HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Hanna Engelhardt

Analyse sicherheitsrelevanter Aspekte von Car2X Protokollen

2018

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Analyse sicherheitsrelevanter Aspekte von Car2X Protokollen

Autorin:
Hanna Engelhardt

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO15w3-B

Erstprüfer:
Prof. Dr. rer. nat. Christian Hummert

Zweitprüfer:
Dipl.-Ing. Heiko Polster

Mittweida, 09 2018

Bibliografische Angaben

Engelhardt, Hanna: Analyse sicherheitsrelevanter Aspekte von Car2X Protokollen, 73 Seiten, 27 Abbildungen, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften

Bachelorarbeit, 2018

Referat

Die Aufgabe der V2X-Kommunikation ist es, zukünftig die Sicherheit und Effizienz im Straßenverkehr zu erhöhen. Das Ziel dieser Arbeit besteht darin, sicherheitsrelevante Aspekte von Car2X Protokollen zu analysieren. Grundlage bildet hier der europäischen ETSI-Standard. Da es sich bei dieser Arbeit um eine Literaturrecherche handelt, werden zu diesem Zweck die Veröffentlichungen des Standards herangezogen. Zunächst wird das Netzwerk aufgezeigt, in dem die Kommunikation zwischen den Fahrzeugen und der Infrastruktur stattfindet. Anschließend werden wichtige Protokolle analysiert und verschiedene Angriffspunkte untersucht. Die verschiedenen Angriffe werden mit anderen Forschungsarbeiten verglichen und analysiert. In dieser Arbeit wurde festgestellt, dass trotz spezieller Sicherheitsvorkehrungen, Angriffe auf das Netzwerk und die Protokolle möglich sind.

Englischer Titel

Analysis of security relevant aspects in Car2X protocols

Abstract

The use of V2X communication is intended to make roads more secure and efficient. This work aims to critically evaluate the security relevant aspects in car2x protocols, and is based on ETSI's globally applicable Standards. This work will review the current literature and use the current publications of standards for this purpose. It begins by outlining the network in which communication between vehicles and infrastructure takes place. Several important protocols are analysed and various points of attack are highlighted and examined. Different attacks are then compared and analysed with other research. This work found that despite the security mechanisms in place there remains a possibility of attack on networks and protocols.

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis

III. Tabellenverzeichnis

IV. Abkürzungsverzeichnis

AA	Authorization Authority
AC	Access Category
AT	Authorization Ticket
AITS	Arbitration Inter Frame Space
BTP	Basic Transport Protocol
CA	Certificate Authority
CAM	Cooperative Awareness Message
CCDF	Complementary Cumulative Distribution Function
CCH	Control Channel
CENELEC	Comité Européen de Normalization Electrotechnique
C-ITS	Cooperative Intelligent Transport System
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
DCC	Decentralized Congestion Control
DCF	Distributed Coordination Function
DENM	Decentralized Environmental Notification Message
DFS	Dynamic Frequency Selection
DUA	Device under attack
EA	Enrollment Authority
EC	Enrollment Certificate
ECDSA	Elliptic Curve Digital Signature Algorithm
EDCA	Enhanced Distribution Coordination Access

ETSI	European Telecommunication Standards Institute
EEBL	Emerging Electronic Brake Light
GAC	Geographically-Scoped Anycast
GBC	Geographically-Scoped Broadcast
GN	GeoNetworking
GN6ASL	GeoNetworking to IPv6 Adaptation Sub-Layer
GUC	Geographically-Scoped Unicast
GVL	Geographical Virtual Link
HST	Header Sub-Type
HT	Header Type
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-AID	ITS-Application Identifier
ITS-S	ITS-Station
LDM	Local Dynamic Map
LS	Location Service
LT	LifeTime
MAC	Medium Access Control
MHT	Mutiple Hypothesis Tracking
MIB	Management Information Base
MTDA	Mean Time Ahead Distance
NH	Next Header

OBD	On-Board-Diagnose
OMNeT++	Objective Modular Network Testbed in C++
OSI	Open Systems Interconnection
PDU	Packet Data Unit
PL	Payload Length
POTI	Position and Time management
R2V	Roadside-to-Vehicle
RCA	Root Certificate Authority
RHL	Remaining Hop Limit
RLAN	Radio Local Area Network
SCH	Service Channel
SHB	Single Hop Broadcast
STRAW	STreetRAndomWaypoint
SUMO	Simulation of Urban MObility
SSP	Service Specific Permission
TDC	Transmit Datarate Control
TPC	Transmit Power Control
TraCI	Traffic Control Interface
TRC	Transmit Rate Control
TS	Time Slot
TSB	Topologically Scoped Broadcast
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network

V2I Vehicle-to-Infrastructure

V2V Vehicle-to-Vehicle

VANET Vehicular Ad Hoc Network

VDP Vehicle Data Provider

1 Einleitung

1.1 Motivation

Das Autofahren soll auch in Zukunft so sicher wie möglich gestaltet werden. Aus Statistiken geht hervor, dass sich die Anzahl von Fahrzeugen im Straßenverkehr häufen und somit die Verkehrsdichte immer mehr zunimmt. Dies hat den negativen Effekt, dass es zu Staus und Unfällen kommt, welche die Sicherheit der Verkehrsteilnehmer gefährden und zu Verspätungen führen.

In den Jahren zwischen 1970 und 2000 ist die Anzahl der Verkehrstoten und Verkehrsverletzten zurück gegangen. Dies ist auf die Implementierung verschiedener elektronischer Systeme wie beispielsweise dem Antiblockiersystem zurückzuführen. Aber auch passive Sicherheitsmethoden wie beispielsweise Airbags und Anschnallgurte bieten Personen Schutz, die in einen Unfall verwickelt sind [Popescu-Zeletin2010, Seite 17-18]. Trotz dieser Sicherheitsvorkehrungen liegt die Anzahl der Unfälle laut der Statistik noch relativ hoch [URL_1].

Verschiedene Forschungsgruppen aus unterschiedlichen Ländern arbeiten daran, die Sicherheit zu erhöhen und somit die Anzahl der Unfälle zu verringern. Dies ist ein Grund dafür, dass sich Forschungsgruppen immer mehr mit der Vernetzung von Fahrzeuge untereinander und der Vernetzung von Fahrzeugen mit der Infrastruktur beschäftigen. Diese Form der Kommunikation hat das Ziel, Autofahrer schon vor einem vermeintlichen Unfall über die Gefahrensituation zu informieren, um damit Schlimmeres zu verhindern.

Die Kommunikation wird mittels eines Nachrichtenaustausches realisiert. Diese Nachrichten beinhalten Informationen zur Verkehrslage.

1.2 Zielstellung

Die vorliegende Bachelorarbeit zielt darauf ab, einen Einblick in das Netzwerk zu vermitteln, in welchem zukünftig die Fahrzeugkommunikation stattfinden wird. Der Fokus liegt auf den Kommunikationsprotokollen.

Ziel dieser Arbeit ist es, Sicherheitslücken bzw. Angriffspunkte in den Protokollen und dem Netzwerk festzuhalten. Die Angriffe, die trotz der Sicherheitsmechanismen möglich sind, werden analysiert und mit anderen wissenschaftlichen Arbeiten verglichen.

1.3 Entwicklung in Europa

Neben Europa befassen sich sowohl die USA wie auch Japan mit dem Thema Cooperative Intelligent Transportation Systems.

In Europa markiert das Projekt PROMETHEUS im Jahr 1987 den Beginn eines kooperativen Fahrsystems [Festag2014]. In den 2000er-Jahren werden erneut weltweit Forschungen betrieben, da ab diesem Zeitraum GPS zur Verfügung steht.

Generell hat sich die Standardisierung in Europa und in den USA parallel entwickelt. Diese wurde auf beiden Kontinenten durch unterschiedliche Forschungsgruppen und Interessenvertreter unterstützt und demnach haben sich auch unterschiedliche Standards entwickelt.

In Europa haben verschiedene Forschungsgruppen an der Erprobung und der Entwicklung von Technologien mitgeholfen. Zu erwähnen sind hier beispielsweise FleetNet, PReVENT etc. [Fuchs2015, Seite 526]. Schließlich wurden Feldversuche durchgeführt, um die Auswirkung von C-ITS auf die Sicherheit und Effizienz im Straßenverkehr zu bewerten.

In Europa sind die Organisationen EN, ETSI und CENELEC für die Standardisierung zuständig, die dafür ein Mandat der Europäischen Union erhalten haben [Fuchs2015, Seite 528].

In den USA sind an dieser Stelle die Organisationen IEEE und SAE zuständig. In Japan ist dies ARIB [Fuchs2015, Seite 528].

1.4 VANET

Car2X, oder auch V2X ist die Kommunikation zwischen Fahrzeugen untereinander sowie zwischen Fahrzeugen und der Infrastruktur. Die Kommunikation zwischen den Fahrzeugen wird als Vehicle-to-Vehicle Kommunikation (V2V) bezeichnet, die zwischen den Fahrzeugen und der Infrastruktur als Vehicle-to-Infrastruktur (V2I) [Wang2012]. Zweck von V2X ist die Erhöhung der Sicherheit auf den Straßen sowie die Verminderung von Unfällen und die Verbesserung der Verkehrseffizienz. Dies soll durch ständigen Nachrichtenaustausch zwischen den Verkehrsteilnehmern realisiert werden.

Um die Kommunikation zwischen Fahrzeugen zu ermöglichen, bedarf es eines eigenen Netzwerkes, dem VANET (Vehicular Ad Hoc Network). Ein VANET ist ein Netzwerk, welches sich selbst aufbaut und organisiert [Tanuja2015]. Solch ein Netzwerk muss mit neuen technischen Herausforderungen umgehen können.

