



Fakultät für
**Mathematik und
Informatik**

Sichere Mobilfunkkommunikation für ein Fahrzeugleitsystem

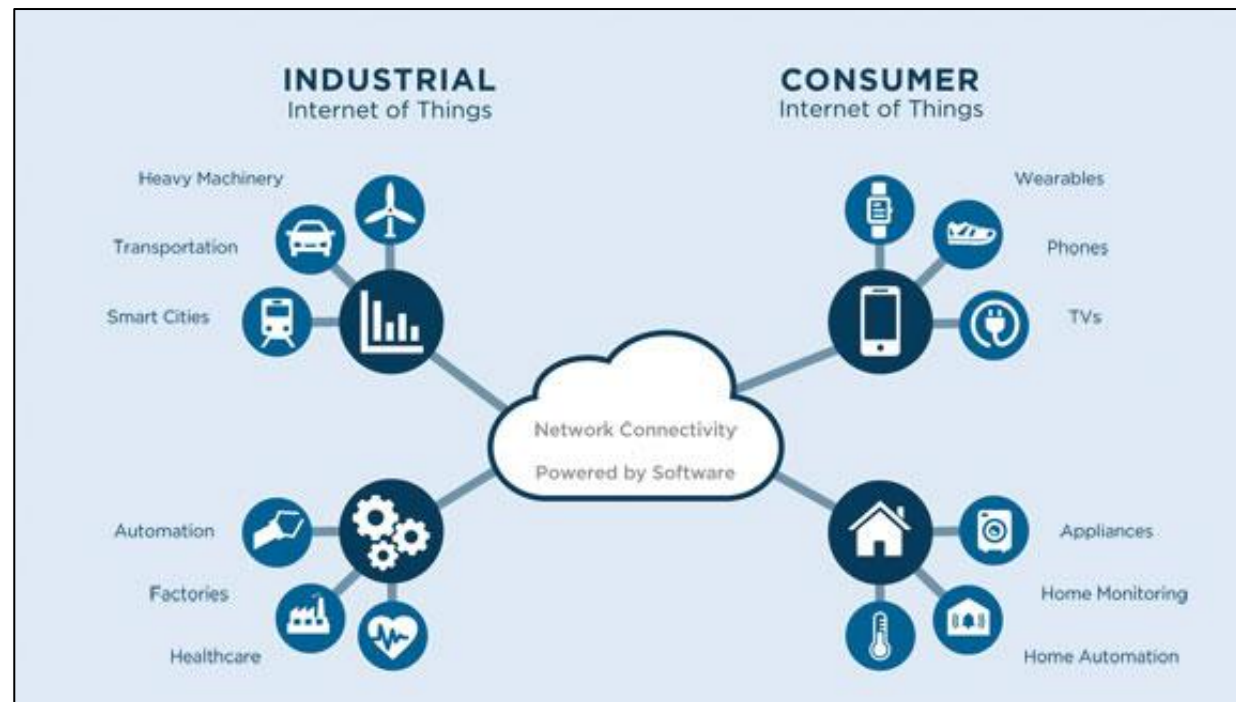
- Christoph Maget -
Workshop Echtzeit 2020
20.11.2020

Inhalt

1. Hintergrund: Internet der Dinge und Fahrzeugsysteme
2. Stand der Technik mit Bewertung relevanter Gesichtspunkte
3. Vorstellung „Sichere Kommunikationsarchitektur für Fahrzeugsysteme (SIKAF)“
4. Implementierung und Evaluation SIKAF
5. Zusammenfassung und Ausblick

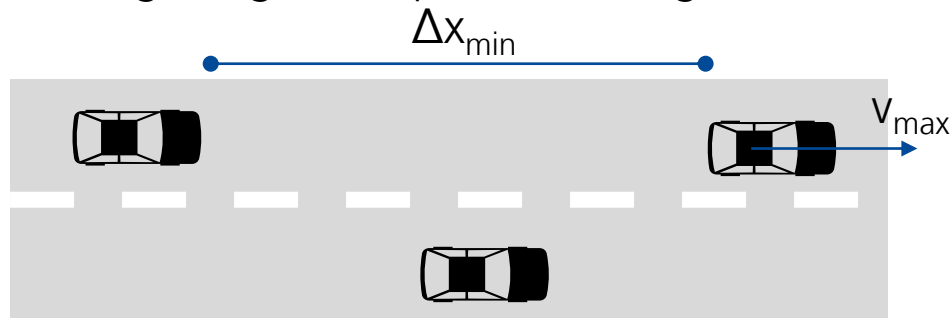
Hintergrund

- Automatisierungssysteme können Aufgaben schneller und präziser ausführen als der Mensch
- Koordination von Automatisierungssystemen erfordert Kommunikation: „Internet of Things (IoT)“

