vehicular Networks

Jong Youl Choi
Indiana University

Markus Jakobsson
Indiana University

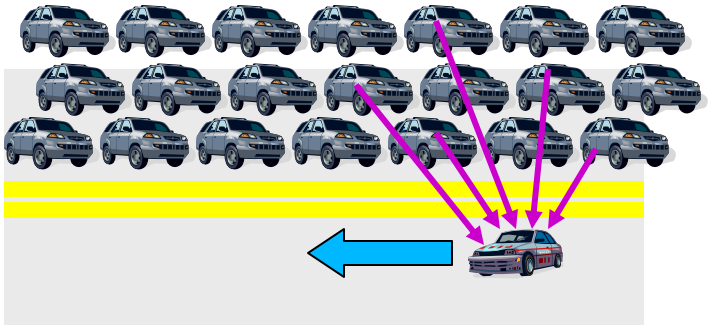
Susanne Wetzel
Stevens Institute Of Technology

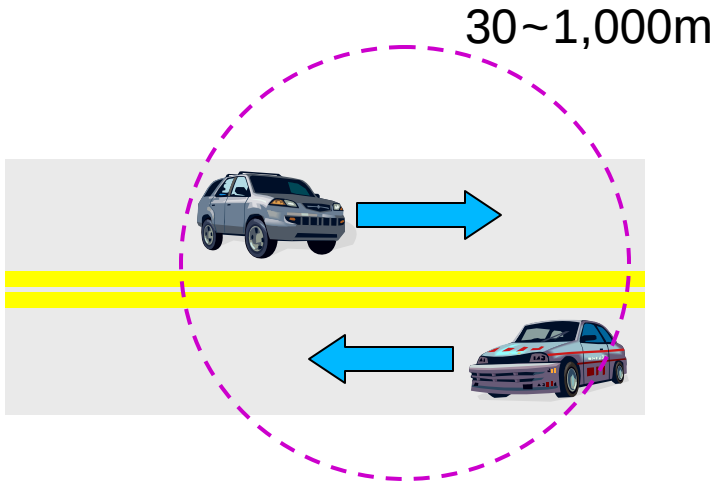
Vehicular Networks

- Benefits
  - Ad-hoc vehicular networks provide ubiquitous environments
  - Abundant information by C2C and C2I
  - Interactiveness can provide location-based services, driving safety, and on-demand services
  - No practical limit on power and computation
- Drawbacks
  - High mobility may restrict bandwidth
  - Security problems : identity, location privacy

Design Decision - Cryptosystem

- Fast cryptosystem





- Less dependent on static infrastructure
  - Infrastructure such as Certificate Authority and Certificate Revocation List may not always be available
  - Static infrastructure may restrict mobility
  - Key distribution problems in symmetric system