Im VANET stellen die Fahrzeuge die Knoten des Netzwerkes dar, welche in der Anzahl variieren können. Je nach Ortslage ist das Verkehrsaufkommen unterschiedlich stark und auch die Geschwindigkeit der Fahrzeuge variiert [Almalag2013, Seite 600].

Eine dauerhafte Kommunikation zwischen zwei Knoten kann nicht aufgebaut werden, da sich durch die permanente Änderung von Netzwerktopologien auch die Nachbarschaften ständig ändern [Schmidt2008].

Um all diesen Herausforderungen gerecht zu werden, wird der WLAN-Standard 802.11 erweitert (802.11p). Mit 802.11p soll beispielsweise eine größere Reichweite sowie die Vernetzung der Knoten bei hoher Geschwindigkeit ermöglicht werden [Dreßler2013].

Für die V2X Kommunikation kommen außerdem andere Netzwerkprotokolle als im Internet zum Einsatz [Schmidt2008]. Die Nachrichten werden hier an eine bestimmte Region geleitet und nicht an eine bestimmte Adresse [Schmidt2008]. Dabei ändern sich die Abstände und die Positionen der kommunizierenden Knoten ständig, dies ist im Internet nicht der Fall [Schmidt2008].

Nicht sicherheitsrelevante Nachrichten basieren meist auf IP und verwenden den TCP/IP Protokollstapel. Bei sicherheitsrelevanten Nachrichten ist dies jedoch nicht der Fall. Grund hierfür liegt unter anderem darin, dass der durch IPv6 erzeugte Overhead zu groß werden würde [Stanica2012]. IPv4 bietet einen zu kleinen Adressraum. Der genauere Protokollstapel wird in Abschnitt 1.5 erläutert.

Ein VANET besteht aus ITS-Stationen. Als solche bezeichnet man sowohl Stationen, die sich an der Straße befinden (Road Side Unit - **RSU**) als auch die Fahrzeuge selbst.

Jede Station enthält eine Communication & Control Unit (**CCU**) und eine Applicati-

on Unit (**AU**) [ETSI2010a]. Diese werden nachfolgend beschrieben.

CCU

CCUs sind Einheiten innerhalb der Fahrzeugvernetzung, die die Datenverbindung mit anderen Fahrzeugen und der Außenwelt herstellen [ETSI2014b].

Eine CCU implementiert den Protokollstapel. Sie muss mit mindestens einer externen Kommunikationsschnittstelle ausgestattet sein, um die Verbindung zum ITS ad-hoc Netzwerk oder zu anderen Netzwerken bereitzustellen [ETSI2014b].

Über eine oder mehrere interne Kommunikationsschnittstellen können AUs mit der CCU verbunden werden [ETSI2014b].

Eine CCU wird auch als On-board Unit bezeichnet [Schröder2013]. Sie kann weiter in logische Netzwerkkomponenten unterteilt werden, wie zum Beispiel in einen ad hoc Router, welcher für das Routen und die Paketweiterleitung verantwortlich ist [ETSI2014b].

AU

Eine AU kann fest im Auto eingebaut sein oder sich mit diesem dynamisch verbinden [CAR2007]. Dabei nutzt eine Application Unit die Kommunikationsfähigkeit der CCU [ETSI2014b]. Ein Beispiel für eine AU wäre das Navigationssystem oder der Laptop des Fahrers. Es besteht die Möglichkeit, dass sich mehrere AUs mit einer CCU im Fahrzeug verbinden.

RSU

RSU beschreibt ein Gerät, das sich an einer Straße befinden kann, aber auch an Orten wie Raststätten, Parkplätzen, Tankstellen usw. In den Aufgabenbereich der RSU fällt beispielsweise die Erweiterung der Kommunikationsreichweite [CAR2007].

Des Weiteren sind RSUs an die Infrastruktur eines Netzbetreibers angeschlossen. Somit können sie von Fahrzeugen als Gateway für eine Internetverbindung genutzt werden [Sandonis2016].

1.5 Architektur

Die Architektur nach europäischem Standard besteht aus vier horizontalen und zwei vertikalen Schichten (siehe Abbildung 1.1). Dabei handelt es sich um die Zugangsschicht,

gefolgt von der Netzwerk- und Transportschicht. Darauf aufbauend befindet sich die Facility-Schicht und schließlich die Anwendungsschicht.

Die Sicherheits- und Management-Schicht bilden jeweils die vertikalen Schichten, die schichtübergreifend auf die horizontalen Schichten zugreifen können. Diese Schichten werden nachfolgend weiter erläutert.

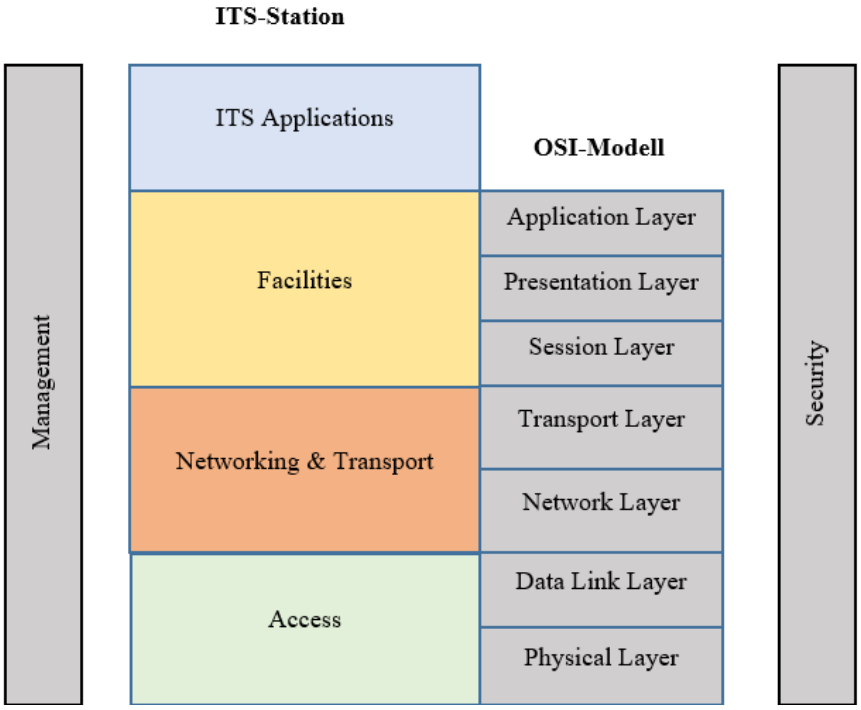

Abbildung 1.1: Zuordnung des OSI-Modells zur ITS-Architektur [Anlehnung an ETSI2012a]

1.5.1 Zugangsschicht (Access Layer)

Die unterste Schicht dieser Architektur wird als Access Layer bezeichnet. Sie spiegelt Schicht 1 und 2 des OSI-Schichtenmodells wieder [Fuchs2015, Seite 528].

Die Zugangsschicht besteht aus dem „Physical Layer“ und dem „Data Link Layer“. Der „Data Link Layer“ ist in zwei Schichten unterteilt, in die „Medium Access Control“ und in die „Logical Link Control Schicht“ [ETSI2012c].

Die Technologie der Zugangsschicht bezeichnet man als ITS-G5. Dies ist eine Technologie für drahtlose Kommunikation [Payerl2013]. ITS-G5 arbeitet in einem 5,9 GHz Frequenzband, welches in Abschnitt 1.5.1.1 genauer erklärt wird [Hobert2015].

Die Hauptmerkmale von 802.11p werden in ITS-G5 übernommen. Bei 802.11p handelt es sich um eine Erweiterung des bekannten IEEE 802.11 Standards, in dem die physika-

lische Schicht und die MAC-Schicht besser an die Fahrzeugumgebung angepasst werden [Schumacher2012]. Der IEEE 802.11 Standard (WLAN Standard) enthält zwei grundlegende Netzwerktopologien. Einmal den „Basic Service Set“ (BSS) und den „Independent Basic Service Set“ (IBSS). Bei einem BSS erfolgt die Kommunikation der Endgeräte über einen Access Point während bei einem IBSS die Endgeräte direkt miteinander kommunizieren [ETSI2012c].

Mit der Einführung von 802.11p wird die Möglichkeit der Kommunikation außerhalb des Kontextes eines Basic Service Sets geschaffen [ETSI2012c]. Hier kann eine Station, die nicht Mitglied eines BSS ist, Daten-Frames übertragen [IEEE2012]. Diese neue Fähigkeit wird durch das Setzen des MIB-Parameters dot11OCBActivated auf „true“ ermöglicht. Authentifizierungsverfahren, welche einen zeitintensiven Prozess darstellen, entfallen somit und vereinfachen die Kommunikation zwischen Fahrzeugen.

Eine weitere Auswirkung besteht darin, dass das Scannen nach einem verfügbaren Frequenzkanal deaktiviert ist. Dies hat zur Folge, dass die Frequenzkanäle vorbestimmt werden.

ITS-G5 unterstützt unicast, broadcast und multicast MAC-Adressen. Die MAC-Adresse sollte regelmäßig geändert werden, um die Privatsphäre der ITS-Station zu schützen [ETSI2012b, ETSI2009b].

1.5.1.1 Frequenzband in Europa

In Europa wird ein Frequenzband im 5,9 GHz Bereich verwendet. Für sicherheitsrelevante Anwendungen wird der Frequenzbereich von 5,875 GHz bis 5,905 GHz genutzt. Dieser Frequenzbereich wird zum ITS-G5A Frequenzband zusammengefasst [ETSI2012c]. Hierfür werden die Kanäle G5-CCH und G5-SCH1 bis G5-SCH2 verwendet.

SCH steht für „Service Channel“ und CCH für „Control Channel“. Der Bereich für nicht sicherheitsrelevante Funktionen liegt im Frequenzbereich zwischen 5,855 GHz bis 5,875 und wird auch als ITS-G5B bezeichnet. Das ITS-G5D Frequenzband, welches sich von 5,905 bis 5,925 GHz erstreckt, ist für zukünftige Nutzung im Straßenverkehr vorgesehen [ETSI2012c].

