Seminar Sommersemester 2009 Automotive Konzepte und Techniken
Prof. Dr. Dieter Zöbel, Universität Koblenz-Landau, FB Informatik

„Car 2 Car/Car 2 X“ Kommunikation

Kommunikation zwischen Fahrzeugen und deren Umgebung

Felix Graf

Eingereicht: 23.06.2009 / Fertiggestellt: 04.09.2009

Zusammenfassung In jedem Auto kommunizieren die einzelnen Komponenten über Datenbusse, z.B. CAN und Flexray, im Fahrzeug (*in-vehicle*). Ein neuerer Ansatz ist die Kommunikation zwischen Fahrzeugen (*car 2 car*) und zwischen Fahrzeugen und deren Umgebung (*car 2 x*). Sie befindet sich noch im Entwicklungszustand und zielt auf eine Verbesserung der Verkehrseffizienz und -sicherheit, eine Verringerung der Umweltverschmutzung und eine Erhöhung des Reisekomforts ab. In diesem Paper wird der aktuelle Forschungsstand mit Herausforderungen, Techniken und Problemen behandelt.

Schlüsselwörter Car2Car · Car2X · VANET · WAVE · WSMP

1 Einleitung

1.1 Fahrzeugkommunikation

Bisher ist bei Kommunikation im Kraftfahrzeugbereich mehr die Kommunikation gemeint, die im Fahrzeug über Datenbusse, z.B. CAN und Flexray, abläuft. Diese ist bis auf Ausnahmen, z.B. Bluetooth, vorwiegend kabelgebunden und verteilt die anfallenden Informationen an die jeweiligen elektronischen Steuergeräten. Im weiteren Verlauf soll aber die Kommunikation zwischen Fahrzeugen und die Kommunikation zwischen Fahrzeugen und deren Umgebung thematisiert werden. Logischerweise funktioniert diese ausschließlich kabellos.

1.2 Motivation und Ziele

Warum eine solche Technik überhaupt als notwendig angesehen wird, sollen die folgenden Daten verdeutlichen:

Felix Graf
Universität Koblenz-Landau
E-Mail: felixgraf@uni-koblenz.de

- jedes Jahr sterben ca. 40000 Menschen bei Unfällen auf den Straßen der Europäischen Union (EU)
- dabei erleiden ca. 1.7 Millionen Menschen schwere Verletzungen
- wegen Verkehrsunfällen fallen ca. 3% des weltweiten Bruttoinlandproduktes oder 1 Billion US$ jährliche Kosten (Krankenhausrechnungn, Sachschäden, ...) an

Des weiteren nimmt die Anzahl der Fahrzeuge schneller zu als die Anzahl der Straßen, wodurch häufiger Staus entstehen, die Umweltverschmutzung zunimmt und es vermehrt zu Parkplatzmangel kommt. Somit ergeben sich die gesetzten Ziele in der Erhöhung der Verkehrssicherheit und -effizienz, der Reduzierung der Umweltverschmutzung und der Erhöhung des Reisekomforts.
[6]

1.3 Car 2 Car Communication Consortium (C2C-CC)

Eine der Haupttriebkräfte in diesem Forschungsbereich ist das „Car 2 Car Communication Consortium“. Dahinter verbirgt sich ein Zusammenschluss von europäischen Automobilherstellern, anderen Firmen, Universitäten und Forschungseinrichtungen, die zur Thematik C2C-CC beisteuern. Sie wollen die in Kap. 1.2 genannten Ziele umsetzen und dabei eine europaweite Standardisierung von Schnittstellen und Protokollen erreichen. Eine weltweite Einführung und Standardisierung ist nicht ausgeschlossen, ist aber fragwürdig. Derzeit sind in Europa, den USA und Japan unterschiedliche Projekte unterwegs.
[3, 5, 10, 18]

1.4 Terminologie

Um Verständnisschwierigkeiten vorzubeugen, werden in diesem Abschnitt kurz bestimmte Terminologien und Abkürzungen erklärt.
Die Kommunikation zwischen Fahrzeugen, kurz *car 2 car (C2C)*, wird auch als *vehicle 2 vehicle (V2V)* oder *inter vehicle (IV)* bezeichnet.
Für die Kommunikation zwischen Fahrzeugen und deren Umgebung, kurz *car 2 x (C2X)* werden auch die Bezeichnungen *car 2 roadside (C2R)*, *vehicle 2 roadside (V2R)* bzw. *vehicle 2 infrastructure (V2I)* verwendet.
Die eingangs erwähnte Kommunikation im Fahrzeug wird häufig auch *in vehicle (InV)* genannt.

1.5 Aufbau der Arbeit

Am Anfang der Arbeit stehen Szenarios und Anwendungen der *C2C-* bzw. *C2X-*Kommunikation, um einen Eindruck von den Einsatzgebieten zu erhalten. Im folgenden werden die Voraussetzungen, die Systemarchitektur sowie das Funk- und Kommunikationssystem erklärt. Diese Reihenfolge wurde gewählt um einem erst die Idee hinter der Funktionsweise zu vermitteln und anschließend konkrete Ideen zur Umsetzung zu präsentieren. Methoden zu Datensicherheit und Datenschutz werden danach kurz angerissen. Beendet wird die Arbeit durch eine Zusammenfassung und Schlussfolgerung.

2 Szenarios der C2C/C2X Kommunikation

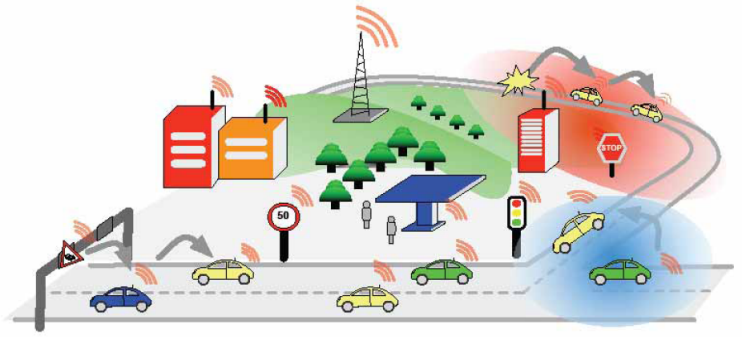


Abbildung 1 Szenarios mit den verschiedenen Teilnehmern, von denen die Systemanforderungen abgeleitet werden [3]

Um die Funktionsweise der Kommunikationstechnik verstehen zu können, werden zu den Bereichen Sicherheit, Verkehrseffizienz und Infotainment beispielhaft einige Szenarios (Abb. 1) vorgestellt.

