Moderne Konzepte für Datenschutz und IT-Sicherheit im Smart Grid

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)

http://svs.informatik.uni-hamburg.de/

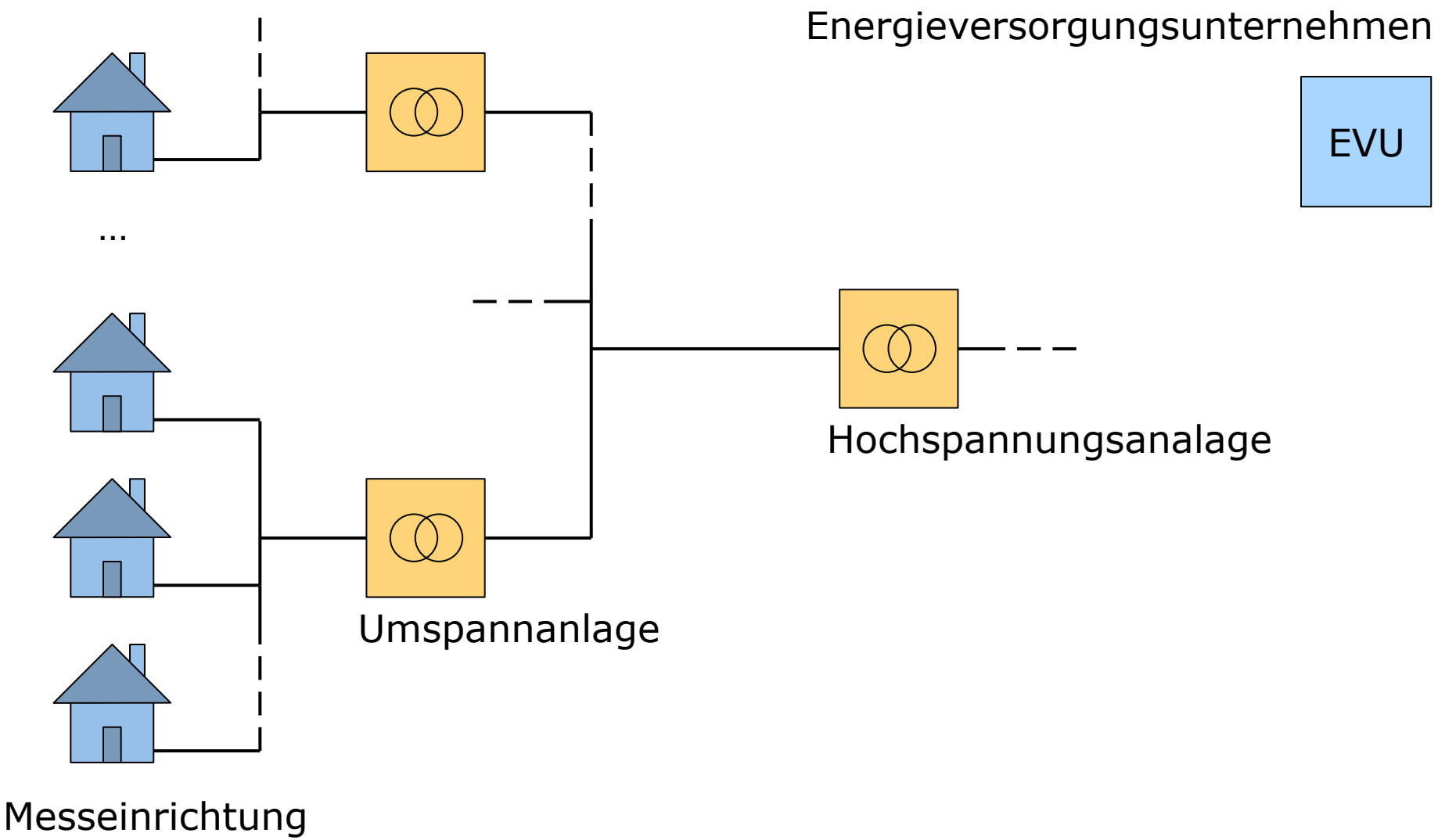
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Stuttgart, 6. November 2012