Design Decision - Incentives

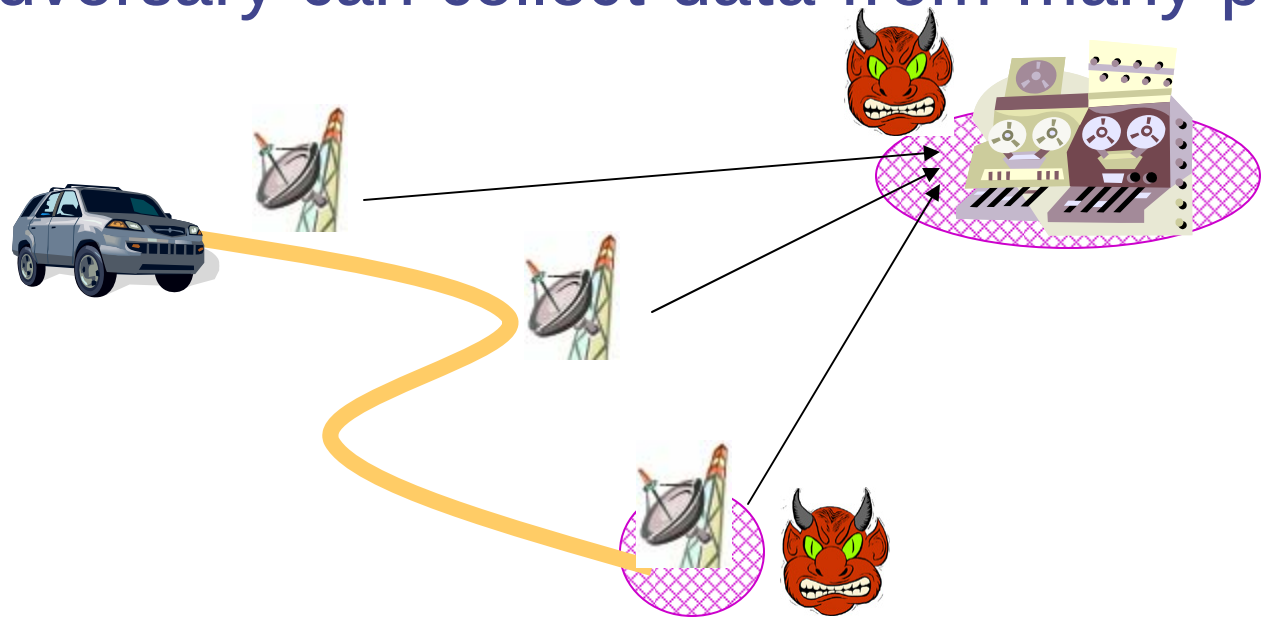
- Objectives
  - Help deployment
  - Make users forward packets instead of dropping
- Lots of services based on data collection with customer's approval
  - Pay-as-you-drive™ insurance
  - Emergency situations (OnStar)
  - Context-aware services or Law enforcement

Pay-as-you-drive™

OnStar by GM

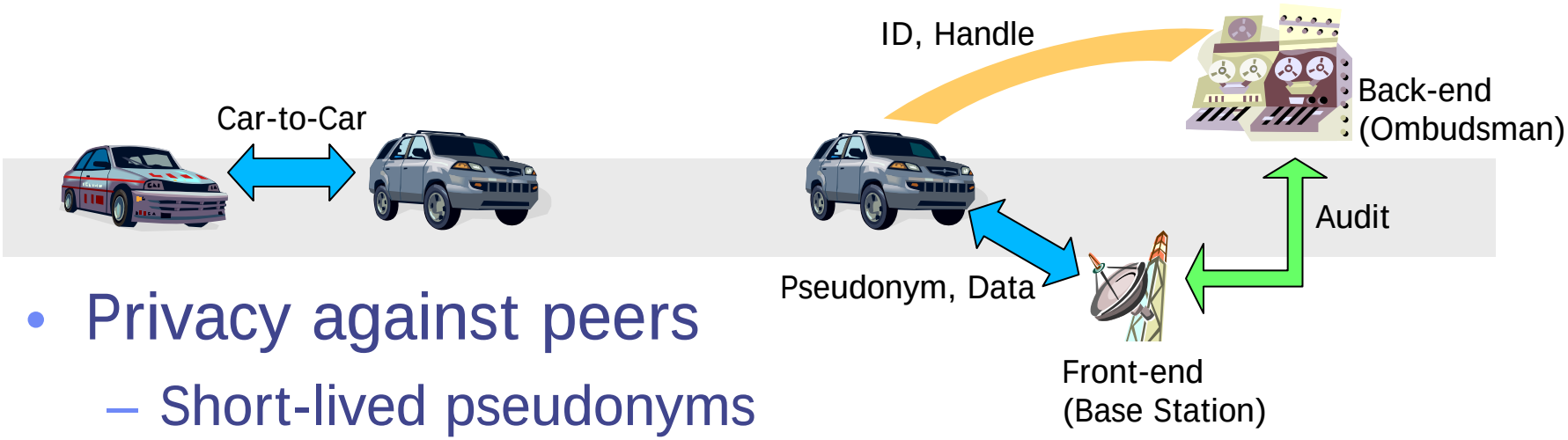
Design Decision - Privacy

- Global adversary model
  - Adversary can collect data from many places



  - Privacy concerns : Location, Context (things to be done or to do), and so on
  - Unauthorized tracing (e.g., tracing by means of toll payments, regarding stealing etc.)

