Sichere Gruppenkommunikation

Von
Benjamin Jochheim

Übersicht

- Einsatz von Gruppenkommunikation
- Sicherheitsaspekte
- Point to Point (PtP) Verschlüsselung
  - Übertragbarkeit auf Broadcast
- Sicherer Broadcast TESLA

Kommunikation via Broadcast

Einsatzgebiete

- Pay-TV
- Sichere Softwareupdates
- Sensornetzwerke
- Multiplayer-Spiele
- Informierte Navigationssysteme

Broadcast Schwierigkeiten

- Verlässlicher Transport
- Empfänger mit unterschiedlichen Ressourcen
- Congestion-Control
- Sicherheitsaspekte

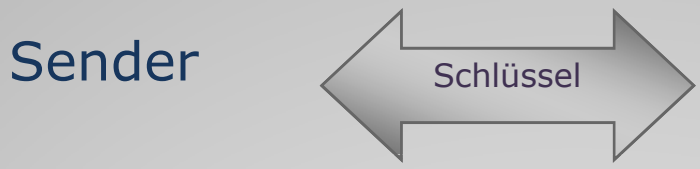
Fokus der Sicherheit

- Empfang ist unsicher (z.B. via UDP)
- Authentisierung auf Paketebene
- Möglichst leicht gewichtig
- Empfänger nicht vertrauenswürdig

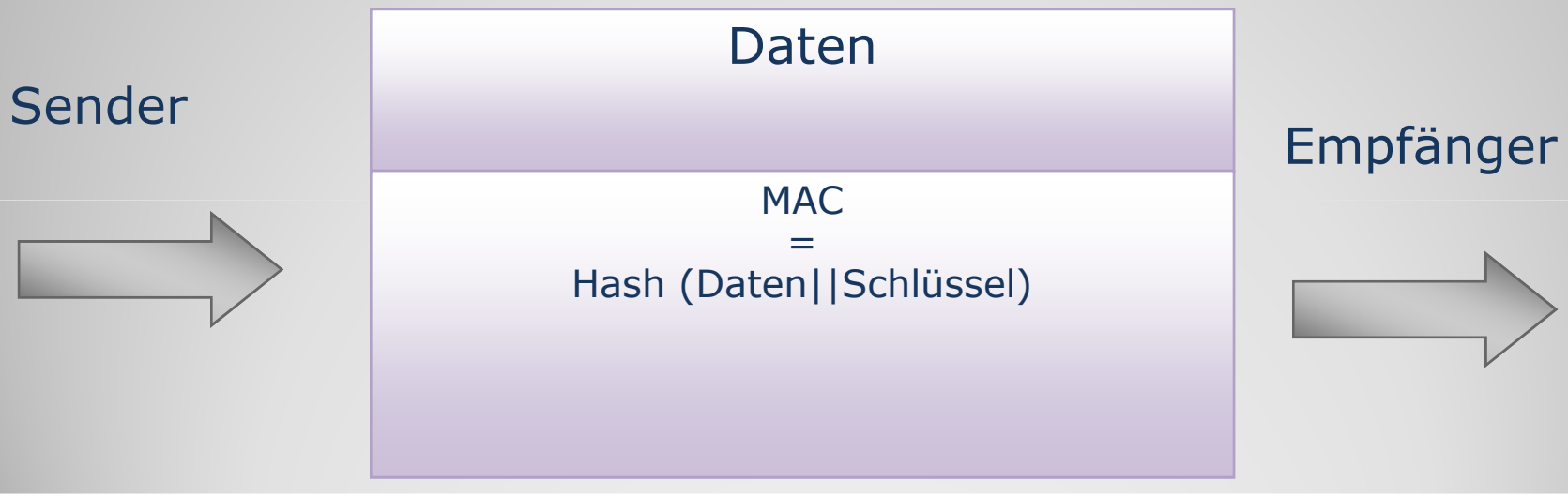
Point-to-Point Authentifizierung

- z.B. eingesetzt bei SSL-Verschlüsselung im Browser
- Public-Key-Verfahren für Verbindungsaufbau
- Austausch von Session-Keys
- Symmetrische Verschlüsselung f. Nutzdaten

Message Authentication Codes



Paket



PtP-Verschlüsselung im Broadcast

Point to Point Verfahren im Broadcast einsetzbar?

- Public-Key Verschlüsselung?
- MAC?
- Symmetrische Verschlüsselung?