2.1 Sicherheit

Szenarien zur Verbesserung der Sicherheit eines Fahrzeugs. Relevante Informationen, z.B. Position, Geschwindigkeit und Fahrtrichtung, müssen regelmäßig zwischen den Fahrzeugen ausgetauscht werden (Abb. 2a).

- *Forward Collision Warning*: Auffahrunfälle sollen durch das Austauschen von den oben genannten relevanten Informationen verhindert werden. Das Austauschen zwischen den Fahrzeugen geschieht automatisch. Der Fahrer wird gewarnt, wenn anhand der vorliegenden Daten eine kritische Situation bevorsteht.
- *Pre-Crash Sensing/Warning*: Wenn ein Zusammenstoß nicht mehr zu verhindern ist, werden anhand der vorhandenen Informationen optimale Vorkehrungen (Airbags, motorisierter Sicherheitsgurtstraffer, erweiterbare Stoßstangen, ...) für die Kollision getroffen.
- *Hazardous Location Warning*: Gefahrenstellen auf der Straße (glatte Fahrbahn, Schlaglöcher, ...) werden zwsichen den Fahrzeugen ausgetauscht. Die herankommenden Fahrer sind gewarnt und Chassis- und Sicherheitssysteme können automatisch optimiert werden.

2.2 Verkehrseffizienz

Die Verkehrs- und Transporteffizienz wird durch das Bereitstellen von Informationen an die Besitzer des Transportnetzwerkes oder an die Fahrzeugführer verbessert (Abb. 2a).

- *Enhanced Route Guidance and Navigation*: Infrastrukturbesitzer sammeln Daten über eine große Region und können diese interessierten Fahrzeugen zur Verfügung stellen, anhand derer die günstigste Route gewählt werden kann.
- *Green-Light Optimal Speed Advisory*: Fahrzeuge erhalten Position und Phasenschaltung von Ampeln. Mit den Daten kann die optimale Geschwindigkeit berechnet werden, um ohne anzuhalten über die Ampel zu kommen.
- *V2V Merging Assistance*: Fahrzeugen wird das Einfädeln in den laufenden Verkehr erleichtert, indem sie mit anderen Fahrzeugen kommunizieren und passende Lücken angekündigt werden.

2.3 Infotainment und andere

Infotainment und andere umfassen die Szenarios, die nicht direkt mit Sicherheit oder Verkehrseffizienz zu tun haben.

- *Internet Access in Vehicle*: Per *multi-hop* wird über eine *road-side unit (RSU)* (Kap. 5.1), die als *Gateway* fungiert, eine Internetverbindung über herkömmliche IP basierte Dienste im Fahrzeug aufgebaut.
- *Point of Interest Notification*: Lokaler Wirtschaft, Touristenattraktionen oder anderen interessanten Punkten ist es möglich, sich nähernden Verkehrsteilnehmern Informationen und Angebote zu senden.
- *Remote Diagnostics*: Servicestationen wird ohne physikalische Verbindung zum Fahrzeug eine Diagnose ermöglicht.

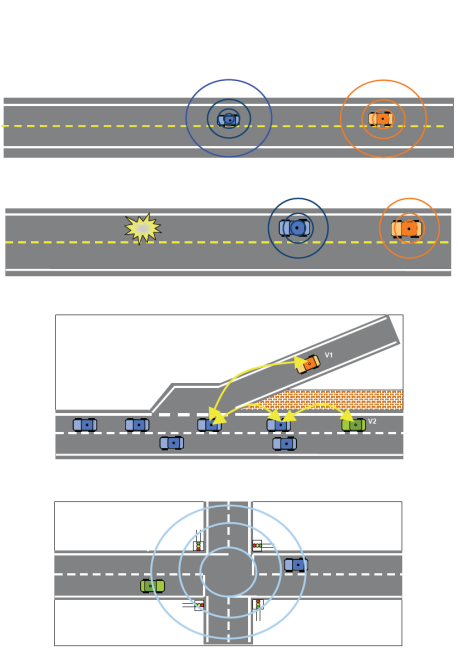
In Abb. 1 sind diverse Kommunikationsteilnehmer, denen unterschiedliche Rollen zu kommen, zu erkennen. Die Fahrer profitieren von der Technik, indem sie von dem System mit hilfreichen Informationen versorgt werden. Der Verkehr wird von den Straßenbetreibern durch die vorliegenden Informationen optimiert. *Hot spot*- (Kap. 5.1) und Internetprovider können Kommunikationseinheiten an z.B. Tankstellen installieren.
Realistisch erscheint die Umsetzung nur, wenn die verschiedenen Teilnehmer zusammenarbeiten. Die Technik muss von allen zur selben Zeit, flächendeckend und in optimaler Dichte installiert werden. Es macht keinen Sinn nur vereinzelte und unzusammenhängende Informationen zu erhalten.
[3]

3 Anwendungen

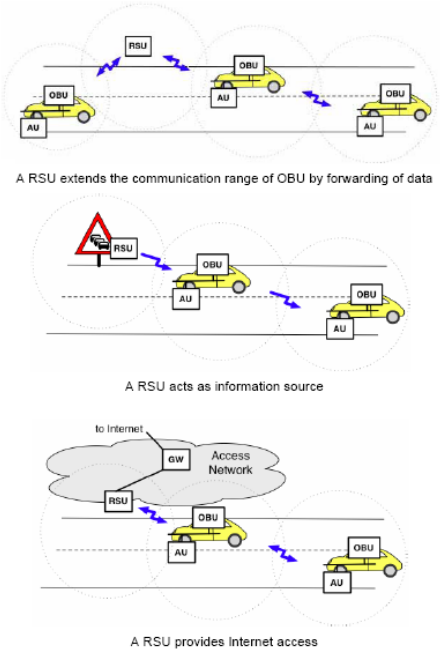
Anwendungen sind Generalisierungen der Szenarios (Kap. 2) und sollen diese in Gruppen zusammenfassen. Sie repräsentieren Funktionalitäten, die in naher oder ferner Zukunft umgesetzt werden sollen. Die Anwendungen werden kurz beschrieben und einige Beispielszenarios aufgezählt.