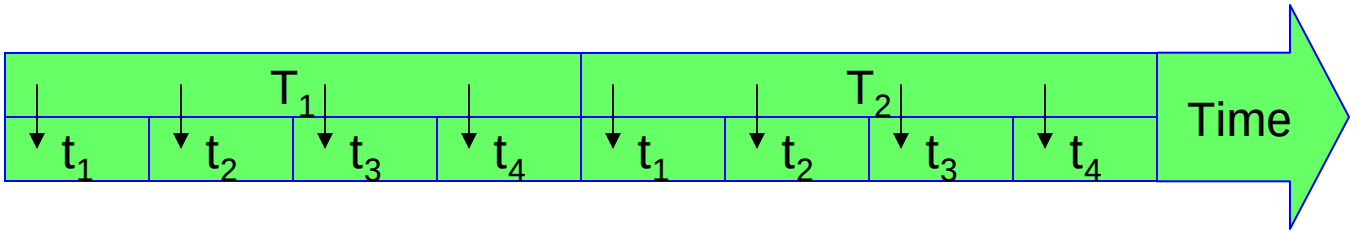
Design Decision - Privacy



- Privacy against peers
  - Short-lived pseudonyms
- Privacy against authorities
  - Front-end authorities (Base stations)
    - No trust relationship with nodes
    - Only allowed to access short-lived pseudonyms
  - Back-end authorities (Ombudsman)
    - Trust relationship
    - Identity information and long-lived pseudonyms (Handles)
    - No transaction data

Key Structure

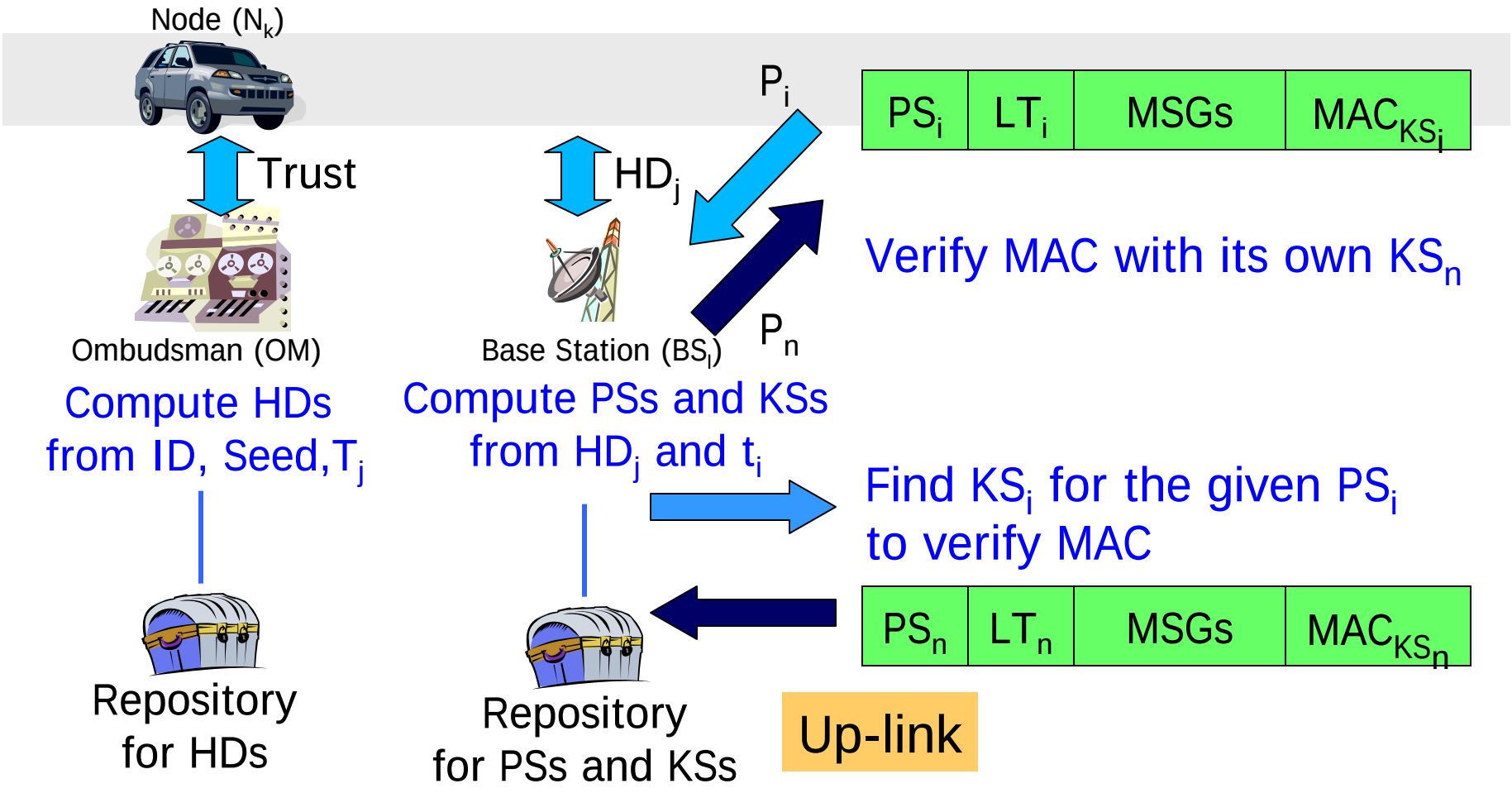
- Two different time intervals : Long time interval T and short time interval t



