Ausarbeitung
zum Fachseminar Wintersemester 2008/09
Referent: Prof. Dr. Linn

V2V
Vehicle-to-Vehicle Communication

Benjamin Schinzel

Fachhochschule Wiesbaden
Fachbereich Design Informatik Medien
Studiengang Allgemeine Informatik

Inhaltsverzeichnis

Zusammenfassung....4
Summary....4
Einführung....5
Motivation....5
Active Safety (Aktive Sicherheit)....5
Traffic Efficiency (Verkehrsoptimierung)....6
Comfort and Infotainment (Komfort und „Infotainment“)....6
Technische Problemstellung....6
Netzwerk....6
Security....7
Regionale Entwicklung....7
USA....7
Japan....7
Europa....8
Das V2V System des C2C CC....9
Physical Layer (PHY) Architektur....9
Funkkanäle....9
Frequenzband....9
Sendeleistung....10
Antennendesign....11
MAC/LLC Layer Architektur....11
IEEE 1609.4....11
MAC Layer Extensions....12
Das Dual-Receiver Konzept....12
MAC Adressen....13
Nachrichten....14
Network/Transport Layer....14
Sparse/Dense Network Situation....14
Packet/Information Centric Forwarding....14
TCP/IP Protocol Suite....15
Forwarding Algorithmen....15
Geographische Adressen....15
Geographical Unicast....15
Topologically Scoped Broadcast....16
Geographical Scoped Broadcast....16
Geographical Scoped Anycast....17
Transport Layer....17
Protokolle....19
Network Layer Protocol....19
Transport Layer Protocol....21
Application Layer....22
Anwendungen....22
Cooperative Awareness....22
Unicast Exchange....23
Decentralized Environmental Notification....23
Infrastructure to Vehicle (one-way)....23
Local Road Side Unit Connection....23
IP Road Side Unit Connection....23

Information Connector (IC)....24
Security....24
Zusammenfassung und Kommentar....24
Quellen und Referenzen....25
Primärquellen....25
Sekundärquellen....25
Sonstige Quellen....27

Zusammenfassung

Unter dem Begriff V2V (Vehicle-to-Vehicle) versteht man eine Technologie, die es ermöglicht, dass Fahrzeuge untereinander kommunizieren. Es existieren viele Begriffe die das gleiche oder ähnliche wie V2V bedeuten: C2C, V2I, IVC, VANET. Anwendungsbeispiele der Technologie in dieser Ausarbeitung beziehen sich konkreter auf Car-to-Car Kommunikation (C2C).

V2V ist eine sehr mächtige Technologie, wenn es darum geht die Straßen weltweit sicherer zu machen. Die Technik erweitert den Horizont des Fahrers. Beispielsweise werden schwer einsehbare Passagen ein geringeres Risiko: Fahrzeuge an einem Stauende warnen sich nähernde Fahrzeuge.

Diese Ausarbeitung beschäftigt sich mit den technischen Aspekten und dem Zustand in der Forschung und Entwicklung. Zunächst könnte man denken: „Es existiert doch schon so viel Wissen über Netzwerke und Mobile Kommunikation, kann es da noch ein Problem geben?“. V2V ist extrem dynamisch. Die Kommunikationspartner wechseln im Straßenverkehr schnell, ebenso schwankt die Dichte an Kommunikationspartnern erheblich und diese bewegen sich auch noch unterschiedlich schnell fort. V2V ist so komplex, dass man es als eigenes Forschungsgebiet bezeichnen könnte. Ziel dieser Ausarbeitung ist es auch aufzuzeigen, wie der aktuelle Stand der Dinge ist.

Summary

The term V2V (Vehicle-to-Vehicle) is known as a technology, which enables communication between vehicles. There are many terms meaning the same or similar like V2V: C2C, V2I, IVC, VANET. In this paper usage examples of the technology refer specific to Car-to-Car Communication (C2C).

V2V is a very mighty technology, when it comes to how make the streets worldwide safer. The technology extends the drivers field of vision. For example difficult visible passages become a lesser risk: Vehicles in a hidden queue warn approaching vehicles.

This paper is about the technical aspects and the state of research and development. First of all you could think: „There is so much knowledge about networks and mobile communication, can there still be a problem?“. V2V is extreme dynamic. The communication partners in traffic switch fast, also the density of communication partners varies significant and they move differently fast, too. V2V is so complex, that you could designate it as an own field of research. Also the goal of this paper is to show the actual state of affairs.

Einführung

Unter V2V (Vehicle-to-Vehicle) versteht man die Ad-Hoc-Kommunikation zwischen Fahrzeugen. Informationen werden gesammelt und erzeugt, Daten werden über Signale und Protokolle ausgetauscht und im empfangenden Fahrzeug verarbeitet. Der Grundgedanke dabei ist, das Informationsspektrum, welches dem Fahrer zur Verfügung steht, zu erweitern – das Fahren sicherer und komfortabler zu machen.

„Fahrzeug“ ist zunächst ein sehr abstrakter Begriff, ein Fahrzeug kann alles mögliche sein. Der Begriff V2V ist jedoch stark durch die Automobil-Industrie geprägt, denn *vermutlich* lässt sich bei Automobilen der größte Nutzen aus dieser Technologie ziehen. Aufgrund der Aktivität der Automobil-Industrie im Bereich der Forschung auf diesem Gebiet existieren noch viele weitere verwandte Begriffe: Car-to-Car (C2C), Vehicle-to-Infrastructure (V2I), Intervehicle Communication (IVC), Vehicular Ad-hoc Networks (VANETs) oder einfach Fahrzeug-Fahrzeug Kommunikation. Abgesehen von V2I sind diese Begriffe gleichbedeutend.

Motivation

Active Safety (Aktive Sicherheit)

„Vorausschauend Fahren“ bekommt man in der Fahrschule gelehrt. Was heißt das für die Praxis? Mit den Augen möglichst alle Daten wahrnehmen, diese dann zu Informationen interpretieren, aus den Informationen eine Gesamtsituation entwickeln, die Gesamtsituation bewerten und entsprechend reagieren.

Bereits bei dem ersten Schritt kann es zu argen Problemen kommen. Je weniger Sicht man hat, desto langsamer muss man fahren, um rechtzeitig entscheiden und reagieren zu können. Der Grund ist meist eine versperrte Sicht, beispielsweise durch Nebel oder einen Wald, der die Sicht blockiert. Bei solchen Gegebenheiten ist es gut zu wissen, ob hinter der Kurve oder der Nebelwand ein Stauende liegt. Dort kann Fahrzeug-Fahrzeug Kommunikation den Fahrer warnen – beziehungsweise können die Fahrzeuge am Stauende alle anderen Fahrzeuge, die sich nähern, warnen.

Weitere Szenarien sind schnell erdacht. Ein Unfallwagen könnte ein Warnsignal senden. Dies würde das Risiko senken, wenn ein Fahrer das aufgestellte Warnschild übersieht. Notarztwagen, Feuerwehr und Polizei könnten so zusätzlich ihre Anfahrt verkünden. Gleiches gilt für Schwertransporte und Gefahrguttransporte. Ein Fahrzeug könnte andere Fahrzeuge mit Traktionsdaten auf rutschigen Untergrund hinweisen. Infrastruktur kann auch in die Kommunikation mit eingebunden werden. Beispielsweise könnten Baustellenschilder Warnsignale senden. In diesem Fall spricht man von V2I (Vehicle-to-Infrastructure).

Für die zuvor genannten Anwendungsbeispiele existiert der zusammenfassender Begriff „Active Safety“. V2V hat also die (Teil-)Motivation Risiken im Straßenverkehr zu *mindern* und den Fahrer zu schützen. Um dies zu erreichen „erweitert V2V den Horizont des Fahrers“, beziehungsweise schließt es eine Lücke: Der Fahrer nimmt mit seinen Augen Informationen bis ein paar hundert Meter Entfernung wahr. Ähnliche Dimensionen gelten für Onboard Sensoren wie Abstandswarner. Alles was danach kommt liegt in einer Grauzone, Gefahren können nur erahnt werden. Um Informationen aus der Ferne zu erhalten, könnte der Mobilfunk verwendet werden, doch das kostet. V2V schließt die Lücke zwischen Onboard Sensoren und Fernkommunikation. Die folgende Abbildung soll diesen Sachverhalt darstellen.

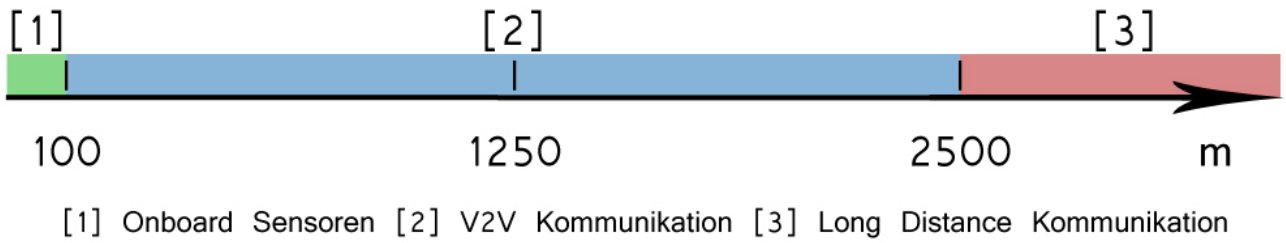


Abbildung 1: V2V bietet Kommunikation von nah bis fern

Traffic Efficiency (Verkehrsoptimierung)

Eine weitere wichtige Motivation von V2V ist die so genannte „Traffic Efficiency“. Bei dieser sehr interessanten Thematik geht es darum, wie der Verkehr effizienter gestaltet werden kann. Durch das Anpassen von Geschwindigkeiten lässt sich Staurisiko vermindern, quasi das was man von Anzeigetafeln kennt. Ebenso könnte man auf der „grünen Welle fahren“, doch dies nur als eine Idee – die Umsetzung wäre sicher alles andere als trivial. Insgesamt käme man früher ans Ziel und hätte Treibstoff und Emissionen gespart.

Comfort and Infotainment (Komfort und „Infotainment“)

Die letzte Motivation im Bunde wird „Comfort and Infotainment“ genannt. Es geht dabei beispielsweise um Informationen die man zu der Stadt erhält, in der man sich momentan befindet. Die Entfernung zur nächsten Tankstelle könnte auch von Interesse sein. Eine Funktionalität, über deren Vor- und Nachteile man diskutieren kann, ist die Voice Kommunikation mit anderen Fahrern.