TESLA Broadcastprotokoll

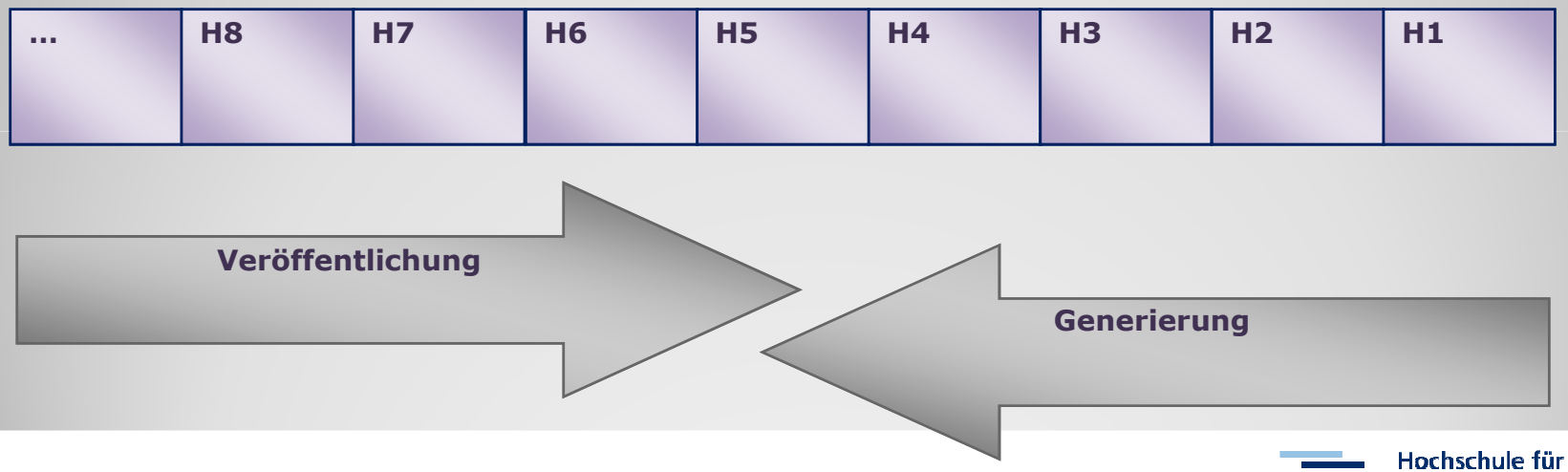
Time Efficient Stream Loss-tolerant Authentication

- Keine Signaturen oder Verschlüsselung
- Keine nicht Abstreitbarkeit, sondern Absender Authentisierung
- Asymmetrie durch Zeit
- Einsatz einer HashFunktion (One Way Chain)