	Channel type	Frequency range [MHz]	IEEE channel number
ITS-G5A	G5-CCH	5 895 to 5 905	180
	G5-SCH2	5 885 to 5 895	178
	G5-SCH1	5 875 to 5 885	176
ITS-G5B	G5-SCH3	5 865 to 5 875	174
	G5-SCH4	5 855 to 5 865	172
ITS-G5C	G5-SCH7	5 470 to 5 725	94 to 145
ITS-G5D	G5-SCH5	5 905 to 5 915	182
ITS-G5D	G5-SCH6	5 915 to 5 925	184

Abbildung 1.2: Frequenzband in Europa [ETSI2012c]

Das ITS-G5C-Band wird für den Betrieb von zum Beispiel RLAN (Radio Local Area Network) verwendet. Hier werden eine dynamische Frequenzwahl und eine gleichmäßige Ausbreitung von Signalen benötigt, um die Signale von Radarsystemen erkennen zu können. Aufgrund dessen ist die Kommunikation zwischen einem Master und einem Slave-Gerät vorgesehen [ETSI2012c].

Ein Master ist eine statische Station am Straßenrand und der Slave stellt ein mobiles Gerät dar. Daher ist in G5C keine Kommunikation zwischen mobilen Geräten möglich [ETSI2009b]. Diese Anforderungen werden nicht unterstützt, wenn der MIB-Parameter auf „true“ gesetzt wird. Somit ist im ITS-G5C-Band keine Kommunikation außerhalb des Kontextes eines BSS möglich [ETSI2012c].

1.5.1.2 Eingesetzter MAC-Algorithmus

Der eingesetzte MAC-Algorithmus wird als „Enhanced Distributed Coordination Access“ (EDCA) bezeichnet. EDCA basiert auf DCF, also einem CSMA/CA Algorithmus. EDCA bietet im Gegensatz zu DCF die Möglichkeit, den Datenverkehr zu priorisieren [ETSI2012c].

Bei CSMA/CA lauscht jeder Knoten vor der Übertragung auf dem Kanal. Ist dabei der Kanal für eine bestimmte Zeit frei, kann der Knoten mit der Übertragung beginnen. Wird der Kanal während der Hörperiode besetzt, muss der entsprechende Knoten einen sogenannten Backoff-Vorgang durchführen, d.h. der Knoten muss seinen Zugriff für eine bestimmte Zeitspanne aufschieben [ETSI2012c].

Die vorgegebene Hördauer wird als „arbitration interframe space“ (AIFS) bezeichnet [ETSI2012c]. Für den Backoff-Wert wird eine Zahl im Bereich [0, W] gewählt. Der Anfangswert von W wird auf CW_{min} gesetzt. Ist der Kanal während der Backoff-Periode besetzt, wird der Backoff Zähler auf dem aktuellen Wert eingefroren [Wu2014]. Wird der Kanal für AIFS als frei erkannt, wird der Backoffwert dekrementiert [Wu2014, Nasrallah2016]. Wird der Wert 0 erreicht, kann das Paket gesendet werden [Nasrallah2016].

Diese Vorgehensweise bezieht sich auf den Broadcastmodus.

Der EDCA Algorithmus verwaltet für jeden Knoten vier verschiedene FIFO-Warteschlangen, welche man auch Access Categories (AC) nennt, mit unterschiedlichen AIFS-Werten und CW-Größen [Yang2009, ETSI2012c]. Des Weiteren werden acht verschiedene „User Prioritys“ (UPs) definiert, die vier verschiedenen ACs zugeordnet werden. Jedes Paket mit einem bestimmten UP-Wert wird einer AC zugeordnet [ETSI2012c, Yang2009]. Weist man beispielsweise dem AIFS Parameter einer AC einen niedrigen Wert zu, stellt man dadurch sicher, dass die entsprechende AC vor den anderen ACs Zugriff auf das Medium bekommt [Nasrallah2016]. Eine Erhöhung des Wertes führt somit zu einer Reduzierung der Priorität für den Zugriff [Nasrallah2016].

1.5.2 Netzwerk- und Transportschicht (Networking & Transport Layer)

Diese Schicht repräsentiert Schicht 3 und 4 des OSI-Schichtenmodells [Fuchs2015, Seite 528]. Die Netzwerk- und Transportschicht umfasst Protokolle für die Übermittlung von Daten zwischen ITS-Stationen und von ITS-Stationen zu anderen Netzwerkknoten [ETSI2010a]. Die Netzwerkprotokolle umfassen auch das Routen von Station A nach Station B. Dabei können die Daten auch in geografische Gebiete verbreitet werden. Die Netzwerkprotokolle werden jeweils mit einem entsprechenden Transportprotokoll zusammengesetzt [ETSI2010a]. Vertretene Netzwerkprotokolle sind GeoNetworking und IPv6. Als Vertreter der Transportprotokolle finden sich beispielsweise das Basic Transport Protocol und die Protokolle UDP und TCP [ETSI2010a].

1.5.2.1 Basic Transport Protokoll (BTP)

BTP stellt ein verbindungsloses Transportprotokoll auf der Netwerk- und Transportschicht dar.

Ähnlich wie UDP sorgt es für einen unzuverlässigen Pakettransport. Pakete können am Ziel beispielsweise doppelt erscheinen. Entitäten, die dieses Protokoll verwenden, müssen gegenüber den beschriebenen Eigenschaften tolerant sein oder Gegenmaßnahmen für einen sicheren Transport ergreifen. So werden beispielsweise Nachrichten wie CAM und DENM vom BTP durch das Multiplexing bearbeitet und über das GeoNetworking-Protokoll übertragen. Am Zielort findet schließlich das De-Multiplexing statt [ETSI2011a].

BTP verwendet für die Adressierung Ports. Ein Port ist eine interne Adresse der ITS-Station, die eine Protokollentität auf der Facility-Schicht identifiziert. Somit stellt der Port den Endpunkt einer logischen Verbindung dar [ETSI2016]. Auch hier finden sich die „Well Known Ports“ wieder, wie sie schon aus IP bekannt sind. Beispielsweise wird dem

CA Service der Port 2001 zugeteilt und dem DEN Service der Port 2002 [ETSI2016]. Bekannte Ports werden an bestimmte Entitäten vergeben. Solche, welchen keine feste Portnummer zugewiesen wird, verwenden dynamisch Nummern von 3000 bis 65536 [ETSI2016]. Eine BTP-Paketstruktur ist in Abbildung 1.3 abgebildet.

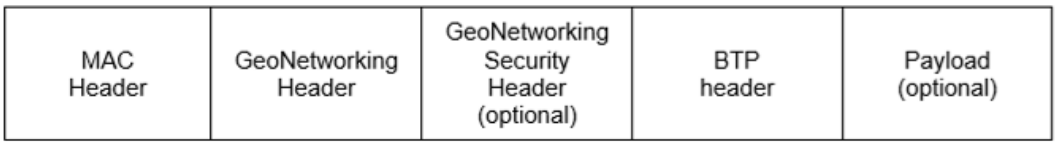

Abbildung 1.3: BTP Paketstruktur [ETSI2011a]

1.5.2.2 GeoNetworking Protokoll

Das GN-Protokoll befindet sich auf der Netzwerk- und Transportschicht und wurde speziell für die Dynamik in Vehicular Ad Hoc Netzwerken designt.

Es werden zwei Hauptfunktionen des GeoNetworking-Protokolls definiert. Diese bestehen in der Geoadressierung und Weiterleitung [Chen2014]. Das Protokoll ermöglicht somit das Routen und die Weiterleitung von Paketen basierend auf geografischen Positionen [ETSI2014c]. Hier werden die Knoten in einem Netzwerk also nicht an einer IP-Adresse sondern an ihrer geografischen Position erkannt.

Da heutzutage die meisten Kommunikationssysteme auf IP basieren, wird die Integration von IP noch genauer in Abschnitt 1.5.2.4 erläutert [Chen2014].

Die GeoNetworking Header Struktur setzt sich aus einem *Basic Header*, einem *Common Header* und einem optionalen *Extended Header* zusammen [ETSI2014c]. Dieser Aufbau ist in Abbildung 1.4 zu sehen.

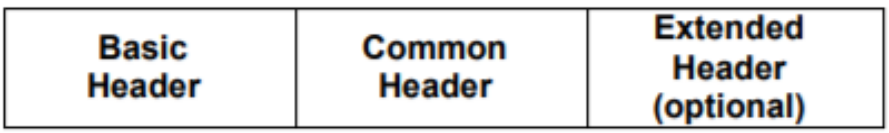

Abbildung 1.4: GN-Protokoll [ETSI2014c]

Der *Basic Header* ist in jedem Paket enthalten und besteht auf insgesamt fünf Feldern. Dies ist in Abbildung 1.5 zu sehen.