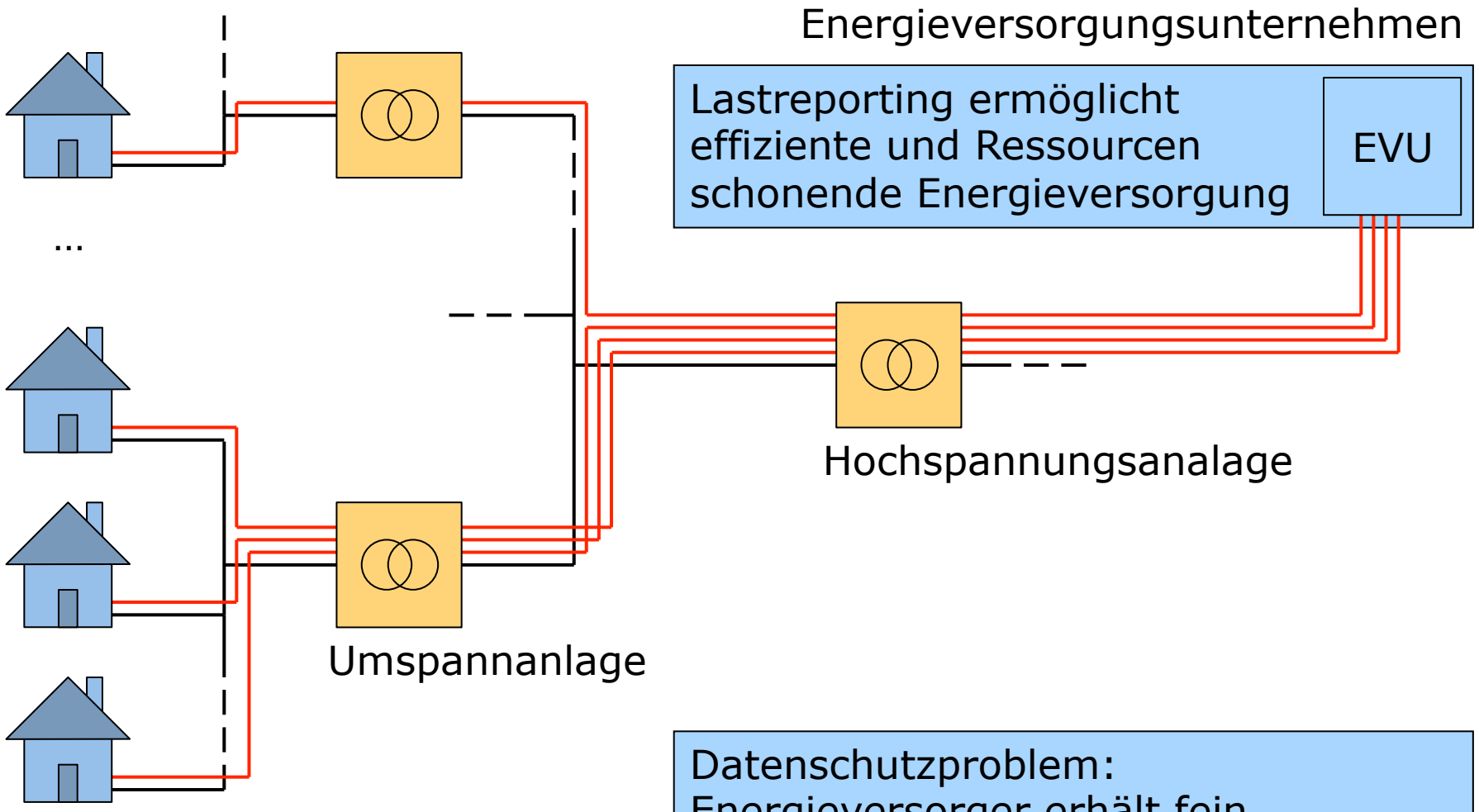
Gliederung des Vortrags

- Einführung
  - Lastreporting: Verletzung der Privatsphäre durch Smart Meter
  - Datenschutzrechtliche Einordnung
  - Schutzziele und Angreifermodell
- Konzepte zum Schutz der Privatheit
  - Triviale Ansätze zur Datensparsamkeit
  - Proxy-basierte Verfahren
  - Verfahren ohne Notwendigkeit eines vertrauenswürdigen Dritten
- Schlussbemerkungen

Typische Architektur



Typische Architektur



Datenschutzproblem:
Energieversorger erhält fein aufgelöste Informationen über Energienutzung eines jeden Haushalts

