Car-to-Car Communication – Technologische Herausforderungen

Andreas Lübke, Volkswagen AG, Wolfsburg, Deutschland

Kurzfassung

Zurzeit beschäftigen sich die Automobilhersteller weltweit mit der drahtlosen Kommunikation zwischen Fahrzeugen sowie zwischen Fahrzeugen und der Infrastruktur. Die möglichen Anwendungen reichen von reiner Unterhaltung über verbesserte Navigation und Fahrerassistenz bis hin zu selbstorganisierendem Verkehr.
Dieser Artikel beschreibt die technischen Herausforderungen sowie mögliche Lösungsansätze. Nach einem kurzen Überblick werden zunächst die Anforderungen an die OSI-Schichten 1-3 betrachtet. Anschließend werden zwei übergreifende Probleme behandelt: Die Security und die gemeinsame Nutzung des Funksystems für sicherheitsrelevante Funktionen und konventionelle Internetanwendungen. Den Abschluss bilden Überlegungen bezüglich des Zugriffs auf die Fahrzeugnetze. Mit der Car-to-Car Communication treffen zwei Welten aufeinander: Zum einen die Fahrzeugwelt mit dem CAN-Bus als typischen Vertreter für Fahrzeugnetze und OSEK als Betriebssystem, zum andern die IT-Welt mit Technologien wie Wireless LAN und Linux.

1. Einführung

Mit der rasanten Verbreitung von Funksystemen auf Basis des Standards IEEE 802.11, auch Wireless LAN genannt, im Heim- und Office-Bereich wird auch der Einsatz dieser Technologie im Kraftfahrzeug interessant.

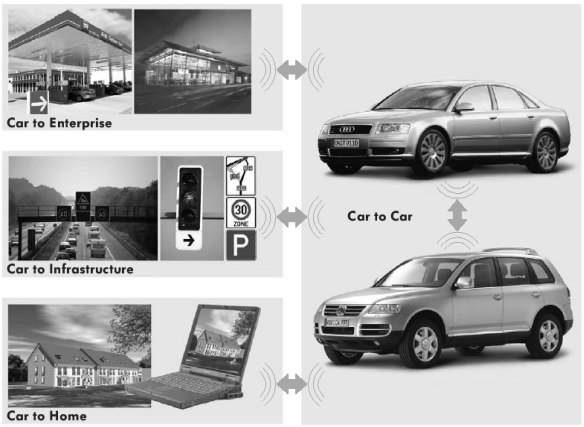

Bild 1: Einsatzfelder für Car-to-Car Communication

Dabei wird zwischen der direkten Kommunikation von Fahrzeugen untereinander (der Car-to-Car Communication) und der Kommunikation von Fahrzeugen mit fest installierten Netzknoten (der Car-to-Infrastructure Communication) unterschieden (siehe Bild 1). Für beide Bereiche sind sowohl sicherheitsrelevante Anwendungen als auch Unterhaltung und Information mögliche Einsatzfelder:

- Car-to-Car Personal Communication: Unterhaltung und Entertainment, z. B. Telefonieren, Kurzmitteilungen und Chat.
- Car-to-Car Traffic Safety Communication: Warnungen, Notruf, Staumeldungen, Kolonnenfahrten etc..
- Car-to-Infrastructure Personal Communication: Datendownload von Hotspots, Bezahlen in Parkhäusern, Location Based Services usw..
- Car-to-Infrastructure Traffic Safety Communication: Z. B. die Kommunikation mit Ampeln, Verkehrsschildern oder Schranken, der Download von aktuellen Verkehrsinformationen oder die Fahrzeugdiagnose.

