Empowered by Innovation NEC

Building Blocks for VANET Security

F. Armknecht, A. Festag, A. Hessler, O. Ugus, D. Westhoff, K. Zeng

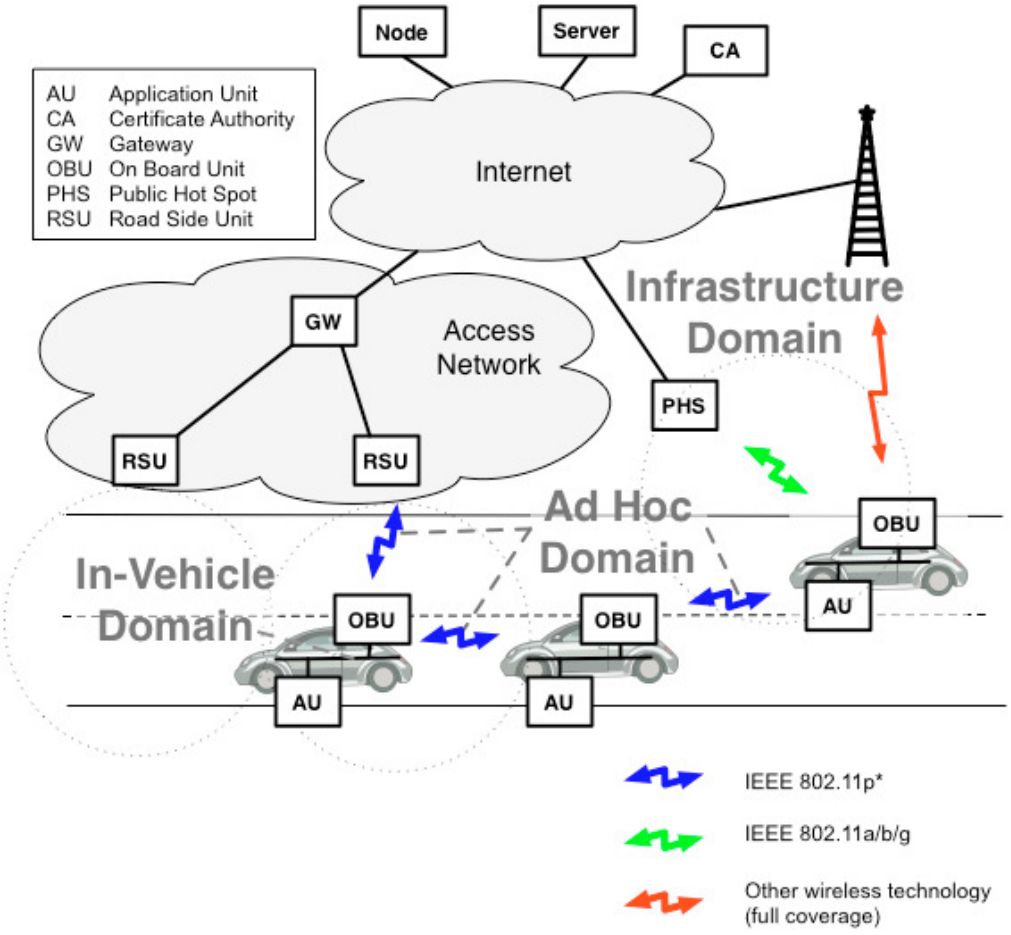
1) Cross-layer privacy enhancement and non-repudiation in vehicular communication

2) Roadside WSNs for Traffic Forensic

Part I

Cross-layer privacy enhancement and non-repudiation in vehicular communication

Intervehicular communication



Scenario:

Vehicles form with road side units a communication network

Goals:

- Improve traffic quality and safety
- Safety messages may warn about accidents, bad road quality, etc.

Security risks:

- Bogus information might cause damage
- Privacy might be compromised if identity is not protected during communication

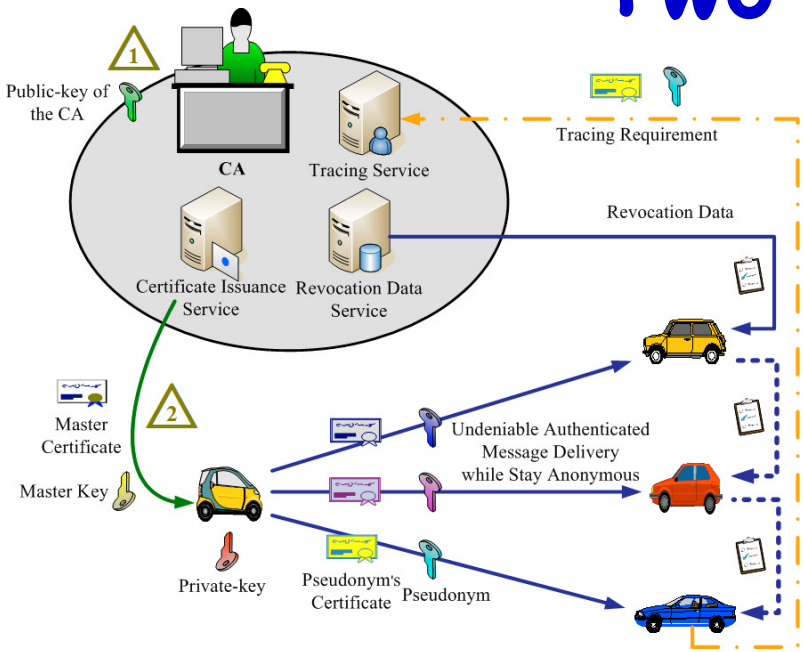
Solution:

- Sign messages with pseudonyms

Non-repudiation vs. Anonymity

- Trade-off between non-repudiation and anonymity
  - Anonymity can be achieved by the use of pseudonyms
  - Non-repudiation “requires” a digital message signature, and thus makes the pseudonyms useless (an attacker is able to track a certain vehicle by analyzing the digital signature of the messages)
- Cross-layer issue
  - Both non-repudiation and anonymity are only useful if ensured on *every* protocol layer

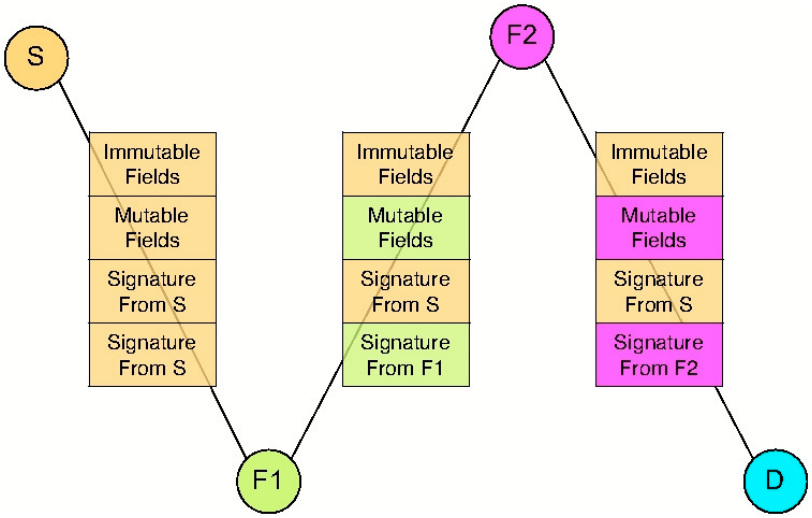
Two methods…



PKI+: [Zen06]

Public key infrastructure with additional advantages

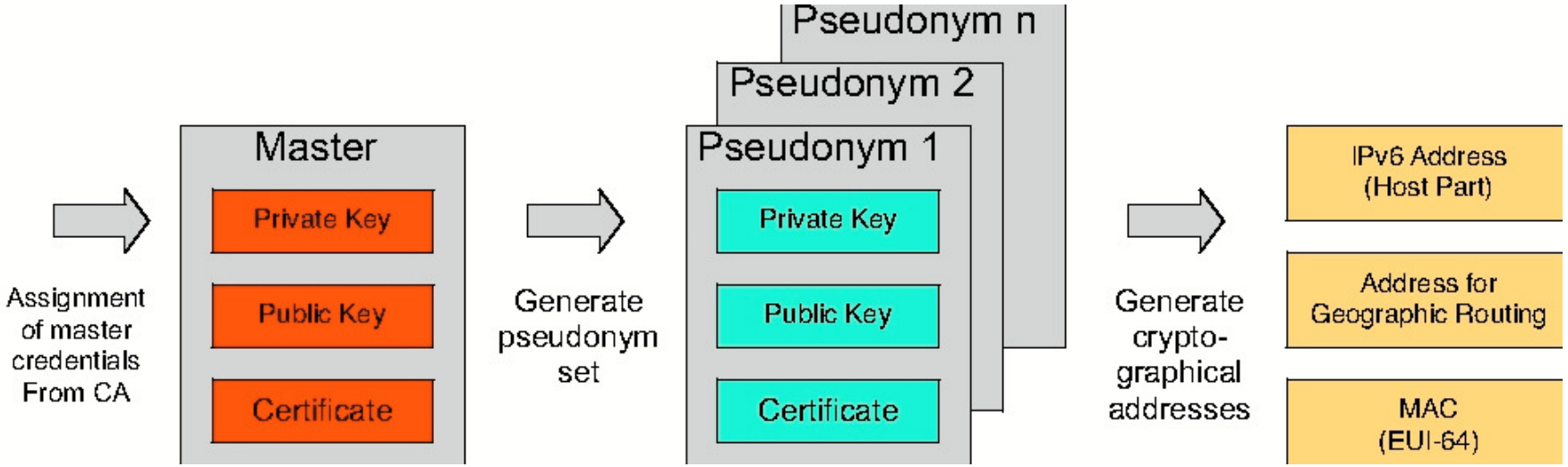
- Provides keys and certificates for signing
- User can create own pseudonyms
- Revocation data is comparatively small



Secure geographical routing: [Har 07]

- Messages are signed (immutable fields by sender S, mutable fields by current forwarder)
- Advantages:
  - Forwarded only by certified nodes
  - Authentication, integrity, non-repudiation