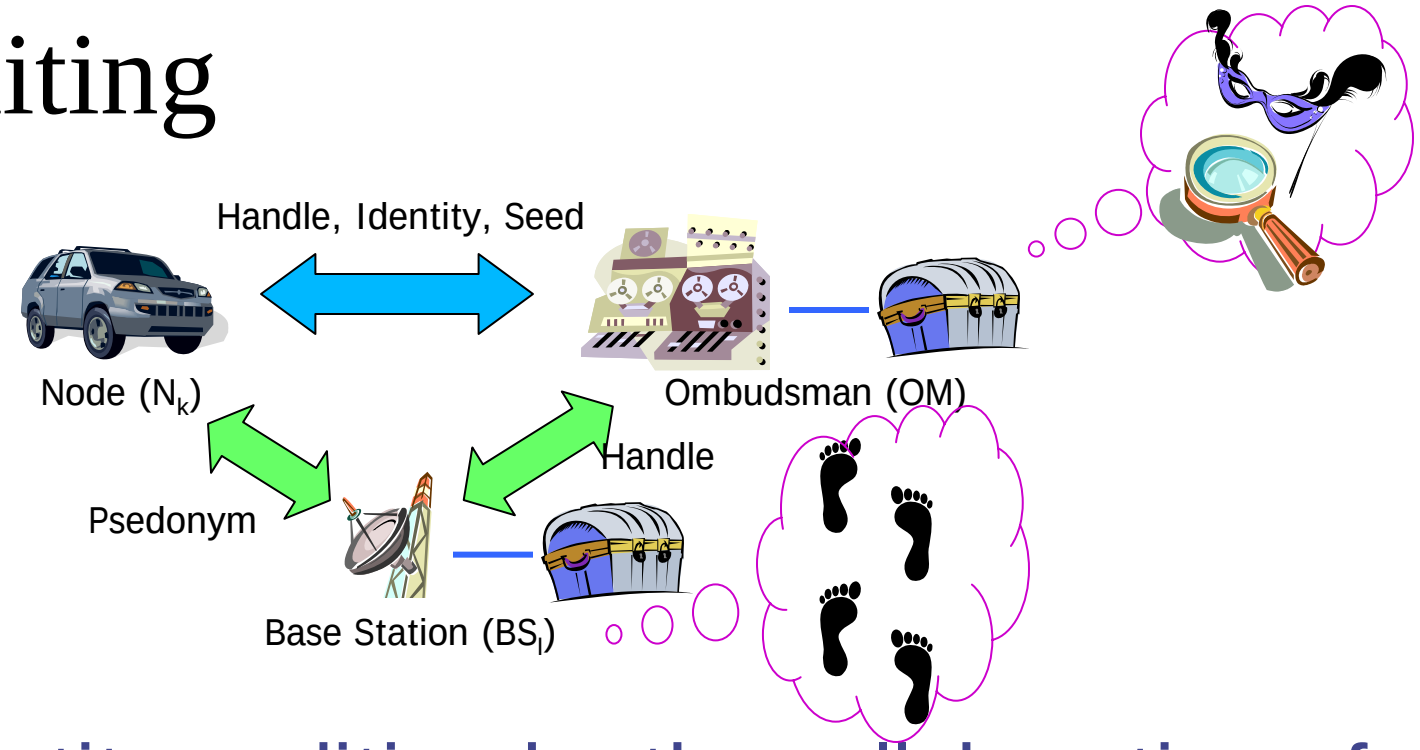
  - Handle changes w.r.t. long time interval T
    - HD_j = hash(ID, Seed, T_j)
  - Short-lived pseudonym w.r.t short time interval t
- Pseudonym(PS) and Shared key(KS) for MAC are tightly coupled
  - O_i = hash (HD_j , t_i) = PS || KS