Um die oben aufgeführten Funktionen dem Fahrzeugnutzer zugänglich zu machen, haben sich die Firmen Audi, BMW, DaimlerChrysler und Volkswagen im Jahr 2002 zu einem Car-to-Car-Communication-Consortium (C2CCC) zusammengeschlossen. Ziel ist die Schaffung von Standards für die Car-to-Car- bzw. Car-to-Infrastructure Communication. In Anlehnung an die Aktivitäten der Automobilhersteller in den USA im Vehicle Safety Communications Project (VSC) soll Wireless LAN die technologische Basis der Car-to-Car Communication werden.
Allen Beteiligten ist klar, dass der existierende Standard nicht den Anforderungen des automobilen Umfelds genügt. Es ergeben sich eine Reihe von Herausforderungen, die sich grob in drei Kategorien unterteilen lassen:

- Schaffung eines robusten Funksystems für das automobile Umfeld
- Gewährleistung der Security: Empfangene Daten sind entweder korrekt oder werden als falsch erkannt
- Einführung in den Massenmarkt und Bereitstellung von interessanten Diensten

Der letzte Punkt klingt auf den ersten Blick nicht wie eine technische Herausforderung. Ein Ziel der Auto-

mobilindustrie ist es aber, für alle oben genannten Einsatzgebiete ein einziges Funksystem zu benutzen. Diese Integration ist wegen der unterschiedlichen Anforderungen an Performance, Verfügbarkeit, Vertraulichkeit eine technische Herausforderung!
Weitere Probleme liegen in der Entwicklung neuer Funktionen und zugehöriger Algorithmen. Beispielhaft sei hier der selbstorganisierende Verkehr genannt. Die Problematik wird in diesem Artikel aber nicht näher betrachtet. In den folgenden Kapiteln 2 bis 4 wird auf die drei in der Liste genannten Herausforderungen genauer eingegangen. Kapitel 5 beschreibt anschließend den Zugriff auf die Fahrzeugdaten. In Kapitel 6 wird ein kurzes Fazit gegeben.

2. Robustes Funksystem

Voraussetzung für alle Arten von Car-to-Car Anwendungen ist ein robustes Funksystem. Auch reine Unterhaltungsanwendungen werden vom Anwender nicht akzeptiert, wenn sie nicht zuverlässig funktionieren.
Bei der Entwicklung des Funksystems unterscheiden sich der Physical Layer und der MAC / LLC Layer von den aus den Heim- und Office-Bereich bekannten Standards. An den Network Layer stellt die Car-to-Car Communication sogar völlig neue Anforderungen.
Ein entscheidender Unterschied zu bereits existierenden Telematik-Lösungen ist auch der Wunsch, dass die Kommunikation als solches kostenlos sein soll.

2.1 Anforderungen an den Physical Layer

Für den Physical Layer ist bisher eine Entscheidung getroffen worden. Die Car-to-Car Communication soll in einem Frequenzband im Bereich 5Ghz erfolgen. Alles andere ist zur Zeit noch offen. Gegenüber dem Einsatz von Wireless LAN im Heim- und Office-Bereich ergeben sich aber einige zusätzliche Herausforderungen:

- Die Reichweite soll bis ca. 1000 m betragen. Dieses gilt für die Kommunikation nach vorne und hinten, zur Seite werden wenige 100 m als ausreichend angesehen. Dieses kann z. B. durch eine geeignete Antennencharakteristik erreicht werden.
- Die Fahrzeuge bewegen sich mit bis zu 250 km/h. Bei diesen hohen Relativgeschwindigkeiten spielt der Dopplereffekt eine Rolle. Allerdings können schon heutige Wireless LAN Karten gewisse Frequenzunterschiede ausgleichen, so dass dieses Problem gelöst werden kann.
- Die Zahl der Netzknoten schwankt stark. Nachts auf Landstraßen befinden sich im Normalfall nur wenige Fahrzeuge im Bereich der jeweiligen Funkreichweite, in Innenstädten oder auf Autobahnen (insbesondere Stausituation) können es aber sehr viele sein. Wenn in letzteren Fällen alle Fahrzeuge mit maximaler Leistung senden, so steigt die Kollisionswahrscheinlichkeit auf den Kanälen. Um ein skalierbares System zu entwikkeln müssen folglich Algorithmen für ein adaptives Kommunikationsverhalten spezifiziert werden, die situationsabhängig eine Anpassung der Sendeleistung vornehmen.
- Das Umfeld der Fahrzeuge kann aufgrund ihrer Bewegung sehr dynamisch sein. Diese Dynamik führt zu Abschattungen (Shadowing) sowie Mehrwegeausbreitung (Multipath Propagation) des Funksignals. Da Fahrzeuge außerdem Geschwindigkeiten von bis zu 250 km/h erreichen können, spielt bei den sich dadurch ergebenden Relativgeschwindigkeiten der Dopplereffekt eine Rolle. Es gilt zu untersuchen, inwiefern die existierende Wireless LAN Technologie diese Anforderungen zu erfüllen vermag.