Datenschutzrechtliche Einordnung

Lastreporting ermöglicht effiziente und Ressourcen schonende Energieversorgung

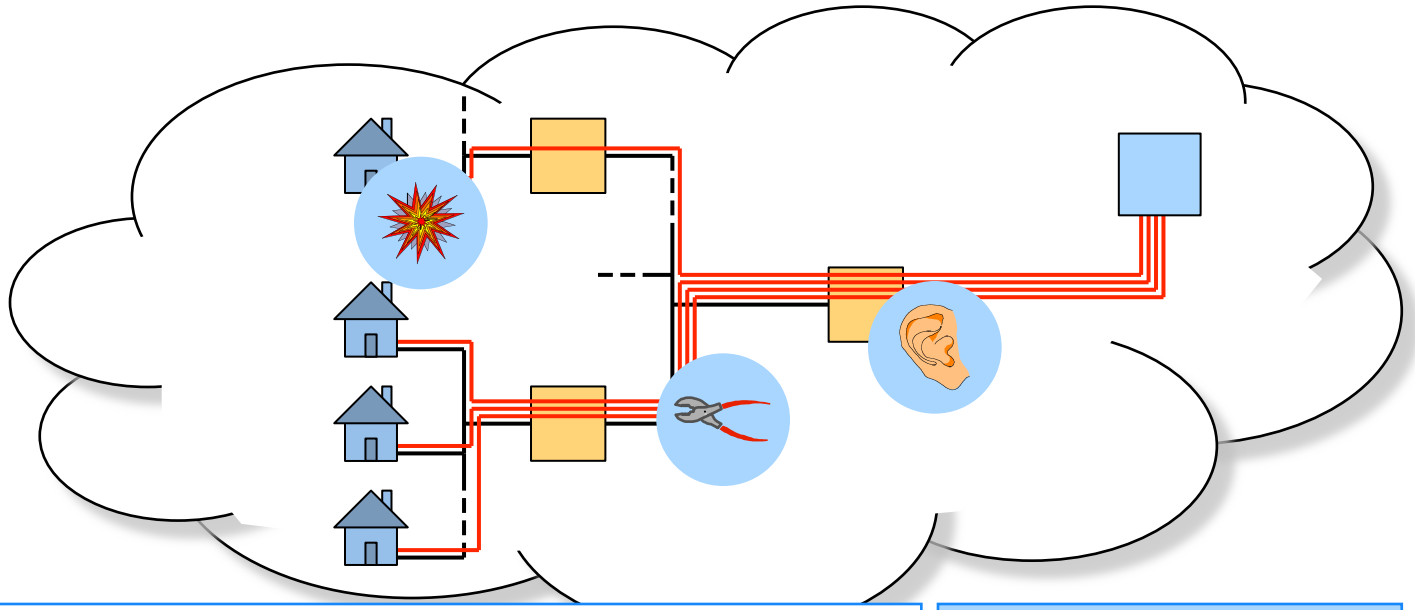
EVU

- § 3a BDSG: Datenvermeidung und Datensparsamkeit:

  Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Gesucht sind Lösungen, die ein Lastreporting zur Ressourcen schonenden Energieversorgung unter Wahrung der informationellen Selbstbestimmung ermöglichen.

Schutzziele und Angreifermodell



Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Triviale Ansätze zur Datensparsamkeit

- Intervalle zur Datenerhebung vergrößern

  oder

- Aggregation mehrerer Haushalte

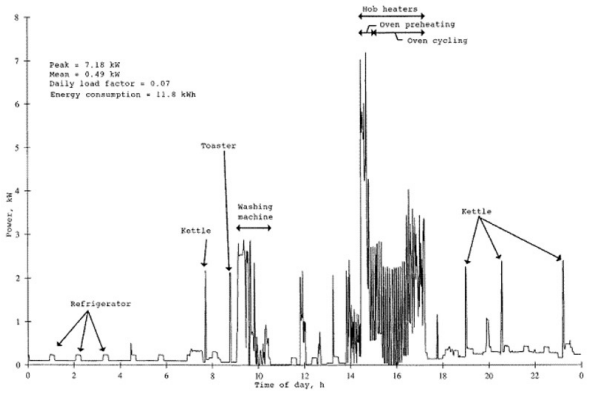
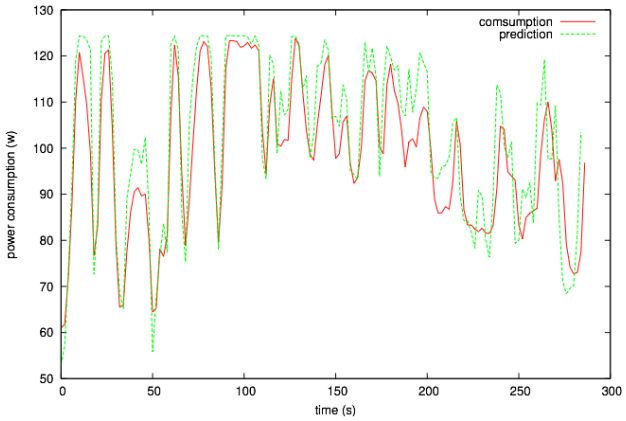


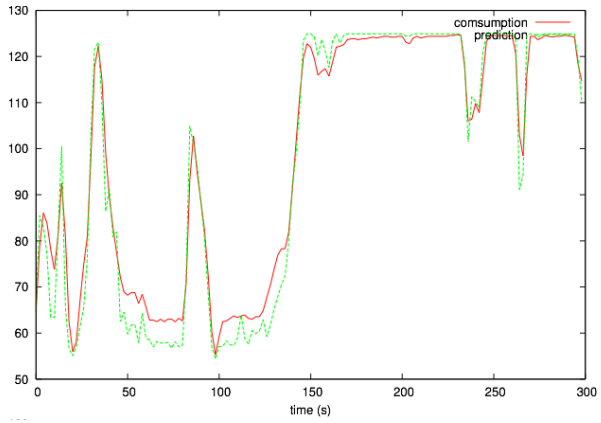
Bild: NIST

- Mit sekundengenauen Daten sind sogar Fernsehprogramme detektierbar (Greveler, Justus, Löhr 2012):