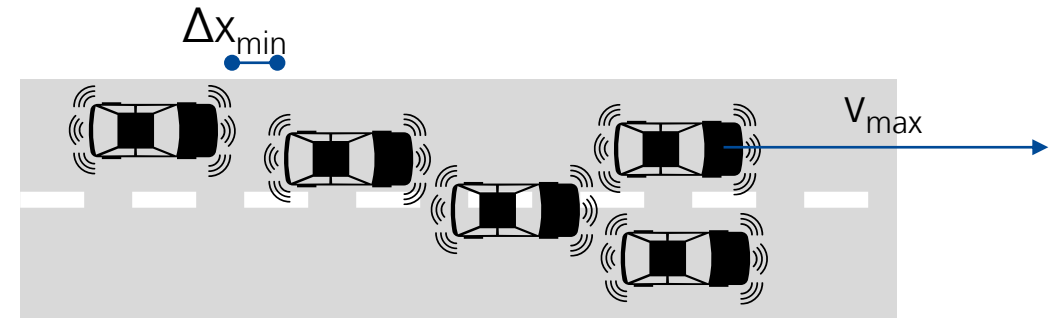


Anwendung: Verkehrssysteme

- Abstände und Geschwindigkeiten können optimiert werden
- Steigerung der Kapazität ist möglich ohne (kostenintensiven) Aus- und Neubau



Manuelle Fahrzeuglenkung



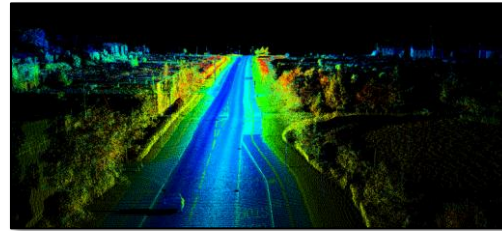
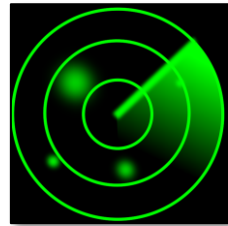
Automatische Fahrzeuglenkung

Voraussetzungen:

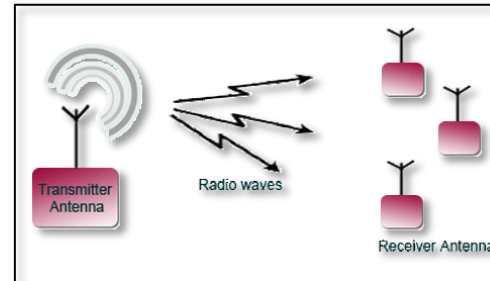
- Autonome Fahrzeuglenkung gem. „SAE-Levels“ (6 Stufen nach SAE J3016)
- Fahrzeugsystem („Intelligentes Verkehrssystem“, IVS) zur Koordinierung
- Sicherer und rechtzeitiger Nachrichtenaustausch

Eingrenzen der Forschungsfrage

Sensing



Reasoning

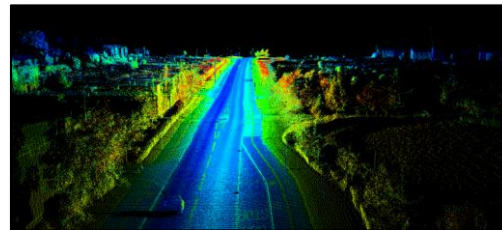
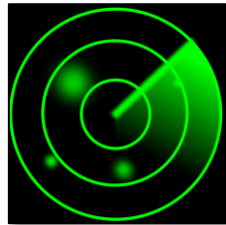