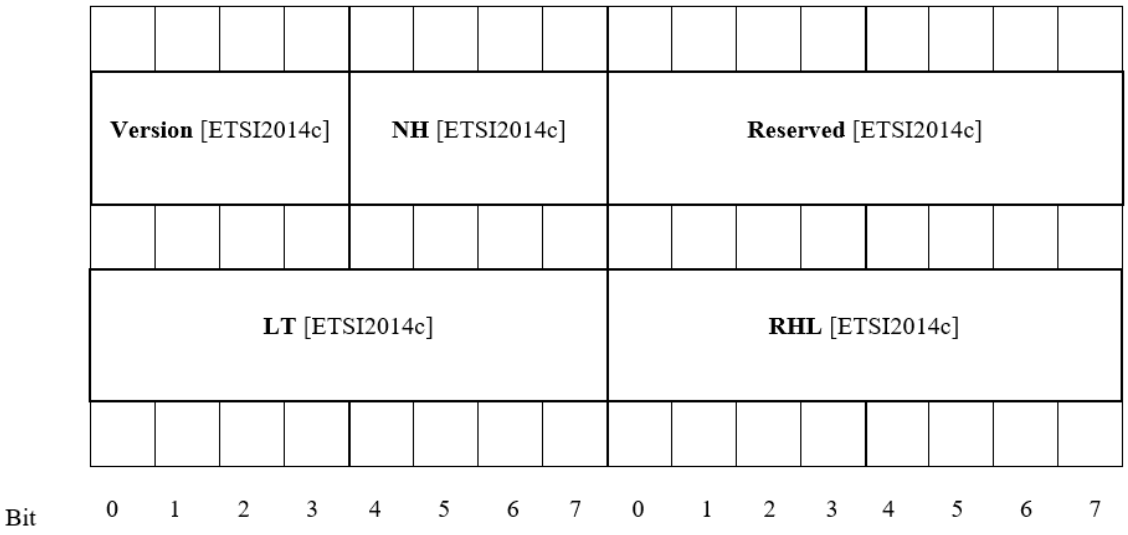

Abbildung 1.5: GN Basic Header. Quelle [eigene Darstellung]

Die Felder werden in folgender Tabelle beschrieben.

Tabelle 1.1: GN Basic Header. Quelle [eigene Darstellung]

Basic Header Felder	**Beschreibung**
Version	Dieses Feld gibt die Version des GN-Protokolls an [ETSI2014c]
Next Header (NH)	Gibt den Header an, der dem Basic Header folgt. Die Kodierung 0 bedeutet unbestimmt, 1 „Common Header“ und 2 „Secured Packet“ [ETSI2014c]
Reserved	Ist reserviert und wird auf 0 gesetzt [ETSI2014c]
Lifetime (LT)	Gibt die maximale Zeit an, die ein Paket gepuffert werden kann, bis das Ziel erreicht ist [ETSI2014c]
Remaining Hop Limit (RHL)	Wird von jedem GeoAdhoc Router dekrementiert, der das Paket weiterleitet. Wird der Wert 0 erreicht, kann das entsprechende Paket nicht mehr weitergeleitet werden [ETSI2014c].

Der *Common Header* ist in jedem GeoNetworking Paket enthalten und besteht aus insgesamt neun Feldern. Diese sind in folgender Abbildung dargestellt.

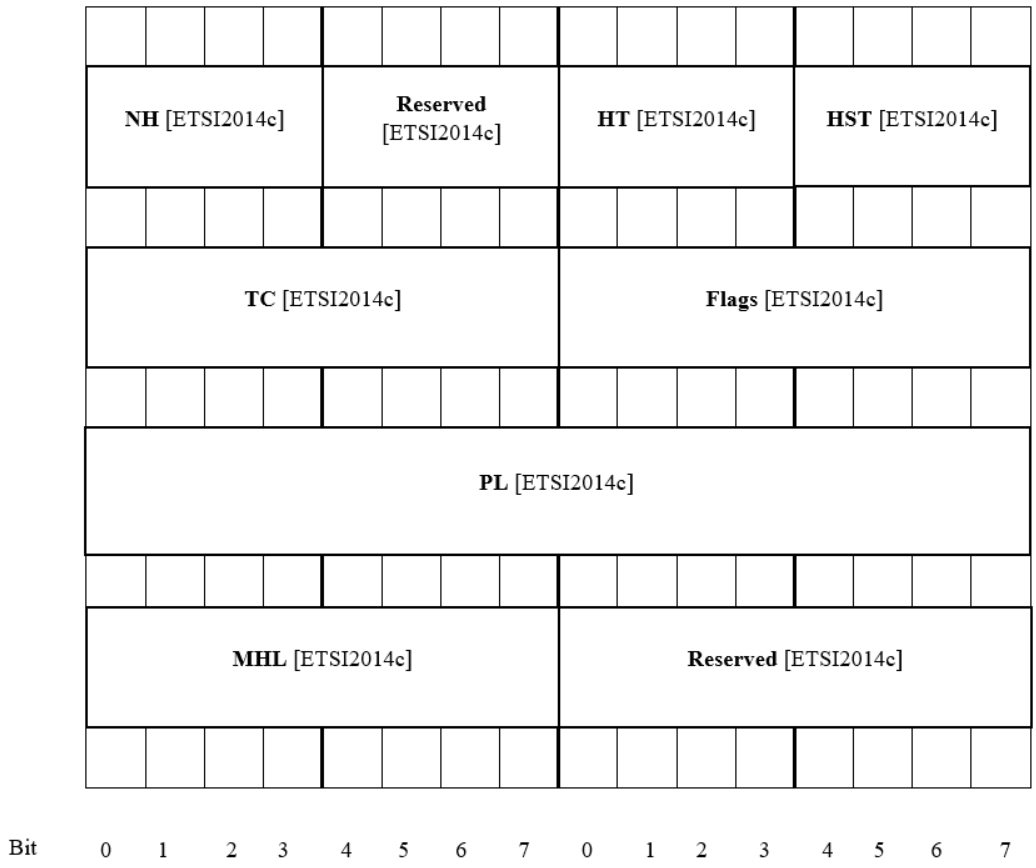

Abbildung 1.6: Common Header. Quelle [eigene Darstellung]

Die Bedeutung der Felder wird in folgender Tabelle erläutert.

Tabelle 1.2: GN Common Header. Quelle [eigene Darstellung]

Common Header Felder	**Beschreibung**
Next Header (NH)	Identifiziert den nächsten Header [ETSI2014c]
Reserved	Das Feld ist reserviert und wird auf 0 gesetzt [ETSI2014c]
Header Type (HT)	Gibt den Typ des GN-Headers an. Es wird zwischen „ANY“, „BEACON“, „GEOUNICAST“,„GEOBROADCAST“, „GEOANYCAST“, „TSB“ und „LS“ unterschieden [ETSI2014c]

Header Sub-type (HST)	Gibt den Subtyp des GN-Headers an. Bei TSB wird zwischen Single-hop Broadcast und Multi-hop Broadcast unterschieden. LS hingegen kann in LS_Request und LS_Replay unterschieden werden. Bei GEOUNICAST und GEOBROADCAST unterscheidet man zwischen einem ringförmigen, rechteckigen und ellipsenförmigen Gebiet [ETSI2014c].
Traffic Class (TC)	Gibt die Anforderungen der Facility-Schicht an den Pakettransport an [ETSI2014c]
Flags	Bit 0 beschreibt, ob die ITS-Station mobil oder stationär ist. Bit 1-7 sind reserviert und werden auf 0 gesetzt [ETSI2014c]
Payload (PL)	Gibt die Länge des Payloads an [ETSI2014c]
Maximum Hop Limit (MHL)	Stellt das maximale Hop Limit dar [ETSI2014c]
Reserved	Reserviert. Wird auf 0 gesetzt [ETSI2014c]

Der Einfachheit halber werden eine Reihe von positionsbezogenen Feldern in dem GN-Header zu einem sogenannten Positionsvektor zusammengefasst. Dabei unterscheidet man zwischen einem „Long“ und einem „Short Position Vector“ [ETSI2014c].

Der „Short Position Vector“ besteht aus Daten wie der GN_ADDR, also der GN-Adresse des Routers, dem Breiten- und Längengrad des Geo-Routers sowie dem Zeitstempel, zu dem die Breiten- und Längengrade des Routers erfasst wurden [ETSI2014c].

Der „Long Position Vector“ enthält neben den eben beschriebenen Feldern noch weitere Felder. Diese beinhalten Informationen zur Geschwindigkeit des Routers sowie eine Anzeige der Positionsgenauigkeit und Richtungsinformationen des Routers [ETSI2014c].

Bei dem GeoNetworking-Protokoll können verschiedene GeoNetworking Headertypen definiert werden, wie aus der Beschreibung des „Header Type“ und „ Header Sub-type“ Feldes des *Common Headers* ersichtlich wird. Diesen verschiedenen Headertypen ist jeweils der *Basic* und *Common Header* gemeinsam. Sie unterscheiden sich in dem *Extended Header*.

Wird beispielsweise der GN/BTP Stapel von dem CAM-Protokoll verwendet, wird der GN-Pakettransporttyp Single-Hop-Broadcasting benutzt [ETSI2014d]. Bei der DENM

hingegen ist GeoBroadcast als GN Pakettransporttyp zu verwenden [ETSI2014e].

1.5.2.3 Kommunikationsszenarien

Das GeoNetworking-Protokoll ist ein Protokoll, welches sich auf der Netzwerk- und Transportschicht wiederfindet. Es ermöglicht die Kommunikation zwischen Fahrzeugen untereinander und zwischen Fahrzeugen und RSUs. Dabei werden folgende Kommunikationsszenarien unterstützt: Point-to-Point, Point-to-Multipoint, GeoBroadcast und GeoAnycast. Diese Szenarien werden im Folgenden genauer erläutert [ETSI2013d].

Point-to-Point

Bei der Point-to-Point Kommunikation beginnt die Kommunikation an einer bestimmten Station. Diese Quellstation hat ein bestimmtes Ziel, bei welchem die Kommunikation endet. Diese Kommunikation ist sowohl bei V2V als auch bei R2V möglich. Abbildung 1.7 veranschaulicht das Kommunikationsszenario [ETSI2013d].

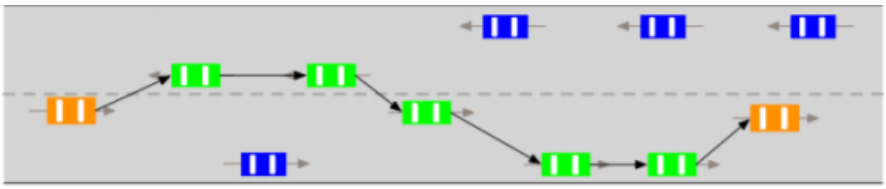

Abbildung 1.7: Point-to-Point Kommunikation [ETSI2013d]

Point-to-Multipoint

Bei der Point-to-Multipoint Kommunikation zielt die Quelle auf mehrere ITS-Stationen im Zielbereich ab. Auch dieses Kommunikationsszenario ist sowohl für die V2V als auch für die R2V Kommunikation geeignet. Abbildung 1.8 zeigt dies [ETSI2013d].