2.2 Anforderungen an MAC und LLC

Die wichtigste Anforderung an den Medienzugriff ist, dass sicherheitsrelevante Anwendungen Vorrang vor Informations- und Unterhaltungsapplikationen haben. Die zugehörigen Daten müssen mit möglichst geringer Verzögerung gesendet werden. Zudem muss gewährleistet sein, dass die Car-to-Car Communication nicht durch normale Wireless LAN Netze oder andere Teilnehmer gestört wird. Dieses soll zum einen durch ein exklusives Frequenzband für die Car-to-Car Communication und zum anderen durch eine Priorisierung wichtiger Daten gemäß 802.11e (MAC Enhancements for Quality of Service) erreicht werden.
Vermutlich werden nur die sicherheitsrelevanten Anwendungen das exklusive Frequenzband nutzen, alle anderen können die normalen Wireless LAN Frequenzen verwenden. Dadurch kann die Breite des Frequenzbandes gering gehalten werden.
Erste Versuche mit Wireless LAN in Fahrzeugen haben gezeigt, dass die Verbindung zwischen zwei Fahrzeugen gelegentlich für eine kurze Zeit, z. B. durch Abschattungen, unterbrochen ist, anschließend aber weiter bestehen soll. Ein Neuaufbau würde unnötig Zeit beanspruchen. Es müssen daher geeignete Methoden spezifiziert werden, wie mit kurzen Unterbrechungen umgegangen werden soll.
Offen ist auch die Behandlung von Übertragungsfehlern. Selbstverständlich müssen Übertragungsfehler erkannt werden, aber zusätzlich muss das Verhalten bei Übertragungsfehlern (Fehlermeldung, automatische Wiederholung usw.) festgelegt werden. Dabei ist zu berücksichtigen, dass viele Nachrichten nicht an ein einziges bekanntes Ziel gesendet werden, sondern dass alle Fahrzeuge in einem bestimmten Gebiet

adressiert sind. Es müssen insbesondere bei Broadcast-Nachrichten Wege für eine Übertragungsbestätigung gefunden werden

2.3 Anforderungen an den Network Layer

Die Adressierung im Internet und in lokalen Netzen erfolgt in der Regel über IP-Adressen. In den Routern sind Tabellen abgelegt, die Informationen darüber enthalten, welche Pakete mit welcher Zieladresse wohin weitergeleitet werden müssen. Natürlich sind diese Tabellen nicht statisch, sondern können dynamisch korrigiert und erweitert werden. Der Normalfall ist aber, dass sich die Routingtabelle nicht ändert. In den hochdynamischen Car-to-Car Netzen ändert sich die Topologie aber ständig. Außerdem würde eine IP-Adresse im Fahrzeug keinerlei Aufschluss geben, welcher Weg der günstigste ist. Für viele Anwendungen ist zudem kein konkretes Fahrzeug das Ziel der Nachrichten, sondern die Position des Fahrzeuges ist das Empfangskriterium. Ein Beispiel hierfür ist die Staumeldung an alle Fahrzeuge bis 10 km hinter dem Stauende. Im Fleetnet-Projekt wurde daher ein Routingverfahren spezifiziert, welches auf der geographischen Position des Fahrzeugs beruht.
Aber selbst wenn sich das Routing im Prinzip an der geographischen Position orientiert, gibt es noch eine Anzahl von möglichen Routing- bzw. Forwardingstrategien:

- Daten werden immer zu dem Fahrzeug gesendet, welches dem Ziel am nächsten ist.
- Kartenbasiert: Im Prinzip wie oben, nur dass nicht die Luftlinie sondern die Straßenkarte als Grundlage genommen wird.
- Wenn sich bestimmte Wege als geeignet herausgestellt haben, so werden sie markiert und entsprechend häufiger genutzt als weniger geeignete Wege (Ameisenalgorithmen und Methoden der Schwarmintelligenz).
- Cluster: Mehrere Fahrzeuge bilden einen Cluster. Die Daten werden dann jeweils von Cluster zu Cluster weitergeleitet.