Acting

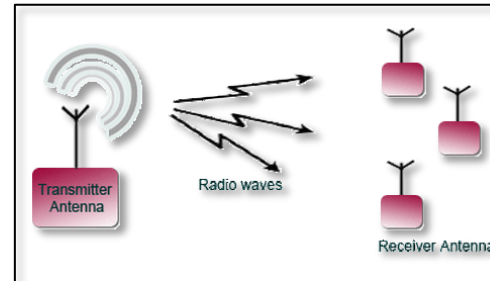


Eingrenzen der Forschungsfrage

Sensing



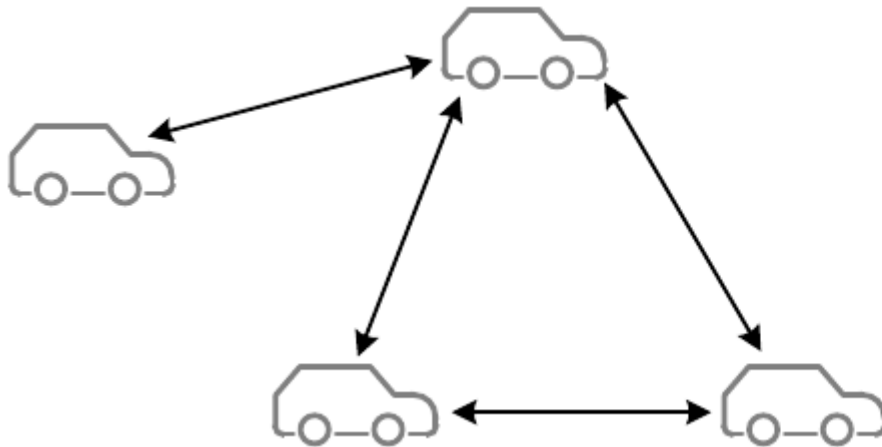
Reasoning



Acting

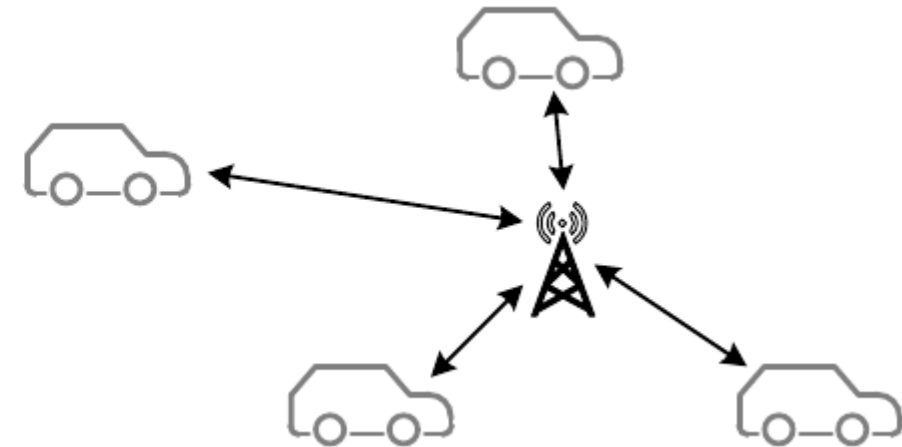


Stand der Technik: Topologie



Ad-hoc Modus (Vehicular Ad-hoc Network, VANet)

- + Keine zusätzliche Infrastruktur notwendig
- Datenweiterleitung teilweise fremdbestimmt

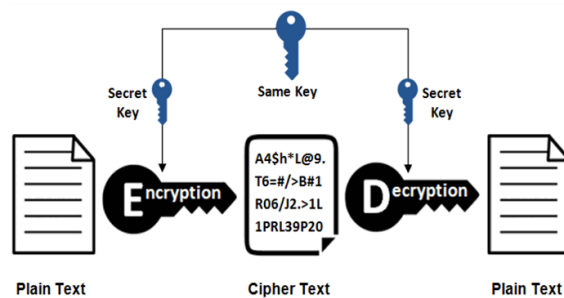


Infrastrukturmodus

- + Übertragungsparameter kontrollierbar
- Zusätzliche Infrastruktur notwendig

Stand der Technik: Kryptologie

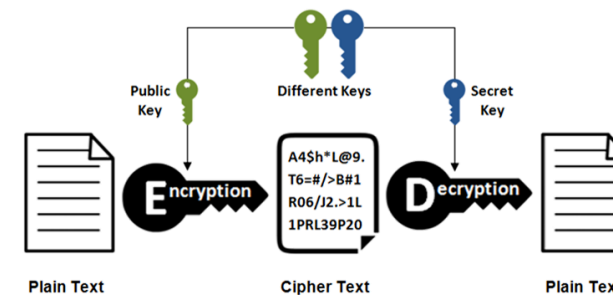
Symmetrische Kryptografie:



Gleicher Schlüssel zur Ver- und Entschlüsselung

- + Schnell
- + Perfekte Sicherheit möglich
- o Schlüsselverteilung aufwändig

Asymmetrische Kryptografie:



Verschiedene Schlüssel zur Ver- und Entschlüsselung

- Rechenaufwand
- Privater Schlüssel berechenbar
- + Gut skalierbar

Stand der Technik: Sicherheit verbreiteter Verschlüsselungsverfahren

- Blockchiffre „Data Encryption Standard (DES)“
 - Schlüssellänge: 56 bit
 - Brechen laut Hochrechnungen in Sekunden möglich (*Electronic Frontier Foundation: Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. O'Reilly, 1998*)
- Stromchiffre „Ron's Code 4 (RC4)“
 - Verbreitet im WLAN-Bereich als WEP
 - Brechen in wenigen Sekunden möglich (*Fluhrer, S. et.al.: Weaknesses in the Key Scheduling Algorithm of RC4, SAC, 2001*)
- Blockchiffre „Advanced Encryption Standard (AES)“
 - Schlüssellänge: maximal 256 bit
 - Aktuell sicher (laut NIST), ggf. „gleiches Schicksal“ wie DES

Beispiele für Fahrzeughacks


heise+ IT Mobiles Entertainment Wissen Netzpolitik

TOPTHEMEN: IPHONE 12 E-AUTO SECURITY WINDOWS 10 CORONAVIRUS HOMEOP

Security > 7-Tage-News > 04/2019 > **Hacker knackt Auto-GPS-Tracker: "Ich kann weltweit den Verkehr beeinflussen"**

Über die Apps iTrack und ProTrack sind tausende Autos nachverfolgbar, deren Besitzer das Standardpasswort der Tracker nicht geändert haben.

Lesezeit: 2 Min. In Pocket speichern 164



Der Hacker hätte nach eigenen Angaben den Motor von Fahrzeugen stoppen können, die mit weniger als 20 km/h unterwegs sind. (Bild: Pixabay)

auto motor sport



HACKER STEuern AUTO FERN

Fahrer kann Jeep nicht mehr lenken

Die Hacker Chris Miller und Charlie Valasek haben bei einem Jeep während der Fahrt per Laptop das Steuer übernommen.

