

Ausarbeitung für das Fach „Protokolle in öffentlichen und privaten Netzen“

---

## Car to Car Communication

---

*Autoren:*

Deniz Kadiogullati 3553892  
Christoph Drost 3576450

*Betreuer:*

Prof. Dr.-Ing. Horst Wieker



# Liste der noch zu erledigenden Punkte

■ Für das PSS die funktionalen Komponenten suchen . . . . .	10
■ Noch was zur ICS finden . . . . .	11
■ Noch was über IVS schreiben . . . . .	13
■ Nicht die blasseste Ahnung ob das mit den Access Networks stimmt . . . . .	16
■ Sollen wir hier noch was zum Thema Network Reference Point schreiben? Ich glaube aber, dass die noch in den Layern kommen . . . . .	17
■ komplette Section ITS Station Reference Architecture überarbeiten . . . . .	18
■ Noch etwas über die Channel herausfinden und schreiben . . . . .	18
■ ISO 21217 finden - Scheinbar infos über die Layer . . . . .	19
■ mal in ETSI TS 102 723-10 reinsehen, ob da was interessantes zu den SAP drin steht . . . . .	19
■ Kanalzugriff erklären, wenn ich weiß, was Kanäle sind. Quelle für TAC: [15] .	21
■ Einzelne Untereinheiten der Grafik erklären, schreiben wo die beschriebenen Dienste angesiedelt sind . . . . .	22
■ rausfinden, was in dieser Phase statt findet . . . . .	25
■ Prüfen, warum die Pfeile bei den Verbindungen genau umgekehrt sind . . . . .	25
■ Management Layer genauer beschreiben . . . . .	25
■ DCC genauer erklären und Text anpassen . . . . .	25
■ Stimmt das mit dem Verwerfen eigentlich? . . . . .	27
■ Vergleiche die Bilder 101 612 S. 11 und Abbildung 3.10 . . . . .	27
■ Noch schreiben was der Security Layer genau macht . . . . .	27
■ Was will man da mit einem Oktett? Das sind 256 ITS Stations.... Original in ts 102 731: During the manufacturing process an ITS-S shall receive a globally unique canonical identity in the form of an octet string. It shall persist for the operational lifetime of the ITS-S. . . . .	30
■ An Authorization Authority weiterschreiben . . . . .	31
■ Dateiendung von jpg zu png geändert . . . . .	35
■ neighbor tabelle hier mit einbeziehen etsi 7.1 da steht was da alles drin ist . . . . .	35
■ Hier nochmal nachhacken ob es tatsächlich keine lösung gibt . . . . .	38
■ Ja, die gibts, nennt sich Decentralized Congestion Control (DCC) und wird im Management Layer erklärt . . . . .	38
■ siehe etsi Kapitel 9.2.1 duplicate address detection ist auch interessant . . . . .	39
■ wofür ist das anonyme verfahren? steht leider nix im etsi und soll man evtl noch was über die ITS Networkung & Transport Layer Management entity schreiben? . . . . .	40
■ Cooperative Awareness Message (CAM), Decentralized Environmental Notification Message (DENM), Signal Phase and Time (SPaT) und Topology Specification (TOPO) übertragen . . . . .	43
■ Applicationlayer einführen, die use cases zu den 3 Kategorien sind geschrieben . . . . .	43
■ was über den applayer erzählen . . . . .	45



# Inhaltsverzeichnis

<b>1 Einleitung</b>	<b>7</b>
<b>2 Funktionsweise</b>	<b>9</b>
2.1 Funktionale Komponenten von ITS . . . . .	9
2.1.1 ITS-S Host . . . . .	9
2.1.2 Roadside ITS-S Gateway . . . . .	9
2.1.3 ITS-S Router . . . . .	9
2.1.4 ITS-S Border Router . . . . .	10
2.2 Personal subsystem and station . . . . .	10
2.3 ITS Central Station . . . . .	10
2.4 ITS Roadside Station . . . . .	12
2.5 ITS Vehicle Station . . . . .	13
<b>3 Architektur</b>	<b>15</b>
3.1 Übersicht über die verschiedenen Netzwerke . . . . .	16
3.1.1 ITS Ad Hoc Network . . . . .	16
3.1.2 ITS Access Network . . . . .	16
3.1.3 Public Access Network . . . . .	16
3.1.4 Private Access Network . . . . .	16
3.1.5 Core Network . . . . .	16
3.2 ITS Station Reference Architecture . . . . .	18
3.3 Horizontal Layer . . . . .	18
3.3.1 Access . . . . .	18
3.3.1.1 Physical Layer (PHY) . . . . .	21
3.3.1.2 Data Link Layer (DLL) . . . . .	21
3.3.2 Networking & Transporting . . . . .	21
3.3.3 Facilities . . . . .	21
3.3.4 Applications . . . . .	22
3.4 Cross/Vertical Layer . . . . .	22
3.4.1 Management Layer . . . . .	22
3.4.1.1 ITS Service Advertisement . . . . .	24
3.4.1.2 Decentralized Congestion Control . . . . .	25
3.4.2 Security Layer . . . . .	27
3.5 Data Security . . . . .	27
3.5.1 Angebotene Services . . . . .	27
3.5.2 ITS Authoritative Hierarchy . . . . .	30
3.5.3 Trust and Privacy Management . . . . .	31
3.5.4 ITS Security Services . . . . .	32
3.5.4.1 Enrolment Credentials . . . . .	33
3.6 Verwendete Protokolle . . . . .	33

<b>4 Network Layer</b>	<b>35</b>
4.0.1 Herausforderung . . . . .	35
4.0.2 Komponenten . . . . .	35
4.0.2.1 Location Table . . . . .	35
4.0.2.2 Beaconing . . . . .	37
4.0.2.3 Forwarding . . . . .	37
4.0.2.4 Location Service . . . . .	37
4.0.2.5 Priority Handling . . . . .	37
4.0.2.6 Packet Assembly . . . . .	38
4.0.2.7 Congestion Control . . . . .	38
4.1 Congestion Control . . . . .	38
4.2 Geo Routing . . . . .	38
4.2.1 Addressierung . . . . .	38
4.2.1.1 Konfiguration der Adressen . . . . .	39
4.2.1.2 Duplicate address detection . . . . .	40
4.2.2 Geo Unicast . . . . .	40
4.2.3 Topologically-scoped broadcast . . . . .	40
4.2.4 Geographically-scoped broadcast . . . . .	41
4.2.5 Geographical Scoped Anycast . . . . .	41
<b>5 Facility Layer</b>	<b>43</b>
5.1 CAM . . . . .	43
5.2 DEN . . . . .	43
5.3 SPaT . . . . .	43
5.4 TOPO . . . . .	43
<b>6 Application layer und Use Cases</b>	<b>45</b>
6.1 Use cases . . . . .	45
6.1.1 Sicherheitsbedingt . . . . .	45
6.1.1.1 Cooperative Forward Collision Warning . . . . .	45
6.1.1.2 Pre-Crash Sensing/Warning . . . . .	46
6.1.1.3 Hazardous Location C2C Notification . . . . .	46
6.1.2 Verkehrseffizienz . . . . .	46
6.1.2.1 Enhanced Route Guidance and Navigation . . . . .	46
6.1.2.2 Green Light Optimal Speed Advisory . . . . .	47
6.1.2.3 C2C Merging Assistance . . . . .	47
6.1.3 Infotainment und andere . . . . .	47
6.1.3.1 Internet Access in Vehicle . . . . .	47
6.1.3.2 Point of Interest Notification . . . . .	48
6.1.3.3 Remote Diagnostics . . . . .	48

# **1 Einleitung**



# 2 Funktionsweise

Intelligent Transportation Systems (ITS) besteht aus verschiedenen Komponenten. Diese Komponenten können mobil oder stationär sein. Die Grafik 2.1 gibt einen Überblick über die in ITS verwendeten Komponenten. Jede dieser Komponenten enthält eine ITS Station. Dieser Abschnitt bezieht sich hauptsächlich auf die ETSIStandards [5] und [8]. Standard [5] definiert Funktionalitäten, Standard [8] definiert die Realisierung dieser Funktionalitäten. Im Folgenden werden die Komponenten beschrieben und anhand von beiden Standards erklärt.

## 2.1 Funktionale Komponenten von ITS

Die funktionalen Komponenten sind in sich geschlossene Einheiten, die in den ITS Untersystemen vorhanden sind. Sie werden in diesem Abschnitt beschrieben. Zusätzlich werden die mindestens definierten Funktionalitäten genannt.

Auf die einzelnen Layer der Komponenten wird im Kapitel 3 eingegangen.

Die einzelnen funktionalen Komponenten müssen nicht physikalisch getrennt werden. Es reicht eine logische Trennung.

### 2.1.1 ITS-S Host

Der ITS-S Host beinhaltet mindestens die ITS-S Anwendungen und die Funktionalität der ITS Station Reference Architektur, die für die ITS-S Anwendungen gebraucht wird. Konkret sind das der ITS Network Layer und die Anwendungsebene.

Die Funktionalitäten des ITS-S Host werden im Standard [8] der Application Unit (AU) zugesprochen. Sämtliche andere Funktionalitäten sind auf die Communication & Control Unit (CCU) ausgelagert. Diese Aufteilung hängt aber von der zu implementierenden Komponente ab, ein Skalieren muss möglich sein.

### 2.1.2 Roadside ITS-S Gateway

Die Funktionsweise des Roadside ITS-S Gateway ergibt sich aus der Grafik 2.2. Die Aufgabe ist die gleiche, wie bei den meisten Gateways. Es verbindet unterschiedliche Protokollstacks miteinander. In diesem Fall werden das ITS interne Netzwerk und ein proprietäres Netzwerk miteinander verbunden. Das proprietäre Netzwerk kann beispielsweise ein IP basierendes Netzwerk sein.

### 2.1.3 ITS-S Router

Ein ITS Router bietet alle Funktionen der International Organization for Standardization (ISO) Referenzarchitektur, ausgenommen die beiden oberen Layer Application und Facilities. Er verbindet zwei unterschiedliche ITS Protokoll Stacks auf Layer 3.

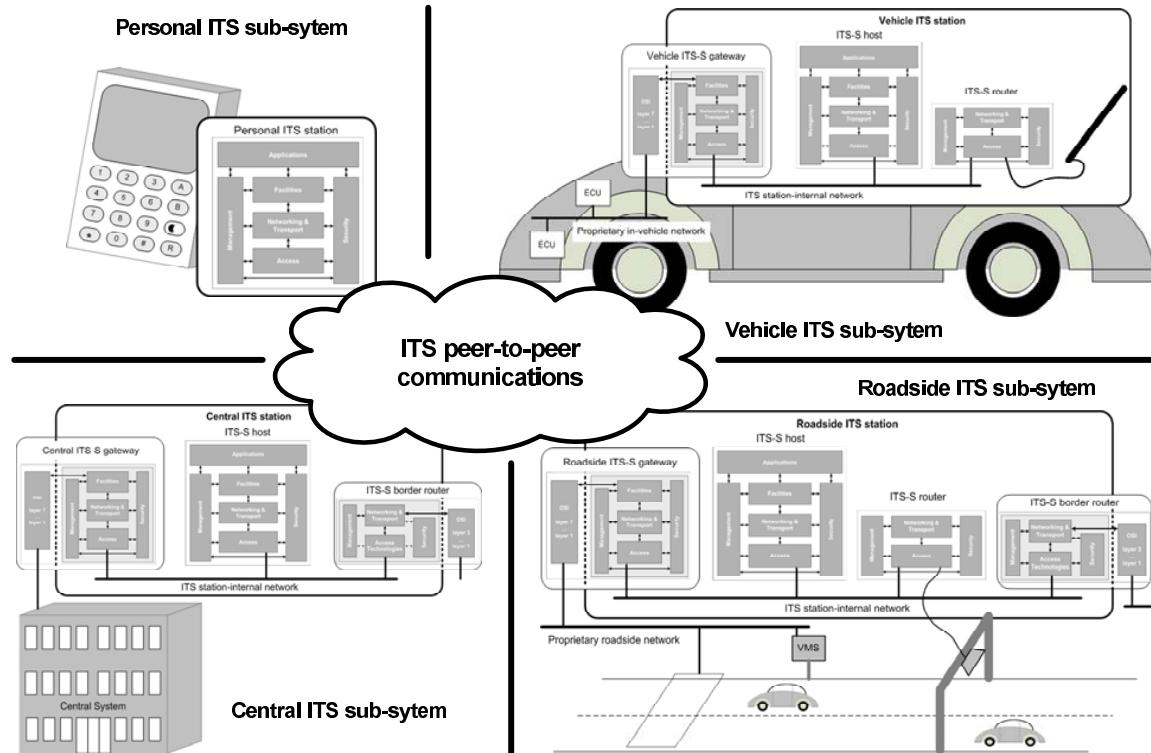


Abbildung 2.1: Überblick über die Komponenten [5]

Einer dieser Protokoll Stacks ist normalerweise mit dem internen ITS Netzwerk verbunden. Router werden genutzt um eine Verbindung zu anderen ITS Komponenten aufzubauen. Die Darstellung der Layer eines Routers befindet sich in Grafik 2.3.

## 2.1.4 ITS-S Border Router

Ein Border Router hat die gleichen Funktionalitäten wie ein Router 2.1.3. Der Unterschied ist, dass ein Border Router zwischen einem ITS Netz und einem Netz ohne die Cross Layer vermitteln kann. Ein Beispiel für ein solches Netz ist das Internet.