Welches Routingverfahren für die Car-to-Car Communication das beste ist, ist offen. Evtl. müssen auch je nach Anwendung oder Verkehrssituation unterschiedliche Verfahren genutzt werden.

3. Security

Mit der Car-to-Car Communication sollen auch sicherheitsrelevante Anwendungen aus dem Bereich der Fahrerassistenz ermöglicht werden. Dafür gibt es eine zwingende Voraussetzung: Die empfangenen Daten sind sowohl in ihrer Syntax als auch in ihrer Semantik entweder korrekt oder werden als falsch erkannt! Damit der Empfänger den Daten vertrauen kann müssen geeignete Maßnahmen getroffen werden. Dabei gilt es, drei Probleme zu lösen:

- Car-to-Car Communication baut auf einem hochdynamischen AdHoc-Netz auf. Es gibt unbekannte Teilnehmer und es steht wenig Zeit für die Kommunikation zur Verfügung.
- Die Funktechnologie setzt auf einem Standard aus dem Heim- und Office-Bereich auf. Entsprechend ist es für Hacker reizvoll, die Kommunikation zu stören und die Systeme zu manipulieren.
- Die Fahrzeuge als Kommunikationsteilnehmer kommen von verschiedenen Herstellern und gehören unterschiedlichen Fahrzeuggenerationen an. Es sollen aber alle Fahrzeuge sicher miteinander kommunizieren können.

Die Aufgabe besteht nun darin, mögliche Angriffe auf die Car-to-Car Communication aufzuzeigen und geeignete Maßnahmen zu spezifizieren, die diese Angriffe verhindern. Neben der Herausforderung überhaupt geeignete Lösungen zu finden, sind im Bereich der IT-Security auch die Themen Datenschutz und Vertraulichkeit zu berücksichtigen. Kann ein Fahrzeug bzw. Fahrer für falsche Daten, die gesendet wurden und die zu einem Unfall geführt habe, verantwortlich gemacht werden?
Ein Grundsatz der IT-Security gilt auch für die Car-to-Car Communication: Ein System, welches nicht aktualisiert werden kann, ist nicht sicher. Wie diese Aktualisierung technisch und logistisch erfolgen kann, ist zur Zeit noch unklar.
Neben der IT-Security muss auch die Safety gewährleistet sein. Ein komplexes System wie es für Car-to-Car Communication und sicherheitsrelevante Anwendungen benötigt wird, kann selbstverständlich auch Fehler enthalten und (in Teilen) ausfallen. Eine umfassende Sicherheitsanalyse mit geeigneten Methoden wie z. B. einer Fehlermöglichkeiten- und Einfluss-Analyse (FMEA) und einer Fehlerbaumanalyse (FTA) ist daher erforderlich.

4. Integration der Funkhardware

Absolut sicher ist es nicht, aber vermutlich wird es aus betriebswirtschaftlicher Sicht nur eine einzige Funkhardware für alle Arten von Anwendungen im Fahrzeug geben. Der Download von Audio- oder Videodateien vom heimischen PC macht auch für den einzelnen Käufer von Wireless LAN im Fahrzeug Sinn. Die meisten Car-to-Car Anwendungen benötigen

aber eine hohe Dichte an entsprechend ausgestatteten Fahrzeugen.
Sicherheitsrelevante Car-to-Car Anwendungen und normale Internetdienste stellen unterschiedliche Anforderungen. Für letztgenannte Anwendungen existieren mit IEEE 802.11a/b/g, IP, TCP und UDP sowie verschiedenen Anwendungsprotokollen (http, ftp usw.) eine Reihe von Standards. Diese werden durch die Automobilindustrie auch nicht geändert werden (können). Die Standards für die neuen und sicherheitsrelevanten Funktionen werden zur Zeit von der Automobilindustrie entwickelt.
Für die einzelnen Schichten gibt es in fast allen Fällen Lösungsideen, wie unterschiedliche Protokolle zusammengefasst werden können. Für die Car-to-Car Communication sind besonders die Schichten 1 bis 3 und die Schicht 7 relevant. Wichtig ist dabei, dass die einzelnen Schichten in ihrem Zusammenspiel betrachtet werden und ein durchgängiges Konzept erarbeitet wird: Es nützt nichts, wenn zwar ständig verschiedenen Frequenzen gescannt werden, aber die Unterhaltungsanwendung nicht unterbrochen werden kann.
Zurzeit wird das spezielle Problem der Integration von IEEE 802.11 a/b/g mit der Dedicated Short Range Communication (DSRC) betrachtet, es soll aber ein allgemeiner Ansatz entstehen, der dem Fahrzeughersteller bei der Entscheidung „Integration der Funksysteme: Ja oder nein?“ hilft.
Welche aktuellen Lösungsideen gibt es zur Zeit schon? Diese werden im Folgenden für die Schichten 1, 2, 3 und 7 kurz angerissen:

Schicht 1

Es wird vermutlich derselbe Frequenzbereich benutzt, so dass die sicherheitsrelevanten Anteile in den normalen Ablauf eingebaut werden können.

Schicht 2

Für die sicherheitsrelevanten Anwendungen werden garantierte Zugriffszeiten benötigt. Eine Lösungsidee ist IEEE 802.11e. Neue Dienste können die neuen Funktionen nutzen, alte Dienste können aber unverändert übernommen werden. Ein ähnliches Problem gab es bei der Entwicklung des Flexray-Protokolls, dort konnte es mit nur geringfügig erhöhten Hardwarekosten gelöst werden.

Schicht 3

IP-Routing und das wie auch immer realisierte Routing zwischen den Fahrzeugen haben unterschiedliche Anforderungen. Ein Problem, welches gewisse Ähnlichkeiten aufweist, ist die Ortsvermittlungsstelle im öffentlichen Telefonnetz. Dort werden über DSL ankommende Daten als IP-Pakete geroutet und Wählverbindungen (analog oder über ISDN), die dieselbe Anschlussleitung nutzen, vermittelt.

Schicht 7

Die Möglichkeit, dass wichtige Anwendungen weniger wichtige unterbrechen und Zugriff auf CPU und Peripherie haben bieten mittlerweile alle Betriebssysteme. Die Schicht 7 sollte daher kein Problem darstellen.

Betrachtet werden muss natürlich immer das Gesamtsystem. In einem angenommen Fall „Schicht 1 und 2 haben keine Gemeinsamkeiten“ könnte die Entscheidung auch lauten: Zwei Protokolltreiber, aber nur ein Router. Auch hierfür gibt es Beispiele, nämlich normale PC mit Modem und Ethernet: Die physikalischen Schnittstellen sind auf den Schichten 1 und 2 völlig getrennt, darauf setzt aber ein TCP/IP-Protokollstack auf und die Schnittstellen werden von denselben Anwendungen (Browser, Mail usw.) auf die gleiche Art und Weise benutzt.

5. Zugriff auf die Fahrzeugnetze

Mit der Car-to-Car Communication treffen zwei Welten aufeinander: Zum einen die Fahrzeugwelt mit dem CAN-Bus als typischem Vertreter für Fahrzeugnetze und OSEK als Betriebssystem, zum andern die IT-Welt mit Technologien wie Wireless LAN und Linux.
In vorhergehenden Projekten wurden in der Volkswagen Forschung mit dem Low Level CAN Framework und der Vehicle API zwei Technologien spezifiziert und realisiert, die den Zugriff auf die Fahrzeugdaten und –funktionen stark vereinfachen.

5.1 Das Low Level CAN Framework

Das Low Level CAN Framework LLCF kann man auch als einen intelligenten CAN-Treiber bezeichnen, der fahrzeugspezifische Bus-Protokolle mit einer Standard IT-Schnittstelle (Sockets) nutzbar macht. Zurzeit existiert das LLCF in einer Realisierung für Linux und ist ein modularer Teil des Linux Kernels. Es liegt als neu entworfene Protokollfamilie PF_CAN analog zu z.B. dem Internetprotokoll PF_INET zwischen dem Network Layer und dem Socket Layer. Bild 2 zeigt schematisch den Aufbau des LLCF.
Das LLCF-Rahmenmodul besteht aus 2 Blöcken: Der RX Dispatcher sorgt dafür, dass von den CAN-Bussen empfangene Daten an die registrierten Protokoll-Module geschickt werden. Der Protocol Dispatcher sorgt dafür, dass die höheren Schichten bzw. der Benutzer des LLCF auf das entsprechende Protokoll in der Protokollfamilie PF_CAN zugreifen können.