ADAC Suchbegriff eingeben... Mein ADAC Kontakt & Notruf

Rund ums Fahrzeug Verkehr Reise & Freizeit Versicherungen & Finanzen Mitgliedschaft Services Der ADAC

Rund ums Fahrzeug > Ausstattung, Technik & Zubehör > Autonomes Fahren > Rechtliche Aspekte beim autonomen Fahren > **Autonomes Fahren: Gefahr durch Hacker?**

20.01.2020



Autonome Autos sind ständig auf Empfang. © iStock.com/bee-light

Selbstfahrende Autos sind Computer auf Rädern. Das kann sie verwundbar für Hacker-Angriffe machen. Diese Risiken gibt es. Und so lassen sie sich begrenzen.

- Die Vernetzung macht Autos angreifbar
- Erste Hacker-Angriffe auf vernetzte Pkw waren erfolgreich
- Experten kritisieren: Die Hersteller tun zu wenig zum Schutz vor Hacker-Angriffen

Stand der Technik: Perfekte Sicherheit

Definition:

Ein Verschlüsselungsverfahren ist perfekt sicher, wenn für alle Klartexte $p \in P$ und für alle Schlüsseltexte $c \in C$ gilt:

$$\Pr(p|c) = \Pr(p)$$

Folge

- Schlüssel von Nachrichtenlänge notwendig

Eigenschaften

- Immun gegen Angriffe mit beliebiger Rechenleistung, „Secure by Design“

Implementierung

- One Time Pad

Stand der Technik: Informationsaustausch

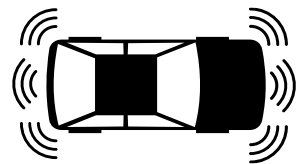
Fahrzeugbezogen (GPS verortet, bidirektional)

Cooperative Awareness Message (CAM)

- ETSI EN 302 637-2
- Zeitgesteuert

Decentralized Environmental Notification Message (DENM)

- ETSI EN 302 637-3
- Ereignisgesteuert
- Forschungscharakter



Streckenbezogen (abschnittsverortet, unidirektional)

Radio Data System - Traffic Message Channel (RDS-TMC)