## 2.2 Personal subsystem and station

Personal Subsystem and Station (PSS) stellen die Funktionalitäten von ITS in Geräten zur Verfügung, die in der Hand gehalten werden können. Der Standard nennt hierzu Personal Digital Assistant (PDA) oder Mobiltelefone als Beispiel. Sie können als eigenständige Komponente dienen, oder als Teil einer anderen Komponente arbeiten.

das PSS die  
nationalen Kom-  
ponenten suchen

## 2.3 ITS Central Station

Die ITS Central Station (ICS), oder Central ITS subsystem and station ist eine zentrale Komponente im ITS System. Sie bietet die Funktionalität an, um die Komponenten des zentralen Systems an das ITS

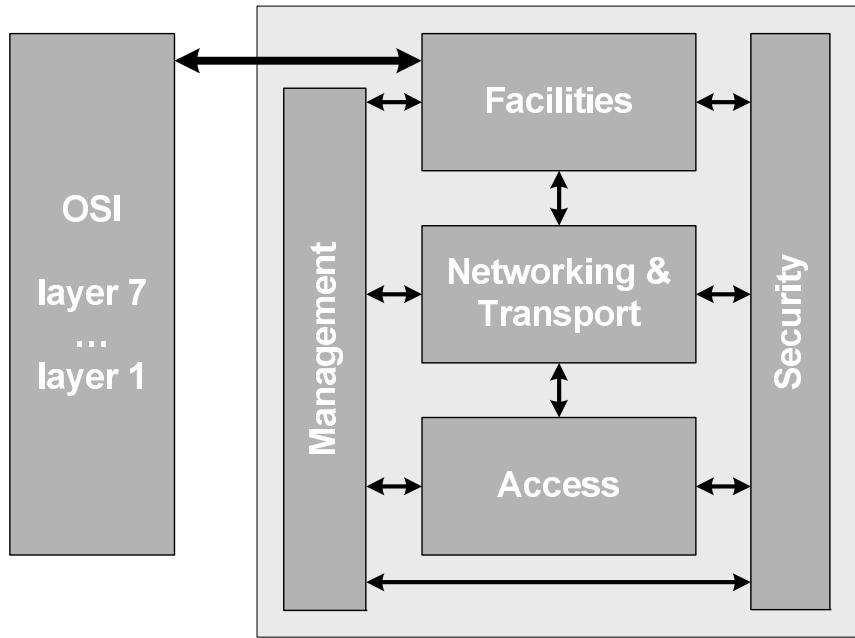


Abbildung 2.2: Überblick über die Layer eines ITS Gateways [5]

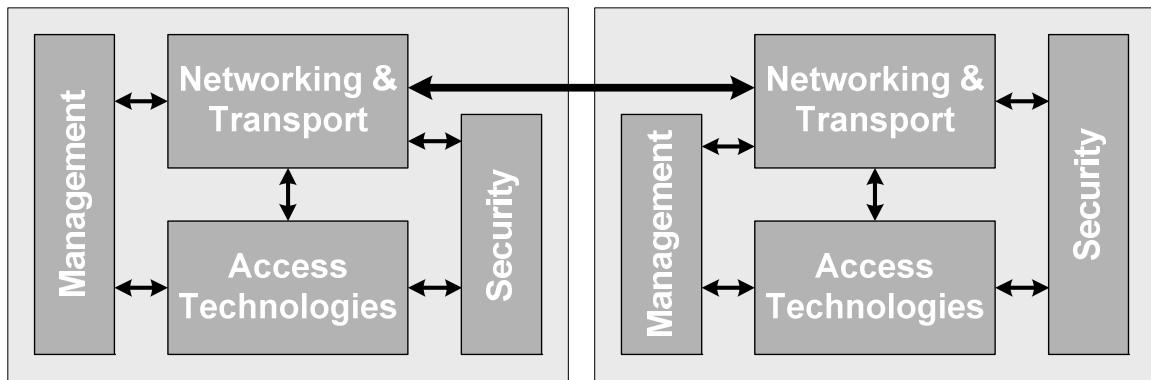


Abbildung 2.3: Überblick über die Layer eines ITS Hosts [5]

Die mindesten funktionalen Komponenten der ICS sind:

- ITS-S Gateway 2.1.2
- ITS-S Host 2.1.1
- ITS-S Border Router 2.1.4

Core component of the architecture is the ITS station, which has two main roles: in its first role, the ITS station is a network node and acts as a communication source or sink. Likewise an ITS station can be a forwarder of data, e.g. in the ITS ad hoc network. In its second role, the ITS station is placed at the network edge and connects the different networks via an ITS station internal network (see Figure 1). [8]

Noch was zur IC finden

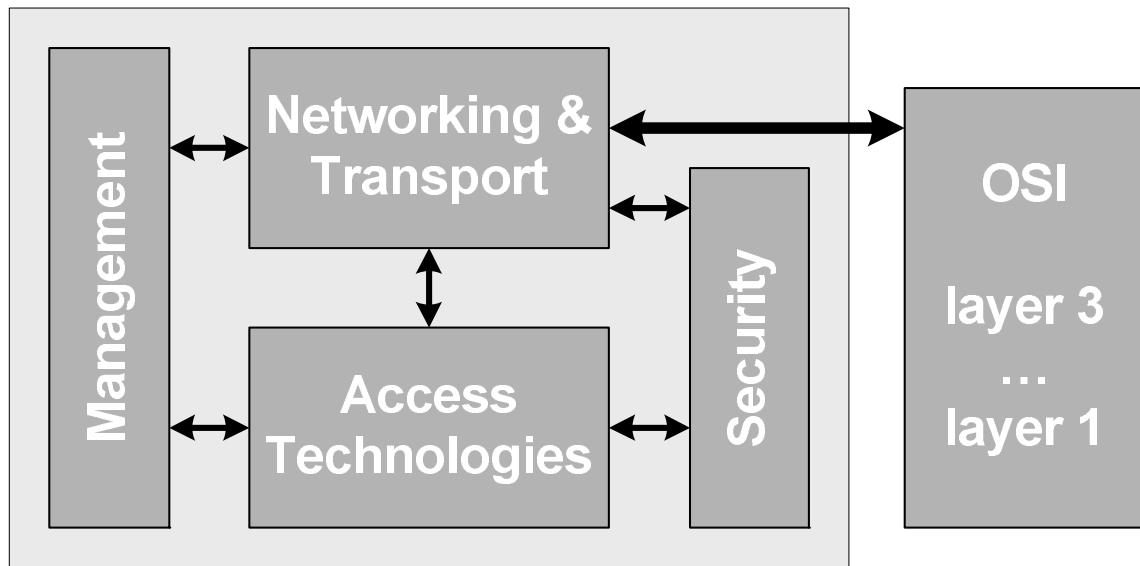


Abbildung 2.4: Überblick über die Layer eines ITS Border Routers [5]

## 2.4 ITS Roadside Station

Die Kommunikation ist nicht auf die Kommunikation von Fahrzeugen untereinander beschränkt. Eine Kommunikation zwischen Fahrzeugen und Verkehrsinfrastruktur ist ebenfalls möglich. Diese Kommunikation wird über ITS Roadside Station (IRS) oder Roadside Unit (RSU) abgewickelt. Da sie den Informationsfluss zwischen ITS Vehicle Station (IVS) und ICS ermöglicht, hat sie einen hohen Stellenwert im System. IRS werden im Normalfall in bereits vorhandene Infrastruktur integriert. Hierfür bieten sich beispielsweise Ampeln oder sonstige Verkehrsleitsysteme an.

Die IRS beherrscht zwei grundlegend unterschiedliche Verbindungsprotokolle. Über das verbindungslose ITS-G5 kann die IRS Verbindungen zu den IVS aufbauen. Die Verbindung zu den ICS erfolgt über TCP/IP.

Normalerweise besteht eine IRS aus den funktionalen Komponenten:

- ITS-S Gateway 2.1.2
- ITS-S Host 2.1.1
- ITS-S Router 2.1.3
- ITS-S Border Router 2.1.4

Neben der Funktion als reine Schnittstelle zwischen IRS und IVS kann die IRS die empfangenen Daten aufbereiten, bzw. ein FunctionFramework zur Verfügung stellen, auf dem Applikationen ausgeführt werden können. Die Funktionen des FunctionFramework sind in der Beschreibung des Hosts 2.1.1 definiert.

Beispiele für Applikationen der IRS sind:

- Store and Forward von Ereignisinformationen Decentralized Environmental Notification Message (DENM)
- Weiterleitung von Ereignisinformationen an Versuchszentrale (Testzentrale)

- Aggregation von empfangenen Fahrzeugdaten zur Verbesserung der Wetter- und Verkehrslage erfassung
- Neue Anwendungen bzgl. der Interaktion zwischen Fahrzeug und LSA
- Kreuzungsassistenz sowie Assistenz im Baustellenbereich.
- Verteilung von Daten der ergänzenden Dienste aus der Versuchszentrale an die Fahrzeuge
- Versendung von Daten zur Kreuzungstopologie

Diese Beispiele sind aus einem Projektergebnis von Sichere Intelligente Mobilität Testfeld Deutschland (sim<sup>TD</sup>) entnommen ([19]).

## 2.5 ITS Vehicle Station

Das IVS ist eine mobile Komponente von ITS. Es hat als Mindestanforderung lediglich Schnittstellen in das ITS Netzwerk. Es besteht mindestens aus folgenden funktionalen Komponenten:

- ITS-S Gateway 2.1.2
- ITS-S Host 2.1.1
- ITS-S Router 2.1.3

---

Noch was über IVS schreiben



# 3 Architektur

Die Netzwerkarchitektur von ITS Stations umfasst sowohl interne als auch externe Netzwerke. Laut Standard [8], bzw. Standard [17] sind dabei folgende externe Netzwerke erfasst:

- ITS ad hoc network.
- Access network (ITS access network, public access network, private access network).
- Core network (e.g. the Internet).

Auf der Grafik 3.1 sind die verschiedenen Netzwerke visualisiert. Diese Art der Darstellung entspricht der höchsten Abstraktionsebene. Die verschiedenen Netzwerke sind in der Grafik als Wolken dargestellt. Neben den Netzwerken sind auch die Verbindungen visualisiert.

Zusätzlich zu den hier beschriebenen Netzwerken kann eine ITS Station ein eigenes Netzwerk, das die Teilkomponenten der ITS Station verbindet, betreiben. Die verschiedenen Netzwerke werden benötigt, damit alle Dienste mit ihren verschiedenen Anforderungen bedient werden können.

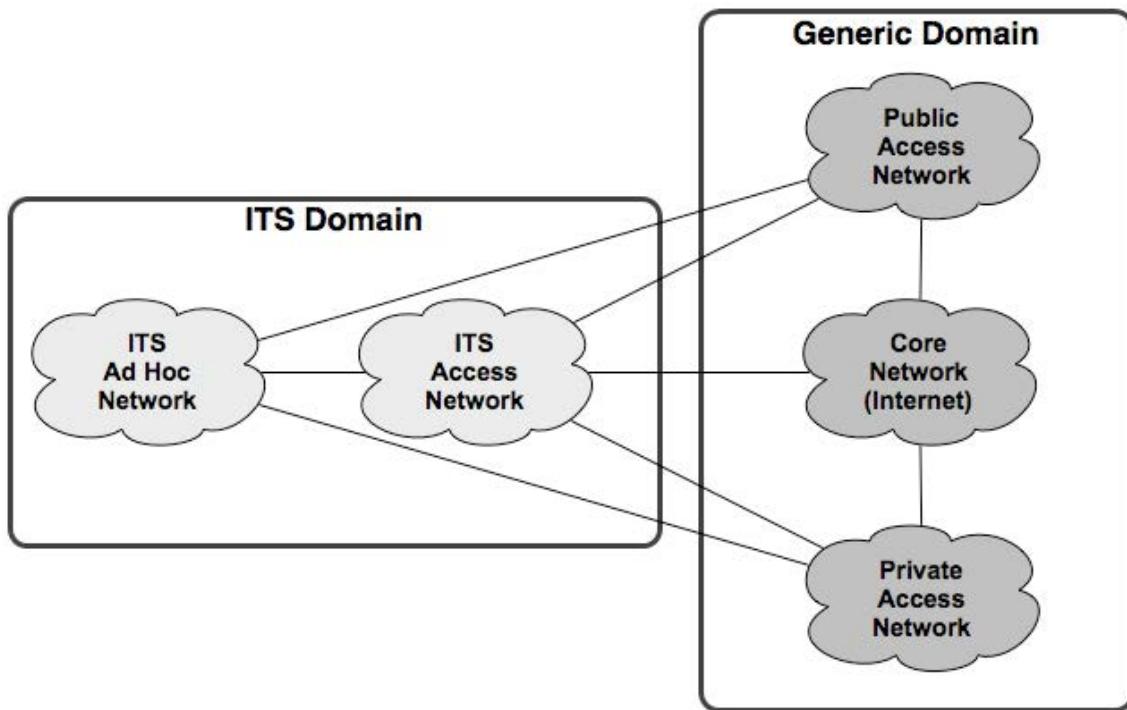


Abbildung 3.1: Überblick über die externen Netzwerke [8]

## 3.1 Übersicht über die verschiedenen Netzwerke

Dieser Abschnitt soll lediglich eine Übersicht über die verwendeten Netzwerke geben. Eine weitere Erklärung der Netzwerke findet an dieser Stelle nicht statt und ist nicht Gegenstand dieser Ausarbeitung. Die Netzwerke dürfen auch nicht isoliert betrachtet werden. Im Abschnitt 2.1 wurden funktionale Komponenten mit Routingfunktionalitäten vorgestellt. Diese können die Netze und somit ihre Vorteile, bzw. ihre Dienste, miteinander verbinden.

Selbstverständlich benötigen die ITS Stations Zugang zu einem der im Folgenden aufgeführten Netze. Der Zugang zum Core Network 3.1.5 erfolgt über eins der anderen Netze.

### 3.1.1 ITS Ad Hoc Network

Das ITS Ad Hoc Netzwerk ist das Netzwerk für die Kommunikation zwischen IRS, IVS und PSS. Die Kommunikation findet über die Luftschnittstelle statt. Sie ist in ihrer Reichweite begrenzt, dafür ist sie mobil einsetzbar. Die Drahtlose Kommunikation wird im Normalfall über den Standard ITS-G5 ermöglicht.

### 3.1.2 ITS Access Network

ITS Access Network werden zur Vernetzung von ITS Komponenten verwendet. Diese Netzwerke bieten den Zugang für die entsprechenden ITS Services. Sie werden als eigene Netzwerke realisiert. ITS Stations werden durch Access Networks verbunden. Das bedeutet, dass IRS untereinander über Access Networks verbunden sein können, es können aber auch Stations, die normalerweise Ad Hoc miteinander kommunizieren dieses Netz nutzen.

### 3.1.3 Public Access Network

Ein Public Access Network ermöglicht den Zugang in öffentlich zugängliche Mehrzwecknetzwerke. Dieses Netzwerk kann beispielsweise dazu genutzt werden, um ITS Stations mit dem Core Netzwerk zu verbinden.

### 3.1.4 Private Access Network

Ein Private Access Network reguliert den Zugang durch die Teilnehmer. Die angebotenen Datendienste stehen nur einer bestimmten Gruppe von Nutzern zur Verfügung. Mit Private Access Networks besteht die Möglichkeit, eine gesicherte Verbindung in ein anderes Netzwerk aufzubauen. So kann beispielsweise ein IVS auf das Intranet einer Firma zugreifen.

### 3.1.5 Core Network

Das Core Network ist ein Verbindungsnetz. Es hat keine ITS Funktionalitäten und wird im Standard auch nicht weiter spezifiziert. Es wird in Verbindung mit den Public Access Network dazu genutzt, traditionelle Dienste, wie Internet oder Email, anzubieten.