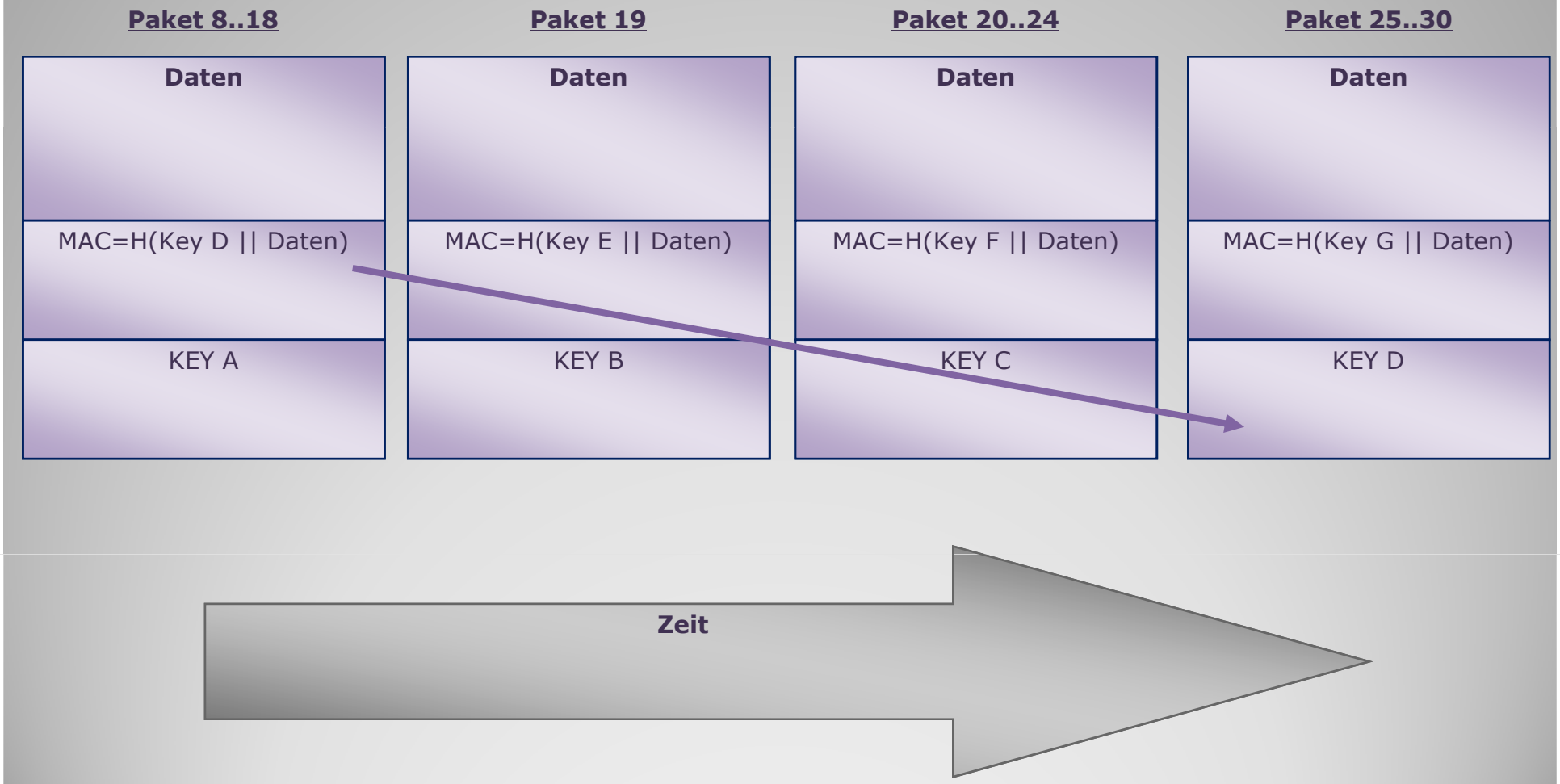
One Way Chain

Wiederholt angewandte Hashfunktion

H1 = H(S)
H2 = H(H(S))
H3 = H(H(H(S)))
...