- *Vehicle 2 Vehicle Cooperative Awareness*: Unterstützt das Austauschen von Informationen zwischen Fahrzeugen ohne dauerhafte Verbindung.

  Beispiele: *V2V Merging Assistance*, *Cooperative Forward Collision Warning*, *Emergency Electronic Brake Lights*, *V2V Lane Change Assistance*, *Approaching*



(a) Sicherheit und Verkehrseffizienz [18]



(b) Road-side unit (RSU) [3]

Abbildung 2 Szenarios für Sicherheit und Verkehrseffizienz, Szenarios für den Einsatz der RSUs

Emergency Vehicle Warning, *Highway/Rail Collision Warning*, *Wrong Way Driving Warning*, *Cooperative Glare Reduction*, *Cooperative Adaptive Cruise Control*

– *Vehicle 2 Vehicle Unicast Exchange*: Ermöglicht die Verbindung zwischen Fahrzeugen zum Informationsaustausch. Besteht aus den vier Phasen Entdeckung, Verbindung, Aufrechterhaltung und Schließung.

  Beispiele: *Pre-Crash Sensing/Warning*, *V2V Merging Assistance*, *Cooperative Vehicle-Highway System (Platoon)*, *Instant Messaging*

– *Vehicle 2 Vehicle Decentralized Environmental Notification*: Stellt Informationen über Ereignisse und Straßeneigenschaften zur Verfügung, die für bestimmmte Zeit in einer bestimmten Region interessant für Fahrzeuge oder Fahrer sind.

  Beispiele: *Slow Vehicle Warning*, *Post-Crash Warning*, *In-Vehicle Ambert Alert*, *Safety Recall Notice*, *Traffic Jam Ahead Warning*, *Hazardous Location V2V Notification*, *Safety Service Point*, *Decentralized Floating Car Data*

– *Infrastructure 2 Vehicle (One-Way)*: Unterstützt Kommunikation von RSUs zu Fahrzeugen ohne dauerhafte Verbindung zwischen diesen.

Beispiele: *Hazardous Location I2V Notification*, *Green Light Optimal Speed Advisory*, *V2I Traffic Optimization*

– *Local RSU Connection*: Daten werden von Fahrzeug zu RSU gesendet, oder in beide Richtungen.

  Beispiele: *Automatic Access Control*, *Personal Data Synchronization at Home*, *Infrastructure-based Cooperative Merging Assistance*, *Remote Diagnostics*, *Free-flow Tolling*, *Drive-through Payment*, *Remote Diagnostics*, *Vehicle Computer Program Updates*, *Signal Violation Warning/Signal Preemption*

– *Internet Protocol Roadside Unit Connection*: Unterstützt Services, die dem Fahrer von Servern im Internet angeboten werden.

  Beispiele: *SOS Services*, *Just-In Time Repair Notification*, *Media Download*, *Map Downloads and Updates*, *Enhanced Route Guidance and Navigation*, *Fleet Management*, *Instant Messaging*

Die Benennung der Anwendungen und Zuordnung der Beispiele kann in anderen Ansätzen unter Umständen abweichen. Die Auflistung soll nur einen Überblick geben, was sich hinter Kommunikation bezogen auf C2C bzw. C2X verbirgt.
[3]

4 Voraussetzungen für die Markteinführung

Wie für alle neuen Entwicklungen ergeben sich auch im Bereich der *C2C* Kommunikation Anforderungen an die Hersteller und sowohl an die neue als auch an die bestehende Technik.

4.1 Wirtschaftlich

Es gibt erforderliche Marktabdeckungen, um einen wirtschaftlich sinnvollen Einsatz zu gewährleisten. Im Bereich Information sind mindestens 5%, für Warnungen mindestens 10% und bei Kooperationen mindestens 95% Marktabdeckung notwendig.
Bei einer optimalen Markteinführung (Kap. 4.2) wird von einer Dauer von mindestens $1\frac{1}{2}$ um 10% und mindestens 6 Jahren um 50% Marktabdeckung zu erreichen gesprochen.
[16]

4.2 Technisch

Die technischen Anforderungen beziehen sich zum einen auf die Automobilhersteller. Diese müssen die Technik für eine optimale Markteinführung in 25% aller neuen Autos verbauen, die gleiche Technologie zur selben Zeit verbauen und dabei auf Abwärtskompatibilität achten. Kein Hersteller darf die Produktion zurückhalten, um

die Entwicklung und den Erfolg des Produktes bei anderen Fabrikanten abzuwarten. Dadurch würde die Markteinführung gebremst werden und es käme zu einer Wettbewerbsverzerrung.
Zum anderen muss die Technik bestimmten Anforderungen gerecht werden. Dazu zählen Anonymität und Datensicherheit (Kap. 8), ein erfolgreich geschütztes Frequenzband (Kap. 6), Skalierbarkeit der Datenmenge (Kap. 7) und die Verfügbarkeit von erforderlichen Sensordaten, z.B. Position, Fahrzeuggeschwindigkeit, Fahrtrichtung, Warnblinker, Bremskraft/-verzögerung, ABS/ESP/ASR Sensoren und Regensensor/Scheibenwischerstatus. In der InV fallen die Sensordaten sowieso an und müssen nur noch über den Datenbus im Fahrzeug bereit gestellt werden.
[16]

5 Systemarchitektur

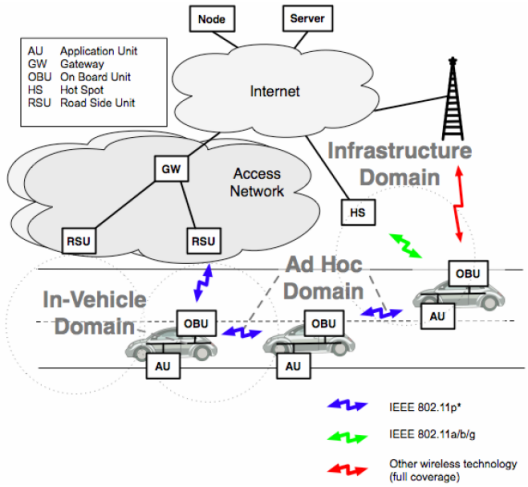


Abbildung 3 Systemarchitektur [3]

Unter Systemarchitektur werden die an der Kommunikation beteiligten Komponenten, die verwendete kabellose Funktechnologie , die Domänen in denen sich die Kommunikation abspielt und die betroffen Schichten im OSI-Schichtenmodell zusammengefasst.