Zurzeit stehen vier Protokolle in der Protokollfamilie PF_CAN zur Verfügung: CAN RAW erlaubt den direkten Zugriff auf die einzelnen Busse. Der CAN Broadcast Manager sorgt dafür, dass Daten regelmäßig gesendet bzw. dass (regelmäßig) empfangene Daten gefiltert an die höheren Schichten weitergegeben werden. Dabei können nicht nur ganze CAN-Botschaften, sondern einzelne Bits und Bytes mit komfortablen Filtern vorverarbeitet werden.

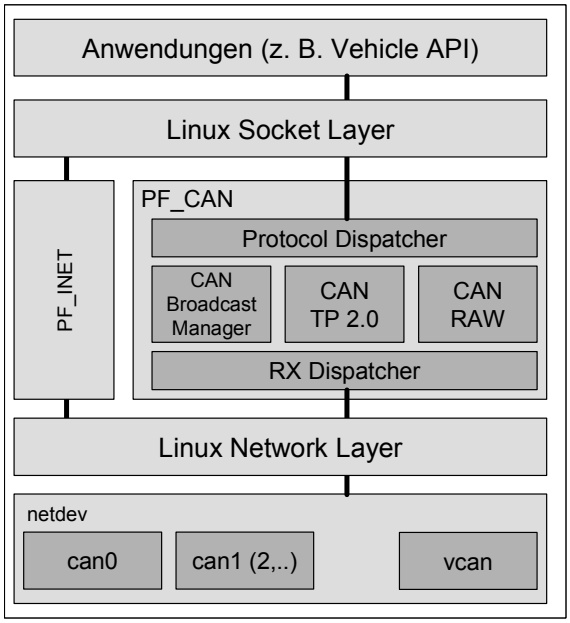

Bild 2: Das LLCF

Das LLCF-Rahmenmodul besteht aus 2 Blöcken: Der RX Dispatcher sorgt dafür, dass von den CAN-Bussen empfangene Daten an die registrierten Protokoll-Module geschickt werden. Der Protocol Dispatcher sorgt dafür, dass die höheren Schichten bzw. der Benutzer des LLCF auf das entsprechende Protokoll in der Protokollfamilie PF_CAN zugreifen können.

Zurzeit stehen vier Protokolle in der Protokollfamilie PF_CAN zur Verfügung: CAN RAW erlaubt den direkten Zugriff auf die einzelnen Busse. Der CAN Broadcast Manager sorgt dafür, dass Daten regelmäßig gesendet bzw. dass (regelmäßig) empfangene Daten gefiltert an die höheren Schichten weitergegeben werden. Dabei können nicht nur ganze CAN-Botschaften, sondern einzelne Bits und Bytes mit komfortablen Filtern vorverarbeitet werden.

Die Protokolle TP2.0 bzw. MCNet erlauben dem Anwender des LLCF einen Transportkanal gemäß den Spezifikationen von VW bzw. BOSCH auf dem CAN-Bus zu eröffnen. Durch die standardisierte Socket-Schnittstelle verläuft dabei die Kommunikation über den Transportkanal zum Motorsteuergerät analog zur Kommunikation mit einem WWW-Server im Internet. Das LLCF integriert die einzelnen CAN-Busse als normale Linux Netzwerkgeräte, wodurch es verschiedenen Anwendungen ermöglicht wird auf einen gemeinsamen Bus zugreifen zu können.

5.2 Die Vehicle API

Der Funktionsumfang in jedem Fahrzeug wird bestimmt durch seine individuelle Soft- und Hardwareausstattung. Neben CAN finden sich weitere Bussysteme wie LIN, MOST, Byteflight etc. Das Format von Botschaften und Protokollen ist herstellerspezifisch und wird ständig an die Bedürfnisse neuer Fahrzeugmodelle angepaßt. Dienste- und Anwendungsentwickler stehen damit vor dem Problem, ihre Software immer wieder an sich verändernde Fahrzeugarchitekturen anpassen zu müssen.