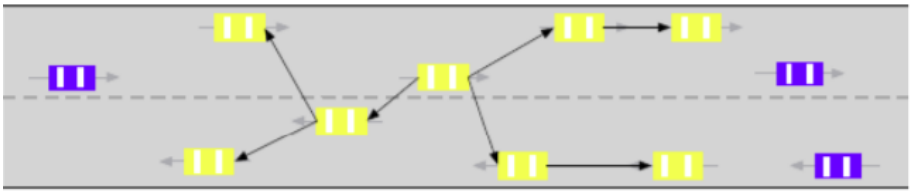

Abbildung 1.8: Point-to-Multipoint Kommunikation [ETSI2013d]

GeoAnycast

Die Kommunikation beginnt bei einer ITS-Station und endet bei einer beliebigen ITS-Station, die sich innerhalb eines bestimmten geografischen Gebietes befindet [ETSI2013d]. Die folgende Abbildung 1.9 zeigt solch ein Kommunikationsszenario, bei dem sich der Quellknoten außerhalb des geografischen Gebietes befindet [ETSI2013d].

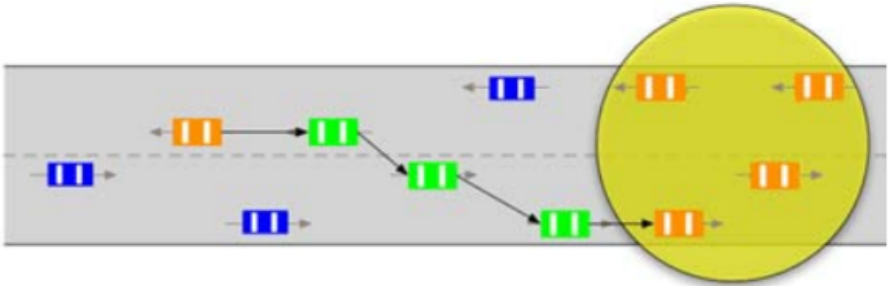

Abbildung 1.9: GeoAnycast Kommunikation [ETSI2013d]

GeoBroadcast

Die Kommunikation geht von einer ITS-S aus und endet bei mehreren Zielknoten in einem bestimmten geografischen Bereich. Es wird die V2V und V2R Kommunikation unterstützt. In der folgenden Abbildung 1.10 liegt die Quellstation außerhalb des geografischen Zielbereiches [ETSI2013d].

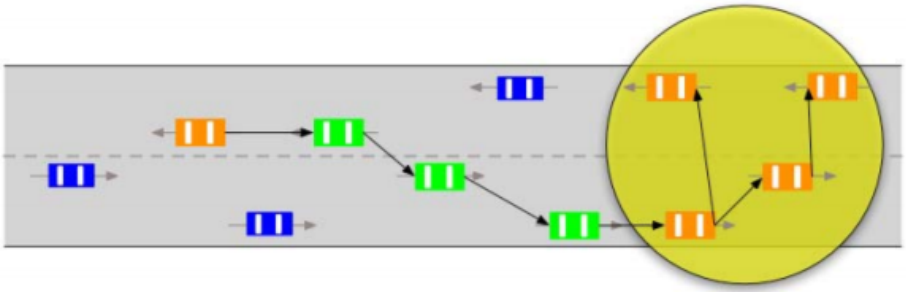

Abbildung 1.10: GeoBroadcast Kommunikation [ETSI2013d]

1.5.2.4 IPv6

Für die Weiterleitung von Daten in einem Ad hoc Netzwerk kommt das GeoNetworking-Protokoll zum Einsatz. Dieses Protokoll benutzt geografische Daten für die Weiterleitung. Auch die Kommunikation im Internet ist möglich. Hierfür wird ein Sublayer mit dem Namen GN6ASL eingeführt, welche die Übertragung von IPv6 Paketen über das GeoNetworking-Protokoll ermöglicht [Gramaglia2012].

Die empfangenen IP-Datagramme werden in das GeoNetworking-Paket verschachtelt und mit dem entsprechenden Header weitergeleitet. Geografische virtuelle Links (GVL) werden definiert, die sich jeweils auf einen geografischen Bereich beschränken und sich

gegenseitig nicht überlappen. Alle Knoten innerhalb des Gebietes eines GVL gehören zum gleichen IPv6 Subnetz [Sandonis2016].

Jeder GVL Bereich wird von mindestens einer RSU verwaltet, die als IPv6 Router fungiert und sogenannte Router Advertisements (RA) sendet, welche die IPv6-Präfix tragen [Gramaglia2012]. Durch die empfangenen RAs können die Knoten jeweils eine gültige IP-Adresse aufbauen. Diese wird aus der entsprechenden Präfix und aus dem Netzidentifikator gebildet, welcher sich aus der MAC-Adresse ableitet [Gramaglia2012].

Ein Fahrzeug bewegt sich in der Regel zwischen verschiedenen geografischen Verbindungen. Die Fahrzeuge können solch eine geografische Änderung erkennen, da die Daten der geografischen virtuellen Verbindung in dem Header der RAs enthalten sind [Sandonis2016].

1.5.3 Facility-Schicht (Facility Layer)

Die Facility-Schicht spiegelt die Schichten fünf, sechs und sieben des OSI-Schichtenmodells wieder [ETSI2010c]. Diese Schicht lässt sich in drei Hauptkomponenten unterteilen. Einmal in die Anwendungsunterstützung, in die Informationsunterstützung und in die Kommunikationsunterstützung.

Der Informationsunterstützung kommt die Aufgabe des Datenmanagements zu. Hierbei ist die Aktualisierung der Informationen besonders wichtig, die auch vor allem durch die Local Dynamic Map unterstützt wird [ETSI2009a]. Diese wird später noch genauer erläutert.

Die Kommunikationsunterstützung arbeitet mit der Netzwerk- und Transportschicht zusammen [ETSI2009a].

Die Anwendungsunterstützung besteht beispielsweise aus dem „Station positioning“ und dem „Message management“. Das „Station positioning“ liefert unter anderem 3D-Positionsinformationen der entsprechenden Station. Diese können zum Beispiel über GPS erhalten werden [ETSI2009a].

Das „Message management“ ist für den Empfang, die Strukturierung und die Formatierung von V2X Nachrichten zuständig. Außerdem können Daten an andere Anwendungen weitergegeben werden [ETSI2009a].

1.5.3.1 LDM

LDM steht für „Local Dynamic Map“ und ist in jeder ITS-S enthalten. Sie befindet sich auf der Facility-Schicht. ITS-Stationen benötigen Informationen über ihre Umge-

bung. LDM ist ein Datenspeicher, in dem Informationen abgelegt sind, die für ITS-Anwendungen relevant sind [ETSI2011c]. Die Daten können aus unterschiedlichen Quellen stammen, wie beispielsweise anderen Fahrzeugen, Sensoren oder Infrastruktureinheiten. Der Zugriff auf diese Datenbank wird über mehrere Interfaces geregelt.

Es gibt drei Schnittstellen. Einmal eine Schnittstelle mit der Applikationsschicht, die als FA-SAP bezeichnet wird. Eine weitere Schnittstelle mit der Netzwerkschicht, die als NF-SAP bezeichnet wird. Die letzte Schnittstelle findet mit der Sicherheitsschicht statt und ist auch unter dem Namen SF-SAP bekannt [ETSI2011c].

Die Schnittstelle mit der Netzwerkschicht sorgt für die Verbindung mit der Kommunikationsfunktion der ITS-Stationen [ETSI2011c]. Dadurch können anhand von Nachrichten wie CAM und DENM die Informationen in der LDM aktualisiert werden. Während die Aktualisierung der Informationen stattfindet, müssen folgende Schritte erfüllt werden. Zunächst muss die entsprechende Nachricht dekodiert und in ein entsprechendes LDM-Objekt umgewandelt werden. Anschließend wird überprüft, ob es sich bei diesen Informationen um ein Update eines Objektes handelt, oder ob ein weiteres Objekt hinzugefügt werden soll [ETSI2011c]. Zum Schluss können diese Informationen in die LDM eingetragen werden.

Die Schnittstelle mit der Anwendungsschicht ermöglicht es Anwendungen, auf die LDM zuzugreifen. Somit können Daten jederzeit abgerufen werden [ETSI2011c]. Die Schnittstelle mit der Sicherheitsschicht ermöglicht den Zugriff auf Sicherheitsfunktionen der ITS-Stationen [ETSI2011c].

1.5.4 Anwendungsschicht (Application Layer)

In der Anwendungsschicht finden sich Anwendungen wieder, die in drei Kategorien klassifiziert werden. Die Verkehrssicherheit, die Verkehrseffizienz und sonstige Anwendungen. Dabei geht es bei den Anwendungen der Verkehrssicherheit primär darum, die Verkehrssicherheit auf den Straßen zu erhöhen. Solche Applikationen umfassen beispielsweise Warnungen vor Straßenarbeiten oder Autopannen [ETSI2009a].

Die Kategorie der Verkehrseffizienz zielt auf die Verbesserung des Verkehrsflusses ab. Beispiele hierfür sind Routenempfehlungen und Verkehrsinformationen.

Jene Anwendungen, die in die Kategorie „sonstige Anwendungen“ eingeordnet werden, können beispielsweise der Aktualisierung der Fahrzeugsoftware dienen [ETSI2009a].