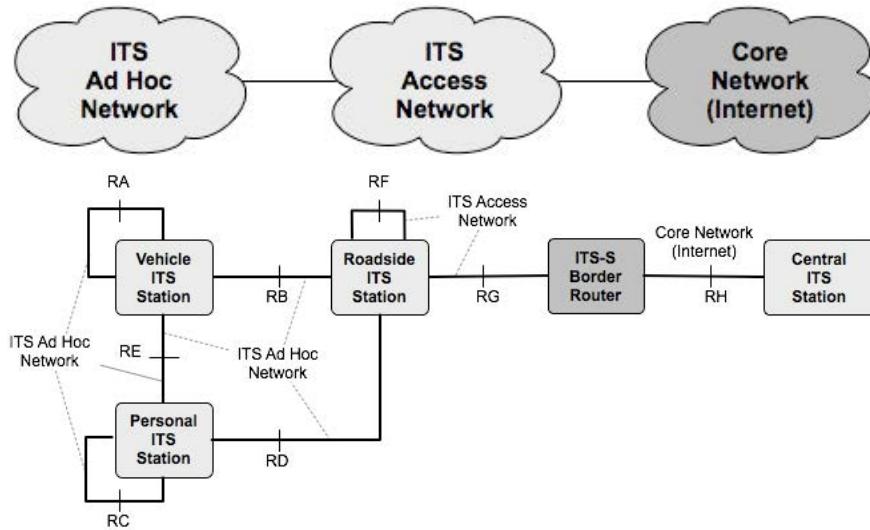


Abbildung 3.2: Netzwerkszenario mit dazugehöriger Implementierung [8]

Die Grafik 3.2 stammt aus dem Standard [8]. Dort ist im oberen Teil der Grafik ein Szenario beschrieben, welche Netzwerke miteinander verbunden sein können. Zu erkennen ist, dass die Netzwerke ITS Ad Hoc Netzwerk 3.1.1, ITS Access Network 3.1.2 und das Core Network 3.1.5 miteinander verbunden sein sollen.

Der untere Teil der Grafik zeigt eine Implementierungsmöglichkeit dieses Szenarios. Die hellen Rechtecke beschreiben die Komponenten, die in dieser Implementierung im System integriert sind, das dunkle Rechteck beschreibt die funktionale Komponente, die in diesem System beteiligt ist. Die Linien sind mit dem Typ des Netzwerks, welches sie repräsentieren beschriftet und zusätzlich mit dem Network Reference Point, den sie benutzen, beschriftet.

Auflistung und kurze Beschreibung der genutzten Network Reference Points:

- **RA:** Reference Point zwischen IVS über das ITS Ad Hoc Network
- **RB:** Reference Point zwischen IVS und IRS über das ITS Ad Hoc Network
- **RC:** Reference Point zwischen PSS über das ITS Ad Hoc Network
- **RD:** Reference Point zwischen PSS und IRS über das ITS Ad Hoc Network
- **RE:** Reference Point zwischen IVS und PSS über das ITS Ad Hoc Network
- **RF:** Reference Point zwischen IRS über das ITS Access Network
- **RG:** Reference Point zwischen IRS und einem ITS-S Border Router<sup>1</sup> über das ITS Access Network
- **RH:** Reference Point zwischen ICS und ITS-S Border Router<sup>1</sup> über das Core Network

Sollen wir hier noch was zum Thema Network Reference Points schreiben? Ich glaube aber, dass die nichts in den Layern kommen

<sup>1</sup>Der Border Router muss nicht explizit aufgeführt werden, da er als funktionale Komponente Teil einer Komponente ist.

Erkennbar ist in dieser Implementierung, dass sich für mobile Stations Ad Hoc Netzwerke verwendet wurden. Diese haben den Vorteil, dass sie bereits in der Spezifikation mit der Luftschnittstelle ITS-G5 ausgestattet sind, was eine Mobilität erst ermöglicht. Was auch erkennbar ist, ist, dass die reinen ITS Netzwerke durch einen Border Router vom Core Network getrennt sind. Auch wenn hier nicht explizit aufgeführt, die ICS benötigt in diesem Fall auch einen Border Router.

## 3.2 ITS Station Reference Architecture

Eine Referenzarchitektur beschreibt ein allgemeines Modell einer Architektur. Das bedeutet, dass basierend auf dieser Architektur verschiedene Implementierungen existieren können.

Die ITS Station Reference Architecture unterscheidet sich grundlegend von bekannten Architekturen. Da sie während der Entwicklung an das Open System Interconnection (OSI) Modell angelehnt war, ergeben sich einige Parallelen:

- Trennung der einzelnen Layer
- Definition von Service Primitiven zwischen den Layern
- Die Standards beziehen die Layer auf die OSI Layer.

Der direkte Vergleich mit dem OSI Modell und die Zuordnung der Layer wird in Abbildung 3.3 deutlich.

Obwohl das ITS Station Reference Protocol bei der Entwicklung an das OSI Modell angelehnt wurde gibt es jedoch einen gravierenden Unterschied: In der ITS Station Reference Architecture sind Cross Layer vorgesehen. Das OSI Referenzmodell ist wasserfallartig aufgebaut. Das bedeutet, dass die einzelnen Layer übereinander angeordnet sind. Jeder Layer hat jeweils nur zu dem direkt über- und unterliegenden Layer eine Schnittstelle. Cross Layer sind Layer, die in mehrere dieser Schichten Schnittstellen haben. Sie erweitern die vorhanden Layer in horizontaler Richtung. Im Fall der ITS Station Reference Architecture sind das die Layer „Management“ und „Security“. Sie haben Schnittstellen, bzw. Primitiven in alle anderen Layer.

## 3.3 Horizontal Layer

Dieser Abschnitt beschreibt die Layer, die klassisch übereinander angeordnet sind. Die Layer und ihre Funktionen entsprechen den Layern des OSI Modells. Sie sind aber anders aufgeteilt.

### 3.3.1 Access

Der Access Layer von ITS entspricht den OSI Layern 1 und 2. Er besteht aus zwei Subaltern und hat drei Interfaces, bzw. Service Access Point (SAP). Die Sublayer sind der „Data Link Layer (DLL)“ und der „Physical Layer (PHY)“. Der DLL kann weiter in den „Medium Access Control (MAC)“ und den „Logical Link Control (LLC)“ Layer

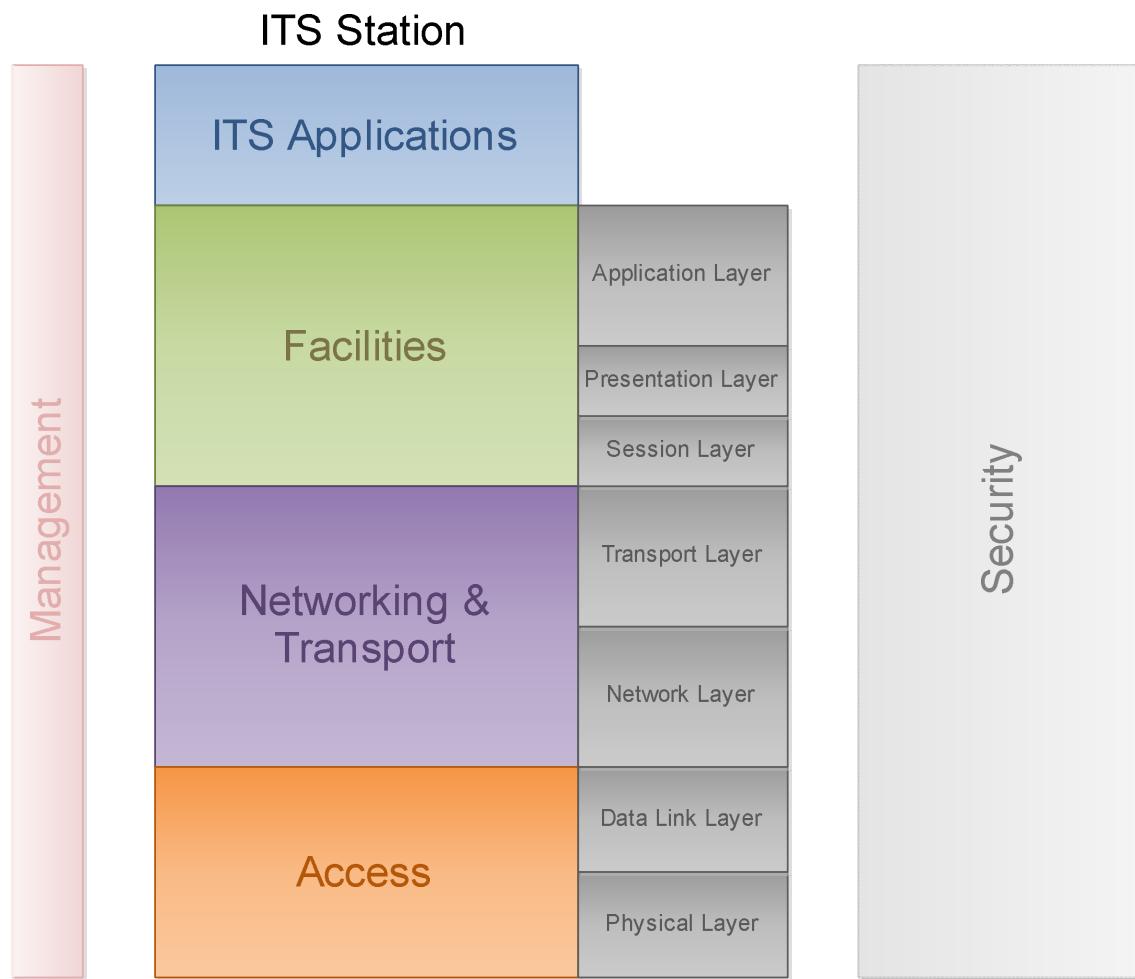


Abbildung 3.3: Der Vergleich zwischen ITS und OSI [12]

unterteilt werden. Zusätzlich zu den Subalayern hat der Access Layer ein Layer Management. Dieses verwaltet die Sublayer. Es arbeitet nur im Access Layer und darf nicht mit dem Management Layer 3.4.1 verwechselt werden.

Die SAP sind:

- **SAP-IN:** Als SAP zu dem nächst höheren Layer Networking & Transporting 3.3.2
- **SAP-SI:** Als SAP zu dem Cross Layer Security Layer 3.4.2
- **SAP-MI:** Als SAP zu dem Cross Layer Management Layer

Der Access Layer ist nicht auf ein bestimmtes Übertragungsprotokoll festgelegt. Beispiele für ein Übertragungsprotokoll sind ITS-G5, WiFi, BlueTooth, Ethernet... In einer reinen Car-to-Car Kommunikation (C2C) Kommunikation bietet sich aber vor allem ITS-G5 an, für eine allgemeine ITS Verbindung haben die anderen Übertragungsprotokolle aber auch ihre Berechtigung. Diese Übertragungsprotokolle müssen aber den ITS Protokollstack transparent übertragen.

ISO 21127 findet Scheinbar Infos über die Layer

mal in ETSI TS 723-10 reinsehen da was interessantes zu den SAP steht

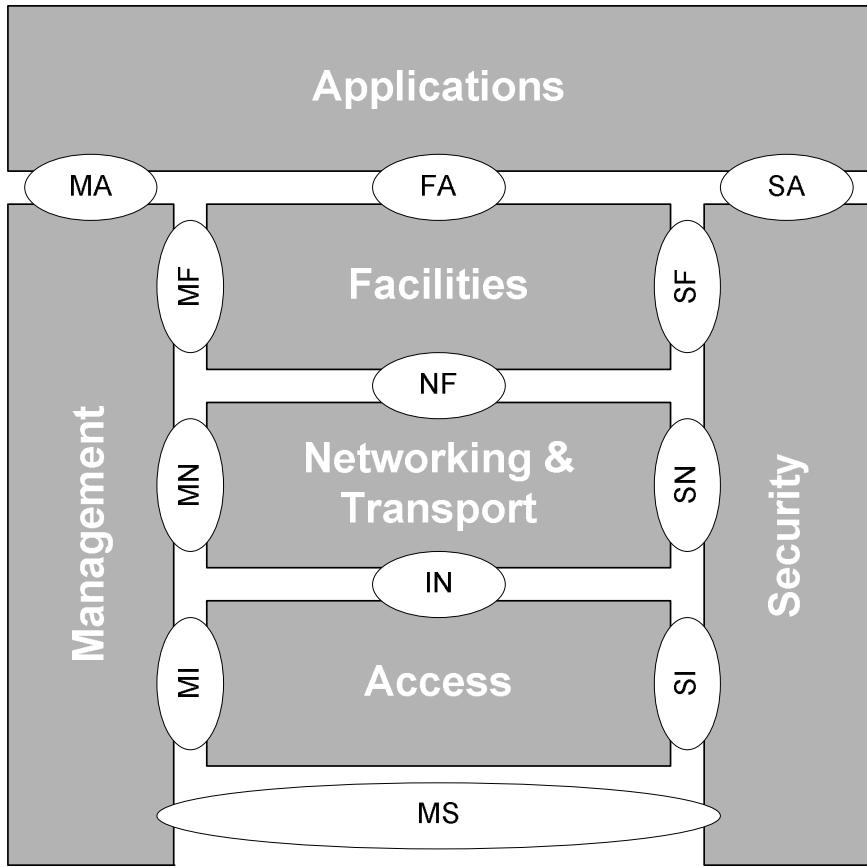


Abbildung 3.4: Darstellung der ITS Station Reference Architecture [5]

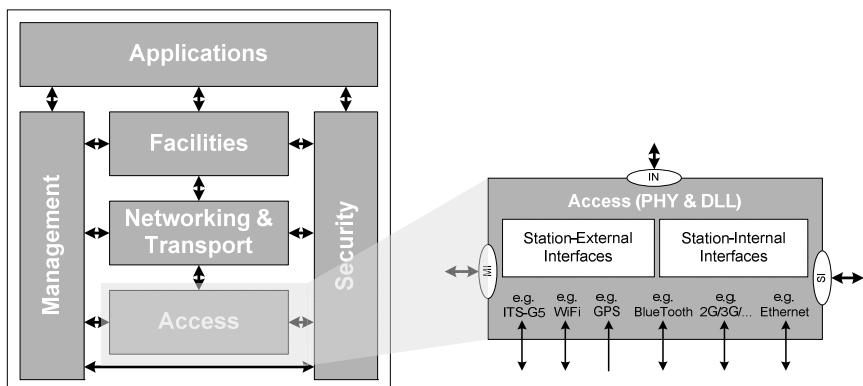


Abbildung 3.5: Darstellung des ITS G5 Access Layers  
citeen302665

Der folgende Abschnitt beschreibt den Access Layer und legt G5 zugrunde.

Die Grafik 3.5 entspricht des untersten Layer der Grafik 3.4. In der Grafik ist zu erkennen, dass der Access Layer drei Interfaces besitzt. Er hat Interfaces zu den Cross Layern und dem Network & Transport Layer.

Im Access Layer finden eine Periodisierung und eine Aufteilung des Datenverkehrs in Logic Channels statt. Diese Aufgaben werden mit verschiedenen Ansätzen gelöst. Deswegen sind sie keinem Sublayer genau zuzuordnen, sondern müssen in der Beschreibung der Sublayer gesondert betrachtet werden.

Eine Funktion des Access Layers ist das im Abschnitt 3.4.1.2 beschriebene DCC. Hier finden die Mechanismen Transmit Power Control (TPC), DCC sensitivity control (DSC), Transit rate control (TRC), transmit datarate control (TDC) und DCC access control (TAC) statt. TPC regelt die Auslastung der Kanäle. Dazu werden Grenzen definiert, die TPC überwacht und einhält. TRC überwacht die Zeiten von Datenpaketen. Dazu gehören beispielsweise die Latenz eines Pakets aber auch die Intervalle zwischen Paketen. TDC überwacht die reine Datenrate eines Channels. Dabei wird nicht nur die maximale Datenrate überwacht, es wird auch beispielsweise die minimale Datenrate überwacht. DSC überwacht, ob der Sender bereit zum Senden ist. Dazu wird anhand von definierten Grenzwerten gemessen, ob der Sender am Senden ist oder nicht. TAC regelt den Kanalzugriff.