Star Treck 11



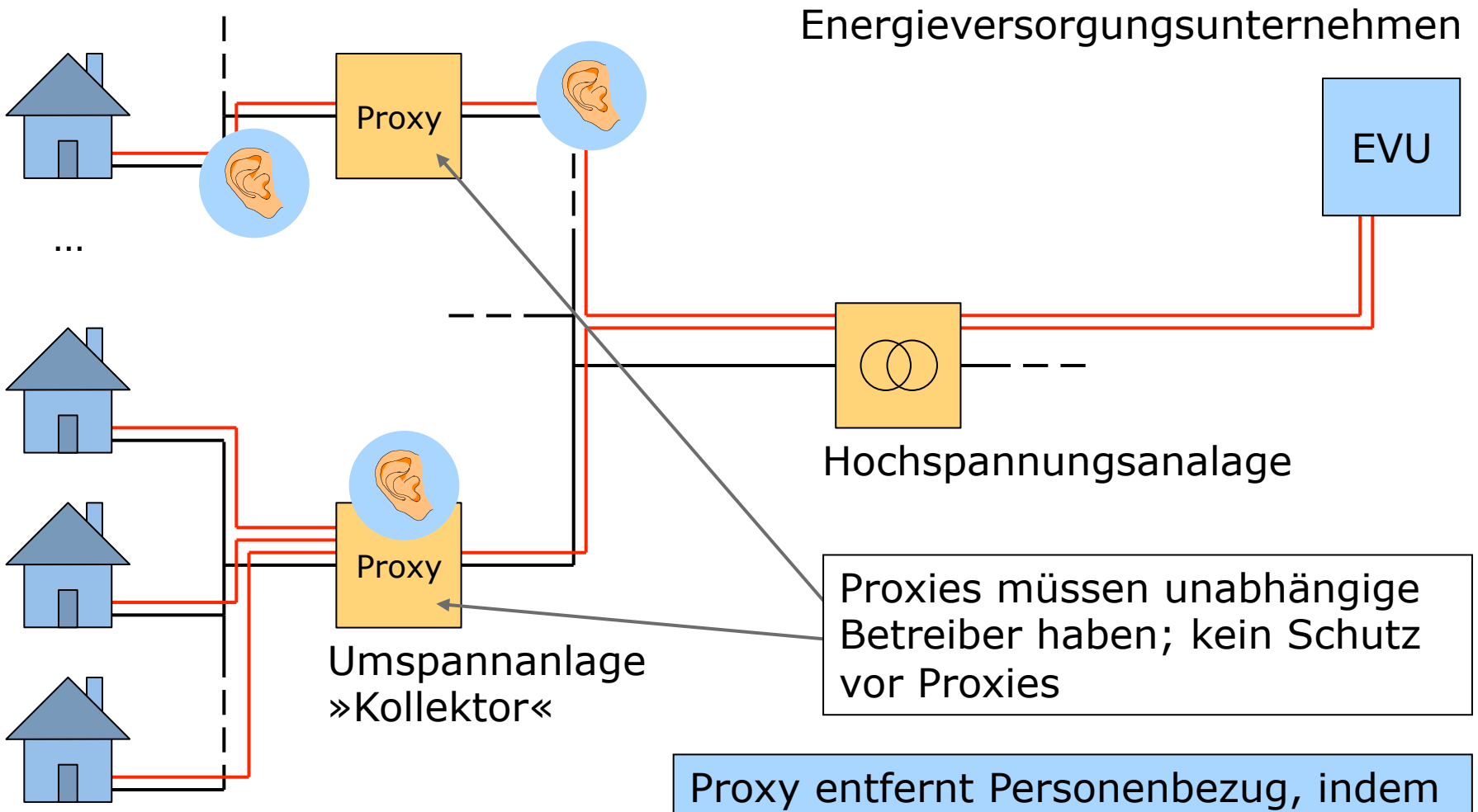
Star Treck TNG



Bilder: NIST, Greveler et. al.