… one solution



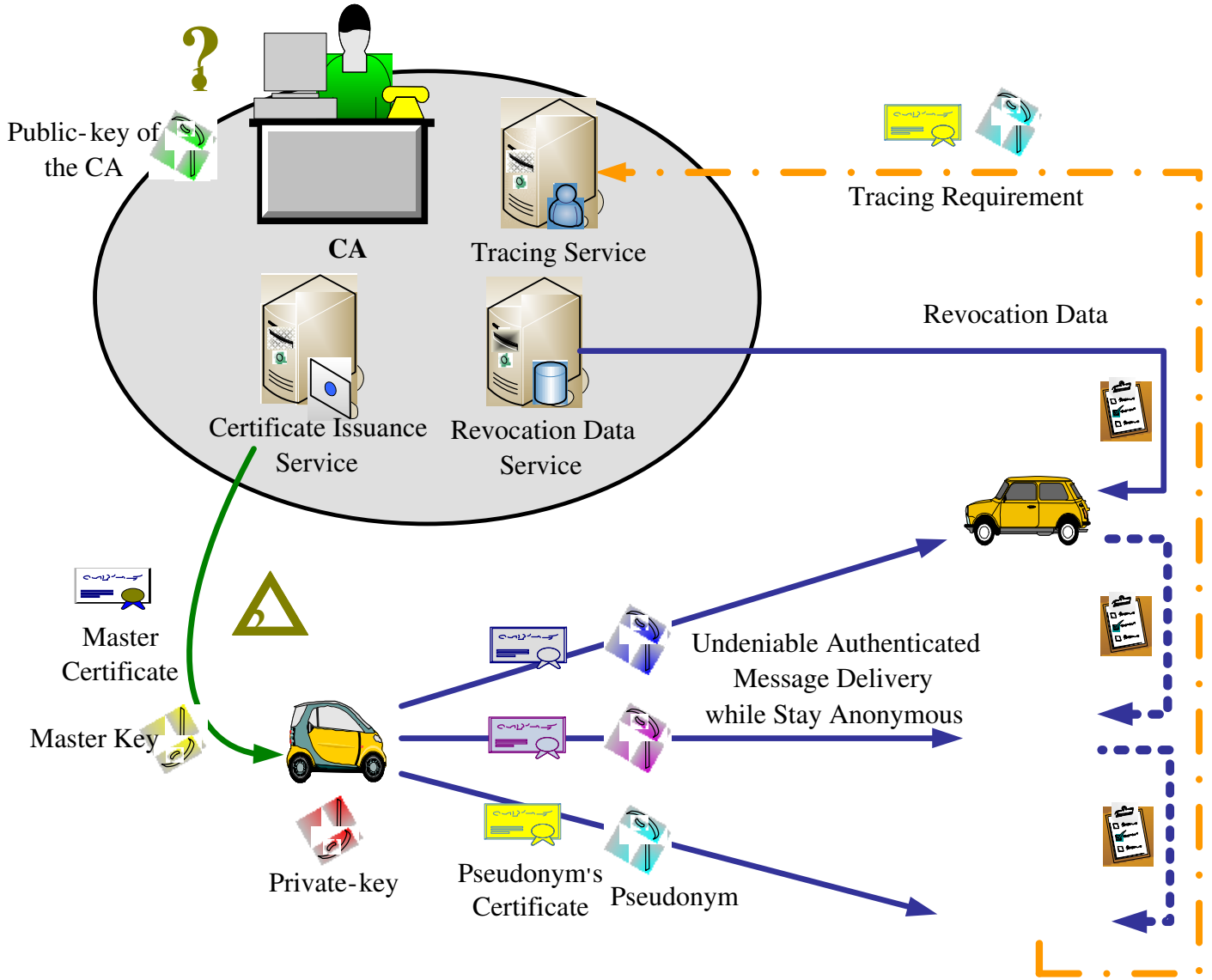
Combined security architecture: PKI+ and secure geographical routing:

- Master information from the certified authority enables user to create pseudonyms
- Pseudonyms are simultaneously used on different layers to provide non-repudiation and support privacy on all layers at the same time

PKI+ (1)

- Retains concept of PKI plus some additional features
- User can autonomously generate practically infinite number of pseudonyms with appropriate certificates
- Makes use of non-super-singular elliptic curve that supports bilinear mapping
- 5 stages:
  - CA setup (offline)
  - User enroll (offline)
  - Authentication
  - Tracing
  - Revocation