5.1 Komponenten

Bei den Komponenten spricht die C2C-CC von *on-board unit (OBU)*, *application unit (AU)* und *road-side unit (RSU)*. Jedes Fahrzeug besitzt genau eine OBU, an die die AUs angeschlossen sind. Über die OBU läuft die Kommunikation mit anderen Netzwerkkomponenten. Von AUs können in einem Fahrzeug mehrere vorhanden

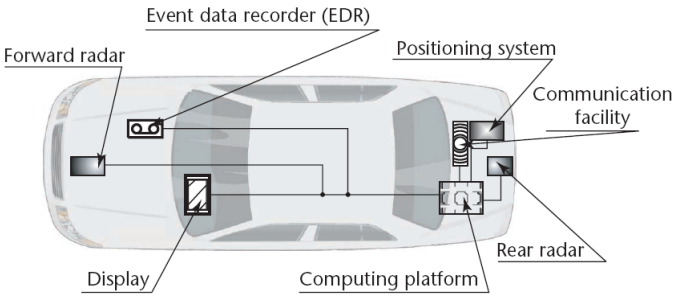


Abbildung 4 Intelligentes Auto [6]

sein, entweder fest eingebaut oder auch als mobile Geräte, z.B. PDAs und Navigationsgeräte, kabelgebunden oder kabellos anschließbar. Die OBU kann in Fahrzeug als zentrale Einheit gesehen werden, während AUs für bestimmte Anwendungen verantwortlich sind. Am Straßenrand werden RSU installiert und bieten entweder Mehrwertdienste an oder erweitern die Kommunikationsreichweite der Fahrzeuge in VANETs (Abb. 2b, 3).
Weitere Einheiten außerhalb des Bereichs des Konsortiums sind *hot spots (HS)*, *event data recorder (EDR)*, GPS Empfänger, Front- und Back-End Radar und Kurzstreckenradar oder Ultraschallsysteme (Abb. 4). Ein HS bietet zusätzlich zu den RSUs Internetzugang im Fahrzeug, wie es von WLAN-Netzen bekannt ist. EDR, Radar und Ultraschall finden beim Thema Sicherheit und Datenschutz (Kap. 8) Anwendung. Das Front- und Back-End Radar, mittels derer Objekte auf der Fahrbahn wahrgenommen werden, haben eine höhere Reichweite als die Radar- bzw. Ultraschallsensoren, die bei Einparkhilfen zum Einsatz kommen. Mittels GPS Empfänger erfolgt die Positionsbestimmung einerseits zur Navigation und andererseits für die Lokalisierung von Kommunikationspartnern.
[3,6,7]

5.2 Domänen

Unterschieden werden die drei Domänen *in-vehicle*, *ad-hoc* oder *vehicular ad-hoc network (VANET)* und *infrastructure* (Abb. 3). Sie korrelieren nicht mit den Szenarios (Kap. 2), da sie technische Einheiten zusammenfassen und sich somit ein Szenario in mehreren Domänen abspielen kann.
Die *in-vehicle* Domäne setzt sich zusammen aus OBUs und AUs und ist vorwiegend kabelgebunden und spielt sich in einem Fahrzeug ab.
OBUs und RSUs zusammengefasst bilden die *Ad-hoc* bzw. *VANET* Domäne. Die Kommuniaktion läuft zwischen Fahrzeugen ab, wobei RSUs zur Vergrößerung der Reichweite mit einbezogen werden können.
In die *infrastructure* Domäne fallen kabellose Kommunikationen mit RSUs und HSs. Zusätzlich können andere Funktechniken genutzt werden, z.B. GSM, GPRS, UMTS, HSDPA, WiMax und 4G. Im Vordergrund stehen Internetzugang im Fahrzeug und weitere ad-on Services.
[3]

5.3 Kabellose Funktechnologien

Eine bekannte Technologie ist IEEE 802.11a/b/g/n (WLAN). Ebenfalls bekannt und weit verbreitet sind GPRS, UMTS, ... Da diese Methoden allerdings aus verschiedenen Gründen (Kap. 7) nicht für *C2C* Kommunikation geeignet sind, sind die neuen Standards IEEE 802.11p und IEEE 1609.4 in Entwicklung. Beide Standards zusammengefasst werden auch *wireless access in vehicular environments (WAVE)* genannt. In Abb. 3 ist zu sehen, wie die Funktechnologien mit den Domänen in Beziehnung stehen. Die *ad-hoc* Domäne basiert auf IEEE 802.11p und die *infrastructure* Domäne auf IEEE 802.11a/b/g bzw. anderen kabellosen Technologien.
[4]

5.4 *Wireless Sensor Networks (WSN)*

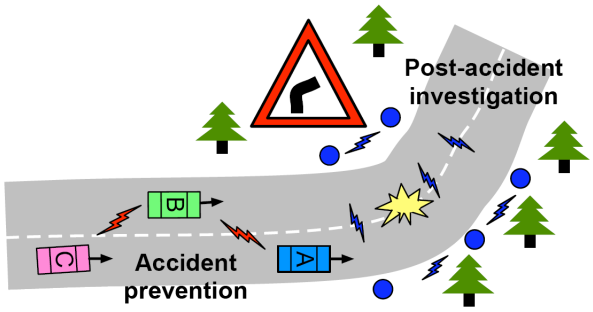


Abbildung 5 *Wireless Sensor Networks (WSN)* [4]

Als Alternative oder Ergänzung zu RSUs können sogenannte *road-side wireless sensors (RSWS)* am Straßenrand installiert und zu *wireless sensor networks (WSN)* (Abb. 5) zusammengefasst werden. Die Sensoren sind energieeffizient organisiert und können sich sehr lange über eine eigene Batterie versorgen. Entweder kann eine ganze Straße ausgestattet werden, wahrscheinlicher werden aber nur Gefahrenstellen (Kurven, Wald, ...) betrachtet. Aufgabe ist das Sammeln von Umgebungsdaten (Temperatur, Feuchtigkeit, Licht, Bewegungen, ...) und die ankommenden Fahrzeuge mit diesen zu versorgen. Im vergleichzu RSUs sind sie billger, können zahlreicher verwendet werden und haben eine statische Netzwerktopologie, bieten aber weniger Funktionalität (kein Internetzugang, keine Mehrwertdienste, ...). Solange die Informationen vertrauenswürdig sind, können sie zur Unfallprävention beisteuern. Der Fahrer kann sich z.B. auf Hindernisse in einer Kurve oder schlechte Straßenverhältnisse einstellen und wird von diesen somit nicht überrascht. auch zur Aufklärung von Unfallursachen können die Daten zu Rate gezogen werden.
[4]