Technische Problemstellung

Netzwerk

Vergleicht man ein gewöhnliches lokales Netzwerk – sei es ein WLAN im Ad-Hoc Modus ohne zusätzliche Infrastruktur – mit einem V2V Ad-Hoc Netzwerk, so fallen einem sofort entscheidende Unterschiede auf: Die Kommunikationspartner in einem V2V Netzwerk wechseln ständig. Man biegt auf einer Kreuzung ab und schon hat man viele neue Kommunikationspartner, während die alten sich sehr schnell aus dem Kommunikationsbereich entziehen werden. Es ist jedoch auch möglich, dass man überhaupt keinen Kommunikationspartner hat, beispielsweise nachts auf einer Landstraße. Im Gegenteil dazu sind auch Peaks möglich, wenn man auf der Autobahn steht und der Verkehr sich doppelspurig staut – redundante Informationen und belastete Kanäle sind die Folge. Die Kommunikationsdichte schwankt also erheblich. Problematisch sind auch die hohen relativen Geschwindigkeiten, wenn Fahrzeuge entgegengesetzt aneinander vorbeifahren. Grundsätzlich gilt, je höher die Geschwindigkeit, desto wichtiger wird es, dass Informationen ohne Verzögerung übermittelt werden. Selbstverständlich müssen auch technische Standards ins Leben gerufen werden, um V2V weltweit nutzen zu können – ein organisatorisch kritischer Aspekt, wenn man bedenkt wie viele Interessen von Herstellern, Regierungen und Standardisierungsinstitutionen aufeinander treffen.

V2V ist sicherlich auch durch andere Technologien die bereits existieren realisierbar. Jedoch wäre dies mit Nutzungs-Kosten der Netze verbunden. Ziel ist es Informationen direkt und ohne Umwege auszutauschen, mit den Fahrzeugen die es unmittelbar interessiert.

Security

Kein Kernthema aber wichtig ist Security im Bereich der V2V Kommunikation. Es darf nicht möglich sein, dass Fahrzeuge anhand ihrer Daten die sie senden von Privatpersonen eindeutig identifiziert und verfolgt werden können. Außerdem muss sichergestellt sein, dass keine manipulierten Daten gesendet werden können, welche den Zweck haben sollen, Schaden durch Irreführung anzurichten. Allgemein ist die Integrität der Daten eine Schwachstelle, denn stabile Verbindungen können nicht aufgebaut werden.

Regionale Entwicklung

Parallel, aber nicht komplett unabhängig, findet Forschung, Entwicklung und Standardisierung in verschiedenen Ländern statt. Primär aktiv im Bereich V2V sind Japan, die Vereinigten Staaten und Europa. Es sei nochmal darauf hingewiesen, dass hier der Begriff V2V schwammig benutzt wird – V2I (Vehicle-to-Infrastructure) sei hier inbegriffen. Die Entwicklungen sind unterschiedlich weit fortgeschritten und haben eine unterschiedliche Vorgeschichte. Darauf wird in den folgenden drei Abschnitten kurz eingegangen.

USA

In den Vereinigten Staaten ist die Entwicklung bereits weit fortgeschritten. Vorangetrieben werden Projekte vom Verkehrsministerium (U.S. Department of Transportation, DOT *[4]*). Das DOT fördert Projekte und die Automobilhersteller beteiligen sich daran. Außerdem beteiligt sind die Konsortien VIIC (Vehicle Infrastructure Integration Consortium) und CAMP (Crash Avoidance Metrics Partnership). Seit 1999 hat die Federal Communications Comission (FCC) im 5,9 GHz Frequenzband *[13]* eine Bandbreite von 75 MHz reserviert. Um genau zu sein im Bereich 5,850-5,925 GHz. Die FCC ist für die Zulassung von Kommunikationsgerären in den Vereinigten Staaten und deren Basen zuständig. Die Reservierung gilt für DSRC *[11]* (Dedicated Short Range Communications), einem Kommunikationsstandard, der auf dem IEEE Standard 802.11p *[5]* (wird später behandelt) basiert. DSRC gehört also zur Funknetzfamilie WLAN (IEEE 802.11). Übrigens hat der IEEE 802.11p Standard noch den Zustand „IN PROCESS“ *[6]*. Effektiv genutzt wird nur der Bereich 5,855-5,925 GHz, also 5 MHz weniger. Die restlichen 70 MHz Bandbreite sind in Kanäle von je 10 MHz breite aufgeteilt. Oberhalb des IEEE 802.11p Standards setzt die Protokollfamilie IEEE 1608.X auf. Hier wird auf den Protokollstack der amerikanischen Version des V2V jedoch nicht weiter eingegangen. Stattdessen soll später der europäische Protokollstack genauer betrachtet werden. Prinzipiell kann man sich einen solchen Protokollstack wie das OSI (Open Systems Interconnection [Reference Model]) Schichtenmodell der ISO vorstellen. In den USA hat V2I zunächst einen höheren Stellenwert – wird auch bereits genutzt. V2V hingegen soll später realisiert werden.

Japan

In Japan sind zum Großteil Ministerien an der Entwicklung von V2V beteiligt: Das Ministry of Land, Infrastructure and Transportation (MLIT), das Ministry of Internal Affairs and Communication (MIC), das Ministry of Economy, Trade and Industry (METI) und die National Police Agency (NPA). In Japan hat V2V bzw. V2I bereits eine Vorgeschichte. Seit längerem existiert ein eletronisches Mautsystem (ETC, Toll Collect). Die DSRC verwendende ETC Infrastruktur ist bereits ausgebaut und kann neben den ETC Daten auch V2I Daten übertragen. Für V2V reicht dies noch nicht, deswegen wird an einem erweiterten WAVE *[9]* Standard und einem vollkommen neuen Standard im 700 MHz Frequenzband gearbeitet. WAVE heißt „Wireless Access in Vehicular Environments“ und steht für die vier IEEE 1609.X Standards.

Neben diesem Mautsystem existiert noch ein anderes etabliertes System. Die National Police Agency fördert das VICS *[7]* (Vehicle Information and Communication System). Das VICS informiert mittels Broadcast Stationen und so genannten Beacons (Radiowellen/Infrarot) Autofahrer über den Verkehrszustand. Weitergehend hat die NPA Unternehmungen im Projekt Driving Safety Support Systems *[8]* (DSSS, gesprochen „D-Triple-S“). Beacons mit Infrarottechnik und V2V werden eingesetzt, um Fahrer vor kritischen Verkehrsabschnitten zu warnen. Dabei wird der Fahrer nicht nur gewarnt, er erhält auch zusätzliche Informationen. Beispielsweise ob ein Fahrzeug entgegenkommt und es beim Rechtsabbiegen zu Problemen kommen kann (in Japan herrscht Linksverkehr).

Das Projekt Advanced Safety Vehicle (ASV) wurde 1991 vom Ministry of Land, Infrastructure and Transportation zusammen mit akademischen Experten und der Autoindustrie ins Leben gerufen. Zunächst ging es dabei um Technische Entwicklungen, die zunächst nichts mit V2V zu tun haben: Einer Stabilitätskontrolle, einem Abstandswarner, einem System welches Alarm schlägt, wenn der Fahrer schläfrig wird („Zigzag driving detection system“) und einem Reifendruckwarner. In einer späteren Phase ging es dann um V2V über DSRC.

Ein weiteres Projekt ist Advanced Cruised-Assist Highway Systems (AHS), welches auf V2I setzt. Verkehrszustandsinformationen werden gesammelt und via DSRC an die Fahrzeuge verbeitet. AHS hat ein großes Ziel: Bei AHS Kategorie „a“ geht es darum, dass die Fahrzeuge vollkommen automatisiert fahren. Dafür sind unter anderem Informationen über Hindernisse, Fahrbahnzustand, Wetter und Positionsdaten anderer Fahrzeuge notwendig. Erreicht werden kann dies natürlich nur mit einer Kombination aus V2V und V2I.

Europa

In Europa werden Projekte sowohl durch die Europäische Union als auch auf nationaler Ebene gefördert. Das gemeinnützige Car 2 Car Communication Consortium *[1]* (C2C CC) setzt sich das Ziel einen V2V Standard ins Leben zu rufen und zu etablieren, so dass in ganz Europa V2V Kommunikation garantiert werden kann. Selbst standardisiert das C2C CC jedoch nicht, dafür ist in Europa das European Telecommunications Standard Institue *[10]* (ETSI) zuständig. Beispielsweise wird dort die IEEE 802.11 Familie als RadioLAN (RLAN) bezeichnet und auf die Synonyme WiFi und WLAN hingewiesen. Das C2C CC will, dass ein gebührenfreies Frequenzband vergeben wird. Dieses Frequenzband soll exklusiv für V2V Anwendungen verwendet werden. Außerdem setzt sich das Konsortium für die Harmonisierung von internationalen V2V Standards, das heißt die unterschiedlichen Standards sollen sich möglichst aneinander annähern, so dass man theoretisch irgendwann überall auf der Welt mit seinem Auto V2V nutzen kann. Das Entwickeln realistischer Markteinführungsstrategien, so dass möglichst schnell ausreichend viele Autos über ein V2V System verfügen, ist ebenfalls von Interesse. Initiiert wurde das C2C CC durch Automobilhersteller, beteiligen können sich jedoch auch Zuliefererunternehmen und Forschungsinstitute.

In den USA ist für Vergabe von Frequenzbändern die Federal Communications Commission *[3]* (FCC) zuständig. In Europa macht dies die Europäische Kommission (EC) in Brüssel *[2]*: Derzeit sind in Europa ein 30 MHz Frequenzbereich im 5,9 GHz Frequenzband vergeben. In Zukunft sollen weitere 20 MHz für Verkehrsoptimierung vergeben werden.

Weil in Europa – im Gegensatz zu Japan – nicht überall Vehicle-to-Infrastructure (V2I) Systeme etabliert sind und ein kompletter Neuaufbau von Infrastruktur immens teuer wäre, geht die Forschung und Entwicklung in Richtung V2V. Die V2I Systeme die man bereits jetzt in Europa hat sind die Electronic Toll Collect *[12]* (ETC) Systeme, welche mit DSRC arbeiten. Dabei kommuniziert die On-Board-Unit (OBU) eines Fahrzeugs mit Kontrollbrücken (Infrastruktur) über Infrarot. Unter anderem werden dabei Kennzeichen, Achsenzahl und Schadstoffklasse des Fahrzeugs übermittelt.

Im folgenden Abschnitt wird genauer darauf eingegangen, wie das europäische V2V System des C2C CC technisch aufgebaut ist. Während der bedeutendste V2V Protokollstack der USA die Abkürzung WAVE trägt, wird der des C2C CC gleichnamig als C2C CC Protokollstack bezeichnet.

Das V2V System des C2C CC

Eine der Anforderungen an ein europäisches V2V System ist natürlich, dass es unter den gegebenen europäische Verkehrsverhältnissen stabil und zuverlässig operiert. In Europa bedeutet dies, dass es möglich sein muss, dass Daten unter der sehr hohen relativen Geschwindigkeit von 500 Km/h (2 * 250Km/h) ausgetauscht werden können. Außerdem soll es möglich sein, dass zwischen Sender und Empfänger bis zu 1000 Meter liegen. Das C2C CC „Radio-System“ basiert auf WAVE, also IEEE 802.11p.