Protocols

Key Registration | Initialization | Down-link

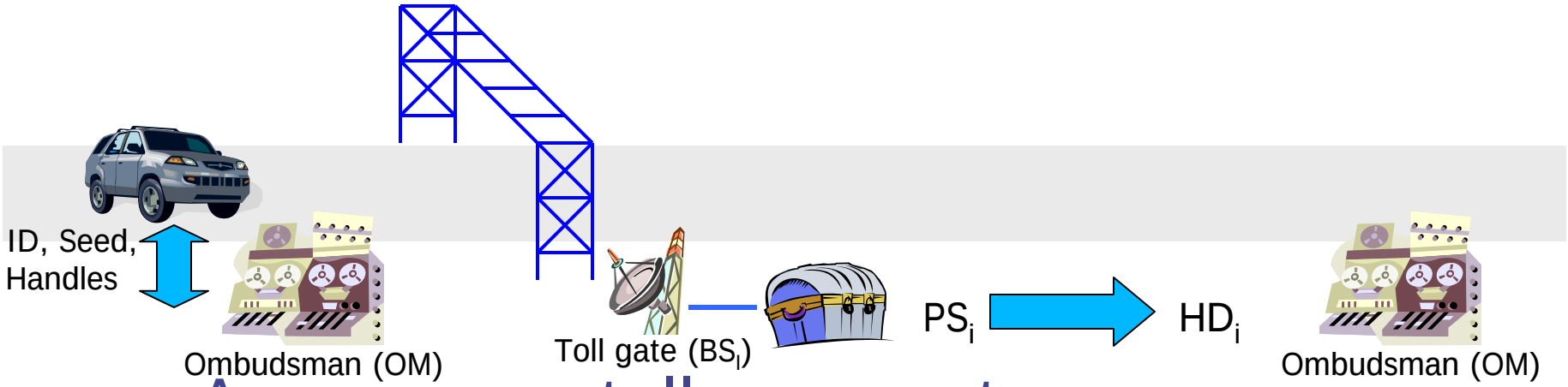


Auditing



- Identity auditing by the collaboration of BS and OM
  - BS queries its repository to find handle HD
  - For given HD, OM can find ID from the repository

Audit Example



- Anonymous toll payment
  1. Drivers have agreement with OM
  2. Toll gate (BS) doesn't need to know ID
  3. Toll gate (BS) collects PS and payment message saying he will pay $$
  4. Send HD computed from PS to OM
  5. OM finds ID from HD and outputs billing information

Conclusion

- Symmetric cryptosystem appears possible in vehicular networks
- Reduced communication overheads
- System with auditability and privacy
  - Privacy by the use of short-lived pseudonyms
  - Authentication with keyed MAC
- Incentives replace local verification

Questions and comments:

jychoi@indiana.edu