5.5 Schichten

Aus dem OSI-Schichtenmodell sind die *physical layer*, *network layer*, *transport layer* und *application layer* betroffen. *Physical* und *network layer* werden von dem C2C-CC zum Funksystem (Kap. 6) gezählt und die restlichen Schichten werden im Kommunikationssytem (Kap. 7) behandelt.
Der Protokollstapel, *wireless access in vehicular environments (WAVE)*, kann je nach Anwendung auf verschiedenen Wegen durchlaufen werden. Sicherheits- und Verkehrseffizienzanwendungen können den Stapel auf allen möglichen Wegen durchlaufen, um durch Redundanz immer die Funktionalität zu erhalten. Infotainmentanwendungen dürfen allerdings nur den mittleren und rechten Teil des Stapels durchlaufen, der bekannte Funktechnologien wie WLAN und z.B. UMTS beinhaltet. Es ist zu beachten, dass es nicht nur einen Protokollstapel gibt. WAVE ist der Ansatz des C2C-CC (Kap. 1.3) und ist hier exemplarisch aus gewählt. Auf Grund des Konsortiums, aus dem er hervorgegangen ist, kann ihm eine hohe Bedeutung beigemessen werden.
[3,11]

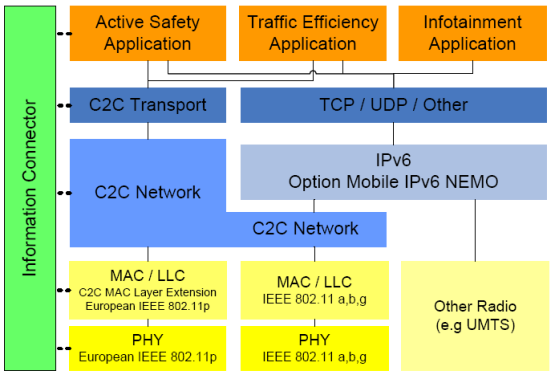


Abbildung 6 *Wireless Access in Vehicular Environments (WAVE)* [3]

6 Funksystem

In diesem Kapitel werden Eigenschaften von und Anforderungen an das Funksystem betrachtet, zu dem auch die *physical* und die *data link layer* gezählt werden. Außerdem werden die Funkkanäle und verwendeten -frequenzen vorgestellt.

6.1 Kommunikationskanäle und Anwendungskategorien

Unterschieden wird bei den Kommunikationssystemen zwischen geschützten und öffentlichen Kanälen. Die unterschiedlichen Anwendungen haben jeweils begrenzte oder keine Kanalzugänge.
[3,9,11]

6.1.1 Geschützte Kanäle

Geschützte Kanäle sind für die Netzwerkkontrolle (*controll channel (CCH)*), sicherheitskritische Anwendungen, Straßensicherheits- und Verkehrseffizienzanwendungen und nicht-sicherheitskritischen Anwendungen bezogen auf C2C bzw. C2X reserviert. Um diese Kanäle geht es im weiteren Verlauf dieser Arbeit. Sie sind nur für diese Anwendungen reserviert und werden ausschließlich von diesen benutzt.
[3,9–11]

6.1.2 Öffentliche Kanäle

Öffentliche Kanäle werden von add-on Services benutzt, z.B. Entertainment/Infotainment und Internet, und werden hier nicht weiter behandelt.
[3,9–11]

6.2 *Physical Layer*

6.2.1 Frequenzbänder

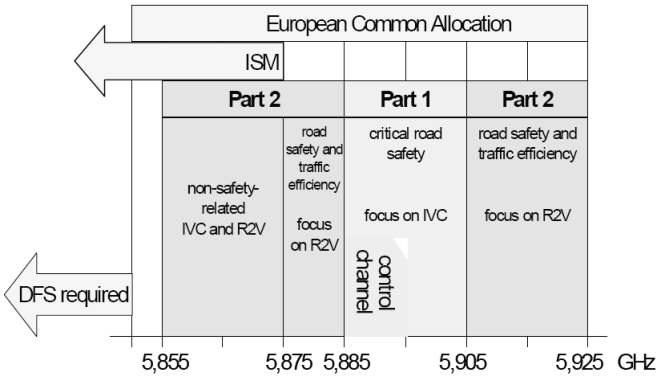


Abbildung 7 Reservierte Frequenzbänder, die in Kanäle unterteilt sind[3]

Die zuvor genannten geschützten Kanäle benutzen die reservierten Frequenzen in Abb. 7. Es gibt zwei 10 MHz Bänder für kritische Straßensicherheitsanforderungen und den CCH (*Part 1*). Drei weitere 10 MHz Bänder dienen der Straßensicherheit und Verkehrseffizienz (*Part 2*). Die letzten zwei 10 MHz Bänder sind nicht-sicherheitskritischen Anwendungen vorbehalten (*Part 2*).
[3,9,11]

6.2.2 Parameter

Die Kommunikationsreichweite beträgt für spezielle Fahrzeuge 1000 Meter und für normale Fahrzeuge 300 Meter. Da Straßen länger als breit sind, kann die Reichweite

nach vorne größer sein, als zu den Seiten. Aufgrund der Echtzeitanforderungen muss die Systemlatenz kleiner als 50 Millisekunden betragen. Standardmäßig ist die Datenrate 6 Megabyte pro Sekunde und maximal 27 Megabyte pro Sekunde. Je nach Kanalauslastung wird die Datenrate des Senders angepasst. Nachrichten haben eine Übertragungsgröße von bis zu 20 Kilobyte, sollen aber so klein wie möglich gehalten werden. Die Parameter beziehen sich auf alle Anwendungen auf den öffentlichen Kanälen (Kap. 6.1.1).
[10,15]