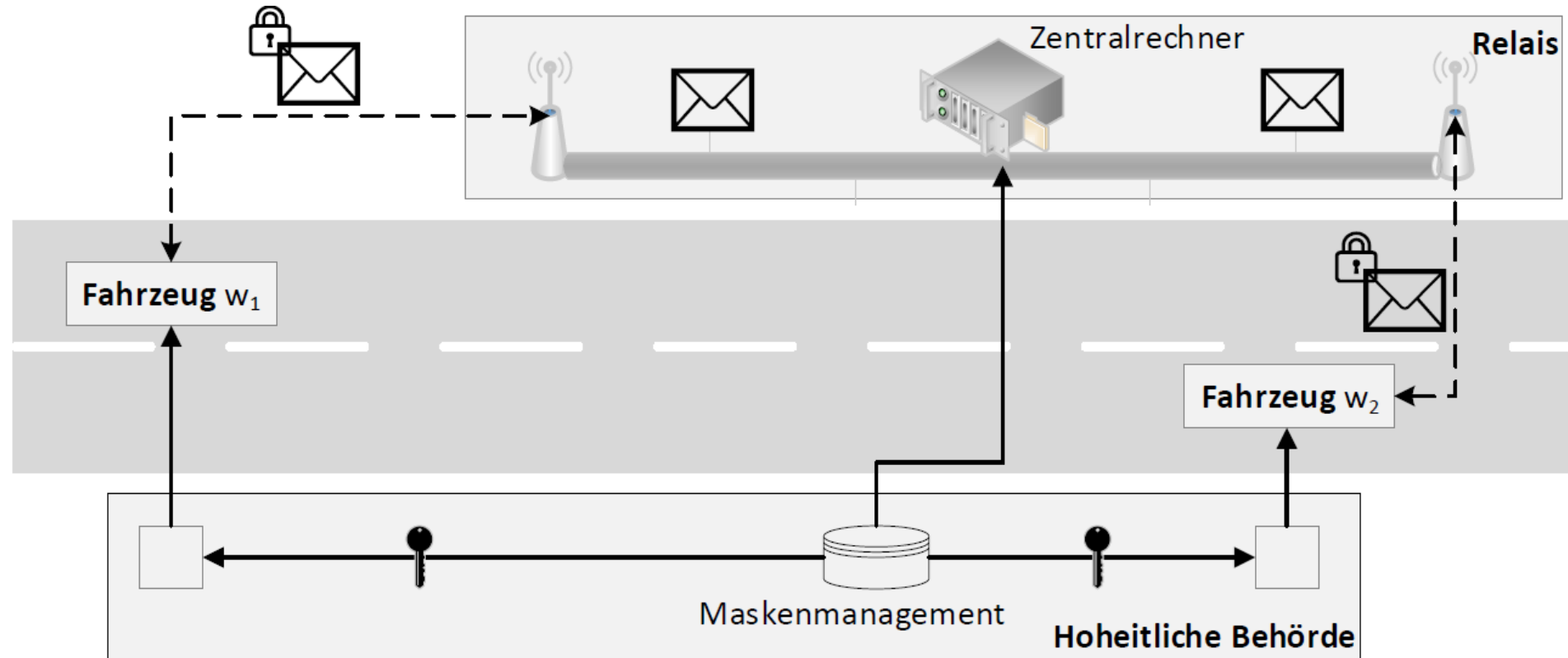
- Positionscodes
- Tabellierte Inhalte

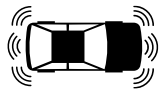
Quelle: Polizei, Verkehrsmeldestellen

- Keine Authentifizierung



Technischer Aufbau der vorgeschlagenen Kommunikationsarchitektur





Exemplarische Nachrichtengrößen

Fahrzeugbezogen

Aktueller und beabsichtigter Fahrzeugzustand

Nachrichteninhalt	Datenmenge		davon
	gesamt	codiert	maskierbar
Nachrichtenspezifikationen	152 bit	127 bit	64 bit
Attribute	7 bit	7 bit	6 bit
Trajektorie	224 bit	33 bit	223 bit
Kraftstoff	12 bit	5 bit	11 bit
Freitext	142 bit	2 bit	140 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	637 bit	174 bit	464 bit



Streckenbezogen

Aktueller und prognostizierter Streckenzustand

Nachrichteninhalt	Datenmenge		davon
	gesamt	codiert	maskierbar
Nachrichtenspezifikationen	119 bit	94 bit	32 bit
Verortung	172 bit	33 bit	0 bit
Fahrbahnoberfläche	5 bit	5 bit	0 bit
Sichtweite	9 bit	1 bit	0 bit
Geschwindigkeitsbegrenzung	11 bit	3 bit	0 bit
Hindernis	6 bit	6 bit	0 bit
Alternativstrecke	34 bit	34 bit	32 bit
Parkplätze	18 bit	2 bit	16 bit
Freitext	142 bit	2 bit	140 bit
Inhaltsverifizierung	10 bit	2 bit	0 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	626 bit	182 bit	240 bit

Exemplarische Nachrichtengrößen



Code	Wert	Größe
0...1023	Versionsnummer SIKAF	10 bit
{0, 1}	{strecken, fahrzeug}bezogen	1 bit
{0x000...00, ..., 0xff...ff}	IRIG-Zeitstempel	60 bit
{0, 1}	Sender maskiert {nein, ja}	1 bit
{0x00000000, ..., 0xffffffff}	dID Sender	32 bit
{0, 1}	Empfänger maskiert {nein, ja}	1 bit
{0x00000000, ..., 0xffffffff}	dID Empfänger	32 bit
1...2048	Gültigkeit in Millisekunden (ms)	11 bit
0...15	Meldungen pro Sekunde (s^{-1})	4 bit

Streckenbezogen

Aktueller und prognostizierter Streckenzustand

Nachrichteninhalt	Datenmenge		davon
	gesamt	codiert	maskierbar
Nachrichtenspezifikationen	119 bit	94 bit	32 bit
Verortung	172 bit	33 bit	0 bit
Fahrbahnoberfläche	5 bit	5 bit	0 bit
Sichtweite	9 bit	1 bit	0 bit
Geschwindigkeitsbegrenzung	11 bit	3 bit	0 bit
Hindernis	6 bit	6 bit	0 bit
Alternativstrecke	34 bit	34 bit	32 bit
Parkplätze	18 bit	2 bit	16 bit
Freitext	142 bit	2 bit	140 bit
Inhaltsverifizierung	10 bit	2 bit	0 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	626 bit	182 bit	240 bit

Exemplarische Nachrichtengrößen

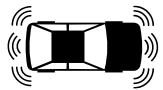


Streckenbezogen

Aktueller und prognostizierter Streckenzustand

Nachrichteninhalt	Datenmenge gesamt	davon	
		codiert	maskierbar
Nachrichtenspezifikationen	119 bit	94 bit	32 bit
Verortung	172 bit	33 bit	0 bit
Fahrbahnoberfläche	5 bit	5 bit	0 bit
Sichtweite	9 bit	1 bit	0 bit
Geschwindigkeitsbegrenzung	11 bit	3 bit	0 bit
Hindernis	6 bit	6 bit	0 bit
Alternativstrecke	34 bit	34 bit	32 bit
Parkplätze	18 bit	2 bit	16 bit
Freitext	142 bit	2 bit	140 bit
Inhaltsverifizierung	10 bit	2 bit	0 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	626 bit	182 bit	240 bit

Code	Wert	Größe
{0, 1}	gemeldet {nein, ja}	1 bit
0	Sichtweite maximal	8 bit
1 ... 255	Sichtweite ($\times 10$ m)	



Exemplarische Nachrichtengrößen

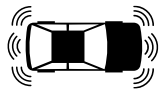
Fahrzeugbezogen

Aktueller und beabsichtigter Fahrzeugzustand

Nachrichteninhalt	Datenmenge		davon
	gesamt	codiert	maskierbar
Nachrichtenspezifikationen	152 bit	127 bit	64 bit
Attribute	7 bit	7 bit	6 bit
Trajektorie	224 bit	33 bit	223 bit
Kraftstoff	12 bit	5 bit	11 bit
Freitext	142 bit	2 bit	140 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	637 bit	174 bit	464 bit