Kanalzugriff erklären, wenn ich weiß, was Kanäle sind. Quelle für [15]

### 3.3.1.1 Physical Layer (PHY)

Der Physical Sublayer verbindet physikalisch zu dem Kommunikationsmedium.

### 3.3.1.2 Data Link Layer (DLL)

Der Data Link Sublayer kann wiederum in den Medium Access Control (MAC) Sublayer und den Logical Link Control (LLC) Sublayer aufgeteilt werden. Der MAC Sublayer regelt den Zugriff auf das Kommunikationmedium.

ITS bietet die Funktionalität von logischen Kanälen.

## 3.3.2 Networking & Transporting

Der Networking & Transporting Layer enthält mehrere verschiedene Netzwerk und Transport Protokolle und entspricht den OSI Layern 3 und 4. Die Aufgabe ist das Routing und der Ende zu Ende Transport von Daten. Er wird im Kapitel 4 genauer beschrieben.

## 3.3.3 Facilities

Der Facilities Layer entspricht den OSI Layern 5, 6 und 7. Er bietet eine Sammlung von Funktionen, die die ITS Anwendungen unterstützen. Der Layer bietet Datenstrukturen um verschiedene Date zu speichern, zu sammeln und zu verwalten. Er wird im Kapitel 5 genauer erklärt.

### **3.3.4 Applications**

Im Applications Layer werden die Use Cases realisiert. Ihnen steht der ITS Protokoll Stack zu Verfügung. Eine genauere Beschreibung des Application Layers findet im Kapitel ?? statt.

## **3.4 Cross/Vertical Layer**

Die Cross Layer weichen stark vom OSI Modell ab. Sie erweitern die traditionellen Layer, die jeweils nur ein Interface zum nächst höheren, bzw. tieferen Layer haben um Layer, die Interfaces zu allen anderen Layern haben. Durch die Interfaces zu allen Layern ergeben sich neue Möglichkeiten. So kann beispielsweise im Application Layer die genutzte Bandbreite an die im Physical Layer zur Verfügung stehende Bandbreite angepasst werden. Dadurch werden Überlastungen, die sich auf die Latenz auswirken oder zu fehlerhaften Übertragungen führen bereits im Vorfeld vermieden.

### **3.4.1 Management Layer**

Der Management Layer übernimmt Alle Aufgaben, die mit der Verwaltung einer ITS Station und deren Protokollstack zusammenzufassen sind. Vereinfacht gesagt verwaltet er im Protokollstack die Cross Layer Funktionalität.

In der Abbildung 3.6 ist der Management Layer mit seinen Interfaces und Untereinheiten dargestellt. Er hat zu jedem anderen Layer ein Interface. Die fünf Untereinheiten ergeben sich aus den definierten Funktionalitäten des Management Layers. Die folgende Auflistung der Funktionalitäten ist dem Standard [5] entnommen:

- Cross-interface Management
- Kommunikation zwischen Einheiten gem. ETSI TS 102 723-1
- Netzwerkmanagement
- Kommunikationsservice Management
- ITS Anwendungs Management
- Station Management
- Management der allgemeinen Congestion Control
- Management des Service Advertisement
- Management des Systemschutzes
- Eine alleine Informationsbasis
- Die Möglichkeit die verschiedenen Layer zu verbinden

zelne Untereinheiten der Grafik  
ärden, schreiben  
die beschriebenen  
iste angesiedelt

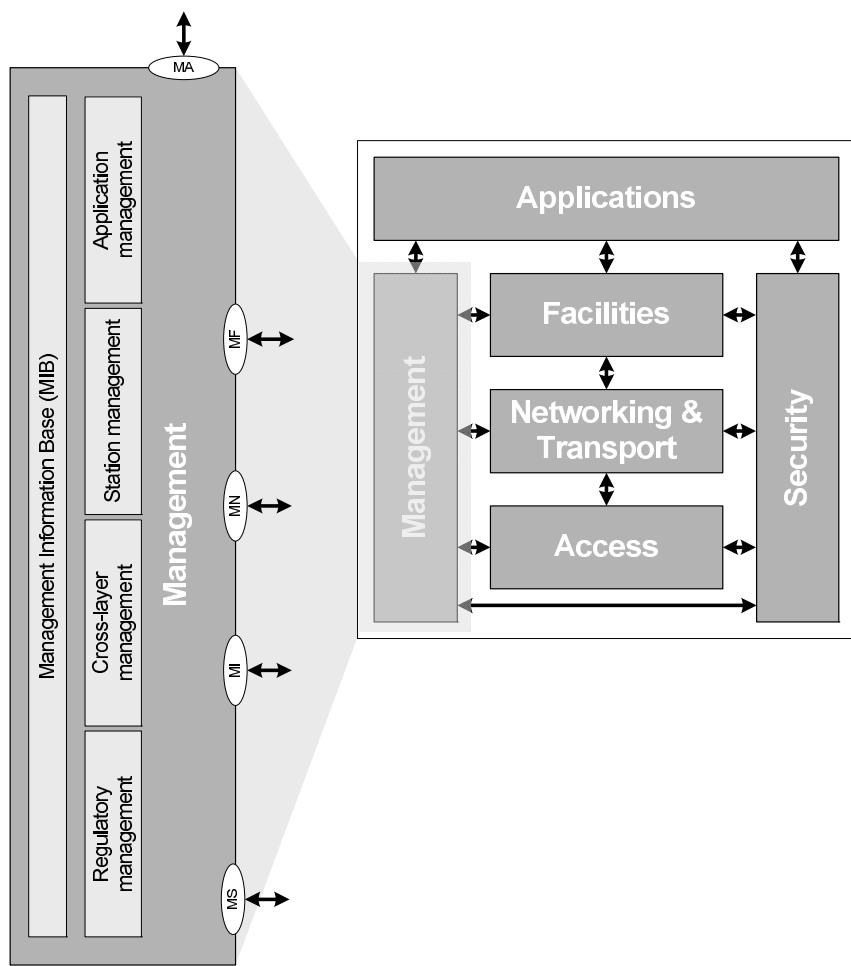


Abbildung 3.6: Der Management Layer im Überblick [5]

### 3.4.1.1 ITS Service Advertisement

ITS Service Advertisement ist der Mechanismus, mit dem eine ITS Station ITS Services erkennen kann. Bei diesem Mechanismus macht eine ITS Station, in dem Fall der Service Provider, aktiv ihre Services anderen ITS Stations, in dem Fall Service User, bekannt. Eine Möglichkeit, die Services bekannt zu machen ist das FAST Service Advertisement. Es ist im Standard ISO/IEC 24102 definiert und eignet sich für die Luftschnittstelle mit lediglich einem Hop. Beim FAST Service Advertisement wird ein Advertisement Manager benötigt. Dieser empfängt die Service Advertisements von den anderen Service Providern und sendet die Service Advertisements der eigenen ITS Station in regelmäßigen Abständen aus.

Für das Aussenden von Service Advertisements gibt es Service Advertisement Message (SAM). Abbildung 3.7 zeigt den Aufbau einer SAM. Sie besteht aus einem Header und einem Body. Der Header enthält die Elemente:

- samID: Identifiziert die SAM
- Version: Die Versionsnummer der SAM
- stationID: Die ID des sendenden Service Providers

Der Body enthält die folgenden Elemente:

- serviceList: Eine Liste mit den angebotenen Services. Sie sind nach dem Standard ISO 17419 eindeutig kodiert
- channelList: Eine Information, welche Channels für die Service Operation Phase genutzt werden
- ipServList: Informationen über Services, die angeboten wurden und der Service Operation Phase IPv6 benötigen.

Service Advertisement Message SAM					
Header		Body			
samID	Version	stationID	serviceList	channelList	ipServList

Abbildung 3.7: Darstellung eines SAM Pakets

Der Service User beantwortet die SAM mit einer Service Context Message (CTX). Die CTX ist ähnlich aufgebaut wie die SAM. In der Abbildung 3.8 ist eine CTX dargestellt.

Context Message CTX					
Header		Body			
ctxID	Version	clientID	servContext- List	ipContextList	

Abbildung 3.8: Darstellung eines CTX Pakets

Der Header der CTX entspricht dem einer SAM. Hier wird aber anstatt der Identifikator (ID) des Providers die ID des Clients mitgesendet. Im Body unterscheiden sich die Nachrichten.

Die Body Inhalte einer CTX:

- servContextList: Informationen über den Service Kontext, der beim Service User verfügbar ist. Kann als Antwort auf einen angebotenen Service in der serviceList der SAM vorliegen.
- ipContextList: Informationen über Service Kontexte, die beim Service User verfügbar sind und IPv6 benötigen. Kann als Antwort auf einen Service, der in der ipServ-List der SAM angeboten wurde vorliegen.

Das Bekanntmachen von Services kann auf zwei Arten erfolgen. Die Möglichkeiten unterscheiden sich darin, dass bei der ersten Möglichkeit die SAM vom Service User mit einer CTX beantwortet wird. Bei der zweiten Möglichkeit wird die SAM nicht beantwortet. Grundsätzlich laufen die Möglichkeiten aber gleich ab.

Die Kommunikation zwischen User und Provider kann man in zwei Phasen aufteilen. Die Service Initialization Phase und die Service Operation Phase.

Der Zweck der Service Invitation Phase ist es die Session aufzubauen. Dabei wird der Service User mit einer SAM eingeladen. Während der Service Invitation Phase wird zwischen den beschriebenen Möglichkeiten unterschieden. Ob eine SAM von einer CTX bestätigt wird, hängt davon ab, ob es sich beim Service User um eine ITS application class oder eine ITS application handelt. Der Unterschied zwischen ITS Application Class und ITS Application ist, dass von einem Application Objekt mehrere Kontexte existieren können. Jeder Kontext kann auf eine ITS Application referenziert werden. Bei der Übertragung wird der Unterschied durch den Abstract Syntax Notation One (ASN.1) Typ „DSRCapplicationEntityID“ als Markierung deutlich gemacht.

Bei der Einladung von Application Classes wird die SAM durch eine CTX bestätigt.

Bei Applications wird keine CTX versendet. Die Service Invitation Phase wird als erfolgreich angesehen, sobald das erste „REQUW“ oder „REQN“ versendet wird.

Nach der erfolgreichen Service Invitation Phase folgt die Service Operation Phase.

In Abbildung 3.9 wird der Ablauf der Phasen darstellen. Die einzelnen Schritte der Kommunikation bedeuten ausgeschrieben:

- Request with no response expected (REQN)
- Request with response expected (REQW)
- Response to a request (RES)

Beschrieben in [16]

rausfinden, was in dieser Phase stattfindet

Prüfen, warum die Pfeile bei den Verbindungen genau gekehrt sind

Management Layer genauer beschreiben

DCC genauer erklären und Text passen

### 3.4.1.2 Decentralized Congestion Control

Congestion lässt sich aus dem Englischen mit Stau übersetzen. DCC ist ein Mechanismus, der verhindern soll, dass Staus auftreten. Besonders bei ITS Anwendungen kommt es auf zuverlässige und Übertragungswege an. Es werden hohe Anforderungen

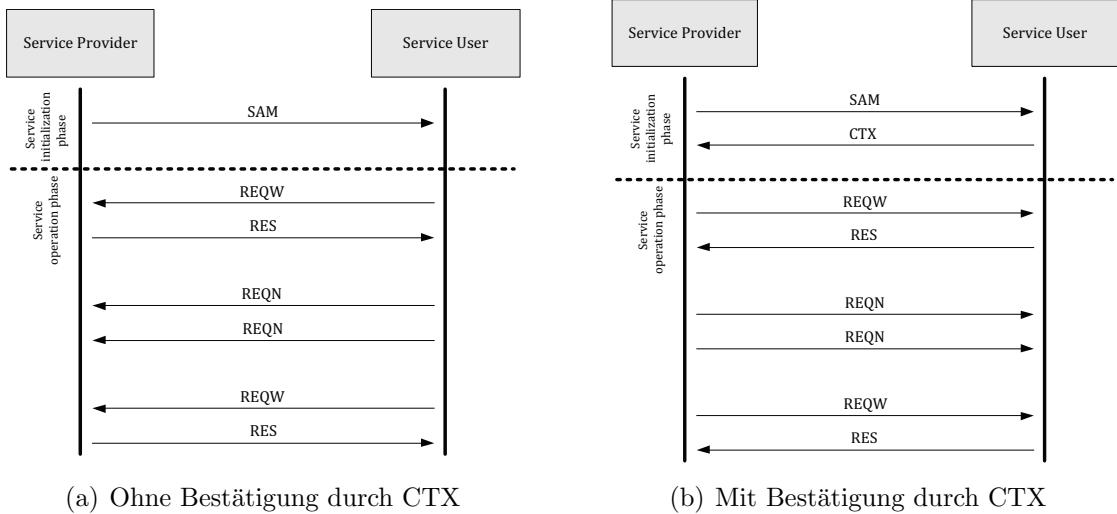


Abbildung 3.9: Ablauf der Phasen des Fast Service Advertisement Protocol [20]

an die Verfügbarkeit und die Latenzen der Übertragungen gestellt. An Luftschnittstellen sind diese Anforderungen ohne eine Komponente wie DCC kaum zu erfüllen. Der Standard [15] definiert folgende Anforderungen an DCC:

- Eine faire Verteilung von Ressourcen und ein fairer Kanalzugriff zwischen allen ITS Stationen in der gleichen Kommunikationszone
- Die Auslastung der Kanäle muss unter vordefinierten Werten bleiben. Dies muss durch eine periodische Messung sicher gestellt werden
- Reservierung von Kommunikationsressourcen für das Verbreiten von hoch priorisierten ereignisgesteuerten Nachrichten
- Schnelle Übernahme einer wechselnden Umgebung (busy / free radio channel)
- Die Änderungen in den Kontrollsleifen müssen in den definierten Grenzen bleiben
- Es muss den spezifischen Systemanforderungen, beispielsweise Zuverlässigkeit, entsprechen

Aus diesen Anforderungen lässt sich herauslesen, dass das Vermeiden von Staus durch mehrere Mechanismen realisiert wird. Eine wichtige Eigenschaft von DCC ist, dass es im Management Layer angesiedelt ist. Diese Tatsache ermöglicht es DCC seine Aufgaben parallel in mehreren Layern zu realisieren. Die Abbildung 3.10 zeigt die Architektur von DCC. Die Abbildung zeigt den ITS Protokoll Stack in den die DCC Komponenten und Interfaces eingezeichnet sind. Der Vorteil dass die Layer vernetzt sind ist, dass der Stau wirklich vermieden werden kann und nicht nur die Auswirkungen des Staus behandelt werden müssen. Ein Beispiel dafür ist, dass DCC das Trafficaufkommen bereits im Network Layer an das Medium anpassen und einzelne Dienste priorisieren kann. IEEE 802.11 beispielsweise muss bei einer Überlast, bzw. einem Pufferüberlauf, Frames verwerten. Dieses Verwerfen muss durch Protokolle höherer Layer abgefangen werden und

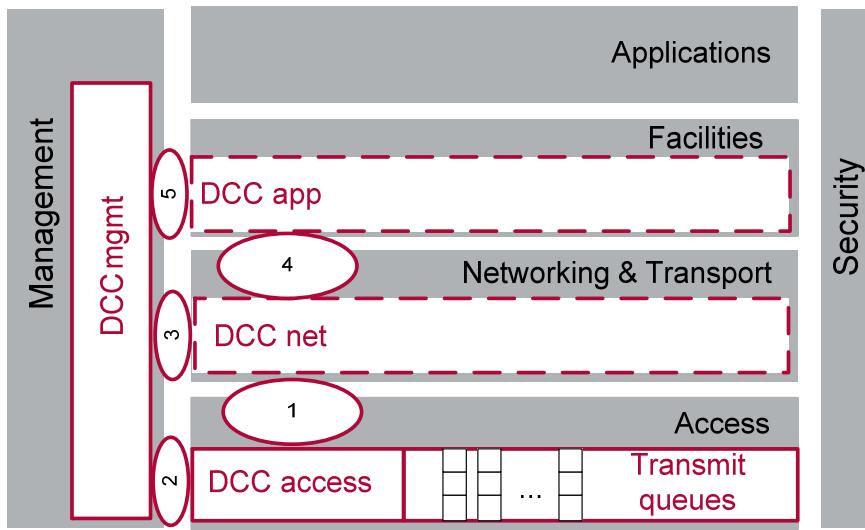


Abbildung 3.10: Die Architektur von DCC [15]

führt aufgrund von Retransmissions zu höheren Latenzen und einer insgesamt höheren Netzwerkauslastung.