Physical Layer (PHY) Architektur

Funkkanäle

Im Folgenden werden die Funkkanäle beschrieben, die ein V2V System nutzt. Nötig ist ein Network-Control-Channel (CCH), welcher zusätzlich für *kritische* Sicherheitsanwendungen verwendet wird. Außerdem existiert einen dedizierter Kanal für kritische Sicherheitsanwendungen, er wird für nichts anderes verwendet. Ein Kanal für *unkritische* Sicherheitsanwendungen und Verkehrsoptimierung, sowie einen Kanal für non-safety Anwendungen wie Infotainment sind ebenfalls vorhanden. Non-saftey Anwendungen dürfen nur ihren dedizierten Kanal verwenden. Die in der WLAN Protokollfamilie definierten öffentlichen Kanäle müssen nicht zwingend implementiert werden. Nutzbar wären diese beispielsweise für Car-to-Hotspot Kommunikation oder Infotainment Anwendungen. Außerdem kann ein V2V System zusätzliche Funktechniken nutzen. Optionale Funktechniken wären zum Beispiel GSM, GPRS, UMTS etc.

Frequenzband

Das Car2Car Communication Consortium hat beim European Telecommunications Standard Institue (ETSI) ein insgesamt 70 MHz breites Frequenzband beantragt. Dies entspricht dem WAVE Frequenzband. Wie zuvor bereits erwähnt sind derzeit aber nur 30 MHz reserviert, mit Aussicht auf weitere 20 MHz. Die Kanäle sind folgendermaßen unterteilt:

- 5,855-5,865 GHz Non-Safety Anwendungen
- 5,865-5,875 GHz Non-Safety Anwendungen
- 5,875-5,885 GHz Unkritische Sicherheitsanwendungen und Verkehrsoptimierung
- 5,885-5,895 GHz Network Control und kritische Sicherheitsanwendungen
- 5,895-5,905 GHz Kritische Sicherheitsanwendungen
- 5,905-5,915 GHz Unkritische Sicherheitsanwendungen und Verkehrsoptimierung
- 5,915-5,925 GHz Unkritische Sicherheitsanwendungen und Verkehrsoptimierung

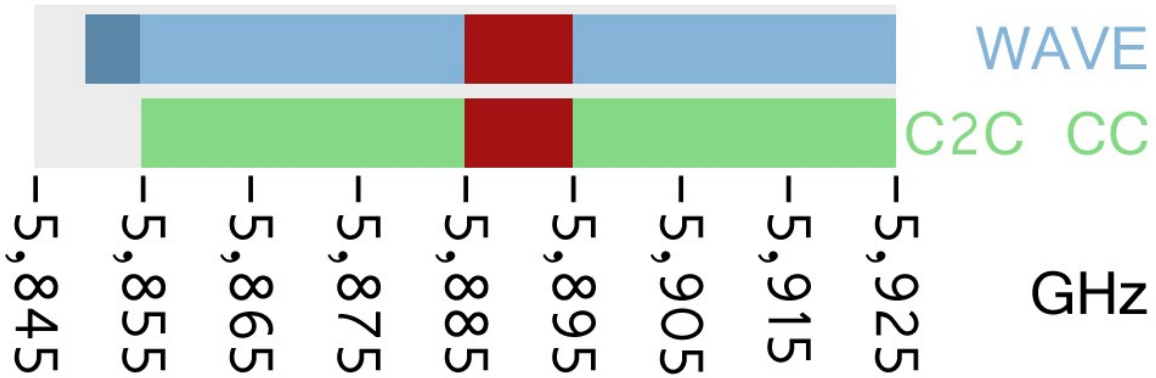


Abbildung 2: Frequenzbereich von WAVE und C2C CC Radio System

Anzumerken sei, dass der Network Control Channel (rote Markierung) beim C2C CC Radio-System und WAVE gleich liegen. Dunkelblau markiert ist der ungenutzte aber reservierte Frequenzbereich von WAVE.

Sendeleistung

Um 500 bis maximal 1000 Meter Distanz bei freiem Sichtfeld zwischen Sender und Empfänger zu ermöglichen, wird mit 33 dBm (Dezibel Milliwatt *[14]*) gesendet. „dBm (...) ist die Einheit des Leistungspegels L_P, der das Verhältnis einer Leistung P im Vergleich zur Bezugsleistung von 1mW (Milliwatt) beschreibt.“ (Quelle: Wikipedia).

$$L_P(\mathrm{dBm}) = 10 \log_{10} \left(\frac{P}{1\,\mathrm{mW}} \right)$$

Abbildung 3: Dezibel Milliwatt dBm
(Quelle: Wikipedia)

Wenn die Leistung in Watt gesucht ist, gilt folgende Formel (der mathematisch sensible Leser erkennt, dass die Klammern den Exponent darstellen):

$$P(\mathrm{mW}) = 10^{\left(\frac{L_P(\mathrm{dBm})}{10}\right)} \cdot 1\,\mathrm{mW}$$

Abbildung 4: Umwandlung dBm zu W
(Quelle: Wikipedia)

Damit lässt sich eine Leistung von 1,995 Watt errechnen. Um andere Funkdienste nicht zu stören verfügt der WLAN Standard über eine dynamische Anpassung von Sendeleistung – die Transmit Power Control *[15]* (TPC). TPC soll im C2C CC Radio-System eine minimale Sendeleistung von 3dBm ermöglichen. Die folgende Abbildung zeigt den amerikanischen WAVE Standard und seine Kanäle. Es werden unterschiedliche Signalleistungen für unterschiedliche Channels bzw. deren Anwendung verwendet:

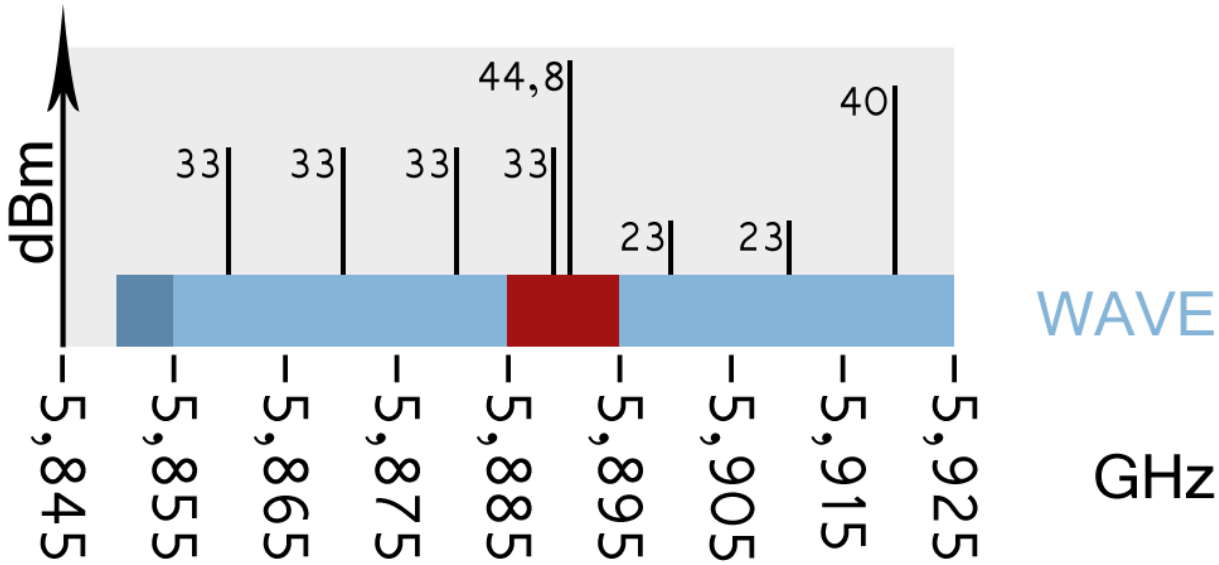


Abbildung 5: Signalstärke der WAVE Channels in Dezibel Milliwatt

Bei WAVE sind für zwei Channels die höchsten Signalstärken zugelassen *[16]*. Der rot markierte Network Control Channel (CCH) wird von 33 bis zu 44,8 dBa betrieben. Der Channel mit der höchsten Frequenz (rechts) ist ein Safety Channel. Er dient beispielsweise Fahrzeugen die sich einer Kreuzung nähern und wird mit maximal 40 dBa betrieben. Die zwei Channels mit 23 dBa werden für Nahkommunikation verwendet. Kommunikation mit einem Maut-Beacon wäre dafür ein Verwendungszweck.

Es existiert eine Abstufung von möglichen Datenraten. Die Datenraten 3 / 4,5 / 6 / 9 / 12 / 18 / 24 / 27 Mbit/s *sollen* möglich sein, wobei 6 Mbit/s der Standard ist. Ein Algorithmus für den Wechsel zwischen Datenraten wurde jedoch noch nicht diskutiert und beschlossen.

Antennendesign

Bezüglich der Antenne lässt sich anmerken, dass Praxistests durchgeführt wurden und sich ein „zirkuläres Abstrahlen“ als am performantesten erwiesen hat. Die Antenne sollte dabei in jedem Fahrzeugtyp individuell platziert werden. Der Fahrer- oder Kofferraum erwiesen sich als ungeeignet. Wie zu erwarten erwies sich der Dachbereich als am geeignetsten. Ebenso wie der Algorithmus zum Datenratenwechsel ist das Antennendesign vom C2C CC noch nicht genauer spezifiziert. Einig ist man sich beim Übertragungsmodus. Halbduplex, also entweder Senden oder Empfangen, und Broadcasts werden für derzeit vorstellbare Anwendungen als geeignet angesehen. Orthogonal Frequency Division Multiplex *[23]* (OFDM) soll unterstützt werden. Dies dient der Reduzierung von Übersprechern bei Trägersignalen. Auf dieses Thema der Signaltechnik wird hier jedoch nicht näher eingegangen. Jedenfalls wird OFDM beispielsweise auch bei Bluetooth 3.0, DVB-T und ADSL verwendet.