Code	Wert	Größe
{0, 1}	maskiert {nein, ja}	1 bit
0 ... 3 599 999 999	Länge (°)*	32 bit
0 ... 3 599 999 999	Breite (°)*	32 bit
0 ... 65 535	Höhe (m)	16 bit
{0x00000000, ..., 0xffffffff}	{„A1“, „A99“, ..., „Zusestrasse“}	32 bit
0 ... 1023	Abschnitt	10 bit
0 ... 1023	Station	10 bit
0 ... 100	Position in Prozent (%)*	7 bit
1 ... 16	Fahrspur	4 bit
0 ... 255	Geschwindigkeit aktuell ($\frac{\text{km}}{\text{h}}$)	8 bit
0 ... 255	Geschwindigkeit in 0,5 s ($\frac{\text{km}}{\text{h}}$)	8 bit
0 ... 255	Geschwindigkeit in 1,0 s ($\frac{\text{km}}{\text{h}}$)	8 bit
0 ... 255	Geschwindigkeit in 1,5 s ($\frac{\text{km}}{\text{h}}$)	8 bit
0 ... 3599	Richtung aktuell (°)*	12 bit
0 ... 3599	Richtung in 0,5 s (°)*	12 bit
0 ... 3599	Richtung in 1,0 s (°)*	12 bit
0 ... 3599	Richtung in 1,5 s (°)*	12 bit

*Codes nicht ausgeschöpft



Exemplarische Nachrichtengrößen

Fahrzeugbezogen

Aktueller und beabsichtigter Fahrzeugzustand

Nachrichteninhalt	Datenmenge		davon
	gesamt	codiert	maskierbar
Nachrichtenspezifikationen	152 bit	127 bit	64 bit
Attribute	7 bit	7 bit	6 bit
Trajektorie	224 bit	33 bit	223 bit
Kraftstoff	12 bit	5 bit	11 bit
Freitext	142 bit	2 bit	140 bit
Prüfsumme	20 bit	0 bit	20 bit
Maskenanzeiger	80 bit	0 bit	0 bit
Summe	637 bit	174 bit	464 bit

Code	Wert	Größe
0 ... 1 048 575	Prüfsumme	20 bit
0x00000000, ..., 0xffffffff	Maskenanzeiger von	40 bit
0x00000000, ..., 0xffffffff	Maskenanzeiger bis	40 bit

Benötigte Maskengröße: Bestimmende Parameter

- Datenmenge des zu maskierenden Nachrichtenteils: $D = D(t)$
- Sendefrequenz maskierter Nachrichten: $f_{send} = f_{send}(t)$
- Empfangsfrequenz maskierter Nachrichten: $f_{empf} = f_{empf}(t)$
- Aktivitätsdauer: $t_A = \sum t'_A$

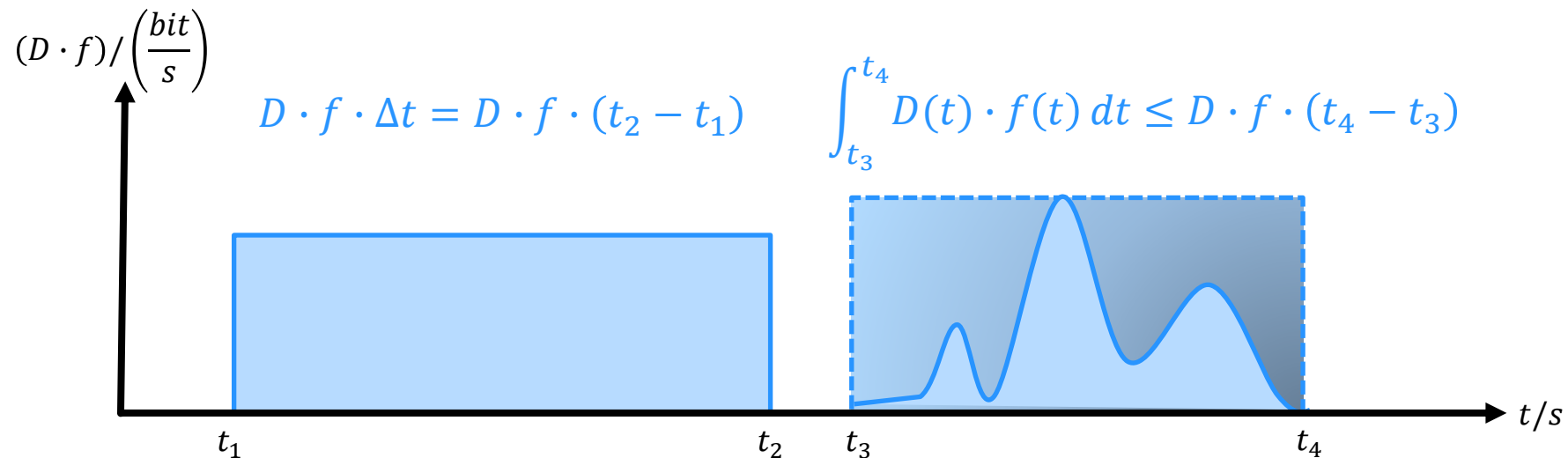
Benötigte Maskengröße: Bestimmende Parameter

- Datenmenge des zu maskierenden Nachrichtenteils: $D = D(t)$
- Sendefrequenz maskierter Nachrichten: $f_{send} = f_{send}(t)$
- Empfangsfrequenz maskierter Nachrichten: $f_{empf} = f_{empf}(t)$
- Aktivitätsdauer: $t_A = \sum t'_A$