Proxy-basierte Verfahren

Petrlic, 2011



Verfahren ohne Notwendigkeit eines vertrauenswürdigen Dritten

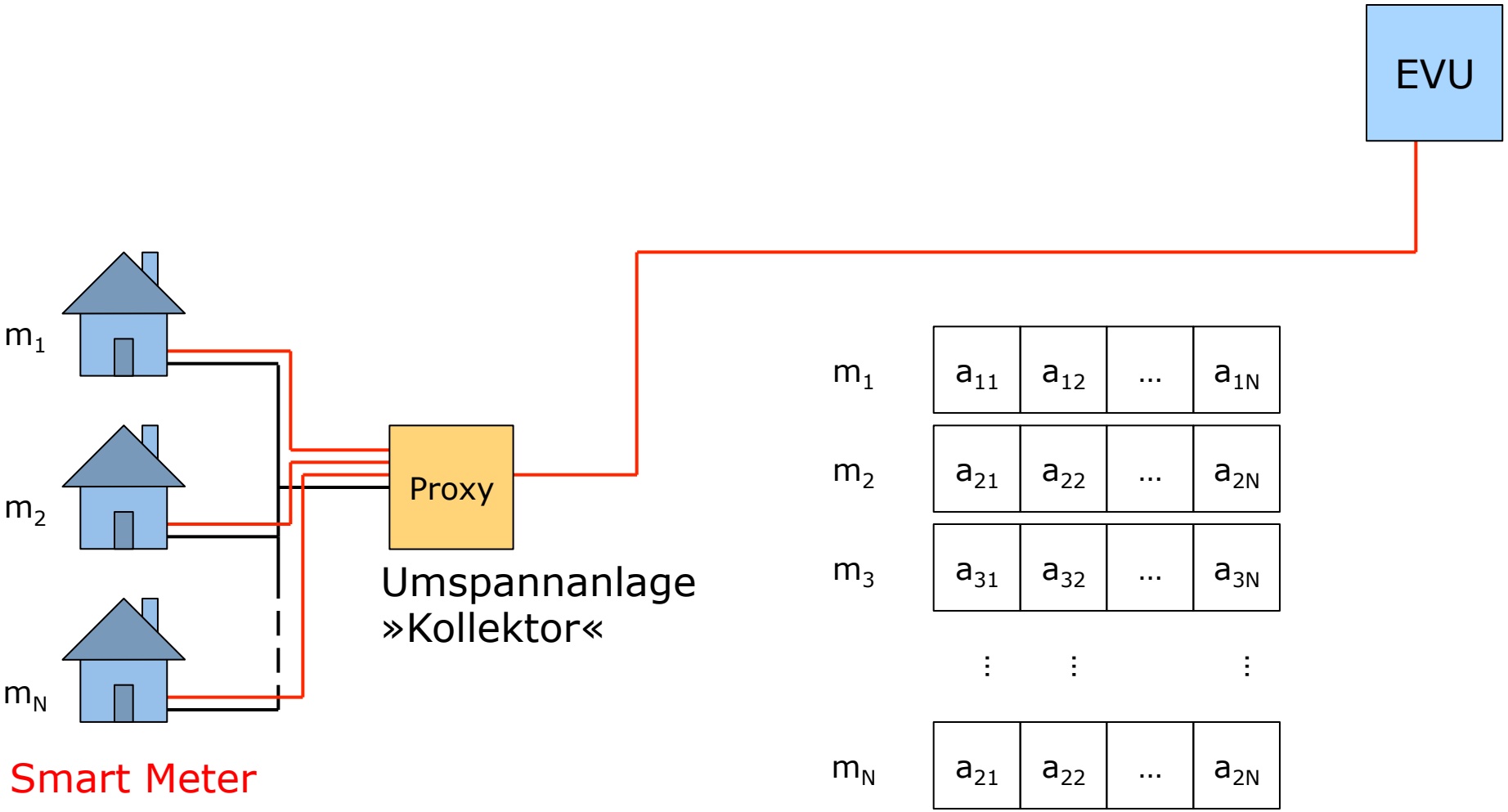
- Ziel: kein Vertrauen in einen zwischengeschalteten Proxy/Kollektor

- Ansatz Homomorphe Verschlüsselung (Garcia, Jacobs, 2010)
  - Zerlegen der Smart Meter Daten in N Teile
  - Teile werden einzeln verschlüsselt
  - Kollektor aggregiert summiert über verschlüsselten Teilen