6.2.3 Anforderungen

Es muss einen CCH für die Netzwerkkontrolle und mehrere *service channels (SCH)* geben. Damit während des Abhörens des CCH keine anderen Nachrichten verpasst werden, muss simultanes Empfangen auf beiden Kanälen (*Part 1*) gewährleistet sein. Der CCH wird in festen Intervallzeiten abgehört.
[3,9,11]

6.3 *Data Link Layer (MAC/LLC)*

Multi channel operation und *dual receiver concept* müssen laut den Anforderungen (Kap. 6.2.3) unterstützt werden. Daher die Entscheidung für mehrere *SCHs*. Selbst wenn sicherheitskritische Anwendungen über einen der entsprechenden Kanäle laufen, müssen andere Kanäle weiterhin abgehört werden, um keine wichtigen Nachrichten zu verpassen. Die ankommenden Anwendungen können dabei von verschiedenen Sendern kommen.
Ausstehend ist noch die Entscheidung bezüglich der Mechanismen für Prioritäten und Wartezeiten. Fest steht, dass sicherheitsrelevante Nachrichten höhere Prioritäten als andere Nachrichten bekommen müssen. Auch die Wartezeiten müssen nach der Notwendigkeit und der Echtzeitanforderung geregelt werden, d.h. dass weniger wichtige Nachrichten bis zum erneuten Versenden eine längere Wartezeit haben können als wichtigere Nachrichten.
Die Kontrolle der Sendeleistung ist von besonderer Bedeutung. Am Anfang der Einführung am Markt wird die Marktabdeckung nur spärlich sein. Nach einiger Einführungszeit wird die Abdeckung allerdings stetig zunehmen. Außerdem muss die Sendeleistungskontrolle damit umgehen können, ob sich das Fahrzeug in einem Stau oder einer leeren Straße befindet. Dabei ist noch nicht klar, ob dafür die Reichweite verändert wird, oder ob die ankommenden Nachrichten einer Selektion unterzogen werden.
[3,9–11]

7 Kommunikationssystem

Damit ein Fahrzeug mit einem anderen oder mit seiner Umgebung kommunizieren kann, muss es diese adressieren können. Im folgenden Abschnitt werden die Anforderungen an und Vorschläge für ein solches System erklärt.

7.1 Herausforderungen

Das Kommunikationssystem steht vor einigen Herausforderung. Fahrzeuge bewegen sich mit hohen Geschwindigkeiten und die Netzwerktopologie ändert sich häufig. Aufgrund des ad-hoc Charakters gibt es keine zentrale Instanz zur Netzwerkorganisation und -koordination. Des weiteren darf die vorhandene Bandbreite nicht überschritten werden und es muss auf spärliche oder dichte Netzwerksituationen reagiert werden.
[3,9,10]

7.2 Designprinzipien

Es sollen zunächst die Adressierungsmethoden genannt werden. Im Anschluss folgen die Übermittlungsalgorithmen mittels derer die Adressaten tatsächlich erreicht werden.

7.2.1 Geografische Adressierung

Adressierung von Kommunikationspartnern erfogt über geografische Methoden. Entweder ist der Empfänger ein einzelner Knoten (*geographical unicast/geounicast*) oder alle Teilnehmer in einer geografischen Region (*geographical broadcast/geocast, geographical anycast/geoanycast*) werden als Empfänger gewählt.
[3,9]

7.2.2 Übermittlungsalgorithmen

Zur Übermittlung verwendete Algorithmen sind *geographical unicast*, *topologically-scoped broadcast (TSB)*, *gepgraphical broadcast* und *geographical anycast* (Abb. 8).
Geographical unicast übermittelt eine Nachricht an genau einen Empfänger. Entweder direkt per *unihop* oder über mehrere Zwischenstationen per *multihop*. Die Zwischenstationen können die Nachricht unverändert weiterleiten oder sie verändern. Dabei werden falls nötig mehrere Nachrichten zu einer zusammengefasst, eine Nachricht in mehrere aufgeteilt oder Informationen verändert bzw. hinzugefügt. *Topologically-scoped broadcast (TSB)* sendet an alle Knoten, die mittels einer festen Anzahl an Sprüngen (*hops*) zu erreichen sind. *Geographical broadcast* beschränkt sich auf eine definierte Region um den Sender herum oder auf eine bestimmte Entfernung zu diesem. *Geographical anycast* schließt alle Fahrzeuge ein, die die Nachricht empfangen können.
[3,9]

7.3 *Network layer*

7.3.1 Eigenschaften

Grundfunktionalität der *network layer* ist das *routing* und *forwarding*. Sie ermöglicht kabellose *multihop* Kommunikation als *uni-* oder *multicast* mittels *geographical adressing/routing*. Außerdem ist sie verantwortlich für die Positionierung durch *beaconing* und *location services*. Für die Datenlieferung stehen die drei Methoden *geographical*

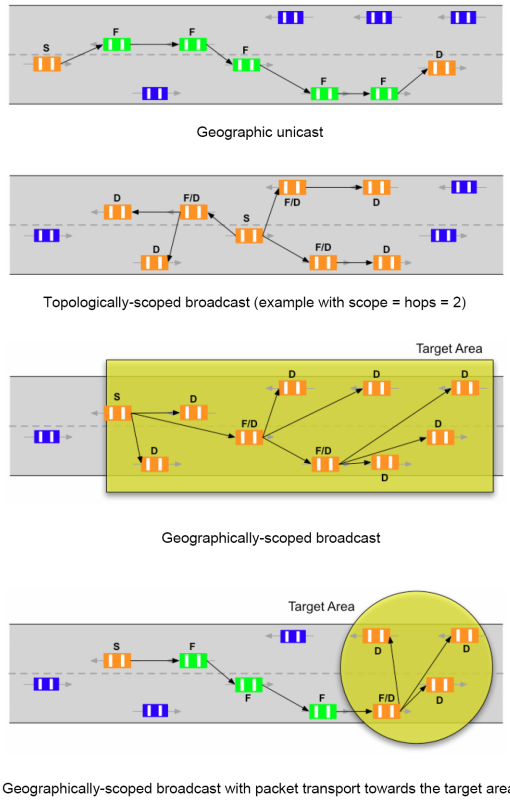


Abbildung 8 Übermittlungsalgorithmen [3]

broadcast, *single hop broadcast* und *periodic beacon packets* zur Verfügung.
Mit *beaconing* ist das periodische Versenden von *beacon packets* gemeint, in denen Positionsinformationen des Fahrzeugs an die Umgebung mitgeteilt werden.
[3,9]