MAC/LLC Layer Architektur

IEEE 1609.4

Auf den zuvor beschriebenen Physical Layer IEEE 802.11p setzt der MAC/LLC Layer auf. Standardisiert ist er durch den IEEE 1609.4 Standard aus der IEEE 1609 Familie. Dieser trägt den Namen „Multi Channel Operations“. Das heißt das C2C CC Radio System arbeitet mit mehreren

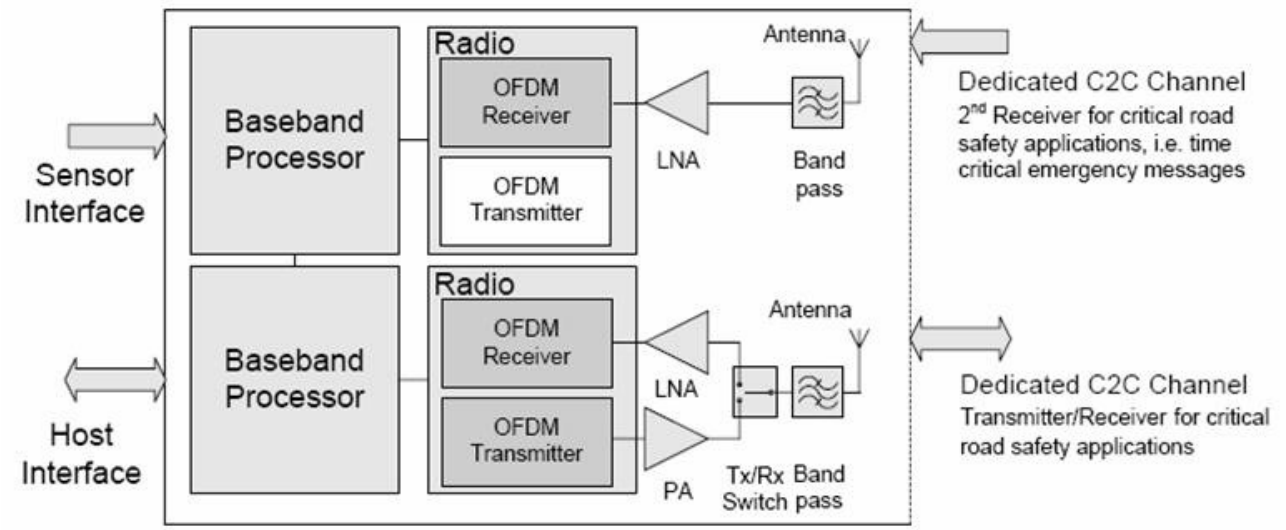
Channels. Als MAC Algorithmus (Media Access Control) wird das gängige Verfahren Carrier Sense Multiple Access with Collision Avoicance (CSMA/CA) verwendet. Die MAC wird benötigt, weil mehrere Geräte sich das gleiche Kommunikationsmedium bzw. Kanäle teilen und es bei konkurrierender Verwendung des physikalischen Mediums zu Datenverlusten kommen würde. Es ist möglich MAC Frames auf Channels zu routen (Channel Routing), je nachdem welchen Servicetyp sie haben. Außerdem kann zwischen unwichtigen und wichtigen Nachrichten unterschieden werden, dies wird als User Priority bezeichnet. Ebenfalls ist es möglich und nötig, dass Channels koordiniert werden (Channel Coordination), weil sie von mehreren Anwendungen bzw. Devices genutzt werden. Alle C2C CC Radio-Systeme werden nach der Coordinated Universal Time (UTC) synchronisiert, damit sie wissen in welchen Zeitabschnitten auf dem Control Channel gelauscht werden soll und kritische Nachrichten eintreffen können.

MAC Layer Extensions

Der C2C CC MAC Layer unterstützt nicht die folgenden (für V2V unnötigen) IEEE 802.11 Standards: Power Management, Roaming (Access Point Scanning), (De-)Authentifizierung. Andererseits bietet der Layer nachfolgende Erweiterungen: Die höheren Layer werden über die Auslastung der Kanäle informiert, so dass sie je nach Last anders reagieren können. Der Logical Link Control Layer *[18]* soll dem Network Layer die Möglichkeit bieten den Nachrichtenpaketen Parameter mitzugeben bezüglich der zu verwendenden Signalstärke. Zwischen MAC Layer und höheren Layern soll es eine Server/Client Struktur geben, so dass Channels abgehört und Kontrollbefehle ausgeführt werden können. Die letzte Erweiterung ist eine Message-Queue, direkt im MAC Layer. Diese soll nach Nachrichtenpriorität abgearbeitet werden, gemäß IEEE 802.11e.

Das Dual-Receiver Konzept

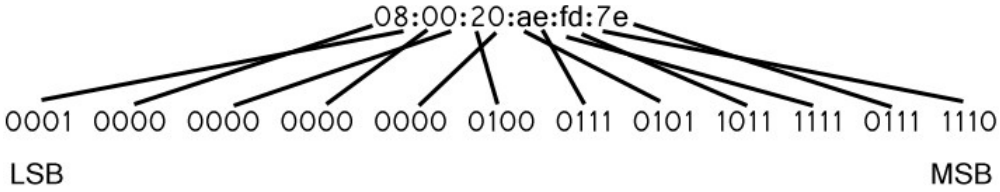
Simuliert wurde der Einsatz von Dual-Receivern, über die das Radio-System Nachrichten auf zwei Kanälen *gleichzeitig* empfangen kann. Die Nachrichten könnten auch von zwei verschiedenen Sendern stammen. Ein Einsatz wäre, dass ein Reciever nur für den Control Channel verwendet wird. So ist zeitgleich ohne Unterbrechuzng das Senden und Empfangen von Safety Nachrichten auf anderen Channels möglich. Insgesamt würden somit die Frequenzbänder effektiver genutzt werden. Dies ist jedoch nur ein Konzept und muss getestet werden. Logischerweise wäre ein Dual-Receiver teurer als ein normaler Receiver. Die folgende vom C2C erstellte Abbildung macht das Dual-Reciever Konzept anschaulich:



Zu sehen ist eine dedizierte Antenne für den Empfang von kritischen Nachrichten. Der dazugehörige OFDM Transmitter bleibt ungenutzt, weil über diese Antenne nicht gesendet wird. Die zweite Antenne verfügt über einen Transmit/Receive Switch und wird wie gewöhnlich verwendet. Die Baseband Prozessoren führen Kommunikationsfunktionen aus.

MAC Adressen

Verwendet werden die IEEE 802.3 (Ethernet) MAC Adressen *[17]*. Diese sind 48 Bit groß und werden kanonisch dargestellt, das heißt das LSB eines Oktetts (Bytes) steht links. In den ersten vier Bytes wird der Hersteller des Gerätes codiert. Somit bleiben 2^{24} individuelle Adressen (16,8 Millionen) je Hersteller. Sinnvollerweise notiert man die Oktetts in Hexadezimal. In der Darstellung können verschiedene Trennzeichen verwendet werden. Ein Beispiel für eine MAC Adresse:



Ein C2C CC Radio-System sollte 64 Bit Adressen unterstützen (64 Bit MAC Adressen werden auf IPv6 *[19]* abgebildet). Zuvor wurde im Abschnitt Security kurz auf die Anonymität von Fahrzeugen eingegangen. Feste MAC Adressen kommen also nicht in Frage – Zufällig muss die Adresse von Zeit zu Zeit verändert werden. Dies bringt ein Problem mit sich, nämlich das Problem der nicht Einzigartigkeit von Adressen. *Statistisch* gesehen ist es jedoch unwahrscheinlich, dass die Adressen von Fahrzeugen in einem Raum kollidieren. Das C2C CC geht in ihrem Manifest nicht näher auf eine Problemlösung ein, außer dass der Adressraum groß genug sein muss. Es wird darauf hingeweisen, dass man das Bit, welches für lokal administrierte Adressen steht, setzen kann. Es handelt sich dabei um das zweite Bit des ersten Bytes, wobei das erste Bit das LSB ist. Folgende Abbildung soll dies illustrieren:

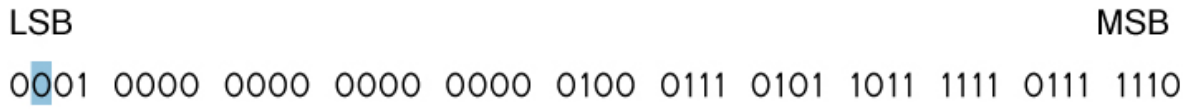


Abbildung 8: Flag für Scope einer MAC Adresse

Setzt man das Flag auf 0, so heißt dies die Adresse ist global gültig bzw. einzigartig (Universally Administered Address (UAA)). Setzt man das Flag auf 1, so heißt dies die Adresse wird lokal Administriert und ist somit auch nur im lokalen Scope gültig (Locally Administered Address (LAA)). Im Falle von MAC 48 Bit schlägt das C2C CC also lokale Administration vor. Bei MAC 64 Bit könne man sich aufgrund des großen Adressraums entscheiden, ob man das Flag als lokal oder universal administriert setzt. Der Logical Link Control Layer soll dann einen uniformen Einstiegspunkt (Service Access Point (SAP)) für den Network Layer anbieten und sowohl IP-basierte als auch Peer-to-Peer Kommunikation von spezifischen C2C Nachrichten trennen.

Auf der Ebene der IPv6 Adressen kann man dem Problem der Mehrdeutigkeit von Adressen mittels V2I entgegentreten. Es ist denkbar, dass über die Infrastruktur, welche mit einem Backbone verbunden ist, IPv6 Adressen dynamisch aber eindeutig vergeben werden.

Nachrichten

Bezüglich der maximalen Größe, Priorität und Wartezeit nach erfolgreichen Übertragungen werden

keine konkreten Aussagen getroffen. Jedoch ist natürlich das Ziel die Kanäle nicht zu überlasten, um bei hochpriore Nachrichten eine geringe Latenz zu gewährleisten. Demnach benötigt man für die dedizierten Channels auf jeden Fall ein Prioritäten-System für Nachrichten. Der IEEE 802.11e Standard soll dabei als Basis dienen.

Network/Transport Layer

Auf dem MAC/LLC Layer setzt das so genannte Communication-System auf. Dieses umfasst den Network- und den Transport Layer. Das Communication-System ermöglicht den eigentlichen Datentransfer (Pakete, Segmentierung), bietet also dem Application Layer seine Transport-Dienste an. Außerden koordiniert dieser Layer das verteilte Netzwerk und sorgt dafür, dass Nachrichten ankommen. Das Communication-System beachtet die Anforderungen der verschiedenen Anwendungen. Eine Safety Anwendung muss beispielsweise zuverlässig und ohne Latenz in eine geographische Zone senden. Dafür sind Broadcasts notwendig. Eine Internetkommunikation hingegen wird an eine konkrete Adresse senden (Unicast) und stellt deutlich niedrigere Anforderungen an Latenz und Zuverlässigkeit. Wie bereits erwähnt wurde, ist ein V2V Netzwerk extrem dynamisch und die Topologie ändert sich ständig. Dies führt zu Paketverlusten und generellen Kommunikations-Overhead. Die Transport Layer Protokolle sind vom C2C CC noch in der Diskussion, es soll entschiedenen werden, ob und welcher vorhandener Standard modifiziert wird oder ob ein neuer Standard nötig ist. Mehr dazu kann im Abschnitt „Transport Layer“ in Erfahrung gebracht werden.