1.5.5 Management-Schicht (Management Layer)

Die Management-Schicht ist für verschiedene Verwaltungsaufgaben zuständig.

Sie ist für die Verwaltung von Anwendungen zuständig, indem sie die Konfiguration, Installation und Aktualisierung von ITS-S Anwendungen unterstützt [ETSI2010c]. Des Weiteren werden generelle Mittel bereitgestellt, um eine zu hohe Belastung des physischen Kanals zu vermeiden. Solche Mittel werden als „General Congestion Control“ zusammengefasst und wirken schichtübergreifend [ETSI2010c]. Weitere Aufgaben der Management-Schicht können in [ETSI2010c] gefunden werden.

1.5.5.1 Decentralized Congestion Control (DCC)

DCC befindet sich auf der Management-Schicht und hat eine schichtübergreifende Funktion auf die Zugangsschicht, die Netzwerk- und Transportschicht und die Facility-Schicht [Payerl2013].

Der „Decentralized Congestion Control“ stehen drei Werkzeuge zur Verfügung. Diese nennen sich TRC, TPC und TDC. TRC ist dafür zuständig, die Anzahl der Pakete bei zu hoher Kanalbelastung zu reduzieren. TDC bietet mehrere Übertragungsraten. Dies hat zur Folge, dass bei einer hohen Kanalbelastung höhere Übertragungsraten verwendet werden können und somit die Paketdauer für jedes Paket verringert wird [Sjöberg2013]. TPC passt die Sendeleistung der Pakete an und verringert bzw. erhöht die Ausgangsleistung je nach Kanalaktivität [Sjöberg2013, Autolitano2013].

1.5.6 Sicherheitsschicht (Security Layer)

Diese Schicht enthält Sicherheitsfunktionen für den Protokollstapel. Dabei können die bereitgestellten Funktionen schichtübergreifend genutzt werden. Aufgaben dieser Schicht bestehen unter anderem in der Authentifizierung und dem Management von Zertifikaten und Kryptoschlüsseln [ETSI2010c]. Die Verwendung der unterschiedlichen Zertifikate etc. wird in Punkt 1.8 genauer erläutert.

1.6 Nachrichten

1.6.1 Cooperative Awareness Message (CAM)

Ein kooperatives Bewusstsein der Verkehrsteilnehmer ist von erheblicher Bedeutung, um die Sicherheit und Verkehrseffizienz zu stärken. Unterstützt wird dies durch den Austausch von Nachrichten zwischen den Fahrzeugen sowie zwischen den Fahrzeugen und der Infrastruktur. Das ITS-G5 Netzwerk verfügt über zwei spezielle Nachrichtentypen, die im Folgenden genauer erläutert werden. Dies sind zum einen periodische Nachrichten, einer der wichtigen Vertreter ist die CAM. Zum anderen gibt es event-basierte Nachrichten, die durch einen bestimmten Event ausgelöst werden. Ein wichtiger Vertreter dieser Gruppe ist die DENM [ETSI2014d, ETSI2011b].

CAM

CAMs werden innerhalb des ITS-G5 Netzwerkes periodisch verteilt. Sie liefern Status- und Attributinformationen. Beispiele für Statusinformationen sind die Geschwindigkeit und die Position des Senders. Attributinformationen beinhalten Informationen über den Fahrzeugtyp und Ähnliches [ETSI2014d]. Diese werden mit hoher Frequenz von einer ITS-Station zu einer anderen ITS-Station übermittelt [Lin2015, Seite 136]. Somit wird gewährleistet, dass ein Verkehrsteilnehmer über seine Nachbarschaft informiert ist. Dies erleichtert es Fahrzeugen, auf bestimmte Situationen zu reagieren. Die Aussendung einer CAM ist unabhängig von anderen Anwendungen. Diese Nachrichten werden von dem „CA basic service“ betrieben, der nun genauer erläutert wird.

CA basic service

Der „CA basic service“ betreibt das CAM-Protokoll und befindet sich auf der Facility-Schicht. Er ermöglicht zwei Dienste, nämlich das Senden und Empfangen einer CAM [ETSI2014d].

Um eine CAM zu generieren und bei dem Empfang einer CAM relevante Informationen zu verarbeiten, arbeitet der „CA basic service“ mit anderen Einrichtungen der Facility- und der Anwendungsschicht zusammen. In Abbildung 1.11 ist dies veranschaulicht, zusammen mit den jeweiligen Schnittstellen zu den anderen Schichten. Die Schnittstelle zur Sicherheitsschicht ermöglicht dabei den Zugriff auf Sicherheitsdienste.

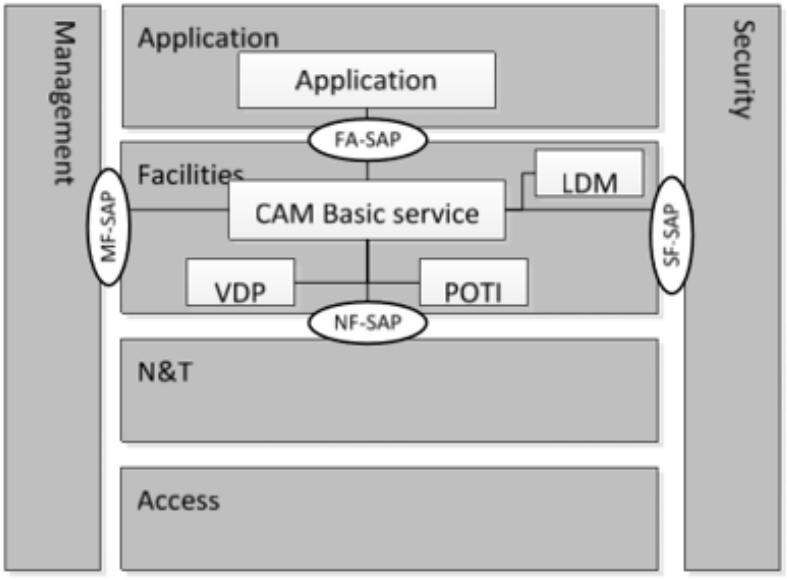

Abbildung 1.11: CA basic service [ETSI2014d]

Als Empfangsgeräte können, wie in Abbildung 1.11 zu sehen ist, der Vehicle Data Provider (VDP), das Positions- und Zeitmanagement (POTI) sowie die Logical Dynamic Map verwendet werden. Dabei sorgt die POTI für die Zeitinformation, während die LDM eine Datenbank darstellt, in der eingehende Nachrichten eingetragen werden können, um somit die Datenbank zu aktualisieren. VDP stellt die Vernetzung mit dem Fahrzeugnetz dar, um die Statusinformationen zu liefern [ETSI2014d].

Sicherheitsmechanismen

Bei der Übertragung von CAMs kommen Zertifikate zum Einsatz, die die Authentifizierung des Senders ermöglichen. Ein Zertifikat gibt die Berechtigung der Person an, für die das Zertifikat ausgestellt wurde. Die ITS-AID und SSP geben die Berechtigung innerhalb des Zertifikates an. ITS-AID zeigt auf, welche Berechtigungen insgesamt vergeben werden, während SSP spezifische Berechtigungen innerhalb der Gesamtberechtigung angibt [ETSI2014d].

Eine empfangene CAM wird nur dann von dem Empfänger akzeptiert, wenn der Inhalt der Nachricht mit dem SSP in dem Zertifikat übereinstimmt [Lin2015, Seite 140-141]. Die Zuweisung des SSP erfolgt durch eine „Public Key Infrastructure“ [Lin2015, Seite 141].

Senden und Empfangen einer CAM

Für die Verarbeitung von CAMs ist in Europa meistens die ITS-G5 Technologie vorgesehen. Für den Fall, dass die ITS-G5 Technologie Verwendung findet, wird die CAM

über den Steuerkanal, G5-CCH, gebroadcastet. Der SHB Pakettransporttyp wird für die CAM Verbreitung verwendet [Lin2015, Seite 137; ETSI2014d]. Die Priorität der CAM wird auf einen hohen Wert gesetzt, während die sogenannte „packet lifetime“ auf einen kleinen Wert gesetzt wird. Man verwendet eine Point-to-Multipoint Kommunikation, wobei die ITS-S, die die CAM empfangen hat, nicht weiterleiten darf [ETSI2014d; Lin2015, Seite 137].

CAMs werden nur gesendet, solange der „CA basic service“ aktiviert ist. Auch werden Unterfunktionen von dem „CA basic service“ bereitgestellt, die für das Codieren und das Decodieren der CAM zuständig sind [ETSI2014d]. Die Häufigkeit der CAM Generierung wird vom „CA basic service“ bestimmt, wobei bestimmte Grenzen eingehalten werden müssen. Dabei darf das CAM Generierungsintervall 100 ms nicht unterschreiten und 1000 ms nicht überschreiten.

Eine weitere wichtige Funktion bei der Erstellung einer CAM ist deren Zeit. Damit die anderen ITS-Stationen, die die CAM empfangen, diese korrekt identifizieren können, ist ein Zeitstempel vorhanden. Hierfür wird eine Zeitsynchronisation zwischen den verschiedenen Stationen vorausgesetzt. Die Generierung einer CAM soll weniger als 50 ms in Anspruch nehmen. Dabei bezieht sich die Zeit auf die Differenz zwischen dem Start der Generierung der CAM und dem Zeitpunkt, an dem die CAM an die Netzwerkschicht weitergegeben wird [ETSI2014d].

Aufbau des Protokolls

Das CAM-Protokoll besteht aus einem PDU Header und mehreren Containern. Enthalten ist immer der *basic container* und der *high frequency container*. Der *low frequency container* und andere *special container* sind optional [ETSI2014d]. ITS-Stationen, die eine besondere Rolle im Straßenverkehr spielen, wie beispielsweise Rettungsfahrzeuge, können zusätzlich einen sogenannten *Special Container* enthalten [ETSI2014d]. In folgender Abbildung wird der allgemeine Aufbau einer CAM beschrieben.