Für die Kommunikation mit mehreren Layern sind in der DCC Architektur vier Komponenten definiert. Die Komponenten sind mit den DCC Interfaces verbunden, die selber auf den Interfaces der Layer zugeordnet werden. Die Komponenten werden in den Layern erklärt, in denen sie liegen.

Die DCCmgmt Komponente ist im Management Layer angeordnet. Sie übernimmt dort die Cross Funktionalität und steuert die anderen Komponenten. Dazu hat sie Unterkomponenten.

Eine Unterkomponente der DCCmgmt Komponente ist die DCC\_CROSS\_Facilities.

Stimmt das mit  
Verwerfen eigentlich

Vergleiche die Bi  
101 612 S. 11 un  
Abbildung 3.10

### 3.4.2 Security Layer

Der Security Layer ist ein Cross Layer der ITS Architektur. Er sorgt für die Sicherheit im ITS System. Er hat Interfaces in alle anderen Layer.

Noch schreiben v  
der Security Laye  
genau macht

## 3.5 Data Security

Der Begriff Security umfasst in ITS verschiedene Bereiche der Sicherheit. Im ITS Netz muss sichergestellt werden, dass die Nachrichten für die berechtigten Teilnehmer lesbar sind, für den unberechtigten Teilnehmer aber nicht. Dabei ist zu beachten, dass über ITS sensible Daten verbreitet werden. Es muss neben dem Schutz gegen unbefugtes Lesen auch ein Mechanismus implementiert sein, der verhindert, dass falsche Informationen übertragen werden. Da die ITS Architektur verschiedene Netzwerktypen Abschnitt 3.1 beinhaltet muss die Architektur auch ein Data Security Konzept beinhalten. Der Standard [12] spezifiziert dieses Konzept.

### 3.5.1 Angebotene Services

Maßnahme		Security Services	
	First Level	Lower Level	Data Accessed
Include pseudonym in all V2V messages	Pseudonym Validation		
Require an ITS-S to be authorized by an ITS authority before its messages are accepted by the ITS system	Obtain Enrolment Credentials		Security Parameters (Authentication Keys)
Limit message traffic to V2I/I2V where possible	Obtain Enrolment Credentials		Security Parameters (Authentication Keys)
		Authorization	Policy Database, Security Parameters (Authorization Ticket)
		Establish Security Association	Security Parameters (Pseudonym, Encryption Keys)
	Send Secured Message	Encrypt Outgoing Message	Security Parameters (Pseudonym, Encryption Key)
		Authenticate Outgoing Message	Security Parameters (Pseudonym, Authentication Key)
	Receive Secured Message	Decrypt Incoming Message	Security Parameters (Encryption Key)
		Validate Authentication on Incoming Message	Security Parameters (Pseudonym, Authentication Key)
	Update Security Association	Remove Security Association	Security Parameters (Pseudonym, Encryption Key)
		Establish Security Association	Security Parameters (Pseudonym, Encryption Key)
	Remove Enrolment Credentials	Authorization	Policy Database, Security Parameters (Authorization Ticket)
		Remove Security Association	Security Parameters (Pseudonym, Encryption Key)

Implement plausibility validation on incoming information	Validate Data Plausibility	Validate Dynamic Parameters	LDM
		Validate Timestamp	
		Validate Sequence Number	
Include a non cryptographic checksum of the message in each message sent	Insert Check Value	Calculate Check Value	
	Validate Check Value	Calculate Check Value	
Use broadcast time (Universal Coordinated Time - UTC - or GPS) to timestamp all messages		Timestamp Message	
		Validate Timestamp	
Include a sequence number in each new message		Insert Sequence Number	
		Validate Sequence Number	
Include an authoritative identity in each message and authenticate it	Validate pseudonym		Security Parameters (Authentication Keys)
Encrypt the transmission of personal and private data	Send Encrypted Data	Encrypt Outgoing Message	Security Parameters (Encryption Keys)
	Process Received Encrypted Data	Decrypt Incoming Message	Security Parameters (Encryption Keys)
Add an audit log to ITS stations to store the type and content of each message sent to and from an ITS-S	Update Audit Log	Record Incoming ITS Messages	Audit Logs
		Record Outgoing ITS Messages	Audit Logs
Digitally sign each message using a Kerberos/PKI-like token	Sign Outgoing Message	Generate Signature	Security Parameters (Certificate, Keys)

		Authorization	Policy database, Security Parameters (Authorization Ticket)
Verify Incoming Signed Message	Verify Signature	Security Parameters (Certificate, Keys)	
	Authorization	Policy database, Security Parameters (Certificate Status Information)	
Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	Obtain Enrolment Credentials	Identification (authoritative identity provider)	Security Parameters (Pseudonym, Encryption Key)
	remove Enrolment Credentials	Identification (authoritative identity provider)	Security Parameters (Pseudonym, Encryption Key)
Allow remote activation and deactivation of ITS-S	ITS-S Remote Management Report Misbehaving ITS-S	Authorization	Policy Database
		Deactivate ITS Transmission	Security Parameters (Authorization Ticket)
		Activate ITS Transmission	Security Parameters (Authorization Ticket)
		Report Misbehaviour	Security Parameters (Authorization Ticket)

Tabelle 3.1: Tabelle mit den Sicherheitsmaßnahmen [11]

Tabelle 3.1 stammt aus dem Standard [11]. Dort werden die Maßnahmen zusammengefasst, die benötigt werden um sie zu erreichen. „First Level“ sind die Security Services, die direkt von den Anwendungen oder anderen Komponenten aufgerufen werden. „Lower Level“ Services sind die, die von anderen Security Services aufgerufen werden.

### 3.5.2 ITS Authoritative Hierarchy

Die ITS Authoritative Hierarchy beschreibt, wer eine Rolle bei der Verwaltung der Sicherheit übernehmen kann.

Die Hersteller von ITS Stations unterstützen die regionalen Autorisierungsstellen indem sie die Identitäten der ITS Stations verwalten. Dazu sollen sie ihnen während der Fertigung eine weltweite einzigartige Identität geben. Diese Identität soll in Form eines Oktett Strings sein. Sie soll während der gesamten Lebensdauer gültig sein. Neben der ID müssen die ITS Stations die Fähigkeit besitzen, die Verbindung mit mindestens einer

Zertifikatsstelle und mindestens einer Autorisierungsstelle zu überprüfen. Außerdem muss sie in der Lage sein, weitere Zertifikats- und Autorisierungsstelle hinzuzufügen. Die Zertifikatsstelle, ist eine Einheit, die die Verwaltung der Zulassungszertifikate verantwortlich ist. Die Zertifikatsstelle werden verwendet um in Nachrichten zwischen ITS Station und einer Security Management Einheit die ITS Station als zugangsberechtigt auszuweisen. Das beinhaltet auch die Prüfung der Identität. Die Informationen zu der ITS Station entnimmt die Zertifikatsstelle dem Zulassungszertifikat. Sie erstellt ein neues Zertifikat, und sendet es an die ITS Station. Dieses Zertifikat bestätigt die Identität der ITS Station und die der Zertifikatsstelle. Es findet lediglich die Bestätigung einer gültigen Identität statt, auf die Identität selber können mit diesem Zertifikat keine Rückschlüsse gezogen werden. Wird eine ITS Station als kompromittiert erkannt, informiert die Zertifikatsstelle die anderen Zertifikatsstellen. Dazu wird die eideutige ID der ITS Station den anderen Zertifikatsstellen mitgeteilt. Die ITS Station bekommt so lange keine neuen Zertifikate, solange sie als kompromittiert bekannt ist.

Die Autorisierungsstelle regelt den Zugang zu allgemeinen und speziellen Diensten. Um die Dienste der Autorisierungsstelle nutzen zu können muss die die Identität der ITS Station durch ein Zertifikat einer Zulassungsstelle nachgewiesen werden. Die ITS Station fragt bei der Autorisierungsstelle wegen der spezifischen Berechtigungen an. Die Anfragen werden Erkennt die Autorisierungsstelle, dass eine ITS Station kompromittiert ist, so informiert sie die Zertifikatsstelle, von der die ITS Station ihr Zertifikat hat. Ihr werden keine weiteren Tickets mehr mitgeteilt. Zusätzlich wird werden alle anderen ITS Stations informiert, dass die Zertifikate ungültig sind.

An Authorization Authority weiter schreiben

### 3.5.3 Trust and Privacy Management

Ein Aspekt der Data Security ist das Trust and Privacy Management. Der Standard [13] definiert für den Begriff Privacy vier Schlüsselattribute:

- Anonymity
- Pseudonymity
- Unlinkability
- Unobservability

Der Begriff anonymity bedeutet übersetzt Anonymität und erklärt sich von alleine. Der Begriff bedeutet, dass jemand anonymes keine Identität zugeordnet werden kann. Ein Beispiel hierfür ist eine völlig zufällige Nummer, die anstelle der Identität angegeben wird. Ihr kann keine Identität zugeordnet werden. Da einigen Services der ITS Architektur eine Authentifizierung zu Grunde liegt ist eine vollständige Anonymisierung nicht möglich. Aus diesem Grund gibt es die drei anderen Schlüsselwörter.

Pseudonymity bedeutet übersetzt Pseudonymisierung. Pseudonymisierung wird oft mit Anonymisierung verwechselt, bedeutet aber etwas Anderes. Hinter etwas pseudonymisiertem steht eine Identität, die durch das pseudonymisierte ersetzt wurde. Ein Beispiel hierfür ist die Matrikelnummer eines Studenten. Einem Angreifer, ohne die Möglichkeit, die Matrikelnummer dem Namen eines Studenten zuzuordnen, ist der Student gegenüber anonym. Besteht die Möglichkeit jedoch kann der Matrikelnummer sehr wohl eine Identität zugeordnet werden. Der Nachteil von Pseudonymen ist, dass

sie wertlos sind, sobald ein Teil des Systems kompromittiert wurde. In ITS wird die Psyeudonymität erreicht, indem nur temporäre Kennungen von ITS Stations verwendet werden.

Ein weiterer Nachteil von Pseudonymen ist, dass mit der erfassten Datenmenge die Chance steigt, von ihnen auf eine Identität zu schließen. Wird die Nutzung eines Pseudonyms verfolgt können die Aktivitäten miteinander Verlinkt werden. Dadurch kann aus dem Pseudonym eine neue Identität werden, von der Rückschlüsse auf die Identität hinter dem Pseudonym getroffen werden können. Es kann aber auch die Identität aus dem Verhalten ermittelt werden. Um bei dem Beispiel mit dem Studenten zu bleiben, kann über ihn, bzw. seine Matrikelnummer, ein Bewegungsprofil erstellt werden, das einzigartig ist. Wird die Matrikelnummer für das Einschreiben in Kurse genutzt kann nach genug Einschreibungen das Studienfach und das Studiensemester ermittelt werden. Diese Sammlung nennt man Verkettung von Daten. Das Schlüsselwort unlinkability fordert, dass eine ITS Station nicht verkettbar ist. In ITS wird die Verkettbarkeit verhindert, indem die Verwendung von nicht, oder kaum, veränderter Informationen. Damit kann Verbindungen von ITS Stations nicht anderen Verbindungen zugeordnet werden.

Unobservability bedeutet, dass der Nutzer eine Ressource nutzen kann, ohne dass andere Nutzer, oder Dritte, feststellen können, dass dieser Dienst genutzt wird.

Durch die Beachtung dieser Schlüsselwörter bei der weiteren Spezifikation und der Implementierung von ITS wird der Datenschutz bereits im Vorfeld beachtet.

Neben dem Datenschutz muss im ITS System aber auch eine Zugangskontrolle realisiert werden. Die Zugangskontrolle teilt sich in zwei Bereiche auf: Die Berechtigung, das ITS System als Ganzes zu nutzen und die Berechtigung, einzelne Services und Anwendungen zu nutzen. Die Prüfung der Identitäten wird über Zertifikate und Public-Key Verfahren realisiert. Zur Verteilung der Berechtigungen werden im Standard [11] definiert.

### **3.5.4 ITS Security Services**

Bei den in ITS versendeten Nachrichten müssen aus Sicht der Sicherheit drei verschiedene Typen betrachtet werden.

Der erste Typ ist die „Individual public message“ Dieser Typ wird per Broadcast an andere ITS Stations versendet. Da es sich um eine Broadcast Nachricht handelt, ist eine Verschlüsselung nicht nötig. Um zu verhindern, dass mit dieser Nachricht Fehlinformationen übertragen werden muss sie lediglich signiert werden. Der Standard [11] nennt für diesen Typ von Nachricht die Schlagwörter: authorization, authentication und integrity. Damit wird ausgedrückt, dass die sendende **iTS!** (**iTS!**) Station im System legitimiert sein muss, die Nachricht wird als Schutz gegen Verfälschungen und fehlerhafte Nachrichten von Angreifern aber signiert.