7.3.2 Komponenten

Hauptkomponenten sind die *neighbors*- und die *location table*. In der ersten Tabelle sind nur die Daten der direkten Nachbarn gespeichert und die zweite enthält alle Knoten, dessen Daten bekannt sind. Die notwendigen Daten zum Aufbau der Tabellen erhält ein Knoten durch periodisches *beaconing*. Beide Tabellen müssen regelmäßig aktualisiert werden.
[3,9]

7.4 Transportprotokolle

7.4.1 WAVE short message protocol (WSMP)

Bekannte Transportprotokolle müssen an die neuen Aufgaben angepasst werden. Resultat soll das *WAVE short message protocol (WSMP)* sein. Entwickelt wird es von dem C2C-CC, ist aber nicht als Referenz, sondern nur als Beispiel zu sehen. Es arbeitet auf *transport* und *network layer* und bestimmt die Kanalnummer und Übertragungsleistung. Viel mehr ist über das neue Protokoll leider noch nicht bekannt. [1,2,17]

7.4.2 Transport- und Überlastungskontrolle

Noch ungeklärt sind die Transport- und Überlastungskontrolle. Offen sind Fragen bzgl. fehlerfreiem Transport (*single protocol/multiple protocols*), Prioritäten von Datenpacketen, Datenaggregation und Payloadgröße. Ausfallsicherheit (*connection-free/conncetion-less*), *Forwarding* (*end-to-end* Prinzip), Transportarten (*unicast/broadcast*), Fairness, Komplexität, Multiplexing sowie Verzögerungen und Ortsgültigkeit sind auch zu klären.
Es bleibt abzuwarten, wie mit den Problemen umgegangen wird. Auf Grund der vielen Anforderungen muss höchste Sorgfalt in die Entwicklung gelegt werden. Eine Herausforderung ist z.B. die Frage der Ortsgültigkeit. Unter Ortsgültigkeit ist zu verstehen, wie lange eine Nachricht in einer bestimmten Region bei der sich schnell ändernden Netzwerktopologie gültig bleibt, oder als veraltet verworfen wird.
[1,2,17]

8 Datensicherheit und Datenschutz

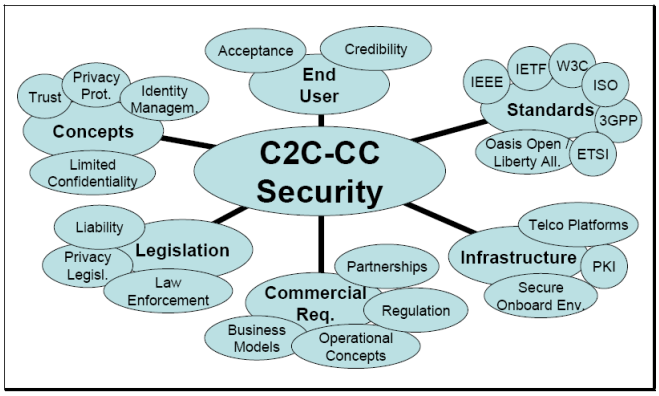


Abbildung 9 Sicherheit [3]

8.1 Sicherheitsanforderungen

Eine vergleichbare Technik kommt bei Kreditkarten und Handykarten zum Einsatz. Mittels einer Sicherheitsnummer wird der Zugang zu den geschützten Services gewährt oder bei Falscheingabe verweigert.
Alle im Netzwerk übertragenen Informationen müssen korrekt und vertrauenswürdig sein. Zurückgegriffen wird dabei auf Authentifikation und nicht auf Verschlüsselung. Auf Verschlüsselung kann verzichtet werden, da die Nachrichten nur gegen Angreifer von außen oder innen geschttzt werden müssen. Sie enthalten keine sensitiven Informatinen, die zu verschlüsseln wären. Verifikation der Datenkonsistenz kann durchgeführt werden, indem Nachrichten von mehreren Sendern verglichen werden. Falls eine Nachricht mehreren anderen konsistenten Nachrichten widerspricht, wird diese als falsch verworfen. Des weiteren muss das Gesamtsystem extrem robust und ausfallsicher sein und der Schutz der Privatsphäre der Teilnehmer muss gewährleistet sein. Außerdem ist Unleugbarkeit sehr wichtig, so dass ein Verkehrsteilnehmer nicht das Senden seiner Informationen verhindern kann, um sich somit z.B. strafrechtlichen Verfolgungen nach einem Unfall zu entziehen.
[6–8, 13, 14]

8.2 Angreifermodelle

Angriffe werden in verschiedenen Modellen kategorisiert. Sie können von innen (authentifiziertes Mitglied) oder von außen (Eindringling) kommen, böswillig (kein persönlicher Gewinn) oder rational (persönliche Vorteile) sein und aktiv (Nachrichtengenerierung) oder passiv (Abhören) sein. Der Fall des unbeabsichtigten Eindringens wird nicht zu den Angriffsmodellen gezählt. Er darf trotzdem nicht eintreffen und muss daher durch die Sicherheitsanforderungen (Kap. 8.1) abgefangen werden.
[8, 13, 14]

8.3 Angriffe/Bedrohungen

Bedrohungen bestehen im Senden von Falschinformationen oder gefälschten Ortsinformationen. Es können die Identitäten von Teilnehmern aufgedeckt werden oder ein Fahrzeugführer kann mittels *Maskierung* anonym bleiben oder sich als jemand anderes ausgeben. Eine weitere Bedrohung ist *denial-of-service*, bei dem das Senden und evtl. auch Empfangen von Nachrichten unterbunden wird.
[6–8, 14]

8.4 Techniken

In diesem Abschnitt sollen nur kurz mögliche Techniken angerissen werden. *Public key infrastructures (PKI)* verwenden digitale Signaturen (*private/public keys*), einen von *certification authorities (CA)* vergebenen *public key* und für die Identifikation von Falschnutzern *certificate revocation lists (CRL)* (Abb. 10, 11). Während Abb. 10 einen Überblick über die Sicherheitsarchitektur gibt, zeigt Abb. 11 ein Beispiel für die Verwendung digitaler Signaturen.