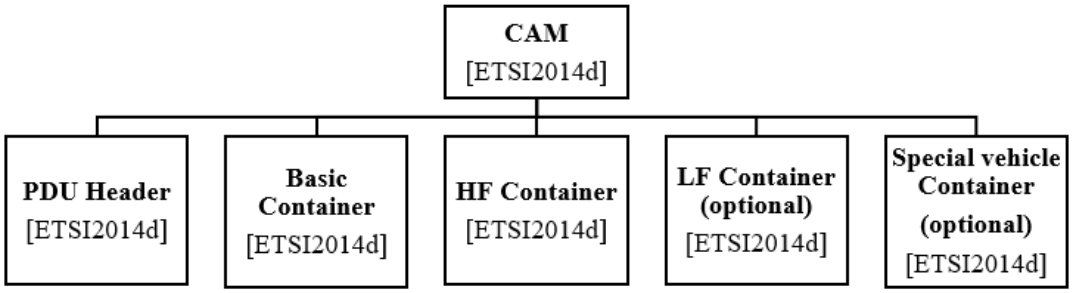

Abbildung 1.12: Aufbau CAM. Quelle [eigene Darstellung]

Hauptzweck der Verwendung von Containern in dem CAM-Format besteht in der Flexibilität für mögliche Erweiterungen des Nachrichteninhaltes in der Zukunft [Lin2015, Seite 139].

PDU Header

Der *PDU-Header* enthält Informationen über die Protokollversion, den Nachrichtentyp sowie die ID der ITS-Station [ETSI2014d]. Der Aufbau des Headers ist in Abbildung 1.13 dargestellt.

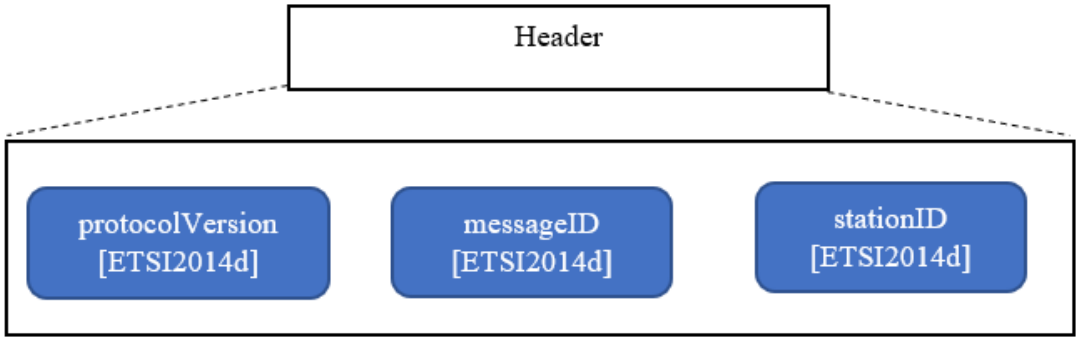

Abbildung 1.13: CAM-Header. Quelle [eigene Darstellung]

Den Feldern des Headers kommt folgende Bedeutung zu.

Tabelle 1.3: CAM PDU Header. Quelle [eigene Darstellung]

CAM-Feldname	**Feldbeschreibung**
protocolVersion	Version der ITS-Nachricht [ETSI2013c].
messageID	Gibt den Nachrichtentyp der ITS-Station an. 1 steht für DENM, 2 für CAM [ETSI2013c].
stationID	Bezeichnung der ITS-Station, kann variieren [ETSI2013c].

Basic Container

In jeder CAM findet sich ein *Basic Container*. Dieser enthält Informationen über die ITS-Station. Der Aufbau des *Basic Headers* ist in Abbildung 1.14 aufgelistet.

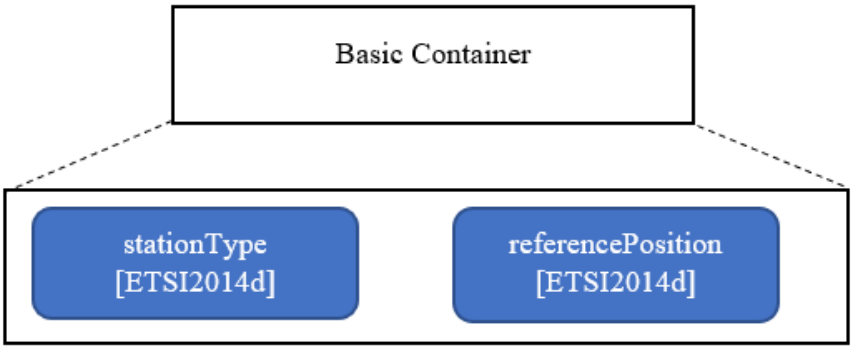

Abbildung 1.14: CAM Basic Container. Quelle [eigene Darstellung]

Den Feldern des *Basic Containers* kommt folgende Bedeutung zu.

Tabelle 1.4: Basic Container. Quelle [eigene Darstellung]

CAM-Feldname	**Feldbeschreibung**
stationType	Gibt den Typ der ITS-Station an 0=unbekannt, 1=Fußgänger, 2=Fahrrad, 3=Moped, 4=Motorrad, 5=PKW, 6=Bus,7=leichter LKW, 8=schwerer LKW, 9=Anhänger, 10=spezielles Fahrzeug, 11=Tram, 15=RSU [ETSI2013c]
referencePosition	Gibt die geografische Position einer ITS-Station an, Längengrad, Breitengrad, Höhe und die Vertraulichkeit der geografischen Position [ETSI2013c]

High frequency container

Jede CAM beinhaltet einen *high frequency container*. Dieser enthält dynamische Informationen über die entsprechende Fahrzeug-ITS-Station. Im Folgenden sind die Felder des *HF Containers* eines Fahrzeuges dargestellt.

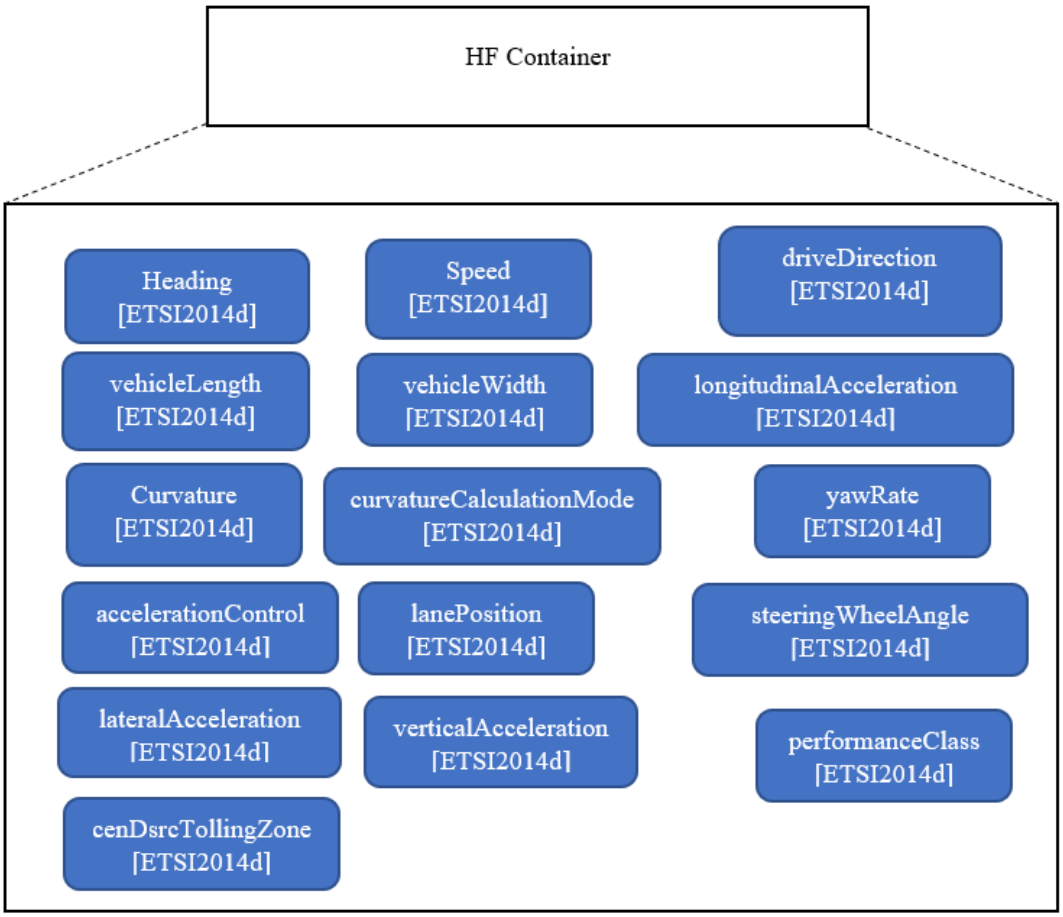

Abbildung 1.15: High frequency Container. Quelle [eigene Darstellung]

Die Bedeutung der einzelnen Felder des *high frequency container* sind in folgender Tabelle dargestellt.