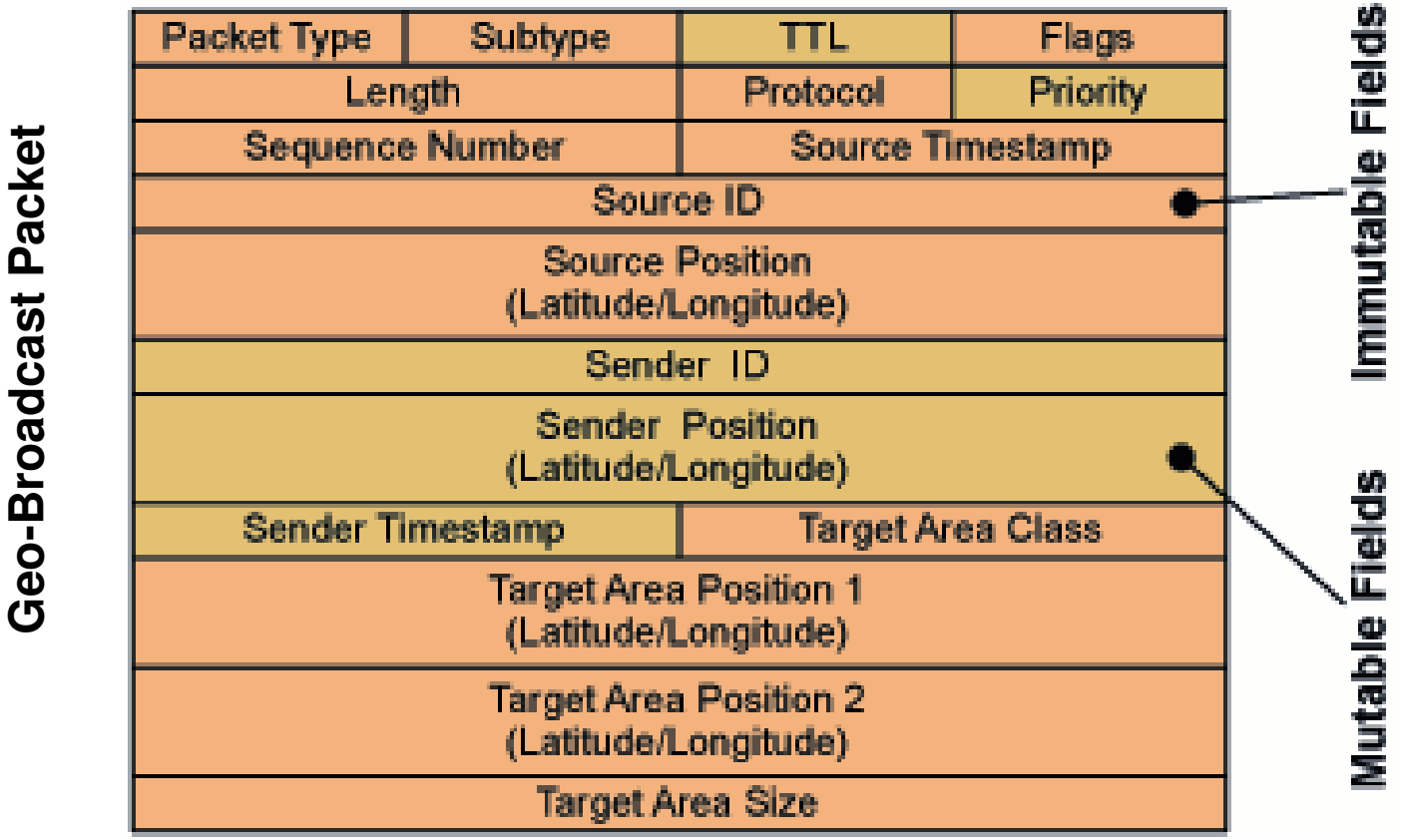
PKI+ (2)


Public-key of the CA
CA
Tracing Service
Tracing Requirement
Revocation Data
Certificate Issuance Service
Revocation Data Service
Master Certificate
Master Key
Undeniable Authenticated Message Delivery while Stay Anonymous
Private-key
Pseudonym's Certificate
Pseudonym

PKI+ (3): Main Benefits

- Protect Individual Privacy
  - Each user is equipped with mass pseudonyms (public-keys) and certificates
  - Efficient in terms of the size of certificate (680b) and the time to verify the certificate
- Protect System Safety
  - Authority can trace and revoke misbehaved user
  - As efficient as conventional public-key technology for signing messages online
  - Size of revocation data per revoked user is minimized (1.367b)
- Reduce Certification Authority Workload
  - Public-keys and certificates are NOT generated by the authority
  - Authority is largely offloaded from revocation