Benötigte Maskengröße: Bestimmende Parameter

- Datenmenge des zu maskierenden Nachrichtenteils: $D = D(t)$
- Sendefrequenz maskierter Nachrichten: $f_{send} = f_{send}(t)$
- Empfangsfrequenz maskierter Nachrichten: $f_{empf} = f_{empf}(t)$
- Aktivitätsdauer: $t_A = \sum t'_A$

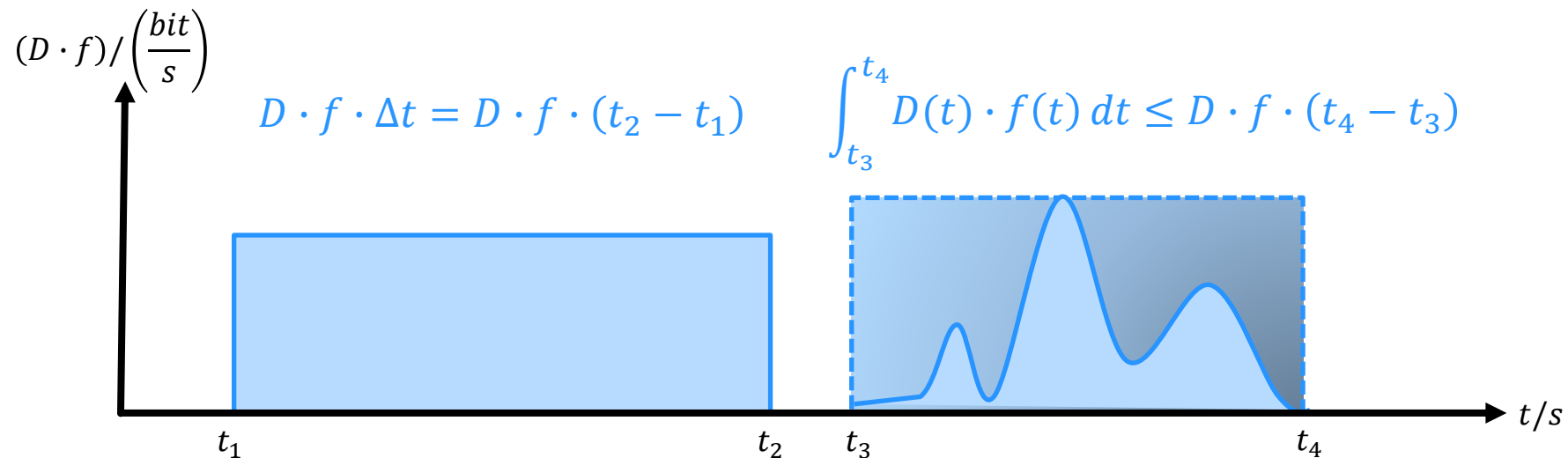


Benötigte Maskengröße: Bestimmende Parameter

- Benötigte Schlüsselgröße

$$G \geq \sum_{t'_A} \int_{t'_A} \left[(f_{send_b}(t) + f_{empfb}(t)) \cdot D_b(t) + (f_{send_w}(t) + f_{empfw}(t)) \cdot D_w(t) \right] dt$$