Sparse/Dense Network Situation

Ein Problem ist die unterschiedliche Verkehrsdichte. Deswegen wird zwischen zwei Situationen unterschieden: „Sparse-“ und „Dense Network Situation“, also karger und dichter Netzwerksituation. In Dense Network Situations wird der Nachrichtenaustausch so geregelt, dass keine Überlastung der Übertragungskanäle eintritt. Im Gegensatz dazu spielt die Belastung der Kanäle in Sparse Network Situations keine Rolle. Im Dichten Verkehr ist Caching und Repeats von Nachrichten realtiv unnötig, vielmehr sind effiziente Forwarding-Algortihmen notwendig, um die Kanäle zu entlasten. Bei karger Verkehrsichte hingegen ist es notwendig, dass Nachrichten wiederholt gesendet werden (Flooding) und zu diesem Zweck auch gecached werden. In diesem Fall sind ganz andere Forwarding-Algortihmen von Bedeutung. Wenn ein Fahrzeug beispielsweise hinter sich keinen Kommunikationspartner hat, weil diese zu weit entfernt sind, so kann es einem entgegen kommenden Fahrzeug eine Nachricht mitgeben. Dieses Fahrzeug cached die Nachricht und informiert wiederum entgegenkommende Fahrzeuge.

Packet/Information Centric Forwarding

Das C2C CC hat zwei semantisch unterschiedliche Lösungsansätze für Forwarding innerhalb eines V2V Netzwerks. Das paketzentrierte und das informationszentrierte Weiterleiten. Die Namensgebung ist etwas unaussagekräftig. Beim Packet Centric Forwarding geht es darum, dass ein Sender Pakete an konkret adressierte Empfänger in einer geographischen Zone schickt und der Forwarding-Algortihmus des Transport Layers dafür sorgt, dass Sprünge über Zwischeneinheiten genommen werden, um die Ziele zu erreichen. Dies entspricht dem Switching, wie man es aus konventionellen Netzwerken kennt. Das Information Centric Forwarding verfolgt einen anderen Ansatz. Hierbei ist nicht der Transport Layer für das Forwarding zuständig. Eine Anwendung sendet eine Information über einen Broadcast an Empfänger in einem Gebiet. Jeder Empfänger muss dann für sich entscheiden, wie er mit der Nachricht weiter verfährt – ob er die Nachricht modifiziert und wieder broadcastet. Das impliziert, dass auf dem Empfänger eine Anwendung installiert sein muss, die mit den Informationen auch etwas anfangen kann. Die Verarbeitung erfolgt also auf dem

Application Layer. In einem C2C CC Communication-System sind beide Ansätze implementiert und eine Anwendung kann sich für ein Verfahren oder eine Mischung aus beidem entscheiden. Beispielsweise würden kritische Safety Nachrichten per Packet Centric Forwarding gesendet werden. Empfänger könnten dann entscheiden wie und ob sie über die Zonengrenzen hinaus repeaten. Tankstellen würden Werbenachrichten über einen non-safety Channel im Information Centric Forwarding Modus senden, natürlich intervallweise mit niedriger Dringlichkeit und Dienstgüte (Best Effort *[20]*).

TCP/IP Protocol Suite

Anwendungen können die Standard TCP/IP Protocol Suite verwenden. Verwendet werden dabei IPv6 Pakete, diese werden in C2C CC Netzwerkpakete gekapselt und nach der Übertragung wieder aufgelöst. In diesem Fall wird das konventionelle Packet Centric Forwarding genutzt. PCF und TCP/IP haben die gemeinsame End-to-End Semantik. Eine Alternative ist die direkte Nutzung des IEEE 802.11a/b/g Netzwerkinterfaces.

Forwarding Algorithmen

Geographische Adressen

Adressen wurden im Abschnitt „MAC Adressen“ bereits behandelt. Zu jeder MAC Adresse gehört eine C2C Communication-System Adresse und folglich auch eine IP Adressierung im höheren Layer. Diese Adressen identifizieren einen Node. Unter geographischen Adressen versteht man die Zuordnung einer solchen Node-Adresse zu Positionsdaten. Weil sich die Nodes bewegen ist eine solche Adresse somit eigentlich nur zu einem konkreten Zeitpunkt gültig. Um zu wissen, wie alt die Adresse ist, wird diese mit einem Timestamp versehen. Das heißt, man weiss, dass zu einem Zeitpunkt ein Gebiet über einen Node kontaktierbar war oder ist. Verwendet werden diese Adressen um Nachrichten in ein Gebiet zu forwarden. Dabei wird eine Node Adresse als Adresse für ein geographisches Gebiet gesehen – einer GeoAdresse. Ein solches Gebiet hat eine gewisse Fläche, beispielsweise in Form eines Kreises mit 300 Meter Radius. Ist eine GeoAdresse bekannt, kann in dieses Gebiet ein Geographical Broadcast (GeoCast) gesendet werden, nämlich indem das Fahrzeug mit dieser Adresse als Broadcaster verwendet wird. Ebenso ist es mittels Geographical Anycast (GeoAnycast) auch möglich an irgend ein Fahrzeug in dieses Gebiet zu senden. Aufgrund der Mobilität der Nodes (die sich um einen GeoAdressen-Node bewegen), weiss man nicht genau wie viele Fahrzeuge man mit einem GeoCast überhaupt erreicht. In den folgenden vier Abschnitten wird auf die Verwendung von geographishen Adressen in Forwarding-Verfahren eingegangen.

Geographical Unicast

Beim GeoUnicast sendet ein Fahrzeug (Source Node) direkt oder über weitere Nodes (Hops) eine Nachricht an genau einen Empfänger (Destination Node). Die folgende Abbildung soll den kürzesten Weg verdeutlichen. Auch der Gegenverkehr kann genutzt werden.

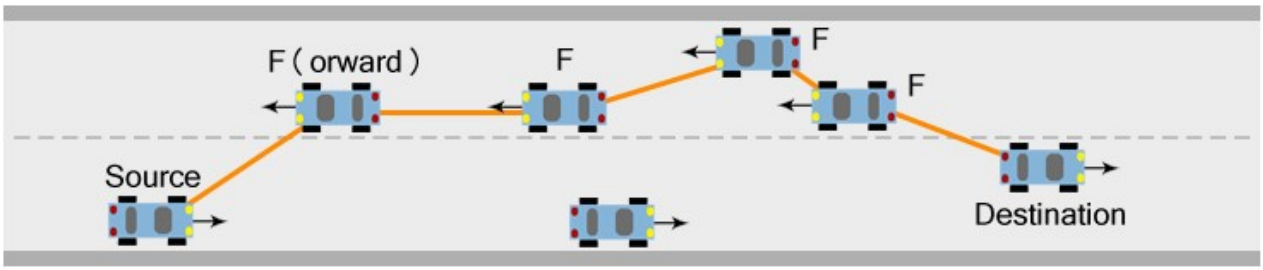
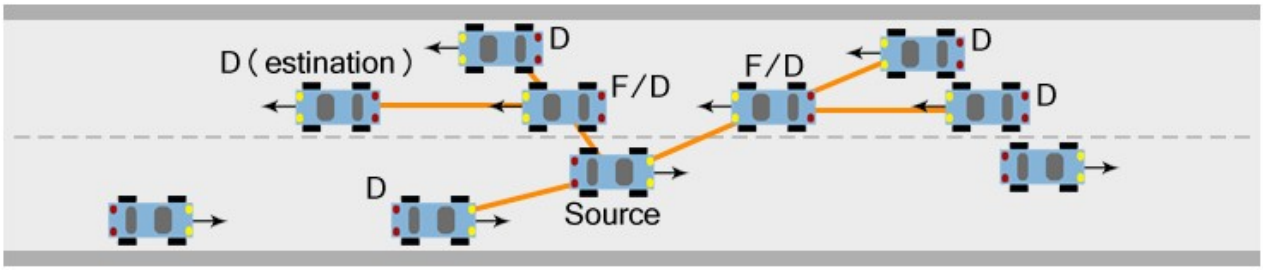


Abbildung 9: Geographical Unicast

Topologically Scoped Broadcast

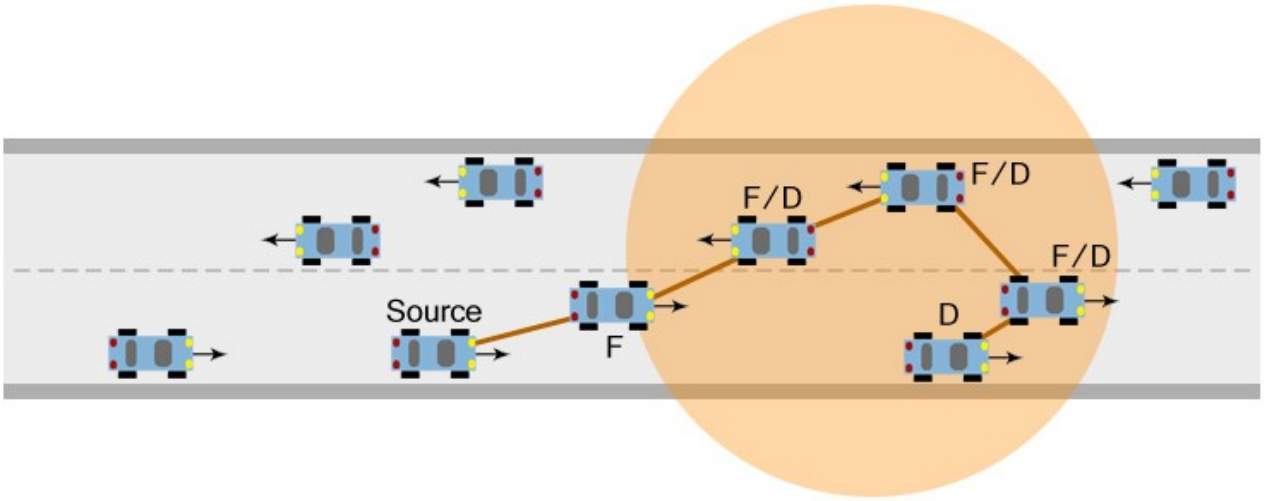
Ein Topologically Scoped Broadcast ist ein Broadcast, welcher auf eine bestimmte Anzahl Hops limitiert ist. Dazu muss jedem Forwarder bekannt sein, wie viele Hops bereits genommen wurden und wie groß das Scope ist, also wie viele Hops maximal gewünscht sind. Das folgende Beispiel zeigt einen Scoped Broadcast mit zwei Hops.



Jeder Forwarder (F) ist auch ein Destination Node. Das Fahrzeug links soll ausser Reichweite sein. Das Fahrzeug rechts liegt ausserhalb des Scopes, ist aber in Reichweite.

Geographical Scoped Broadcast

Beim Geographical Scoped Broadcast spielt die Anzahl der Hops keine Rolle. Es wird ein geographisches Gebiet mit einer geometrischen Form definiert. Jeder Node in dem Gebiet soll sich von dem Broadcast angesprochen fühlen. Die Abbildung zeigt einen Source Node, der jedoch nicht in dem Zielgebiet liegen muss, einen Forwarding Node außerhalb des Gebiets, und diverse Forwarding- und Destination Nodes im geographischen Zielgebiet.



Geographical Scoped Anycast

Diese Form des GeoCasts ist eine leicht abgewandelte Form des Geographical Scoped Braodcasts. Der Einzige Unterschied ist, dass innerhalb des Zielgebiets kein Forwarding stattfindet, sondern abgeschlossen ist, sobald irgend ein Node im Gebiet erreicht wurde.