Secure Routing

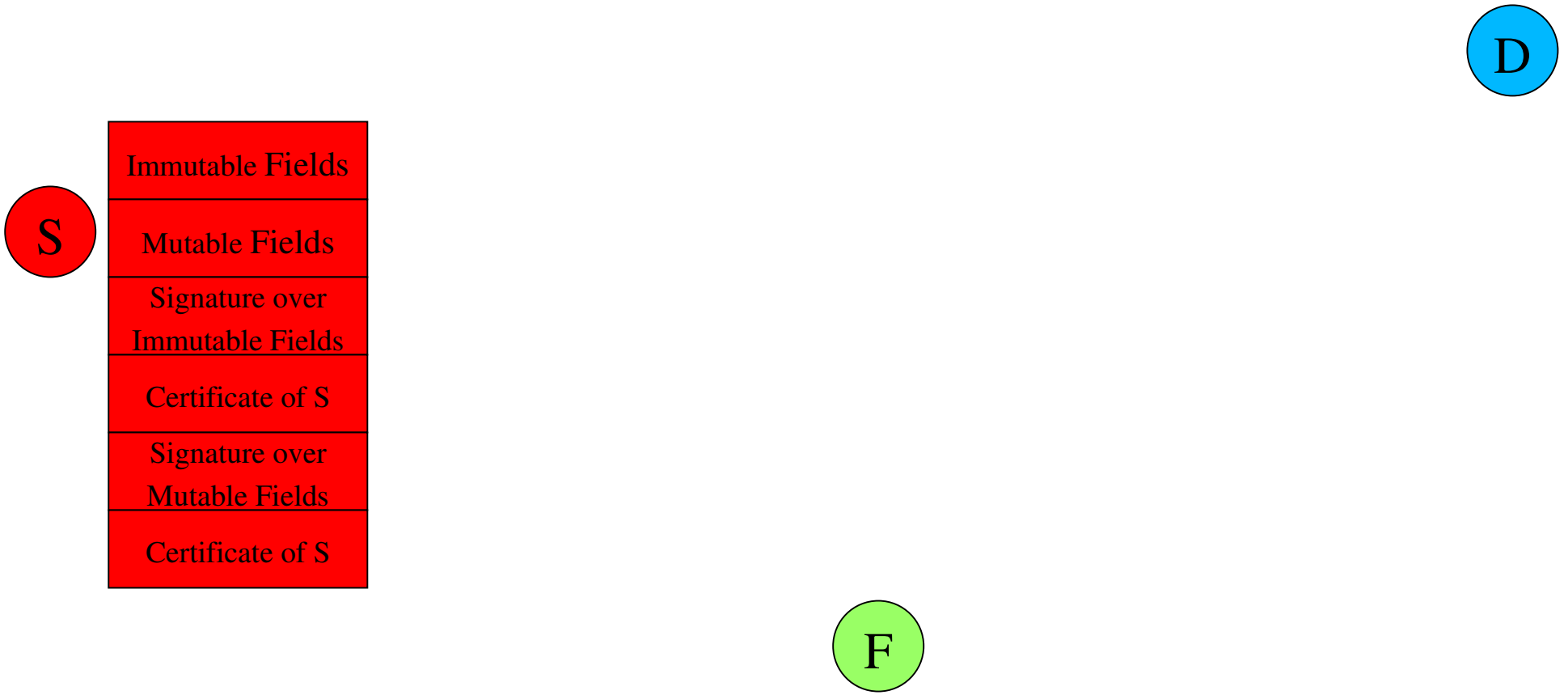


Immutable fields: not changed by forwarders

Mutable fields: updated during forwarding

Secure routing: Source

- Generate one signature over the immutable fields
- Generate another signature over the mutable fields

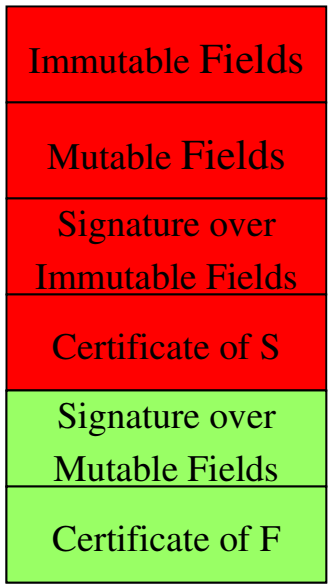


Secure routing: Source

- Verify timestamps and plausibility of position information
- Verify both signatures
- Update location table
- Verify if S does not exceed maximal allowed sending rate
- Replace mutable fields signature

S

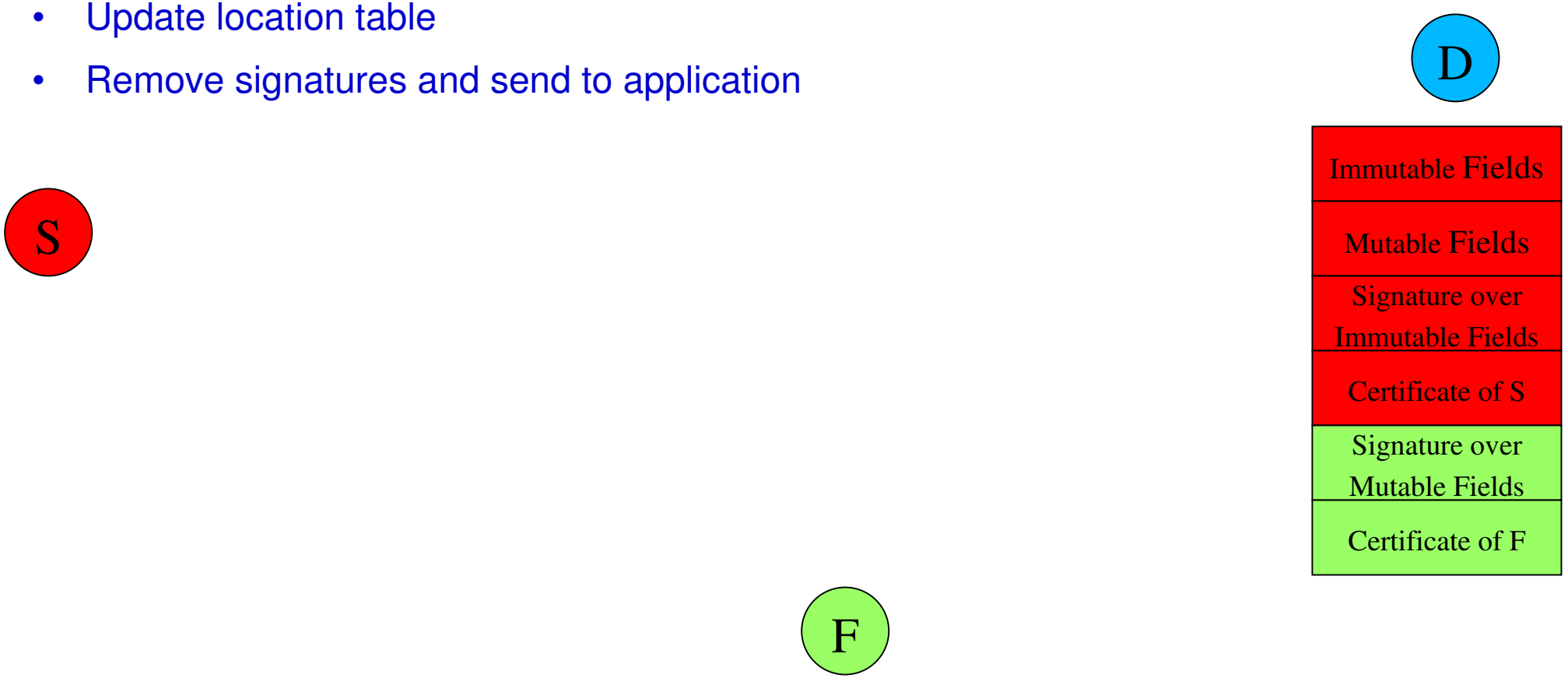
D



F

Secure routing: Source

- Verify timestamps and plausibility of position information
- Verify both signatures
- Update location table
- Remove signatures and send to application