Die Vehicle API bietet Anwendungen und Diensten durch die Abstraktion von typ-, hersteller- und markenspezifischen Merkmalen eine standardisierte Schnittstelle für den Zugriff auf Daten der Fahrzeugbussysteme. Die Daten des Fahrzeugs werden hierbei in einem Objektmodell dargestellt. Die Datenobjekte beschreiben ihre Schnittstelle selbst. Die Menge der Datenobjekte und die Umsetzung von Daten in das Objektmodell ist frei konfigurierbar. Für die Kommunikation und die Darstellung der Daten werden offene Standards verwendet, wie sie auch schon erfolgreich bei Internet-Anwendungen zum Einsatz kommen.

Für den Zugriff auf CAN ist die Verwendung des LLCF realisiert, aber nicht Voraussetzung. Die Vehicle API kann nicht nur auf CAN-Daten zugreifen, auch der Zugriff auf GPS-Daten ist bereits umgesetzt. In unseren Prototypen ist GPS über eine serielle Schnittstelle angebunden. Eine Erweiterung der Vehicle API um LIN und Flexray ist vorgesehen.

Bild 3 zeigt den schematischen Aufbau der Vehicle API

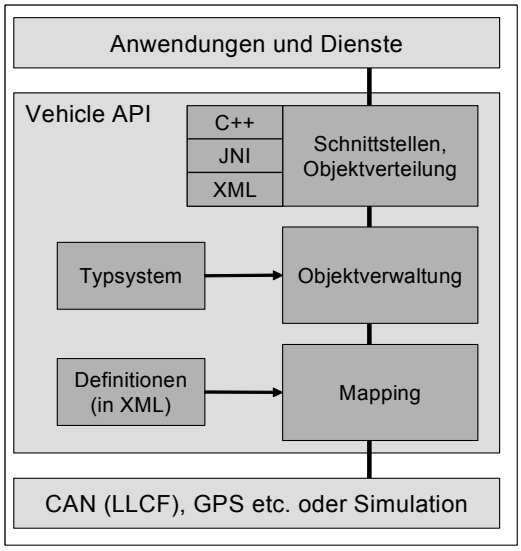

Bild 3: Die Vehicle API

6. Fazit

Die Herausforderungen der Car2Car-Communication lassen sich in technische und betriebswirtschaftliche Aspekte aufteilen. Durch die Verbreitung von Wireless LAN im öffentlichen und privaten Bereich werden die Fahrzeughersteller um die Einführung in das Automobil nicht herumkommen, so dass die technischen Probleme jetzt gelöst werden müssen.
Die Schaffung eines robusten Funksystems für alle sinnvollen Anwendungen im Fahrzeugumfeld ist machbar. Auch die Integration von sicherheitsrelevanten Anwendungen und normalen Internetanwendungen ist möglich, so dass nach Einführung von Wireless LAN im Fahrzeug auch neue Fahrzeug-Fahrzeug-Anwendungen realisiert werden können. Dieses könnte schon in der nächsten Fahrzeuggeneration der Fall sein.
Als größte Herausforderung stellt sich im Moment die Security dar. Hundertprozentige Sicherheit wird es nicht geben können, daher ist die Einführung von Funktionen wie „Selbstorganisierender Verkehr“ oder „Konvoi“ - wenn überhaupt - erst in einigen Jahren zu erwarten.

7. Literatur

[1] IEEE 802.11: „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications“, IEEE Standard, 1999

[2] Gläser, St.: „Entwicklung einer modularen Architektur für ein intelligentes Fahrzeuggateway“, AUTOREG 2004, 2.+3.3.2004, Wiesloch

[3] Franz, W.: „Geographical Addressing and Forwarding in FleetNet“, Whitepaper, 2002

[4] Vehicle Safety Communications Project: Task 3 Final Report “Identify Intelligent Vehicle Safety Applications Enabled by DSRC”, 2004

[5] Eberhardt, R.: „Car to Car Communication Consortium“, EuCar SGA, 23.10.2003