Der zweite Typ ist die „Individual private message“ . Sie wird an eine bestimmte ITS Station verschickt. Da hier kein Broadcast vorliegt, macht es auch Sinn diese Nachricht zu verschlüsseln. Der Standard nennt zu diesem Nachrichtentyp die Schlüsselwörter require authorization, authentication, integrity, privacy und confidentiality. Diese Schlüsselwörter erweitern die Schlüsselwörter der „Individual public message“ um den Faktor, dass der Inhalt von Dritten nicht mitgelesen darf. Aus diesem Grund findet zusätzlich eine Verschlüsselung der Nachricht statt.

Als drittes sind die „Security Associations“ zu nennen. Sie werden zwischen zwei oder

mehreren ITS Stations aufgebaut und beinhalten einen Satz von Krypto Algorithmen, Schlüsseln und andere private und öffentliche Parameter. Sie werden genutzt um eine Ende zu Ende Verbindung aufzubauen. Der Standard nennt die Schlüsselwörter confidentiality, authentication und integrity. Diese entsprechen prinzipiell den Schlüsselwörtern der „Individual private message“. Diese Verbindungen können auf andere autorisierte Teilnehmer dupliziert werden. Jeder Teilnehmer kann mehrere sichere Verbindungen haben. Wenn die sichere Verbindung aufgebaut wird, sollen die Zertifikate und die Kryptwerkzeuge die mit den sicheren Verbindungen verknüpft sind genutzt werden. Die sichere Verbindung soll ab und zu neu verhandelt werden.

Die beschriebenen Nachrichtentypen benötigen Zertifikate. In ITS sind zwei verschiedene Sorten von Zertifikaten definiert. Es gibt ein „authorization ticket“. Es ist als ein Datenobjekt beschrieben, dass bestätigt, dass der gültige Inhaber berechtigt ist, verschiedene Aktionen auszuführen. Es wird von der ITS Autorisierungsstelle 3.5.2 ausgestellt. Die zweite Sorte Zertifikat ist das „enrolment credential“. Es wird als ein Datenobjekt das im Nachrichtenaustausch zwischen ITS Stationen und Security Einheiten genutzt und beweist, dass der gültige Inhaber berechtigt ist, authorization tickets anzufragen. Es wird von der Zertifikatsstelle ausgestellt. Die folgenden Abschnitte erläutern wie die Verarbeitung der Zertifikate statt findet.

#### **3.5.4.1 Enrolment Credentials**

Enrolment Credentials können ausgestellt, erneuert und gelöscht werden.

### **3.6 Verwendete Protokolle**



# 4 Network Layer

Der Networklayer in der Car-to-Car Kommunikation, übernimmt die Aufgabe Nachrichten durch das Netz zu Routen. Er bietet also seine Transportdienste dem Applicationlayer an. Darüber hinaus ist er für die Koordination des Netzwerkes zuständig. Das bedeutet im genauen das er dafür Sorge trägt, dass die Nachrichten auch wirklich ankommen. Dafür beachtet er die Anforderungen der verschiedenen Anwendungen, wie z.b. das senden von Zeitkritischen Nachrichten einer Safety Application. Um bei einem Netzwerk wie es in der Car-to-Car Kommunikation zu finden ist die Kommunikation zu steuern stellen sich einige Anforderungen und Herausforderungen. Vor allem bei der Adressierung der richtigen Knoten.

## 4.0.1 Herausforderung

Da sich die Topologie des C2C-Netzes ständig ändert, da die Knoten sich nicht nur mit unterschiedlichen Geschwindigkeiten bewegen sondern auch die Anzahl an Kommunikationspartnern sich dauernd ändert, kommt es in dem Netz zu häufigen Paketverlusten und einem allgemeinen Overhead an Informationen. Außerdem muss gewährleistet werden das die einzelnen Fahrzeuge jederzeit wissen wie sie andere Fahrzeuge erreichen können. Zudem kommt noch hinzu das bei der hohen Informationsdichte und Komplexität des Netzwerkes noch unterschiedlich wichtige Nachrichten gesendet werden.

## 4.0.2 Komponenten

Im folgenden werden die einzelnen Komponenten des Networklayers genauer erläutert. Dazu wird darauf eingegangen aus welchen Komponenten der Layer besteht und wie die einzelnen Komponenten arbeiten und welche Aufgaben sie erfüllen. Wie auf Abbildung 4.1 zu sehen befindet sich der Networklayer zwischen dem Applicationlayer und dem Logical Link Control oder MAC-Layer. Das Protokoll das auf dem MAC-Layer läuft ist das, in der WLAN-Technik häufig genutzte CSMA/CA, das als bekannt vorausgesetzt wird. Es wird verwendet da sich mehrere Kommunikationseinheiten das selbe Medium teilen und es daher zu Kollisionen kommen kann.

### 4.0.2.1 Location Table

Jedes Fahrzeug verfügt über einen Location Table. In dieser Tabelle werden Informationen über die naheliegenden Knoten, also andere Fahrzeuge die C2C unterstützen, gespeichert. Diese Tabelle ist für das Forwarding notwendig da hier unter anderem die Adressen und Positionen der zu erreichenden Fahrzeuge gespeichert sind. Im Folgenden werden einige der Informationen aufgeführt die in einer solchen Tabelle enthalten sind. Jedoch können noch weitere Informationen dort gespeichert werden. Das genaue Format der Datensätze ist nicht spezifiziert und kann somit von diesem Dokument abweichen. Die Daten die in dem Location Table gespeichert sind sind nur zeitweise

Dateiendung von  
zu png geändert

neighbor tabelle  
mit einbeziehen  
7.1 da steht was  
alles drin ist

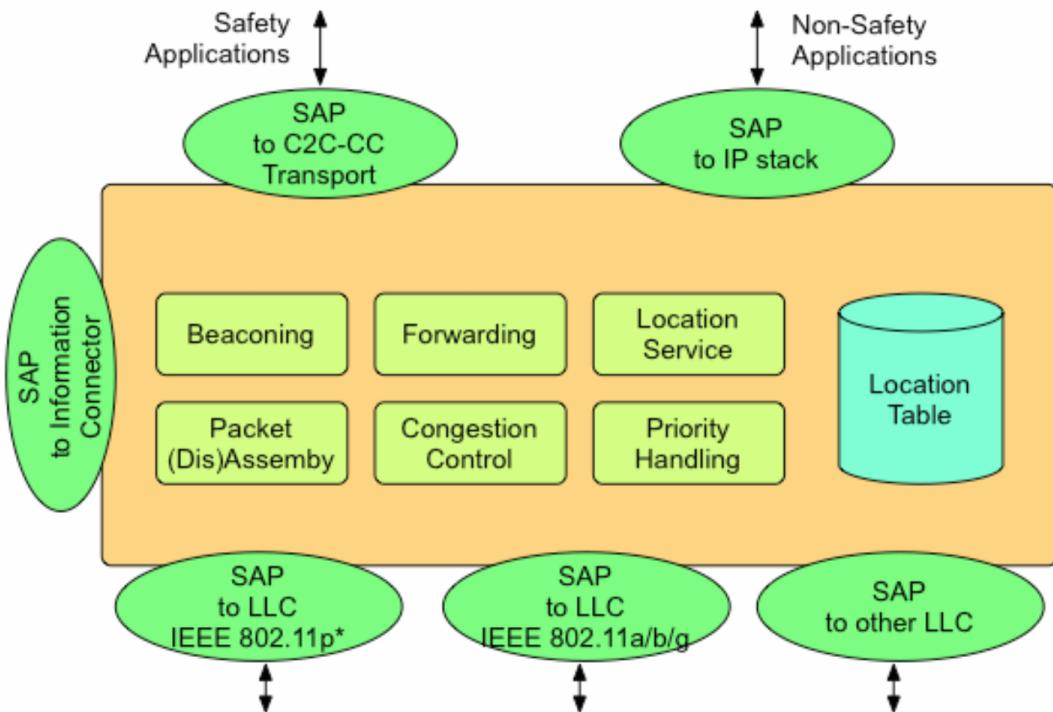


Abbildung 4.1: Die Komponenten des Networklayers[3]

korrekt, daher sind sie mit einem Timestamp versehen und werden nach einer gewissen zeit verworfen. Die Informationen des Positionsvektors sollten mindestens über die unten aufgeführten Informationen verfügen.

1. C2C Netzwerkadresse
2. MAC Adresse
3. IPv6 Adresse
4. Positionsvektor
  - a) Geschwindigkeit
  - b) Heading
  - c) Geo. Position
  - d) Zeitstempel des Vektors
  - e) Genauigkeit des Vektors
5. Version des Protokolls
6. Typ des Fahrzeuges
7. Zeitstempel des zuletzt erhaltenen Paketes
8. Datenrate des ITS
9. Direkter Nachbar Flag

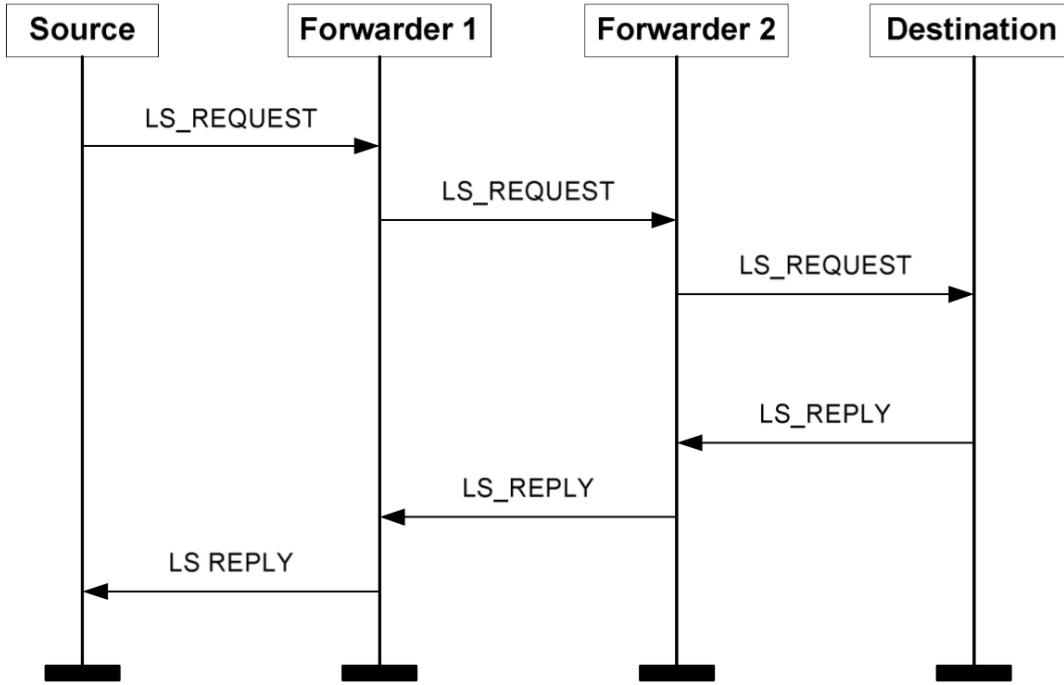


Abbildung 4.2: Ablauf einer Anfrage des Location Service

#### 4.0.2.2 Beaconing

Um die Informationen in der Location Table zu füllen sendet jedes Fahrzeug im periodischen Abstand eine sogenannten Beacon-Nachricht an seine Umgebung. In dieser Nachricht sind die oben aufgeführten Informationen enthalten. Dadurch wird die Location Table von dem empfangenden Fahrzeug aktualisiert.

#### 4.0.2.3 Forwarding

Der Networklayer unterstützt verschiedene Arten von Forwarding Algorithmen diese werden im späteren Kapitel Abschnitt 4.2 genauer erläutert.

#### 4.0.2.4 Location Service

Da es durchaus vorkommen kann das der Location Table leer ist aber dennoch eine Nachricht gesendet werden muss, d.h. es wird nach einer Weiterleitungsmöglichkeit gesucht, existiert der Location Service. Über diese kann explizit nach Informationen eines Knoten gefragt werden der die Nachricht weiterleiten kann. Im vergleich zu den Beacon-Nachrichten ist der Location Service eher ein On-Demand Dienst der für Routenaufbau zuständig ist. In Abbildung 4.2 ist erkennbar wie über den Location Service Informationen des Ziels über zwei Forwarding Knoten abgerufen wird.

#### 4.0.2.5 Priority Handling

Anhand der Paketpriorität wird entschieden wie mit dem Paket verfahren wird. Damit wichtige Pakete zuerst gesendet werden können und andere dennoch empfangen werden

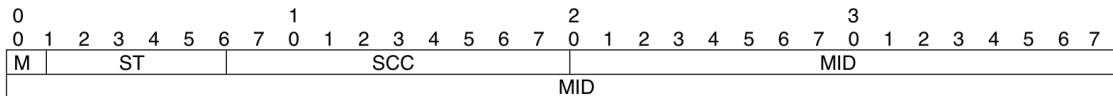


Abbildung 4.3: Format der Geo Networking Adresse

gibt es eine Paketqueue in die die unwichtigeren Nachrichten eingereiht werden.

#### 4.0.2.6 Packet Assembly

Da sich beim versenden von Paketen die eigenen Positionsangaben sowie die Hops oder Time-to-Live ändern, muss der Networklayer dafür sorgen das die Pakete beim weitersenden modifiziert oder aktualisiert werden. Hierfür werden die Informationen aus der Location Table verwendet bevor das Paket weiter gesendet wird.

#### 4.0.2.7 Congestion Control

Da die Paketdichte in einem C2C-Netz sehr hoch werden kann und es zu Überläufen oder Paketstaus kommen kann, muss in extremen Situationen das Netz reguliert werden. Hierauf wird in Abschnitt 4.1 genauer eingegangen.

### 4.1 Congestion Control

er nochmal  
hacken ob es  
ächlich keine  
ng gibt  
  
die gibts, nennt  
DCC und wird  
Management  
er erklärt

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/connectionless), 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.

### 4.2 Geo Routing

Um in der Car-to-Car Kommunikation die richtigen Routen zu finden und die Ziele zu adressieren benötigt jeder Teilnehmer in dem Netzwerk eine einmalige Adresse. Diese ist als Geo Networking Adresse spezifiziert.

#### 4.2.1 Adressierung

Die Geo Networking Adresse besteht aus acht Bytes die verschiedene Informationen repräsentieren. Die ersten zwei Bytes zeigen ob die Adresse manuell oder Automatisch konfiguriert wurde, um was es sich für ein Fahrzeug handelt und den ITS-S Country Code. Die restlichen sechs Bytes repräsentieren die MAC Adresse.[6] Die auf der Abbil-

dung 4.3 zu sehenden Felder sind in der nachfolgenden Tabelle 4.1 noch einmal genauer erläutert.

Feld	Feldname	Bedeutung
1	M	wird auf 1 gesetzt wenn die Adresse manuell vergeben worden ist, andernfalls au
2	ST	Identifiziert um was es sich für eine ITS handelt
3	SCC	ITS-S Country Code
4	MID	erster Teil der MAC-Adresse
5	MID	zweiter Teil der MAC-Adresse

Tabelle 4.1: Felder und Bedeutung der GNW Adresse[6]

Für das zweite Feld ST sind folgende Werte in Tabelle 4.2 spezifiziert.