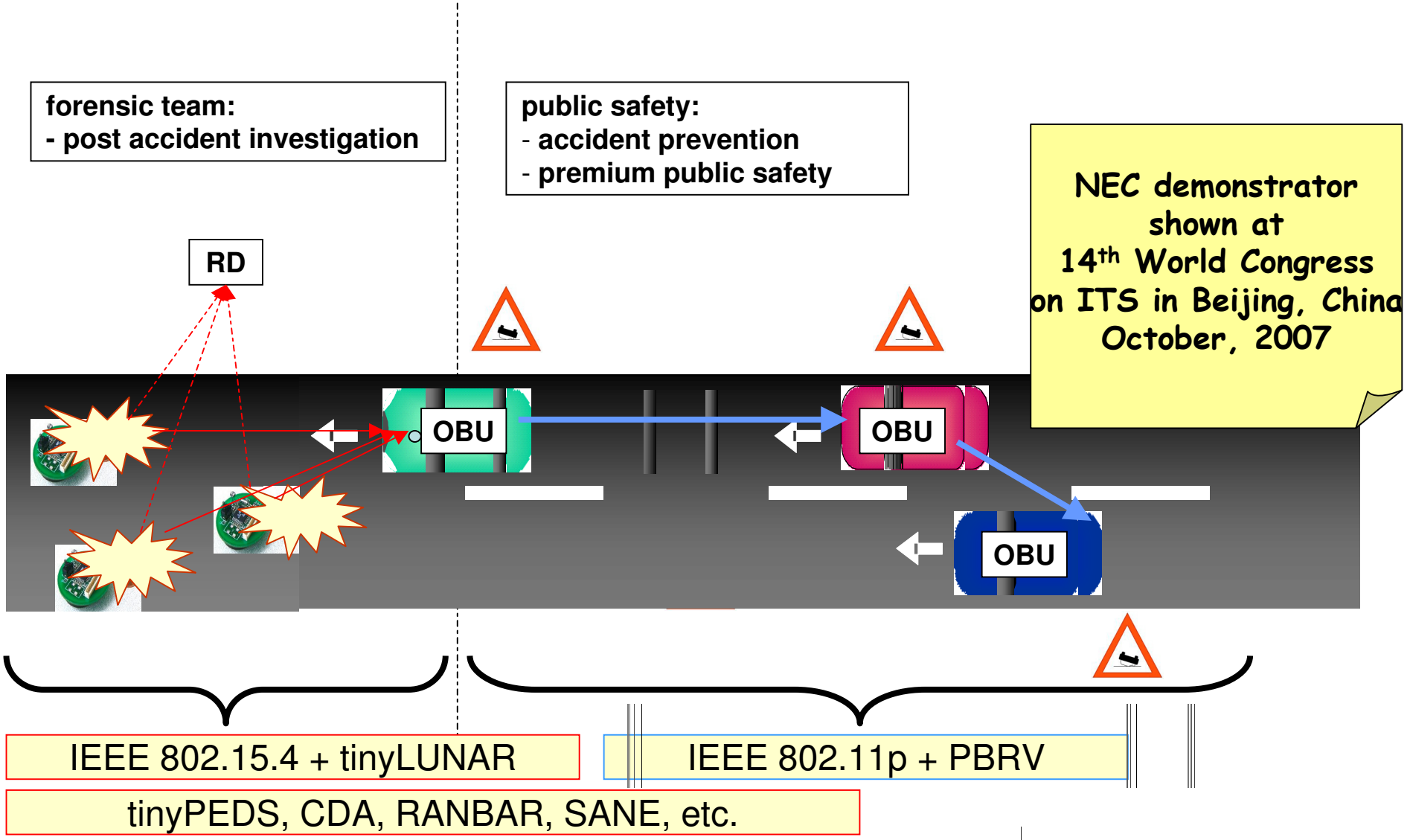


Conclusions

- Goals of intervehicular communication: improve traffic security and efficiency
- Anonymity and non-repudiation are mandatory for the user‘s acceptance of intervehicular communication
- Only effective if ensured over all protocol layers
- Our proposal: use PKI+ and digital signatures on every layer
- Secure routing through digital signatures, plausibility checks, and robustness mechanisms

Part II
Roadside WSNs…

WSN Roadside to Vehicular…

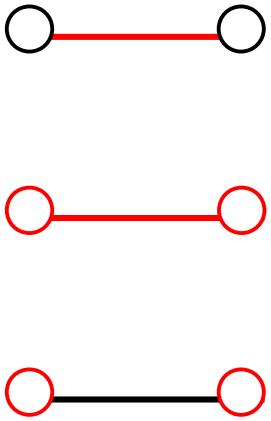


WSN adapted Threat Model…

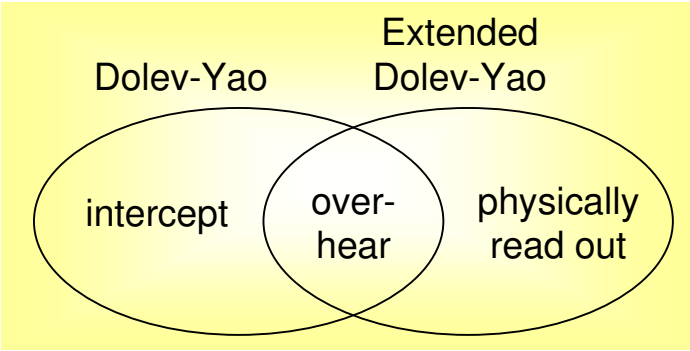
1) Dolev-Yao:
(known)