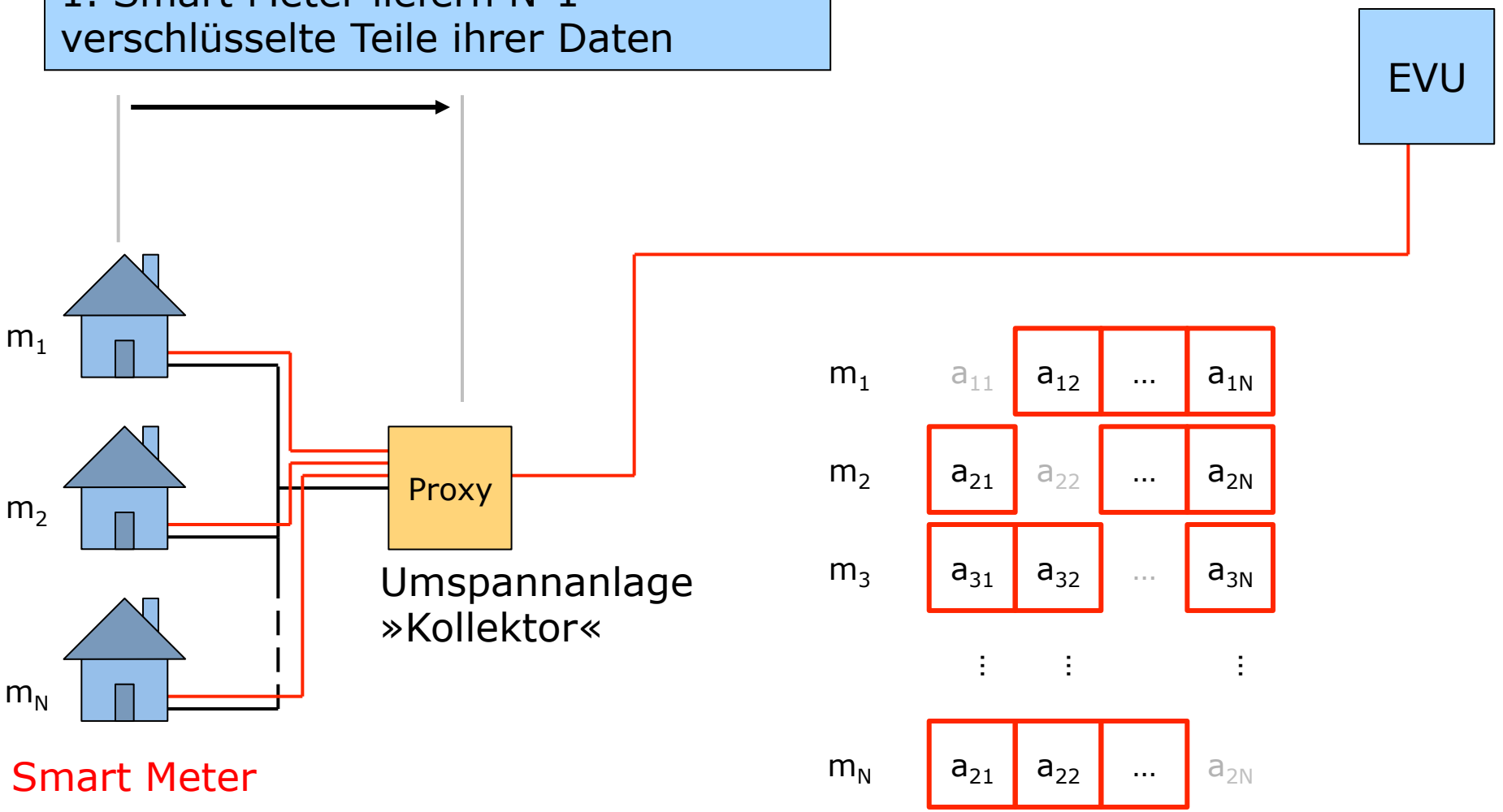
- Ansatz Zero Knowledge Proof of Knowledge (Jeske, 2011)
  - Smart Meter Daten werden anonym an Kollektor übermittelt
  - Es wird bewiesen, dass die Daten von einem »echten« Smart Meter stammen, ohne dies identifizieren zu können
    - Wäre auch realisierbar mit anderen kryptographischen Primitiven
    - Setzt Schutz der Kommunikationsbeziehung voraus