Nummer	Bedeutung
0	Unknown
1	Pedestrian
2	Cyclist
3	Moped
4	Motorcycle
5	Passenger Car
6	Bus
7	Light Truck
8	Heavy Truck
9	Trailer
10	Special Vehicle
11	Tram
15	Road Side Unit

Tabelle 4.2: Werte für Feld zwei der GNW Adresse[6]

- Geschwindigkeit
- Heading
- Geo. Position
- Zeitstempel des Vektors
- Genauigkeit des Vektors

#### 4.2.1.1 Konfiguration der Adressen

Um eine Geo Networking Adresse zu konfigurieren gibt es drei Vorgehensweisen.

1. Auto-address configuration
2. Managed address configuration
3. Anonymous address configuration

siehe etsi Kapitel  
9.2.1 duplicate address detection is  
auch interessant

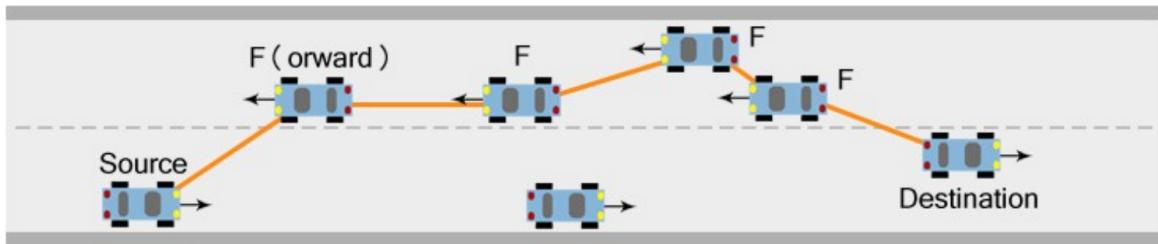


Abbildung 4.4: Geo Unicast [4]

Für die beiden ersten Verfahren ist das Duplicate address detection vorgesehen um zu verhindern das Adressen mehrfach vorkommen. Bei dem ersten Verfahren wird die Adresse automatisch von dem Fahrzeug generiert und sollte im nachhinein nur noch bei Duplicate address detection geändert werden. Managed address configuration stellt eine Anfrage an die ITS Networkung & Transport Layer Management entity um seine Adresse zu konfigurieren. Hier darf die Adresse erneut von dem Fahrzeug angefordert werden oder die ITS Networkung & Transport Layer Management entity sendet diesem eine neue. Das anonyme Verfahren erlaubt es dem Fahrzeug eine anonyme Adresse zu konfigurieren die von einer Sicherheitseinheit kontrolliert wird.

Über ist das  
anonyme Verfahren?  
Leider nix im  
Sicherheitseinheit  
und soll man  
noch was über  
ITS Networkung  
Transport Layer  
Management entity  
einbeziehen?

#### 4.2.1.2 Duplicate address detection

Um zu gewährleisten das die Geo Networking Adresse tatsächlich einzigartig ist, kommt die Duplicate address detection zum Einsatz. Sobald ein Empfänger eine Nachricht erhält. Vergleicht er seine eigene Geo Networking Adresse mit der des Paketes und danach die beiden MAC Adressen. Bei Übereinstimmung fordert er eine neue MAC-Adresse an. Und teilt dem System mit das eine Doppelte Adresse vorgefunden wurde. [6]

#### 4.2.2 Geo Unicast

Um einen einzelnen Knoten zu adressieren wird der Geo Unicast spezifiziert. Die Autos die zwischen Sender und der Empfangseinheit liegen dienen als Zwischenstationen. Über den Geo Unicast werden Nachrichten entweder über einen Hop an das Ziel gesendet oder über Zwischenstationen mit mehreren Hops. Die Nachricht kann bei den Zwischenstationen verändert werden. Das heisst zwei oder mehr Nachrichten werden zu einer zusammengefasst bevor sie weitergesendet werden. Dieser Vorgang ist auch umgekehrt durchführbar, sodass eine Nachricht aufgeteilt werden kann. Der Inhalt der Nachricht kann ebenfalls verändert oder Informationen hinzugefügt werden.

#### 4.2.3 Topologically-scoped broadcast

Der Topologically-scoped broadcast sendet einen Nachricht mit einem bestimmten Hop Count an alle um den Knoten erreichbaren Einheiten. Diese Nachricht wird dann von den Knoten empfangen, bei denen der Hop Count endet.

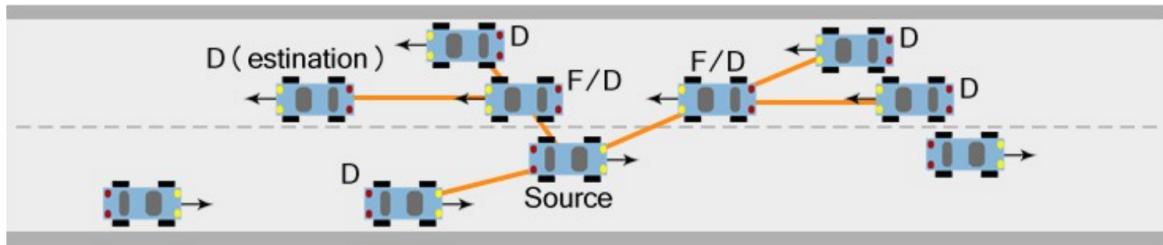


Abbildung 4.5: Topologically-scoped broadcast mit Hop Count 2 [4]

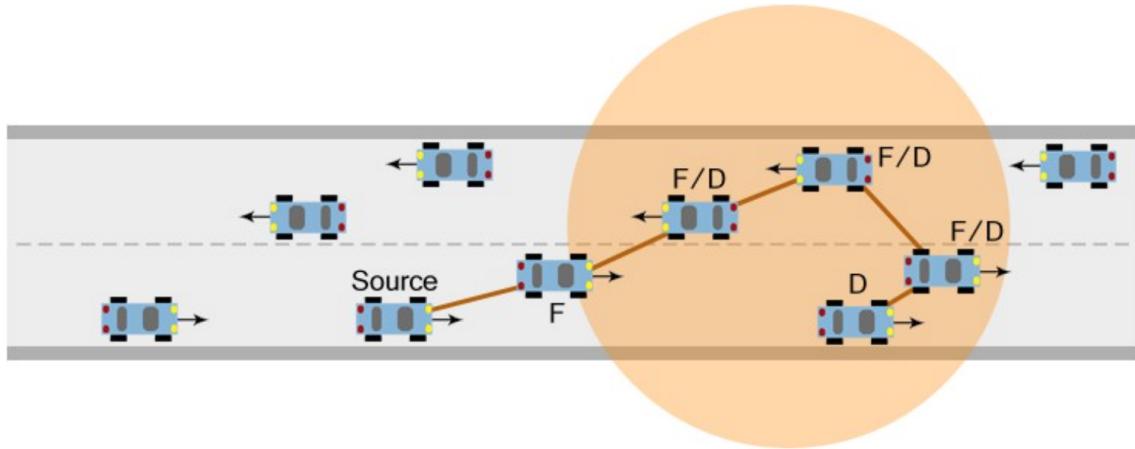


Abbildung 4.6: geographically-scoped broadcast [4]

#### 4.2.4 Geographically-scoped broadcast

Über den Geographically-scoped broadcast ist es einem Knoten möglich, um sich herum oder in einer bestimmten Entfernung zu sich selbst eine definierte Region zu erreichen. Dabei spielt die Anzahl der Hops keine Rolle und alle in dem Bereich liegenden Fahrzeuge sollen sich angesprochen fühlen.

#### 4.2.5 Geographical Scoped Anycast

Der Geographical Scoped Anycast ist ähnlich zu dem Geographically-scoped broadcast nur das hier die Nachricht nicht weitergeleitet wird sondern das Routing stoppt sobald ein Ziel innerhalb der Region die Nachricht empfangen hat.

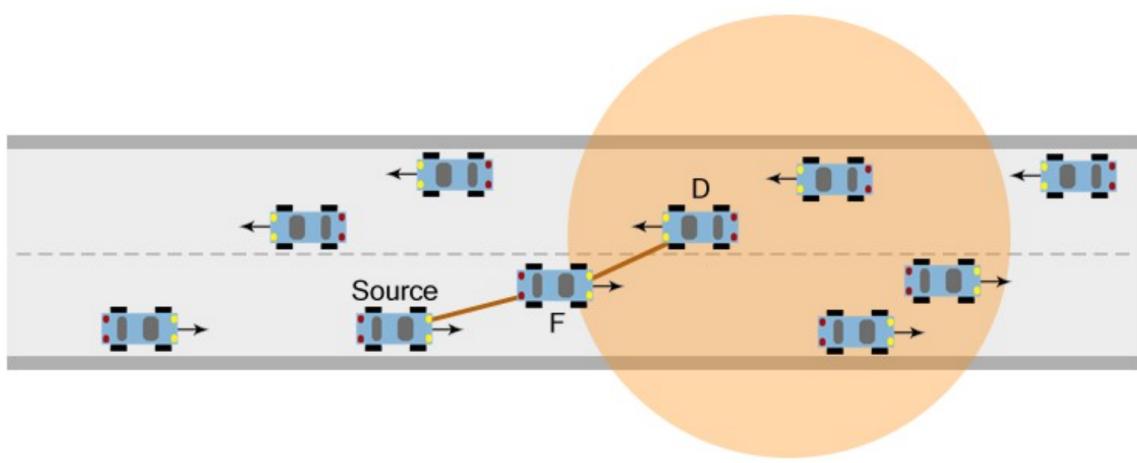


Abbildung 4.7: geographically-scoped anycast [4]

# 5 Facility Layer

Der Facility Layer in der C2C übernimmt unter anderem die Aufgaben des Application, Presentation und Session Layers des OSI Models. Dazu gehört vor allem das verschlüsseln von Nachrichten.

Cooperative Awareness Message (CAM), Decentralized Environmental Notification Message (DEN), Signal Phase and Timing (SPaT) und Topology Specification (TOPO) übertragen

## 5.1 CAM

## 5.2 DEN

## 5.3 SPaT

## 5.4 TOPO

Applicationlayer einführen, die use cases zu den 3 Kategorien sind geschaffen



# 6 Application layer und Use Cases

Die Car-to-Car Kommunikation bietet eine große Vielfalt an verschiedenen Einsatzmöglichkeiten.

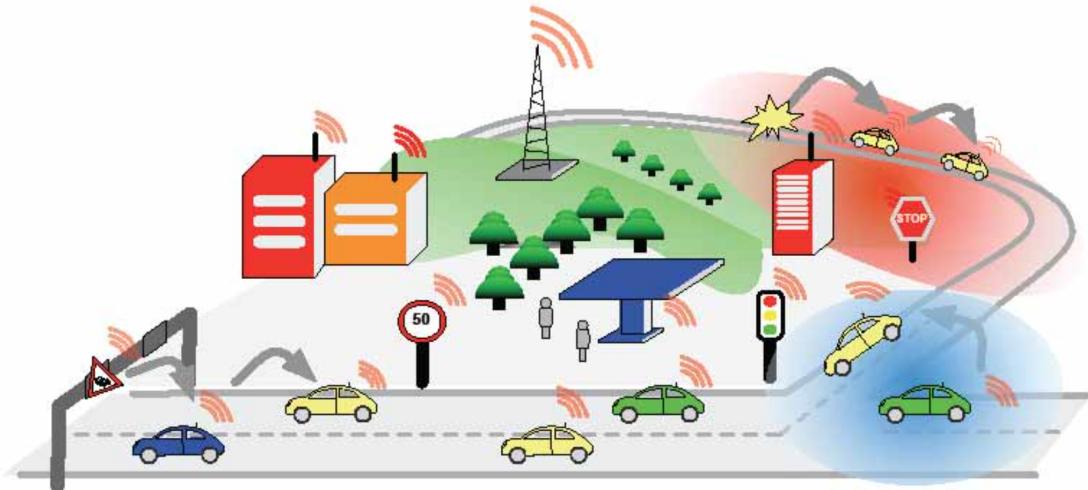


Abbildung 6.1: Die Komponenten der Car-to-Car Kommunikation

Da es sich bei dem gesamten Projekt nicht nur darum handelt das Fahrzeuge untereinander kommunizieren, sondern wie auf Abbildung 6.1 zu sehen auch andere Verkehrs komponenten. Um das Zusammenspiel der Komponenten besser zu verstehen und zu sehen wie groß das Potential der Car-to-Car Kommunikation ist, werden im folgenden mehrere Szenarien aufgezählt und erklärt.

## 6.1 Use cases

### 6.1.1 Sicherheitsbedingt

Sicherheitsbedingte Szenarien sind Fälle bei denen ein Möglicher Unfall verhindert werden kann. Im Folgenden werden drei Szenarien erklärt bei denen das Unfallrisiko minimiert werden kann.

#### 6.1.1.1 Cooperative Forward Collision Warning

Einer der häufigsten Ursachen für Verkehrsunfälle sind plötzliche Bremsmanöver von Vorräusfahrenden Fahrzeugen und die Unaufmerksamkeit eines Fahrers. Aus diesen Ursachen besteht ein erhöhtes Risiko für Auffahrungen. Cooperative Forward Collision Warning versucht genau dieses Risiko zu vermindern. Um dies zu vollbringen überwacht jedes Fahrzeug die eigenen Informationen, wie die Geschwindigkeit, Richtung und Position und vergleicht diese mit den Daten der anderen Fahrzeugen. Bei

Auffälligkeiten und Abweichungen warnt das System dem Fahrer frühzeitig vor einer möglichen Kollision. Diese Warnung kann durch auditive, visuelle oder haptische Alarne signalisiert werden. Da es durchaus sein kann das noch Fahrzeuge, die nicht in dem C2C Netz kommunizieren, unterwegs sind, können über Objekterkennungssensoren diese ebenfalls identifiziert werden. Dadurch sinkt das Risiko noch einmal für die C2C Teilnehmer. Die Informationen werden innerhalb von 20 bis 200 meter geteilt womit auch genug Zeit bleibt um diese Auszuwerten und den Fahrer frühzeitig zu informieren.

### **6.1.1.2 Pre-Crash Sensing/Warning**

Natürlich können nicht alle Unfälle durch die Cooperative Forward Collision Warning vermieden werden. Daher ist davon auszugehen das dennoch Auffahrunfälle geschehen werden. Dafür hat man sich das Pre-Crash Sensing/Warning Szenario ausgedacht, bei dem man von einem Unvermeidbaren Unfall ausgeht. Dies soll durch die Car-to-Car Kommunikation erkannt und Vorbereitungen für den Unfall getroffen werden. Damit dieses System funktioniert muss wie bei dem vorherigen Szenario dauerhaft Informationen der Fahrzeuge ausgetauscht werden. Dabei geht man davon aus das die Informationen der Fahrzeuge die sich im Umkreis von 20 bis 100 meter befinden überwacht werden müssen. Entdeckt das System einen unvermeidbaren Unfall muss sichergestellt sein das diese Fahrzeuge die kollidieren werden sicher miteinander kommunizieren können um Daten wie die, Fahrzeuggröße und genaue Position bekannt zu geben. Über diese Informationen können dann Sicherheitsmaßnahmen wie Airbag, Gurtstraffer oder erweiterbare Stoßstangen gesteuert werden und effektiv genutzt werden.