2) Extended
Dolev-Yao:
(WSN relevant)

3) Paradox
State of the art:



Threat-Model
with up to
5 years delay [Gligor05]



Options…

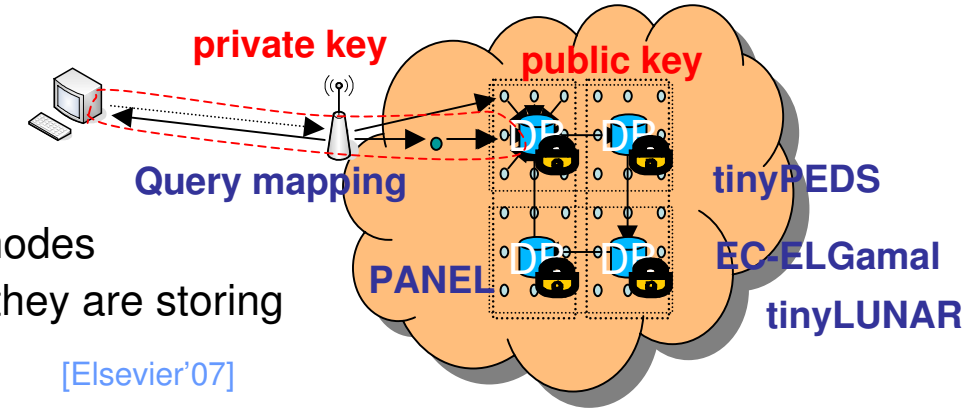
- Tamper-resistant unit (? too expensive)
- "Probabilistic" security (? attacker receives only limited gain)

TinyPEDS

Objectives

- long term data storage of the region's *"environmental fingerprint"*
- minimized transmission costs
- storage space balanced over multiple sensor nodes
- sensor nodes know the region NOT the value they are storing

[Elsevier'07]

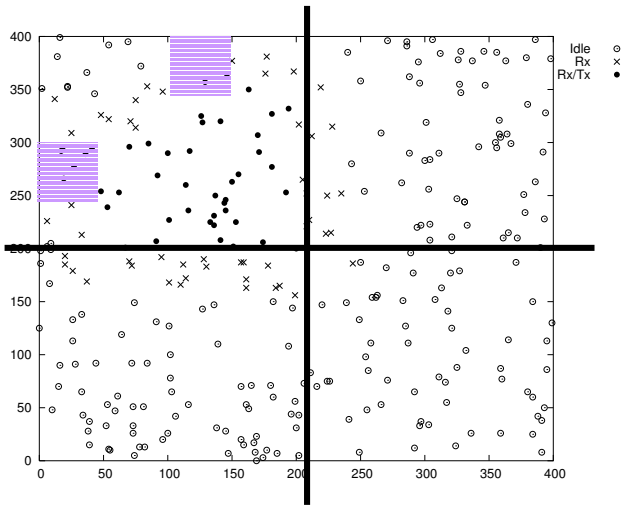


Approach

- first approach for *encrypted distributed data storage for WSNs*
- hybrid approach uses *symmetric* and *asymmetric* PHs

symmetric PH: $a_1+a_2 = D_k[E_k(a_1)+E_k(a_2)]$ [Mobiquitous'05]

asymmetric PH: $a_1+a_2 = D_q[E_p(a_1)+E_p(a_2)]$ [ICC'06]



- efficient linkage from "database query" to "controlled flooding message"
- restoring rules of remaining quarters in case of a disaster
- Optional: Overlapping WSNs: WSN_{PH} and WSN_{OPES} [WiOpt'05]

Asymmetric PH: EC-ElGamal

- **Private key**: $x \in GF(p)$

  Public key: E, p, G, Y (E of order n)

  whereby $Y=xG$ and E over $GF(p)$ with $G, Y \in E$

- **Encryption:** plaintext $m \in [0, p-1]$, random $r \in [1, n-1]$,

  $M=map(m)$

  $C=enc(m)=(R, S)=(rG, M+rY)$

- **Decryption:**

  $M=dec(C)=dec(R, S)=-xR+S$

  $m=rmap(M)$ ← **ECDLP!!**

  (brute force at sink node)

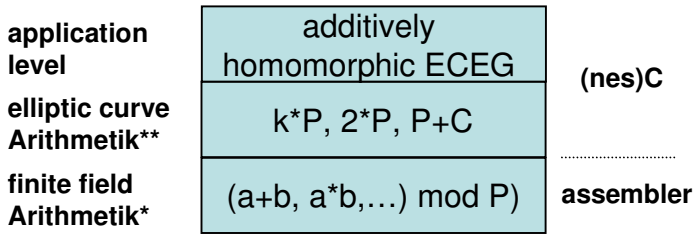
- **Mapping function:**

  from multiplicative to additive homomorphic

  $map(a_1+a_2) = (a_1+a_2)G = a_1G + a_2G$
  $= map(a_1) + map(a_2)$

[Asiacrypt'00]

Design Architecture



Implementation Results on MicaZ

#Pr points	Ex. Time [sec]	Code size [bytes]	Memory size [bytes]
0	2.52	2790	320
0	2.14	3162	561
2	1.4	3996	621
4	1.17	6158	683