Als Hardware sind elektronische Nummernschilder (*electronic license plate (ELP)*), elektronische Chassisnummern (*electronic chassis number (ECS)*) und *event data recorder (EDR)* notwendig (Abb. 4). Alle Hardwarekomponenten müssen manipulationssicher sein und evtl. mit einem Alarm ausgestattet sein.
Um die Privatsphäre zu bewahren, werden Pseudonyme eingesetzt, die nur mit Gerichtsbeschluss in besonderen Fällen von autorisierten Behörden aufgedeckt werden dürfen.
[6–8, 12–14, 20]

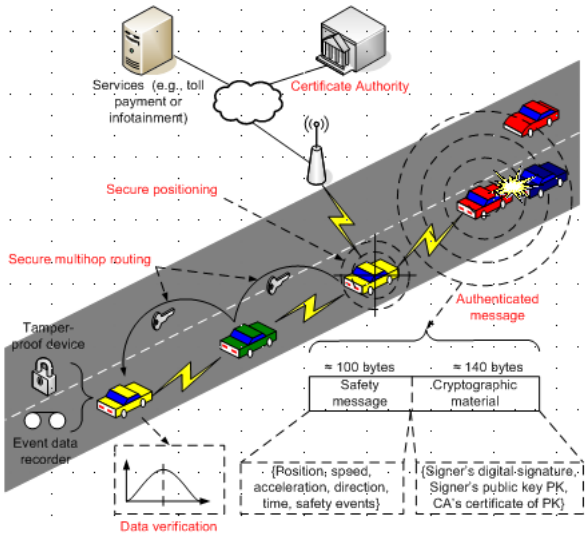


Abbildung 10 Sicherheitsarchitektur [13]

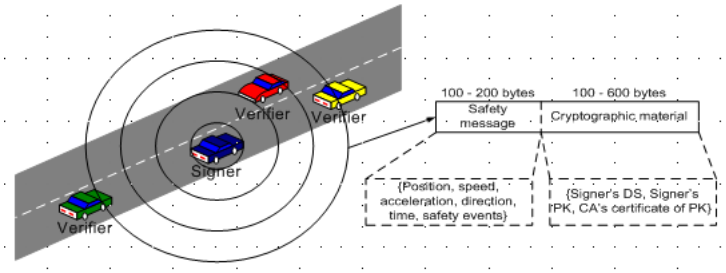


Abbildung 11 Signieren und Verifizieren von Nachrichten [13]

9 Zusammenfassung und Schlußfolgerung

Auch wenn die Idee und Motivation hinter der zuvor besprochenen Kommunikationstechnik gut ist, bleibt die Konkretisierung und Umsetzung abzuwarten. Der Staat ist als Triebkraft an der Entwicklung der neuen Techniken noch nicht beteiligt, könnte aber durch das Beschließen neuer Gesetze die Einführung deutlich beschleunigen. Bisher konzentriert sich die Arbeit des C2C-CC auf einen europäischen Standard. Ein internationaler Standard ist noch nicht absehbar und es ist auch fragwürdig, ob eine internationale Kompatibilität überhaupt sinnvoll ist.
Wie bei allen Assistenzsystemen ist die Frage der Verantwortung zu klären. Liegt sie bei Fehlverhalten beim Hersteller oder beim Fahrer, vgl. Fahrassistenzsystem oder Fahrerassistenzsystem. Selbstverständlich ist bei der heutigen Diskussion um *big brother* die Akzeptanz fraglich, da die Privatsphäre geschützt und die Verfolgbarkeit unterbunden werden muss.

Literatur

1. Bilstrup, Katrin: *A Survey Regarding Wireless Communication Standards Intended for a High-Speed Vehicle Environment*, Halmstad, 2007
2. Bilstrup, Katrin; Uhlemann, Elisabeth; Ström, Erik G.: *Medium Access Control in Vehicular Networks Based on the Upcoming IEEE 802.11p Standard*
3. Car 2 Car Communication Consortium: *Manifesto*, Version 1.1, 2007
4. Festag, Andreas; Hessler, Alban; Baldessari, Roberto; Le, Long; Zhang, Wenhui; Westhoff, Dirk: *Vehicle-to-Vehicle and Road-Side Sensor Communication for Enhanced Road Safety*, Heidelberg, 2008
5. Franz, Dr. Walter: *Car-to-Car Communication – Anwendungen und aktuelle Forschungsprogramme in Europa, USA und Japan*, Ulm
6. Hubaux, Jean-Pierre: Capkun, Srdjan; Luo, Jun: *The Security and Privacy of Smart Vehicles*, 2004
7. Hubaux, Jean-Pierre; Capkun, Srdjan; Luo, Jun; Raya, Maxim: *The Security and Privacy of Smart Vehicles*, 2007
8. Krul, Robert: *Vehicular Ad-Hoc Networks*, 2007
9. Lenardi, Dr. Massimiliano: *Status of the C2C-CC Phy/Mac/Net Working Group*, 2006
10. Lübke, Andreas: *Car-to-Car Communication – Technologische Herausforderungen*, Wolfsburg, 2004
11. Menouar, Hamid; Lenardi, Dr. Massimiliano: *Réseaux VANETs et norme 802.11p*, Paris, 2008
12. Plößl, Klaus; Nowey, Thomas; Mletzko, Christian: *Towards a Security Architecture for Vehicular Ad Hoc Networks*, Regensburg, 2006
13. Rao, Jayanthi: *Security in Vehicular Ad hoc Networks (VANETs)*, 2008
14. Raya, Maxim; Hubaux, Jean-Pierre: *Securing vehicular ad hoc networks*, 2007
15. SIRIT Technologies: *DSRC Technology and the DSRC Industry Consortium (DIC) Prototype Team*, Texas, 2005
16. Specks, Will; Matheus, K.; Morich, R.; Paulus, I.; Menig, C.; Lübke, A.; Rech, B.: *Car-to-Car Communication – Market Introduction and Success Factors*
17. Weigle, Dr. Michele: *Standards: WAVE/DSRC/802.11p*, 2008
18. Wewetzer, Christian: *Car-2-Car Communication Consortium, Applications Working Group - Current Status*, 2006
19. Wischhof, Lars: *Self-Organizing Communication in Vehicular Ad Hoc Networks*, Braunschweig, 2007
20. Zhou, Lidong: Haas, Zygmunt J.: *Securing Ad Hoc Networks*, New York, 1999