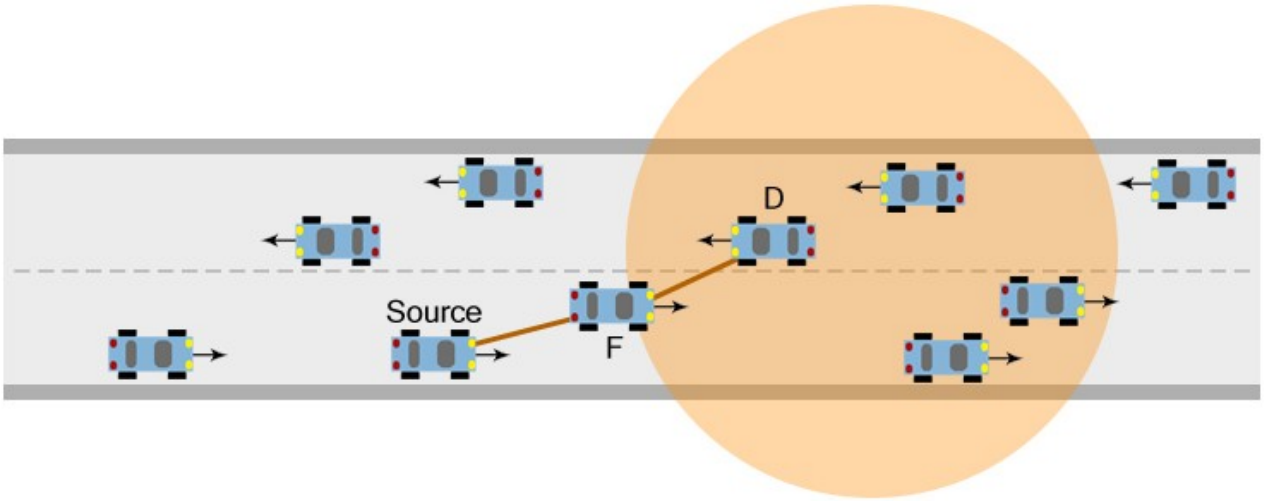


Abbildung 12: Geographical Scoped Anycast

Transport Layer

Der Transport Layer abstrahiert alle niedrigeren Layer aus sicht der Anwendungen. Er sorgt für den zuverlässigen Datentransfer (Flusskontrolle, Fehlerkontrolle) zwischen Anwendungen. Die Transparenz erkennt man deutlich, wenn man eine TCP oder UDP Anwendung schreibt: Man benötigt als Informationen nur IP-Adresse und Portnummer. Im Gegensatz zum Network Layer existieren für den Transport Layer noch keine V2V spezifischen Standards im Bezug auf Protokolle. Es wird diskutiert, ob und welches Protokoll modifiziert oder erweitert werden könnte, oder ob man ein neues Transport Protokoll entwickeln muss. Letzteres wäre außerordentlich aufwendig. Dies habe man bei der Entwicklung von TCP gesehen. Es sollte vermieden werden, dass das Protokoll bei neuen Anforderungen, die mit der Zeit auftreten können, ständig neu entwickelt werden muss. Wie zuvor erwähnt hängt das Design des Transport Layers von den Anforderungen der

Anwendungen und potentiellen zukünftigen Anwendungen ab. Auch dies ist an TCP und UDP verdeutlichbar – UDP legt im Gegensatz zu TCP keinen Wert auf Fehlerkontrolle (z.B. wenn Pakete verloren gehen), das müssten dann die Anwendungen implementieren. Die Anforderungen an das Transport Protokoll aus Sicht der Anwendungen werden im folgenden genauer betrachtet.

- **Types of Transport**

  Safety- und Non-Safety-Anwendungen benötigen die zwei Kommunikationsmechanismen Broadcast und Unicast. Eine Safety-Anwendung möchte beispielsweise einen GeoCast in ein entferntes Gebiet senden, dann werden die Daten per Unicast in das Zielgebiet geleitet und dort per Broadcast verteilt. Die Werbung einer Tankstelle sollte auch per Broadcast gesendet werden – Kartenmaterial-Updates für das Navigationsgerät hingegen per Unicast.

- **Error-free Transport**

  Trivial aber wichtig ist die Erkennung von korrupten Paketen, weil Anwendungen nichts mit zerstörten Daten anfangen können. Prüfbits und Summen sind gängige Praxis.

- **Reliability**

  Hier muss zwischen Broadcasts und Unicasts unterschieden werden. Safety-Anwendungen fordern, dass bei einem Broadcast möglichst viele gewünschte Nodes die Information erhalten. Bei einem Unicast sind gängige Mechanismen wie SYN ACK sinnvoll.

- **Multiplexing**

  Wenn mehr als eine Anwendung zwischen zwei Nodes oder mehr Nodes *gleichzeitig* kommuniziert ist Multiplexing notwendig. Auf die Form des Multiplexings wird nicht eingegangen. Vielleicht kann es Codemultiplexing wie bei UMTS sein.

- **Delay constraint and location validity**

  Aufgrund der Mobilität der Nodes und dem Bezug von Informationen auf spezielle geographische Zonen – also Raum und Zeit – werden spezielle Anforderungen an die Flusskontrolle gestellt. Es muss entschiedenen werden, ob Daten wiederholt oder überhaupt gesendet werden sollen und ob Caching sinnvoll ist.

- **Priority of data packets**

  Die Flusskontrolle ist ebenfalls von der Priorität der Pakete betroffen. Es macht keinen Sinn Non-Safety Nachrichten zu cachen wenn man Platz für Safety Nachrichten braucht. Ebenso sollten Safety Nachrichten als erste gesendet werden.

- **Forwarding**

  Wie im Abschnitt „Packet/Information Centric Forwarding“ beschrieben muss der Transport Layer Packet Centric Forwarding unterstützen, also Routen finden, um das Ziel einer Nachricht zu erreichen. Information Centric Forwarding ist nicht die Aufgabe dieses Protokolls, denn die

Anwendung des Empfänger Nodes muss selbst Daten verarbeiten und Entscheidungen treffen.

- **Data aggregation**

  Ein gängiges Verfahren ist das volle Ausnutzen von Paketgrößen. Statt mehrere Pakete mit geringem Dateninhalt und folglich massivem Overhead zu senden, werden mehrere Daten in ein Paket zusammengefasst und beim Empfänger wieder zerlegt. Die Daten können von verschiedenen Anwendungen stammen.

- **Application payload size**

  Ein weiteres gängiges Verfahren ist das Zerlegen von Daten und das Aufteilen in mehrere Pakete, wenn die Daten zu groß sind für nur ein Paket. Auch dies kennt man von TCP.

Protokolle

Network Layer Protocol

In den folgenden Abschnitten soll auf die grundlegenden technischen Komponenten des Network Layer Protokolls eingegangen werden. Dabei werden ihre Aufgaben und teilweise Arbeitsweisen erläutert.

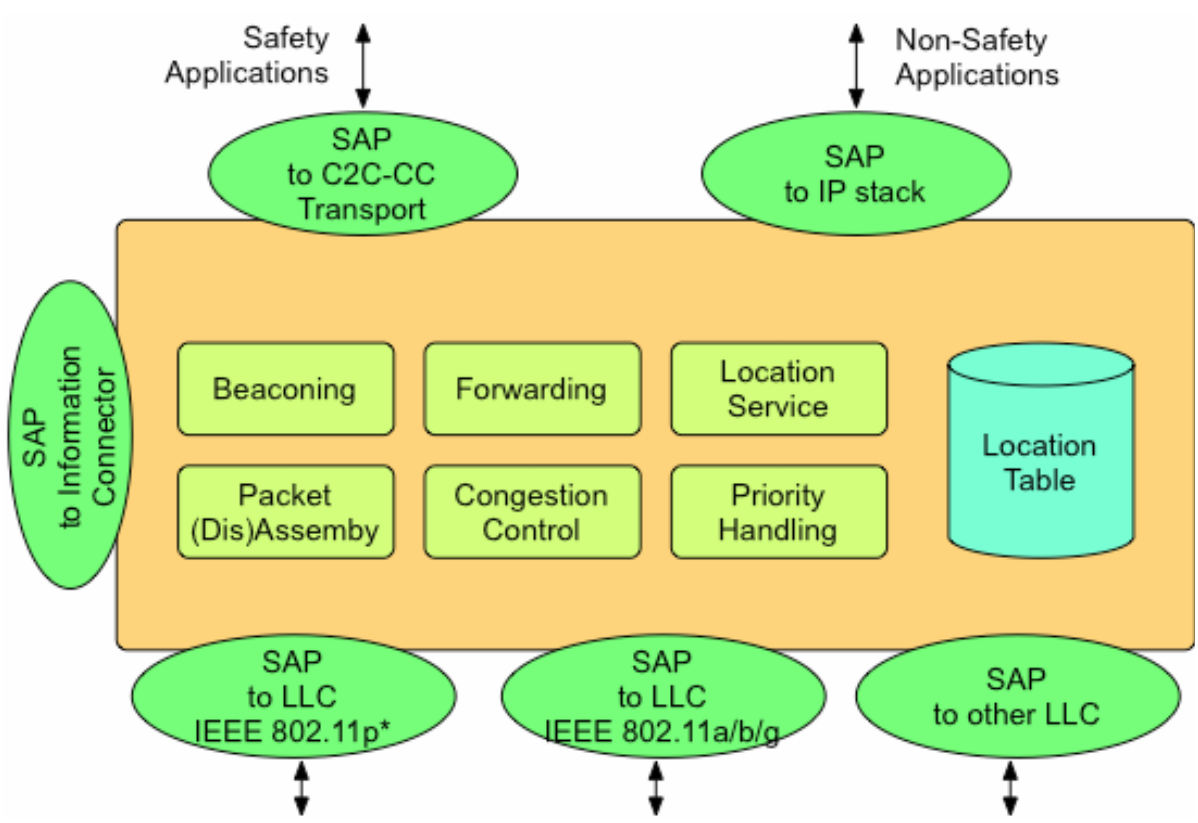


Abbildung 13: Das Network Layer Protocol und dessen Komponenten (Quelle: C2C CC)

- **Location Table**

  Damit Anwendungen und Netzwerk-Flusskontrolle sinnvolle Entscheidungen treffen können, benötigen sie umfangreiche Informationen über die Nodes im Umfeld. Die Location Table ist eine sozusagen flüchtige Datenbank. In ihr werden Positionsdaten und ein Timestamp von benachbarten (1 Hop entfernten) *oder* entfernten Nodes (> 1 Hops) gespeichert. Die Einträge müssen aktuell gehalten werden und deswegen werden Einträge mit einem gewissen Alter entfernt. Folgende Informationen werden in einem Eintrag gehalten:

C2C Netzwerk Adresse	*MAC Adresse*	*IPv6 Adresse*	*Geographische Position*	*Geschwindigkeit*	*Richtungs-vektor*	*Timestamp*	*...*
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**

  Zusätzlich wird festgehalten, um welche Art von Node es sich handelt. Dabei wird unterschieden zwischen mobilen Onboard Units (OBUs) und Roadside Units (RSUs). Außerdem wird unterschieden zwischen Safety und Non-Safety Nodes. Ein weiteres Flag wäre zum Beispiel, ob der Node Internetzugang anbietet. Anhand dieser Daten ist es auch möglich Aussagen über die Glaubwürdigkeit einer Information zu treffen. Beispielsweise kann ein sich schnell bewegender Node keine 180° Drehung machen. Für diese Überprüfungen ist Caching von vorherigen Einträgen notwendig.