Ciphertext size: 2(p+1), e.g. 328bit

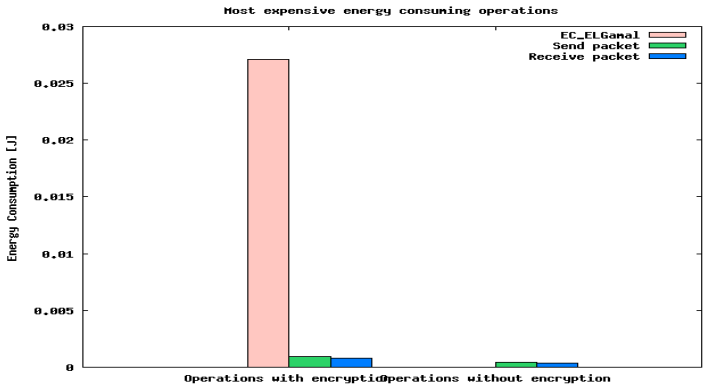
[OU'07]
[MobiCom'07]

**multiplication: interleave method, signMOF
*pseudo-Mresenne prime reduction

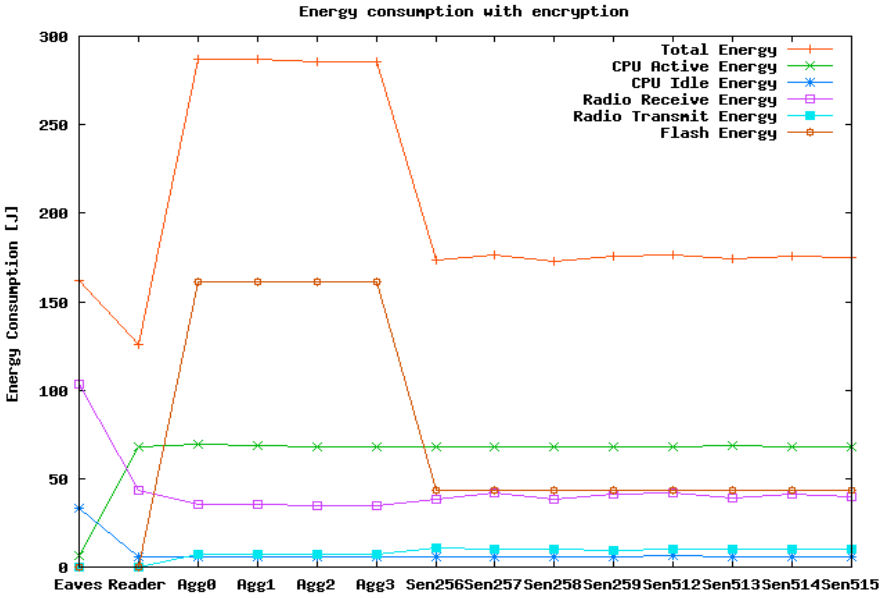
AVRORA: Energy Consumption

- Initial energy emulation with AVRORA
- more work required

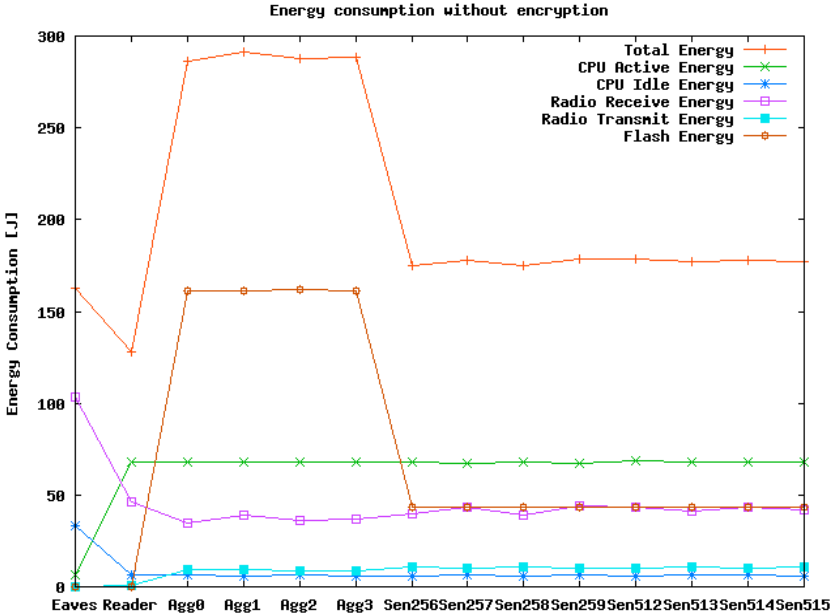
(1h emulation, epoch:= 1min, slot:=20 sec)



tinyPEDS with encryption:



tinyPEDS without encryption:



Publications…

PKI+

F. Armknecht, A. Festag, D. Westhoff, K. Zeng
Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication,KIVS WMAN, Bern, Swiss, February 2007.

K. Zeng
Pseudonymous PKI for Ubiquitous Computing, EuroPKI, pp.207-222, Turin, Italy, 2006.

Roadside WSN

J. Girao, D. Westhoff, E. Mykletun and T. Araki
TinyPEDS: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks, Elsevier Ad Hoc Networks Journal, Vol. 5, Issue 7, pp. 1073-1089, September 2007.

- Hessler, J.M. Bohli, O. Ugus, D. Westhoff

Secure and Resilient WSN Roadside Architecture for Intelligent Transport Systems, under submission

O. Ugus, A. Hessler, D. Westhoff
Performance of Additive Homomorphic EC-ELGamal Encryption for TinyPEDS, 6te Fachgespräch Sensornetze der GI/ITG-Fachgruppe Kommunikation und Verteilte Systeme, Technischer Bericht der RWTH Aachen ISSN 0935-3232, Germany, July, 2007.