Ansatz Homomorphe Verschlüsselung

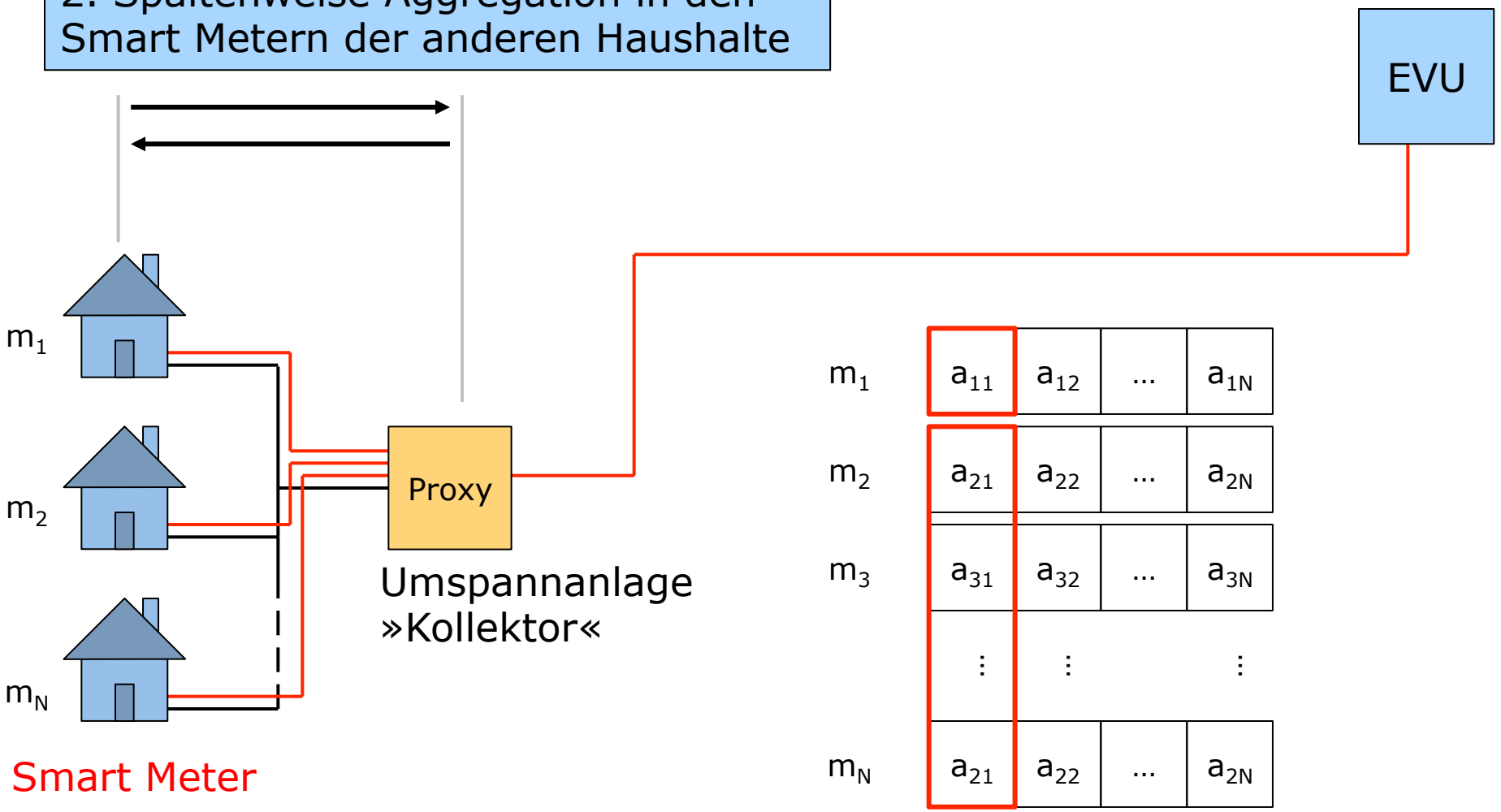
Garcia, Jacobs, 2010



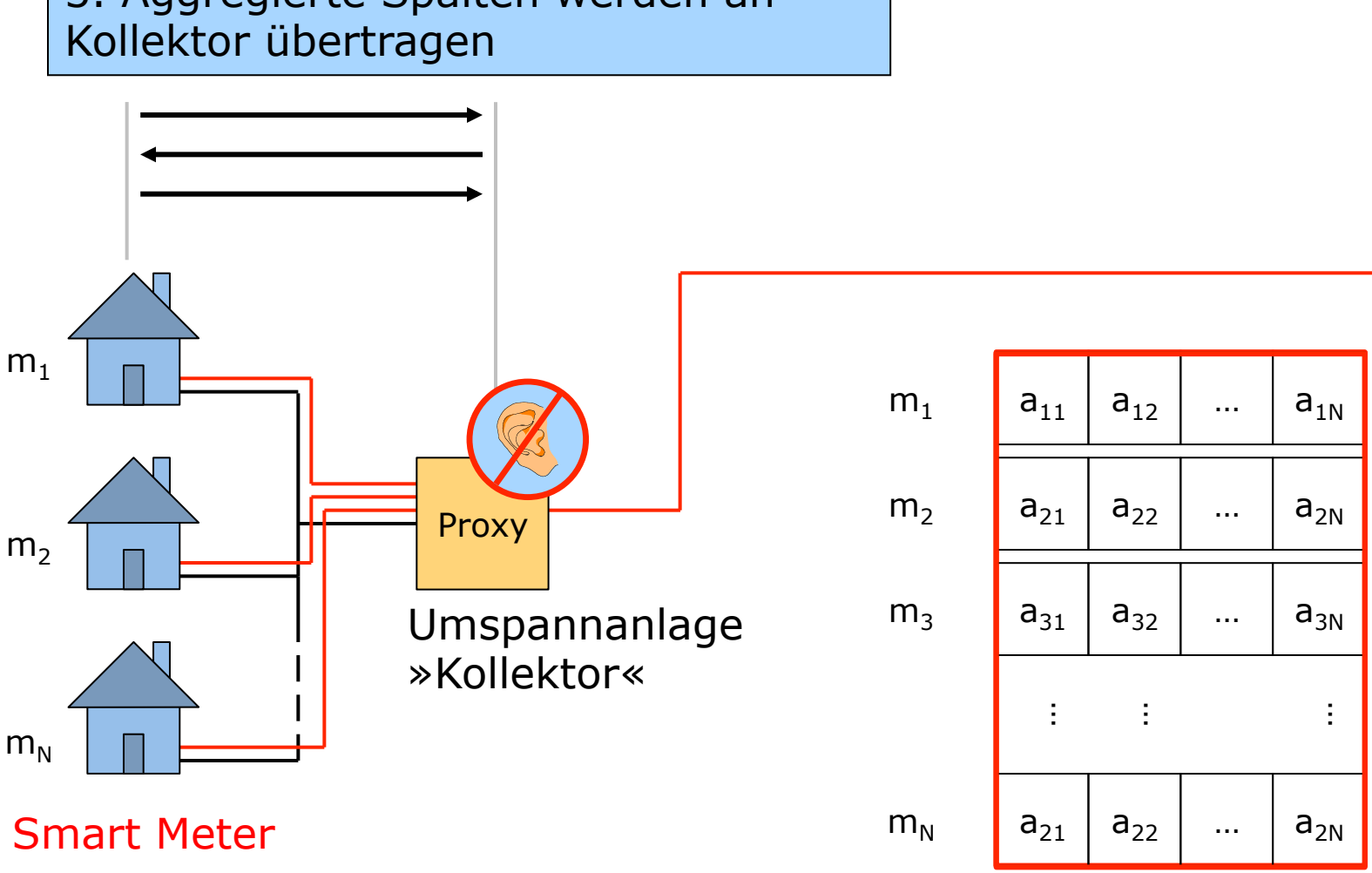
1. Smart Meter liefern N-1 verschlüsselte Teile ihrer Daten