- **Packet assembly/disassembly**

  Das Network Layer Protocol ist für das Verarbeiten, Modifizieren und Erzeugen von Headerinformationen von empfangenen und zu sendenden Paketen zuständig. Eine Modifikation beziehungsweise Update ist zum Beispiel notwendig, wenn ein Paket weitergeleitet wird. Wenn das Paket ankommt haben sich sowohl die eigenen Positionsdaten usw. geändert, als auch die des nächsten Hops. Dafür muss auch die Location Table abgefragt werden. Beispielsweise muss auch der Time-to-Live Wert (TTL) entsprechend der aktuellen Zeit reduziert werden.

- **Beaconing**

  Nodes fragen idR. andere Nodes nicht explizit ab, wer sie sind und wo sie sind. Nodes verkünden ihre Anwesenheit durch sogenannte Beacons. Beacons sind periodisch gesendete Broadcast Pakete mit Informationen wie geographischer Position, Geschwindigkeit, Bewegungsvektor, Timestamp und Identitätsinformationen. Die Periodendauer des Beaconing ist von der Kanalauslastung abhängig.

- **Forwarding**

  Wie im Kapitel „Forwarding Algorithmen“ behandelt, muss das Network Layer Protocol unterschiedliche Forwarding Algorthmen unterstützen. Ziel ist es, Pakete direkt an Nodes oder gar eine Gruppe von Nodes in einem bestimmten geographischen Gebiet weiterzuleiten. Für die Unicasts soll als Algorithmus Greedy Forwarding *[24]* mit der Regel „Maximum Progress Within Radius“ (MFR) verwendet werden. Beim Greedy Forwarding wird versucht eine Nachricht mit jedem Hop näher an das Zielgebiet zu bringen. Als Hop wird also einer der Nodes gewählt der die Minimaldistanz zum Ziel hat. Minimaldistanz wird dabei unterschiedlich definiert. Beim MFR muss man sich eine Gerade zwischen Source (oder Forwarder) und

Destination vorstellen. Jeder Node zwischen Source und Destination hat einen Lot durch seine Koordinaten auf diese Gerade. Der Node, bei dem der Lot auf die Gerade am nächsten zum Ziel ist, wird nächster Hop.

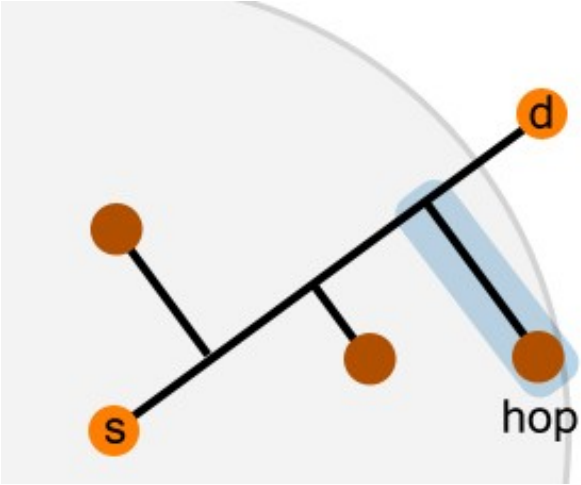


Abbildung 14: Greedy Forwarding mit Maximum Progress Within Radius (MFR)

Für Forwarding in einem geographischen Scope wird der Algorithmus „Simple flooding with duplication detection“ verwendet, also einfaches Flooden mit Erkennung von Duplikaten.

- **Location Service**

  Wenn die Location Table leer oder ungültig ist, aber ein Node zum Forwarding gesucht wird, dann ist es auch möglich Nodes bzw. Gebiete nach ihren Nodes mit Positionsdaten zu befragen. Im Gegensatz zu den Beacon Nachrichten ist dies ein On-Demand Verfahren zum Aufbauen von Routen und wird auch von dem Routing Protocol verwendet.

- **Priority Handling**

  Auf Paketebene wird anhand der Priorität (priority value) entschieden, wie mit einem Paket verfahren wird. Wichtige Pakete werden natürlich zu erst verschickt, während weniger wichtige Pakete in einer Queue angehängt werden können. Dies ist insbesondere dann wichtig wenn die Kanäle ausgelastet sind und Safety Nachrichten ausgetauscht werden müssen.

- **Congestion Control**

  Wenn Kanäle ausgelastet sind und die Datentransferrate sinkt, dann ist es notwendig den Datentransfer zu steuern. Die Datentransferrate, die Anwendungen bereit gestellt wird, muss reguliert werden. Im Extremfall müssen unwichtige Pakete weggeworfen werden. Für die Regulierung erhält das Protokoll Informationen über die Kanalauslastung aus den tieferen Layern.

Transport Layer Protocol

Wie bereits im Kapitel „Transport Layer“ beschrieben ist sich das C2C CC unsicher, welche Protokolle im Transport Layer Verwendung finden sollen. Für Non-Safety Anwendungen ist das

verbindungsorientierte TCP grundsätzlich denkbar, aber innerhalb von Ad Hoc Netzwerken unpraktisch. TCP müsste zumindest erweitert werden oder ein TCP-ähnliches Protokoll neu entwickelt werden. Bezüglich Safety Anwendungen ist man der Auffassung, dass UDP mit seinen Broadcast und Unicast Mechanismen ohne Verbindungsaufbau ein geeignetes Protokoll ist. Es ist zwar nicht garantiert, dass Pakete ankommen, aber es existiert eine Checksumme über den Paketheader. Trotzdem muss natürlich garantiert werden, dass Safety Nachrichten ankommen. UDP müsste auch insofern erweitert werden, dass die Checksumme aktualisiert wird, nachdem ein Hop den Header und Payload modifiziert hat. Dies wäre der Fall beim Information Centric Forwarding, wenn Anwendungen entscheiden wie sie die Daten forwarden und diese manipulieren (können). UDP unterstützt ebenfalls keine Congestion Control, im Gegensatz zu TCP *[26]*. Diesbezüglich existiert jedoch ein neues Protokoll, welches derzeit vom IETF *[25]* (Internet Engineering Task Force) standardisiert wird. Datagram Congestion Control Protocol (DCCP) basiert auf TCP, die Zuverlässigkeitsfunktionen wurden jedoch entfernt. Man dachte TCP würde dadurch leichtgewichtiger werden, jedoch hatte das Entfernen der Zuverlässigkeitsfunktionen einschneidende Auswirkungen auf sehr viele Aspekte von TCP und folglich musste sehr viel neu designed werden. DCCP wurde nicht für V2V entwickelt, man analysiert es jedoch und sucht Lösungen, wie man Congestion Control in unzuverlässige Protokolle wie UDP integrieren kann.

Application Layer

Der Application Layer bietet den Anwendungen die Möglichkeit des Senden und Empfangens von Nachrichten. Außerdem werden Datenbankservices angeboten, die von Anwendungen genutzt werden können. Um den Anwendungen weitere Informationen zur Verfügung zu stellen, können diese über einen gewöhnlichen CAN-Bus *[22]* (Controller Area Network Bus) mit der Sensorik im Fahrzeug interagieren. Beispielsweise können Regen-, Helligkeits- und Temperatur-Sensoren oder ABS/ESP und Abstandsradar das Informationsspektrum des Systems erweitern. Ebenfalls können Anwendungen über ein Human-Machine-Interface mit dem Fahrer und den Mitfahrern interagieren. Ein C2C System bringt Standard-Anwendungen mit sich, das System kann aber auch um Anwendungen erweitert werden.

Anwendungen

Cooperative Awareness

Bei der Cooperative Awareness (CA) ist der Grundgedanke Informationen zwischen den Fahrzeugen zu teilen. Aus der Perspektive eines Nodes sollen bis zu einem Radius von einem Kilometer Informationen gesammelt und verbreitet werden. Dabei wird „Local Vehicle Data“ gesendet und beim Empfänger als „Remote Vehicle Data“ verarbeitet. Ein Anwendungsfall wäre das Erkennen von potentiellen Vorwärtskollisionen. Der Empfänger vergleicht die Remote Vehicle Data und die eigenen Fahrzeuginformationen und versucht festzustellen ob eine Kollision droht. Im Falle einer solchen „Cooperative Forward Collision Warning“ wird der Fahrer gewarnt. In Videos von japanischen Entwicklern wird dies beispielsweise demonstriert. Der Fahrer wird über sein Navigationsgerät-Display und per Voice Ansage gewarnt. Die CA kann auch Hilfe leisten beim Einreihen oder Spurwechsel auf der Autobahn. Fahrer können darauf hingewiesen werden, dass sie entgegenkommende Fahrzeuge blenden können oder gar als Geisterfahrer unterwegs sind. Auf dem Plan steht auch die Abstandswarnung (Adaptive Cruise Control (ACC)).

Unicast Exchange

Die direkte V2V Unicast Kommunikation ist in vier grobe Schritte unterteilbar. Die Reihenfolge der

Schritte lautet: Discovery, Connection, Maintenance, Closure. Diese Schritte sind fast vergleichbar mit einer gewöhnlichen TCP Netzwerkkommunikation. Wenn ein Node beschließt, mit einem anderen Node kommunizieren zu müssen, dann sucht er sich einen Node. Dabei kann sich der Node auf die Informationen beziehen, die ihm vom Transport Layer angeboten werden. Dies ist die Discovery Phase. Wenn ein Node gefunden wurde, dann fragt der Node an, ob der Gegenüber eine Verbindung akzeptiert. Lehnt der Gegenüber nicht ab, so wird eine feste Verbindung initiiert (Connection Phase). Dann erfolgt der Datenaustausch (Maintenance). Wenn einer der Kommunikationspartner beschließt, dass er die Kommunikation beenden möchte, so ist er dafür jederzeit in der Lage (Closure). Ein Unicast Exchange ist bis zu einer Distanz von fünf Kilometern denkbar. Ein Anwendugsfall ist das „Pre-Crash Sensing/Warning“. Wenn festgestellt wird, dass ein Unfall nicht mehr vermeidbar ist, werden zum Beispiel Daten wie Fahrzeuggewicht und Stoßstangenhöhe ausgetauscht, um die Fahrzeuge auf den Crash vorzubereiten.