TESLA Funktionsweise Sender

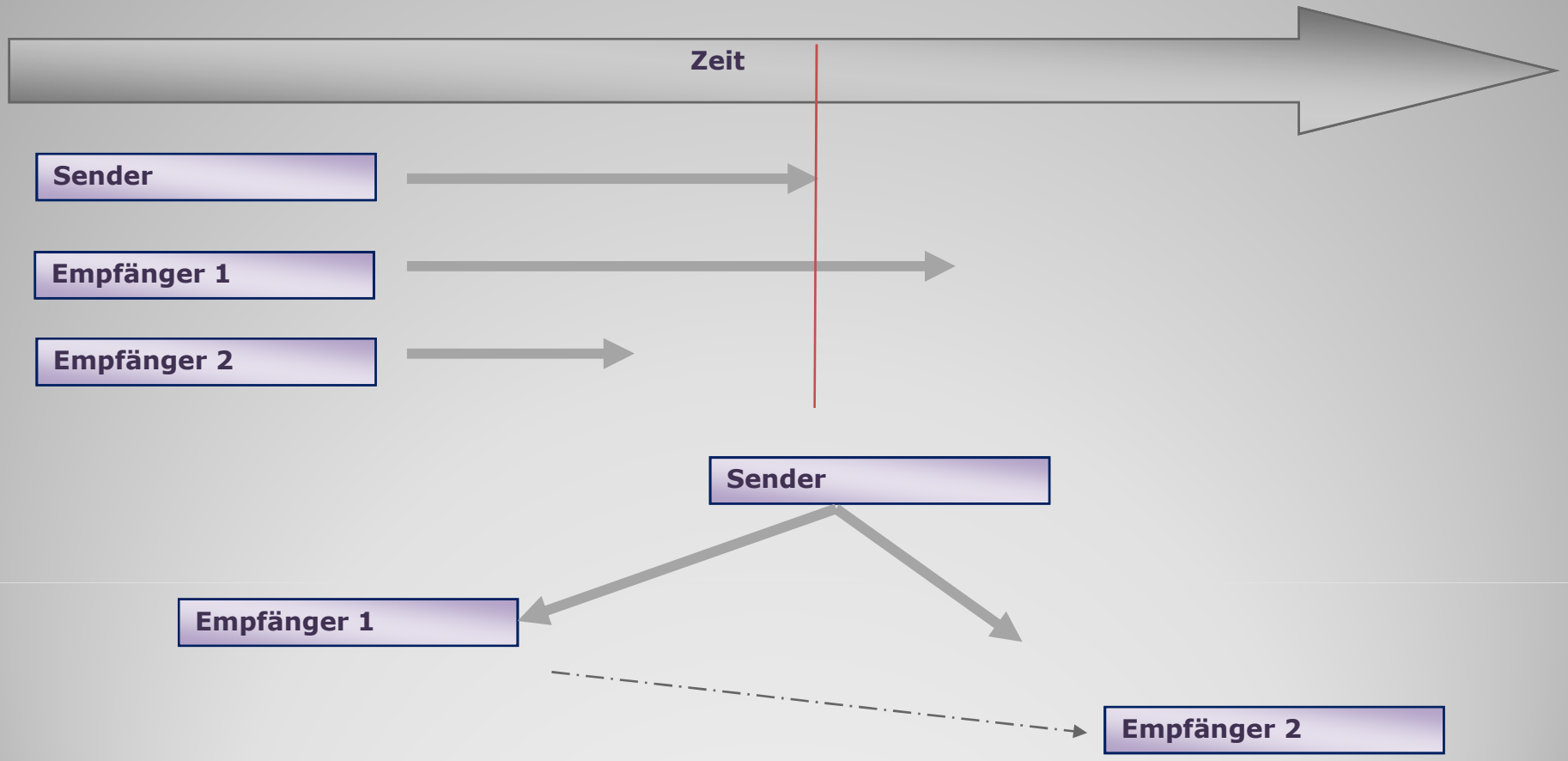


TESLA Bootstrapping

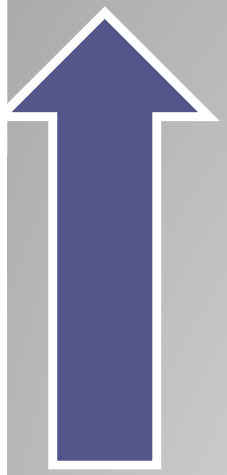
Empfänger Bootstrapping

- Einstieg in die One-Way-Chain d. Senders
- Zeitsynchronisation
  - Direkt
  - Indirekt
  - Verzögert
    - itrace

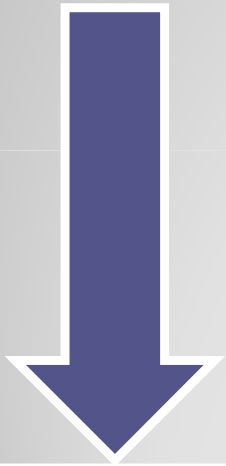
TESLA: lose Zeitsynchronisation



TESLA



- Hauptarbeit steckt in der Berechnung einer „billigen“ Hashfunktion
- Resistent gegen Paketverlust lose Zeitsynchronisation



- Problem bei Echtzeitanwendungen
- Zeitsynchronisation bei Empfängern mit unterschiedlichem Delay
- Keine nicht - Abstreitbarkeit

Eigenes Thema

Simulation und Vergleich verschiedener Broadcast Protokolle

Einsatz der Multicast-Protokolle im Overlay (P2P) Umfeld

Risiken des eigenen Themas

Simulation und Vergleich vorhandener Protokolle

- Protokolle sind bereits bekannt und im Einsatz
- Risiko: gering

Verbesserung eines bestehenden Protokolls

- Risiko: mittel

Entwicklung eines neuen Protokolls

- Risiko: hoch

Fazit

- Es gibt bereits mehrere Broadcast-Protokolle
- Es gibt noch Raum (und Bedarf) für eigene Forschung

Vielen Dank für Ihre Aufmerksamkeit

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Quellenangaben

- [1] Secure Broadcast Communication von Adrian Perrig; Kluwer Academic Publishers 2004
- [2] A Taxonomy of Multicast Data Origin Authentication: Issues and Solutions; aus: IEEE Communications 2004, Volume 6 No. 3
- [3] Applied Cryptography v. Bruce Schneier, 2005
- [4] Paper: The Tesla Broadcast Authentication Protocol / RFC4082, 2005
- [5] Understanding Cryptography von Christof Paar und Jan Pelzl, 2009
- [6] Handbook of Peer-to-Peer Networking von Xuemin shen et.al, 2009