2. Spaltenweise Aggregation in den Smart Metern der anderen Haushalte



3. Aggregierte Spalten werden an Kollektor übertragen



Verfahren ohne Notwendigkeit eines vertrauenswürdigen Dritten

- Ziel: kein Vertrauen in einen zwischengeschalteten Proxy/Kollektor

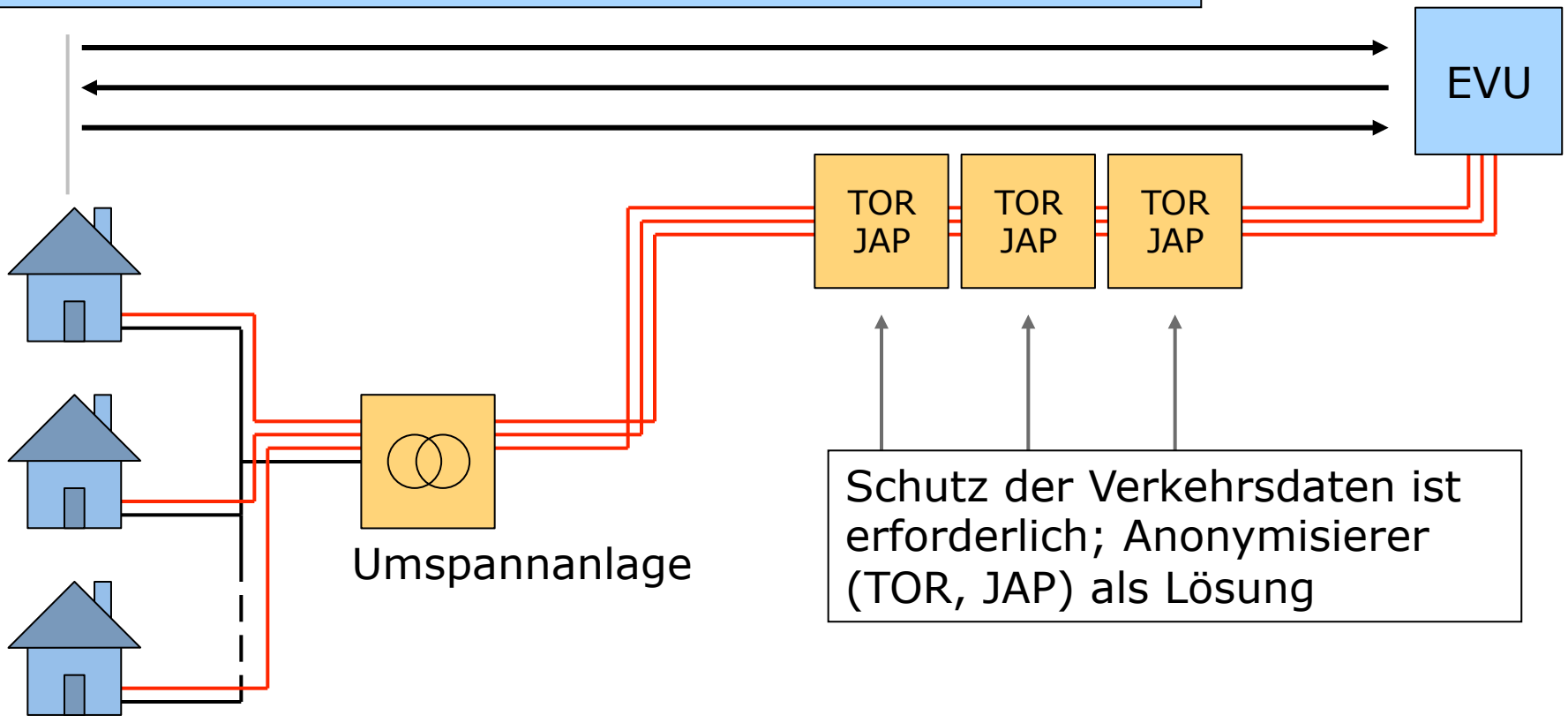
- Ansatz Homomorphe Verschlüsselung (Garcia, Jacobs, 2010)
  - Zerlegen der Smart Meter Daten in N Teile
  - Teile werden einzeln verschlüsselt
  - Kollektor aggregiert summiert über verschlüsselten Teilen

- Ansatz Zero Knowledge Proof of Knowledge (Jeske, 2011)
  - Smart Meter Daten werden anonym an Kollektor übermittelt
  - Es wird bewiesen, dass die Daten von einem »echten« Smart Meter stammen, ohne dies identifizieren zu können
    - Wäre auch realisierbar mit anderen kryptographischen Primitiven
    - Setzt Schutz der Kommunikationsbeziehung voraus

Ansatz Zero Knowledge Proof of Knowledge

Jeske, 2011

Interaktives Protokoll ermöglicht ohne Identifizierung den Nachweis der Echtheit der Smart Meter Daten



Schlussbemerkungen

- Notwendige Infrastrukturmaßnahmen zum Schutz der Privatheit
  - Gewaltenteilung vorsehen; unabhängige Betreiber
  - Trennung von Energieversorgungsnetz und Kommunikationsnetz

- Keine Lösungen ohne Sicherheitsexperten entwickeln

Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de