Decentralized Environmental Notification

Bei dezentralen Nachrichten die für ein Gebiet und in einem gewissen *längeren* Zeitraum gültig sind wird auch Infrastruktur in die Kommunikation einbezogen. Die Infrastruktur wird als stehende Fahrzeuge interpretiert. Wenn beispielsweise ein Unfall stattgefunden hat, dann ist es zwar wichtig, dass die Fahrzeuge unmittelbar gewarnt werden, aber die Information ist auch wichtig für Fahrzeuge, die sich erst zu einem späteren Zeitpunkt nähern. Dann kann die Infrastruktur diese Fahrzeuge warnen, auch wenn außer den Unfallwagen keine anderen Fahrzeuge für ein Ad Hoc Netzwerk zur Verfügung stehen. Die Semantik ist also gegenüber dem Unicast Exchange und CA eine andere. Eine populäre Anwendung wäre eine frühzeitige Stauwarnung. Vorgesehen ist eine Reichweite von bis zu 20 Kilometer.

Infrastructure to Vehicle (one-way)

Beim I2V geht es konkret um Nachrichten, die von der Infrastruktur an Fahrzeuge gebroadcastet werden. Eine Interaktion der Parteien ist nicht vorgesehen. Denkbar sind periodische Broadcasts von Tempolimits in dem aktuellen Fahrbahnabschnitt. Eine dynamisch berechnete Geschwindigkeitsempfehlung, um Staus zu vermeiden, ist ebenso vorstellbar. Hinsichtlich Traffic Efficiency sind sogar Hinweise bezüglich der „Grünen Welle“ geplant.

Local Road Side Unit Connection

Bei der Kommunikation zwischen OnBoard Units und Road Side Units handelt es sich wieder um eine verbindungsorientierte Kommunikation. Die RSU bietet Services an und OBUs können diese Services nach einer „Service Discovery“ nutzen, bzw. eine Connection herstellen. Eine RSU kann dabei sehr umfangreich ausgestattet sein. Versehen mit einem großen nicht flüchtigen Speicher kann die RSU sogar Multimediadaten zu beispielsweise Sehenswürdigkeiten anbieten. Kartenmaterial Updates oder das Wissen wo die nächste Tankstelle ist, wären auch möglich. Man könnte auch gewisse Probleme am Fahrzeug per Remote diagnostizieren lassen.

IP Road Side Unit Connection

Hierbei geht es um eine spezielle Form der Local Road Side Unit Connection. Während diese nur eine lokale Verbindung zur RSU erlauben und nicht direkt in das Internet (auch wenn die RSU selbst das Internet nutzen kann), wird bei einer IP Road Side Unit Connection von der RSU eine valide IP Adresse bezogen. Somit ist über einen verschlüsselten Kommunikationsweg (z.B. HTTPS) voller Internetzugriff möglich. Ein Anwendungsfall wäre beispielsweise das Beziehen von Verkehrsinformationen auf der geplanten Route.

Information Connector (IC)

Der Zweck des Information Connectors ist die effiziente Vermittlung von uninterpretierter RAW Data zwischen den Layern des C2C CC Kommunikationssystems. Für die Interpretation der rohen Daten ist dann der jeweilige Layer zuständig. Als Kommunikationsmodell zwischen den Layern ist ein Publisher-Subscriber Modell (Observer Pattern) vorgesehen. Protokolle können sich also als Subscriber für ein „Topic“ beim Information Connector anmelden. Ebenso melden sich untere Layer als Publisher für ein Topic an. Der Information Connector sorgt dann für die Distribution der Daten. Auf den genauen Mechanismus geht das C2C CC nicht detailiert ein.

Security

Das V2V Netzwerk muss sicher gegenüber technischen Angriffen wie manipulierte Nachrichten und Denial of Service (DoS) sein. Manipulierte Nachrichten können zu Verkehrstoten führen. Weiterhin muss die Anonymität des Fahrzeugs bzw. Fahrers gewährleistet werden. Die MAC Adressen Problematik wurde bereits erläutert. Nicht zwingend im Widerspruch dazu steht die Signierung der Nachrichten. Ein Node muss wissen, ob die Nachricht nicht bei einem Forwarding Node manipuliert wurde (Integrität). Ob die Nachricht von dem Node kommt, welcher er zu sein vorgibt (Authentizität) ist dabei *weniger* wichtig. Dabei spricht man von anonymer Signierung beziehungsweise dynamischen Zertifikaten. Bezüglich des Kryptoalgorithmus, der Keylänge und der Public Key Infrastruktur (PKI) ist jedoch noch Forschung notwendig und keine Entschlüsse getroffen. Das RSA und ECC *[21]* (Elliptic Curve Cryptosystems) Verfahren sind mögliche Kandidaten für asymmetrische Verschlüsselung. Dabei ist es wichtig, dass ein angemessenes Verhältnis zwischen Latenz und Sicherheit gefunden wird. Die Verschlüsselung nimmt je nach Algorithmus Zeit in Anspruch – kostbare Zeit in kritischen Situationen. Ein weiterer Angriffspunkt der Anonymität ist das Aufzeichnen eines „Driver Pattern“. Das Wiederfinden eines Fahrers anhand seiner Beschleunigungs- und Brems-Muster soll durch die dynamischen Adress- und Zertifikatwechsel unterbunden werden. Prinzipiell soll die Identifikation eines Fahrzeugs wenn möglich geheim gehalten werden. Ein Zeitpunkt, wann dies nicht möglich ist, ist wenn von einer Infrastruktur ein neues Bündel Adressen bezogen wird. Denn dann ist ein Verbindungsaufbau und Authentifizierung notwendig.

Zusammenfassung und Kommentar

V2V ist etwas, was ich mit Spannung erwarte! Anwendungsbeispiele der V2V Technologie haben das große Potential gezeigt. Viele Aspekte machen das Fahren sicherer und komfortabler. Eine notwendige breite Marktpenetration wird V2V in jede Klasse Fahrzeug bringen, nicht nur in die Oberklasse. Das Thema V2V erfordert umfangreiches Backgroundwissen aus den Disziplinen Signaltechnik, Netzwerktechnik, verteilter Systeme und theoretischer Informatik. Ganz zu schweigen von der letztendlich Elektro-/Digital-/Softwaretechnischen Implementierung. Meiner Meinung nach ist es gerechtfertigt, V2V als eigenes Forschungsgebiet zu bezeichnen. Diese Ausarbeitung kratzt nur an der Oberfläche, erläutert Begriffe und Pläne der Konsortien und Industrie. Präzise technische Umsetzungen werden selten genau definiert und auch das C2C-CC Manifesto ist letztendlich oberflächlich.

Ich danke für Ihr Interesse an diesem Dokument.

Quellen und Referenzen

Primärquellen

- Car 2 Car Communication Consortium Manifesto - Overview of the C2C-CC System
  http://www.car-to-car.org/fileadmin/downloads/C2C-CC_manifesto_v1.1.pdf
- V2X Kommunikation (Robert K. Schmidt, Tim Leinmüller and Bert Böddeker DENSO AUTOMOTIVE Deutschland GmbH, Eching)
  http://www.tu-ilmenau.de/fakia/fileadmin/template/startIA/telematik/Mitarbeiter/schmidt/slb08v2x.pdf

Sekundärquellen

- *[1]* Car 2 Car Communication Consortium
  http://www.car-to-car.org/
- *[2]* EU vergibt Frequenzen
  http://www.heise.de/newsticker/EU-vergibt-Frequenzen-fuer-Car-to-Car-Communication--/meldung/113900
- *[3]* Federal Communications Commission FCC
  http://de.wikipedia.org/wiki/Federal_Communications_Commission
- *[4]* U.S. Department of Transportation DOT
  http://www.dot.gov/
- *[5]* IEEE 802.11p
  http://de.wikipedia.org/wiki/IEEE_802.11p
- *[6]* IEEE Timeline für 802.11
  http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
- *[7]* Vehicle Information and Communication System VICS
  http://www.vics.or.jp/english/index.html
- *[8]* Driving Safety Support System DSSS (mit sehr schöner Flash-Animation)
  http://www.utms.or.jp/english/system/dsss.html
- *[9]* WAVE (ab Seite 27)
  http://www.internet-sicherheit.de/fileadmin/docs/publikationen/seminararbeit-2008-Die-Zukunft-auf-Schicht-1-2-2008.pdf
- *[10]* ETSI „RadioLAN“
  http://www.etsi.org/WebSite/technologies/RadioLAN.aspx
- *[11]* Dedicated Short Range Communication DSRC
  http://de.wikipedia.org/wiki/Dedicated_Short_Range_Communication
- *[12]* Deutsches Toll-Collect und DSRC
  http://www.allbusiness.com/electronics/commercial-industrial-electronics-radio/4986679-1.html

- *[13]* Frequenzband (sehr schöne Übersicht)
  http://de.wikipedia.org/wiki/Frequenzband
- *[14]* Leistungspegel (dBm)
  http://de.wikipedia.org/wiki/Leistungspegel#dBm
- *[15]* Transmit Power Control (TPC)
  http://netzikon.net/lexikon/t/tpc-wlan.html
- *[16]* WAVE Kanäle und Leistungspegel (Seite 23)
  http://www.ict-aragorn.eu/docs/Aragorn_D21_State_Of_the_Art_Report_v1_00.pdf
- *[17]* Media Access Control MAC
  http://de.wikipedia.org/wiki/Media_Access_Control
- *[18]* Logical Link Control LLC (IEEE 802.2)
  http://en.wikipedia.org/wiki/IEEE_802.2
- *[19]* IPv6
  http://de.wikipedia.org/wiki/IPv6
- *[20]* Best Effort
  http://de.wikipedia.org/wiki/Best_Effort
- *[21]* Elliptic Curve Cryptography ECC
  http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography
- *[22]* Controller Area Network CAN Bus
  http://de.wikipedia.org/wiki/CAN_Bus
- *[23]* Orthogonal Frequency Division Multiplex OFDM
  http://de.wikipedia.org/wiki/OFDM
- *[24]* Geographic Routing
  http://en.wikipedia.org/wiki/Geographic_routing
- *[25]* Internet Engineering Task Force
  http://www.ietf.org/
- *[26]* TCP Congestion Control
  http://en.wikipedia.org/wiki/Transmission_Control_Protocol#Congestion_control

Sonstige Quellen

- NISSANs Safety Shield (ein interessantes Video über die konkrete Anwendung von V2V)
  http://nissannews.com/show-video-gallery.do;jsessionid=1575E9B080C951F7806796CB6BC1922C?key=&cID=11&method=view
- Industrial Scientific And Medical Band ISM
  http://de.wikipedia.org/wiki/ISM-Band

- V2V (arg spärlich)

  http://en.wikipedia.org/wiki/Vehicle-to-vehicle

- IEEE Approves WAVE Communication Standard (IEEE 1609.1-4) (über die Zulassung der ersten zwei von vier Standards)

  http://auto.ihs.com/news/2006/ieee-wave-communication.htm