### **6.1.1.3 Hazardous Location C2C Notification**

Die Hazardous Location C2C Notification soll dafür sorgen das gefährliche Fahrpassagen weitergegeben werden. Das heißt das System warnt nachkommende Fahrzeuge vor glatten Straßen oder Schlaglöchern. Die Schwierigkeit hierbei ist die Gewinnung der Informationen. Als Beispiel wird genannt das ein Fahrzeug das auf einer glatten Straße fährt und das ESP einsetzt, speichert an welcher Stelle, Geschwindigkeit etc. eingetreten ist und diese Nachricht dann weiter sendet. Fahrzeuge die diese Warnnachricht erhalten können dann auf den Umstand mit Verbesserung der Sicherheitsmaßnahmen reagieren oder zumindest dem Fahrer darüber informieren.

## **6.1.2 Verkehrseffizienz**

Die Effizienz des Verkehrs zu steuern ist der ursprüngliche Sinn der Car-to-Car Kommunikation. Durch die bessere Leitung des Verkehrs entstehen weniger Staus auf den Straßen, was zu verminderten Stresssituationen für Fahrer führt. Dadurch entstehen verkürzte Wartezeiten für die Teilnehmer am Verkehr und geringere Wartungskosten für die Straßen. Außerdem kann dadurch die Umwelt mehr geschont werden und die Energiekosten sinken.

### **6.1.2.1 Enhanced Route Guidance and Navigation**

Navigation ist ein großes Thema das bereits über Navigationssysteme stark verbessert wurde. Enhanced Route Guidance and Navigation soll die Navigation noch ein-

mal verbessern. Dies soll erreicht werden in dem die Fahrdaten von den Roadside Stations gesammelt und ausgewertet werden. Dadurch können Verkehrsaufkommenisse vorhergesagt werden und Fahrzeuge auf ihrem Weg an einer solche Station vorbeikommen können über die aktuellen Verkehrsinformationen aufgeklärt werden und den effektivsten Weg berechnen um die Verkehrsdichte zu verbessern. Damit dieses Szenario funktioniert müssen die Roadside Stations die Möglichkeit besitzen vorbeifahrende Fahrzeuge zu erkennen und zu informieren.

### **6.1.2.2 Green Light Optimal Speed Advisory**

Green Light Optimal Speed Advisory beschäftigt sich mit der optimalen Geschwindigkeit zwischen Ampeln. Damit Fahrzeuge zwischen Ampelabschnitten nicht die Geschwindigkeit reduzieren und nach Möglichkeit nicht immer wieder neu Anfahren müssen, kann durch eine Kreuzung die an der Car-to-Car Kommunikation teilnimmt Informationen über die Rot-Grün Schaltzeit eingeholt werden. Über den bekannten Abstand zum vorherfahrenden Auto kann die optimale Geschwindigkeit berechnet werden, die das Fahrzeug sich vorwärts bewegen sollte um während einer Grünphase der Ampel dort einzutreffen. Dadurch wird der Verkehrsfluss verbessert und schont die Tankfüllung eines Autos.

### **6.1.2.3 C2C Merging Assistance**

Bei einfahren in den Verkehr von kann es vorkommen das ein Fahrzeug den fliesenden Verkehr stört. Dadurch entstehen nicht selten Rückstaus die im schlimmsten Fall zu Auffahrunfällen führen. Dies soll über C2C Merging Assistance bereits beim einfahren in den fliesenden Verkehr verhindert werden, in dem das Fahrzeug das in den Verkehr einfliessen möchte die betroffenen Fahrzeuge darüber informiert. Die Fahrzeuge die betroffen sind sollen ihre ihre Geschwindigkeit automatisch reduzieren oder zumindest sollen die Fahrer darüber informiert werden wie sie sich am besten Verhalten sollen. Dadurch kann der Verkehr weiter sauber fliesen ohne das es im Nachhinein zu einem stillstand kommt.

## **6.1.3 Infotainment und andere**

Hier werden die Anwendungsfälle aufgeführt die nicht zur Sicherheit oder Verkehrseffizienz beitragen aber dennoch über die Car-to-Car Kommunikation realisiert werden. Dazu gehören allgemeine Informationen, Entertainment oder Fahrzeugdaten wie der Verbrauch reduziert werden kann.

### **6.1.3.1 Internet Access in Vehicle**

Hierbei wird die im Fahrzeug vorhandene Hardware, die dafür da ist mit den anderen Fahrzeugen und Komponenten der Car-to-Car Kommunikation zu kommunizieren, dafür genutzt um über die Roadside Station ihren Border Gateway auf das Core Netzwerk zuzugreifen und damit auf sämtliche Dienste des Internets. Das bedeutet das alle IP basierten Dienste in einem Fahrzeug nutzbar sind.

Hier nochmal in manifest nachles

### **6.1.3.2 Point of Interest Notification**

Dieser Anwendungsfall ist besonders für Kommerzielle Werbezwecke interessant. Hier werden durch eine Roadside Station Informationen über für den Fahrer interessante Orte zu den Umliegenden Fahrzeugen gesendet. Die Masse an Informationen kann durch das Fahrzeug gefiltert werden und immer Situationsbedingt die passenden Orte vorgeschlagen werden. Zum Beispiel wenn der Benzinstand des Fahrzeuges niedrig ist können die in der Nähe befindlichen Tankstellen mit Öffnungszeiten und Preisen dem Fahrer vorgeschlagen werden. Dadurch wird die Werbung deutlich effektiver da die Zielgruppe richtig gewählt wird und sich in der unmittelbaren Umgebung aufhält.

### **6.1.3.3 Remote Diagnostics**

Der Remote Diagnostics Anwendungsfall beschreibt ein Szenario zum Warten des Autos ohne dafür in eine Werkstatt fahren zu müssen. Dadurch können Informationen über das Fahrzeug abgerufen werden und mit Hilfe der Problembeschreibung des Fahrers kann schnell festgestellt werden um was es sich handelt. Die Daten über Werkstattbesuche und was an dem Auto angefallen ist soll alles in eine Datenbank geschrieben werden sodass die Werkstatt die das Fahrzeug wartet immer weiß was gemacht worden ist. So wird die Zeit die für die Wartung eines Fahrzeugs reduziert und damit auch die Länge des Besuches in der Werkstatt für den Kunden. Um die Software eines Autos aktuell zu halten wird überhaupt kein Werkstattbesuch mehr benötigt, da das Update direkt beispielsweise über das Internet geladen werden kann.

<b>ASN.1</b>	Abstract Syntax Notation One
<b>AU</b>	Application Unit
<b>C2C</b>	Car-to-Car Kommunikation
<b>CCU</b>	Communication & Control Unit
<b>CTX</b>	Service Context Message
<b>DCC</b>	Decentralized Congestion Control
<b>DENM</b>	Decentralized Environmental Notification Message
<b>GNW</b>	Geo Networking
<b>ICS</b>	ITS Central Station
<b>ID</b>	Identifikator
<b>IRS</b>	ITS Roadside Station
<b>ISO</b>	International Organization for Standardization
<b>ITS</b>	Intelligent Transportation Systems
<b>IVS</b>	ITS Vehicle Station
<b>OSI</b>	Open System Interconnection
<b>PDA</b>	Personal Digital Assistant
<b>PSS</b>	Personal Subsystem and Station
<b>RSU</b>	Roadside Unit
<b>SAM</b>	Service Advertisement Message
<b>SAP</b>	Service Access Point
<b>sim<sup>TD</sup></b>	Sichere Intelligente Mobilität Testfeld Deutschland



# Literatur

- [1] Roberto Baldessari u. a. »Car-2-car communication consortium-manifesto«. In: *DLR Electronic Library [http://elib. dlr. de/perl/oai2]/(Germany)* 3.4 (2007), S. 4.
- [2] CALM - Continuous Communication for Vehicles. *ITS Netzwerk Übersicht*. <http://calm.its-standards.eu>.
- [3] CAR 2 CAR Communication Consortium. »Manifesto«. In: (2007).
- [4] EN ETSI. »102 636-1(V1.1.1)«. In: (2010).
- [5] EN ETSI. »302 665 (V1. 1.1),“ « in: *Intelligent Transport Systems (ITS)* (2010).
- [6] EN ETSI. »ETSI EN 302 636-4-1 V1.2.1«. In: (2014).
- [7] EN ETSI. »Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 2: Management information base«. In: *Intelligent Transport Systems (ITS)* (2012).
- [8] EN ETSI. »Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture«. In: (2014).
- [9] ETSI, EN. *ETSI EN 302 665; Intelligent Transport Systems (ITS); Communications Architecture*. V1.1.1 (2010-09). European Telecommunications Standards Institute. 2010.
- [10] ETSI, EN. *Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*. European Telecommunications Standards Institute. 2012.
- [11] ETSI, TS. *ETSI TS 102 731; Intelligent Transport Systems (ITS); Security; Security Services and Architecture*. V1.1.1 (2010-09). European Telecommunications Standards Institute. 2010.
- [12] ETSI, TS. *ETSI TS 102 940; Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*. V1.1.1(2012-06). European Telecommunications Standards Institute. 2012.
- [13] ETSI, TS. *ETSI TS 102 941; Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*. V1.1.1 (2012-06). European Telecommunications Standards Institute. 2012.
- [14] ETSI, TS. *ETSI TS 103 097, Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. V1.1.1(2013-04). European Telecommunications Standards Institute. 2013.
- [15] ETSI, TS. *Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part*. European Telecommunications Standards Institute. 2011.
- [16] ETSI, TS. *Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 2: Management information base*. European Telecommunications Standards Institute. 2012.

- [17] ETSI, TS. *Intelligent Transport Systems (ITS); Vehicular Communications; Geo-Networking; Part 3: Network architecture*. European Telecommunications Standards Institute. 2010.
- [18] Felix Graf. »Seminar Sommersemester 2009 Automotive Konzepte und Techniken«. In: (2009).
- [19] Hagen Stübing – Adam Opel GmbH (Editor), Marc Bechler – BMW Group Forschung und Technik (Editor), Stephan Buchta – Adam Opel GmbH (Editor), Bechir Allani – Hochschule für Technik und Wirtschaft des Saarlandes, Thomas Baum – Hochschule für Technik und Wirtschaft des Saarlandes, Thomas Biehle – Volkswagen AG Norbert Bißmeyer – Fraunhofer SIT, Murat Caliskan – Volkswagen AG, Kurt Eckert – Robert Bosch GmbH, Jörg Freudenstein – Albrecht Consult GmbH, Manuel Fünfrocken – Hochschule für Technik und Wirtschaft des Saarlandes, Martin Goralczyk – Technische Universität Berlin, Matthias Haug – Robert Bosch GmbH, Florian Häusler – Technische Universität Berlin, Dieter Heussner – Hessisches Landesamt für Straßen- und Verkehrswesen, Andreas Hiller – Daimler AG, Arno Hinsberger – Hochschule für Technik und Wirtschaft des Saarlandes, Attila Jaeger – Technische Universität Darmstadt, Josef Kaltwasser – Albrecht Consult GmbH, Volker Kanngießer – Stadt Frankfurt am Main, Anselm Keil – Continental Teves AG & Co ohG, Carsten Kemper – Gevas Software GmbH, Sascha Kilb – T-Systems, GEI GmbH, Oliver Klages – ICT Software Engineering Nord GmbH, Felix Klanner – BMW Group Forschung und Technik, José Luis Mateo – T-Systems, GEI GmbH, Manuel Mattheß – Fraunhofer SIT, Thomas May – Robert Bosch GmbH, Marc Menzel – Continental Teves AG & Co ohG, Karl Naab – BMW AG, Carsten Neumann – Fraunhofer FOKUS, Anastasia Petrou – BMW Group Forschung und Technik, Ilja Radusch – Technische Universität Berlin, Horst Rechner – Fraunhofer FOKUS, Oliver Sawade – Fraunhofer FOKUS, Gunter Schaaaf – Robert Bosch GmbH, Björn Schünemann – Technische Universität Berlin, Winfried Stephan – T-Systems GEI GmbH, Markus Trauberg – ICT Software Engineering Nord GmbH, Peter Vogel – Robert Bosch GmbH, Jonas Vogt – Hochschule für Technik und Wirtschaft des Saarlandes, Michael Wagner – Adam Opel GmbH, Sebastian Weber – Hochschule für Technik und Wirtschaft des Saarlandes, Peter Zahn – BMW Group Forschung und Technik, Jens Zech – TU Berlin. *Projektergebnis: Validierungsziele*. [http://www.simtd.de/index.dhtml/deDE/backup\\_publications/Projektergebnisse.html](http://www.simtd.de/index.dhtml/deDE/backup_publications/Projektergebnisse.html). 2009.
- [20] ISO. *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 5: Fast service advertisement protocol (FSAP)*. First edition 2013-07-01. International Organisation for Standardization. 2013.
- [21] Michelle Wetterwald, Fatma Hrizi und Pasquale Cataldi. »Cross-layer identities management in ITS stations«. In: *ITST 2010, 10th IEEE International Conference on ITS Telecommunications, November 9-11, Kyoto, Japan*. Kyoto, JAPON, Nov. 2010. URL: <http://www.eurecom.fr/publication/3205>.

# Abbildungsverzeichnis

2.1	Überblick über die Komponenten [5] . . . . .	10
2.2	Überblick über die Layer eines ITS Gateways [5] . . . . .	11
2.3	Überblick über die Layer eines ITS Hosts [5] . . . . .	11
2.4	Überblick über die Layer eines ITS Border Routers [5] . . . . .	12
3.1	Überblick über die externen Netzwerke [8] . . . . .	15
3.2	Netzwerkszenario mit dazugehöriger Implementierung [8] . . . . .	17
3.3	Der Vergleich zwischen ITS und OSI [12] . . . . .	19
3.4	Darstellung der ITS Station Reference Architecture [5] . . . . .	20
3.5	Darstellung des ITS G5 Access Layers citeen302665 . . . . .	20
3.6	Der Management Layer im Überblick [5] . . . . .	23
3.7	Darstellung eines SAM Pakets . . . . .	24
3.8	Darstellung eines CTX Pakets . . . . .	24
3.9	Ablauf der Phasen des Fast Service Advertisement Protocol [20] . . . . .	26
3.10	Die Architektur von DCC [15] . . . . .	27
4.1	Die Komponenten des Networklayers[3] . . . . .	36
4.2	Ablauf einer Anfrage des Location Service . . . . .	37
4.3	Format der Geo Networking Adresse . . . . .	38
4.4	Geo Unicast [4] . . . . .	40
4.5	Topologically-scoped broadcast mit Hop Count 2 [4] . . . . .	41
4.6	geographically-scoped broadcast [4] . . . . .	41
4.7	geographically-scoped anycast [4] . . . . .	42
6.1	Die Komponenten der Car-to-Car Kommunikation . . . . .	45