w: Fahrzeugbezogen; *b*: Streckenbezogen



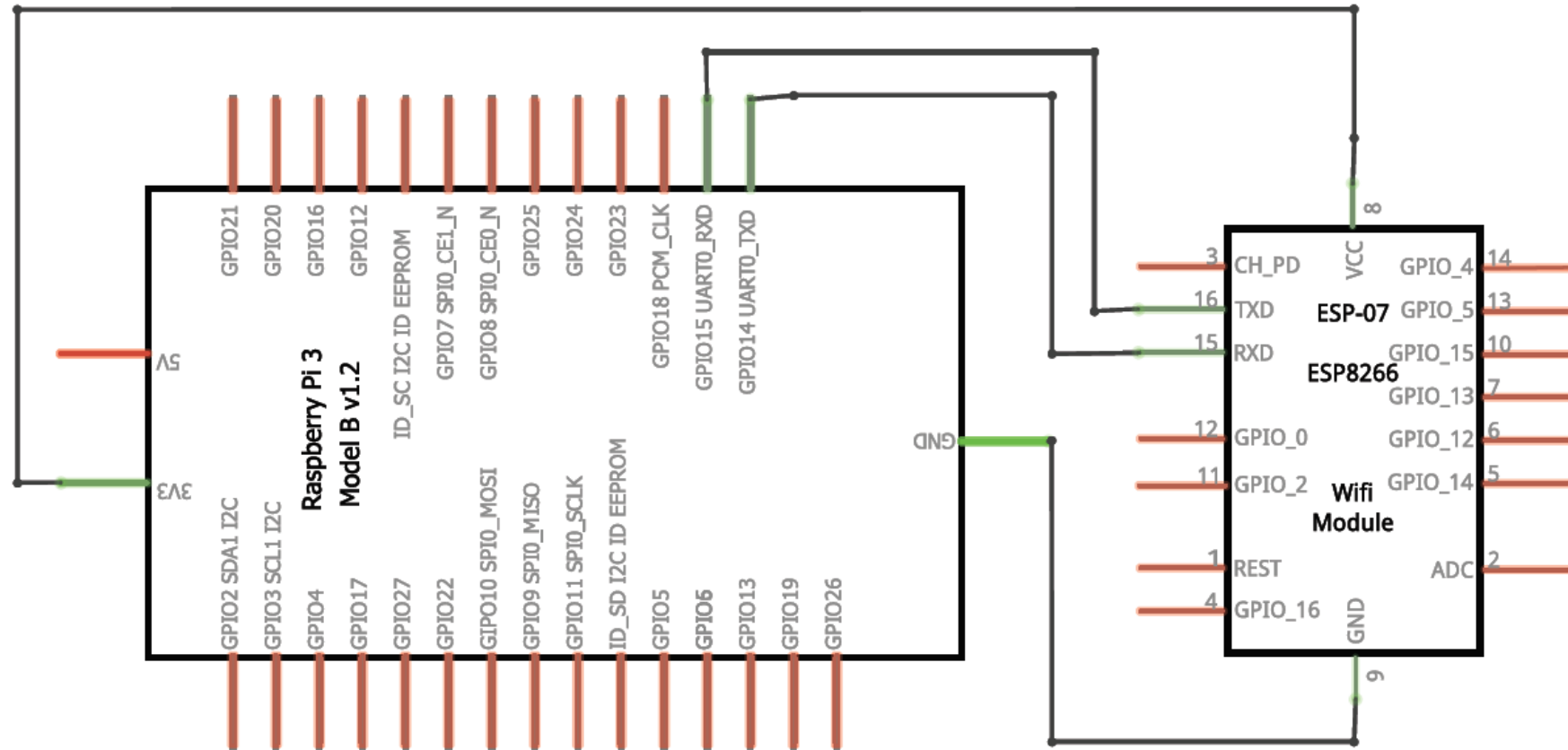
Szenarienbetrachtung

Szenario	Mindestgröße	Automatisch	Vollautonom
D_b	20 bit	626 bit	626 bit
D_w	20 bit	637 bit	637 bit
f_{send_b}	1 Hz	10 Hz	10 Hz
f_{send_w}	1 Hz	10 Hz	10 Hz
f_{empfb}	1 Hz	10 Hz	10 Hz
f_{empfw}	1 Hz	10 Hz	10 Hz
t_A^*	105 h	105 h	7.300 h
Summe	3,60 MiB / a	1,11 GiB / a	77,28 GiB / a

*) Aktivitätsdauer = Fahrleistung / Geschwindigkeit

Prototyp

Beispiel Relais



Zusammenfassung

Feststellung: Bestehende Konzepte zur Fahrzeugvernetzung sind nicht sicher oder nicht echtzeitfähig

Mit SIKAF wurde eine Kommunikationsarchitektur vorgestellt, die

- perfekt sichere Verschlüsselung nutzt,
- echtzeitfähige Datenübertragung ermöglicht und
- den Schlüsselnachschub organisatorisch löst.

Insgesamt wurde damit gezeigt, dass sich perfekt sichere Verschlüsselung im Internet der Dinge einsetzen lässt.

Ausblick

- Weiterentwicklung der Software hinsichtlich
 - Evaluierung Verschlüsselungsverfahren: <https://github.com/ChrisMg1/CryptEval>
 - Software Prototyp: <https://github.com/ChrisMg1/Prototyp-SIKAF>
- Weitere Auswertung und Optimierung des Zeitverhaltens
 - Anpassen der Nachrichtenstruktur
 - Auswahl des Übertragungsprotokolls
- Blockchain als dezentrale Datenbank zur Speicherung eines „Vertrauens“ parameters

Diskussionspunkte

Ist eine hoheitliche Behörde eine adäquate Institution zur Schlüsselerzeugung und -verwaltung?

Ja – denn

- der Trend im Internet (of Things) geht ohnehin zu zentralen Plattformen (Amazon, Google, SWIFT)
- eine demokratisch legitimierte Institution ist vertrauenswürdig(er) und mindert Interessenkonflikte

Ist der Aufwand perfekt sicherer Verschlüsselung (OTP) notwendig und angemessen?

Ja – denn

- die Entwicklung der Rechnertechnik (vgl. Mooresches Gesetz) senkt Zeitbedarf für Angriffe (Quantencomputer)
- perfekte Sicherheit macht keinen Ersatz des Verschlüsselungsalgorithmus notwendig („Secure by Design“)
- Erfüllt (stillschweigend) angenommene Voraussetzung vieler Protokolltests („Verschlüsselung ist sicher“)



Fakultät für
**Mathematik und
Informatik**

Danke für die Aufmerksamkeit

christoph.maget@studium.fernuni-hagen.de

Bildquellen

The Noun project (Dalpat Prajapati, Adrien Coquet, Thak Ka)

Internet (heise.de, adac.de, auto-motor-und-sport.de, de.wikipedia.org)

www.jkoolcloud.com

www.slideshare.net

cryptobook.nakov.com

Yeping Chu, Lin Pan, Kaijun Leng: International Journal of Advanced Manufacturing Technology