Tabelle 1.5: HF Container. Quelle [eigene Darstellung]

CAM-Feldname	**Feldbeschreibung**
Heading	Gibt die Kursrichtung an [ETSI2013c]
Speed	Beschreibt die Geschwindigkeit und die entsprechende Genauigkeit der Geschwindigkeitsinformation für ein sich bewegendes Objekt [ETSI2013c]
driveDirection	Zeigt an, ob ein Auto vorwärts oder rückwärts fährt. 0=vorwärts, 1=rückwärts, 2=keine Information [ETSI2013c]
vehicleLength	Länge des Fahrzeuges [ETSI2013c]
vehicleWidth	Breite des Fahrzeuges inklusive Seitenspiegel [ETSI2013c]

longitudinalAcceleration	Fahrzeugbeschleunigung in Längsrichtung [ETSI2013c]
Curvature	Krümmung der Fahrzeugbahn und die Genauigkeit der vorgegebenen Krümmung [ETSI2013c]
curvatureCalculationMode	Beschreibt, ob die Giergeschwindigkeit (Winkelgeschwindigkeit) vom Fahrzeug verwendet wird, um die Krümmung der Kurve zu berechnen [ETSI2013c].
yawRate	Giergeschwindigkeit des Fahrzeuges zu einem bestimmten Zeitpunkt [ETSI2013c]
accelerationControl	Zeigt an, ob ein bestimmtes Fahrzeugbeschleunigungssystem eingeschaltet ist oder nicht. Bit 0=Bremspedal, Bit 1=Gaspedal, Bit 2=Notbremse, Bit 3=Kollisionswarnung, Bit 4= Adaptive Cruise Control ein/aus, Bit 5=Tempomat ein/aus, Bit 6=Geschwindigkeitsbegrenzung ein/aus [ETSI2013c]
lanePosition	Gibt die Fahrspur des Fahrzeuges an, die vom Außenrand der Straße gezählt wird [ETSI2014d].
steeringWheelAngle	Gibt den Lenkradwinkel des Fahrzeuges zu einem bestimmten Zeitpunkt an [ETSI2013c]
lateralAcceleration	Fahrbeschleunigung in Querrichtung, negativer Wert=Beschleunigung nach rechts, positiver Wert=Beschleunigung nach links, Wert 161=keine Information verfügbar [ETSI2013c]
verticalAcceleration	Fahrzeugbeschleunigung in vertikale Richtung [ETSI2013c]
performanceClass	Fähigkeit eines Fahrzeuges, aktuelle Informationen an andere ITS-Stationen weiterzugeben. 0=unbekannte Leistungsklasse, 1=Leistungsklasse A (weniger als 150 ms Übertragungsdauer von Sensor zu CAM/DENM basic service), 2=Leistungsklasse B (weniger als 1,4 s) [ETSI2013c, ETSI2013a]

cenDsrcTollingZone	Information über die Position einer Mautstelle im 5,8 GHz Frequenzbereich [ETSI2014d]

Low frequency container

Optional kann eine CAM einen *low frequency container* enthalten. Dieser beinhaltet statische Informationen der Fahrzeug-ITS-Station. Die folgende Abbildung zeigt den Aufbau des *LF Containers* eines Fahrzeuges.

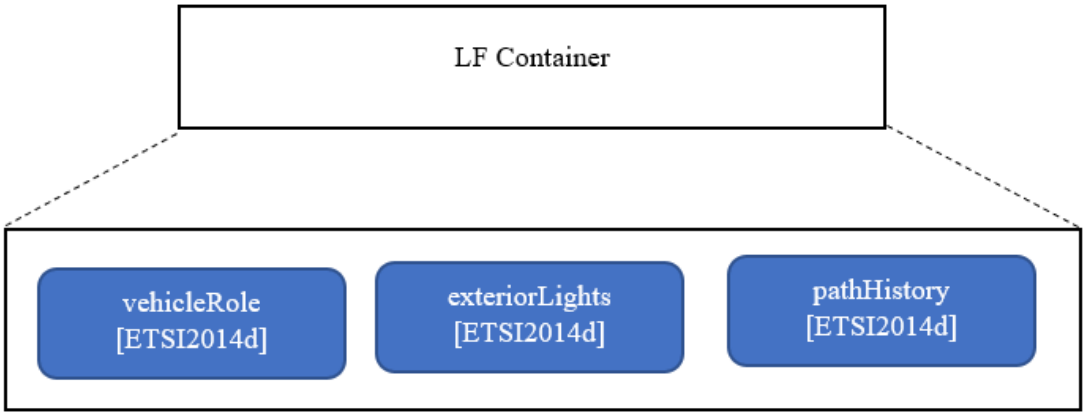

Abbildung 1.16: Low frequency Container. Quelle [eigene Darstellung]

Die Beschreibung der Felder ist in folgender Tabelle aufgezeigt.

Tabelle 1.6: LF Container. Quelle [eigene Darstellung]

CAM-Feldname	Feldbeschreibung
vehicleRole	0=Default, 1=öffentlicher Transport, 2=spezieller Transport, 3=Gefahrgut, 4=Straßenarbeiten, 5=Rettung, 6=Notfall, 7=Sicherheitsfahrzeug [ETSI2013c]
exteriorLights	Bit 0=Abblendlicht, Bit 1=Scheinwerfer, Bit 2=Blinker links, Bit 3=Blinker rechts, Bit 4=Tagfahrlicht, Bit 5=Rückfahrscheinwerfer, Bit 6=Nebelscheinwerfer, Bit 7=Parklicht [ETSI2013c]
pathHistory	Definiert den Weg eines Fahrzeuges mit einer Menge von Pfadpunkten [ETSI2013c]

Special Container

Fahrzeuge, die eine spezielle Rolle im Straßenverkehr übernehmen, enthalten einen weiteren Container, in dem Statusinformationen vorhanden sind. Dabei wird zwischen folgenden Special Containern unterschieden. Zum einen soll ein *public transport container* vorhanden sein, falls es sich bei der ITS-Station um ein öffentliches Verkehrsmittel handelt [ETSI2014d].

Ein *special transport container* sollte verwendet werden, falls es sich bei der ITS-Station um ein spezielles Transportsystem handelt, wie zum Beispiel ein Schwertransporter. Bei Gefahrguttransportmitteln ist der *dangerous good container* vorhanden. Falls das Fahrzeug in Straßenarbeiten involviert ist, wird ein *road work container* verwendet [ETSI2014d].

Handelt es sich um ein Rettungsfahrzeug ohne Privilegien, ist ein sogenannter *rescue container* vorhanden [ETSI2014d]. Bei einem Einsatzfahrzeug mit besonderen Privilegien wird ein *emergency container* verwendet. Es kann sich auch um ein Sicherheitsfahrzeug handeln, das ein anderes Transportfahrzeug begleitet. Wenn dies der Fall ist, wird ein *safety car container* benutzt [ETSI2014d].

1.6.2 Decentralized Environment Notification Message (DENM)

DENMs sind ereignisorientierte Nachrichten, die durch ein bestimmtes Event ausgelöst werden. Road-Hazard-Warning (RHW) – Anwendungen sind solche Auslöser und liefern Informationen über ein Verkehrsereignis an ITS-Stationen. Bei RHW-Anwendungen handelt es sich um Verkehrssicherheitsanwendungen [ETSI2010b]. DENMs geben Informationen über Ereignisse, die sich sowohl auf die Verkehrssicherheit als auch auf die Verkehrseffizienz beziehen.

DEN basic service

Der „DEN basic service“ sitzt auf der Facility-Schicht und ist für das DENM Protokoll zuständig. Er arbeitet mit verschiedenen Einrichtungen auf der Facility-Schicht zusammen und bietet Funktionen wie das Kodieren und Dekodieren von Nachrichten an [ETSI2014e, ETSI2010b]. In Abbildung 1.17 sind die wichtigsten Komponenten des „DEN basic service“ aufgezeichnet.

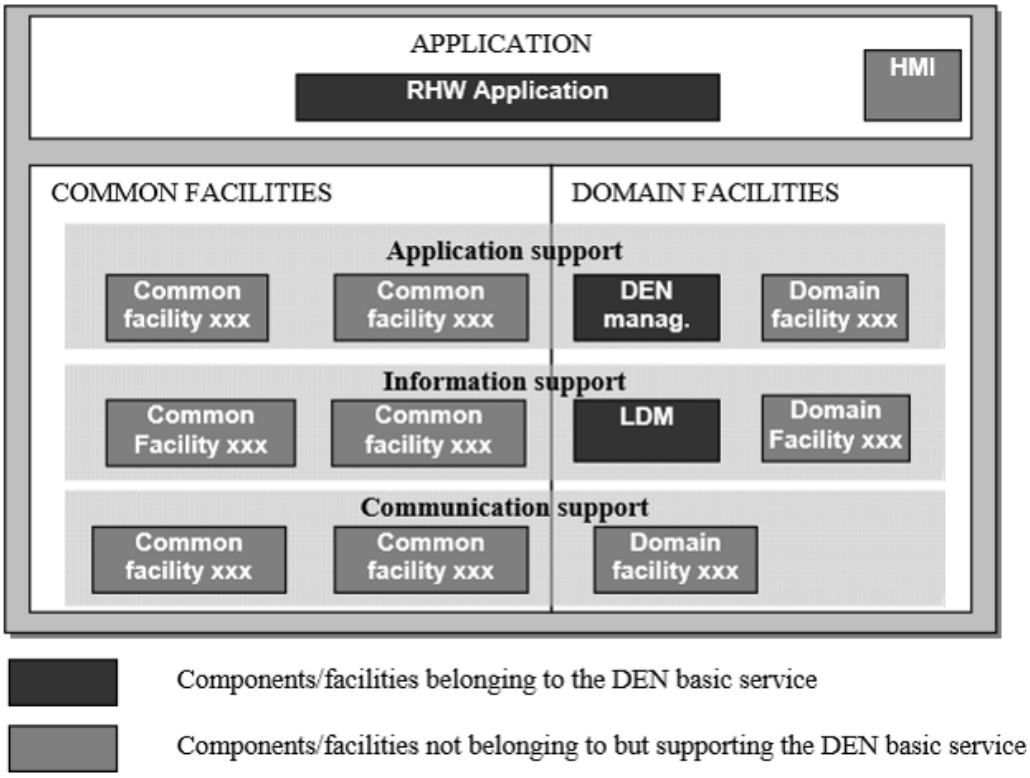

Abbildung 1.17: DEN basic service [ETSI2010b]

LDM, RHW Applikationen und das DEN Management sind die wichtigsten Bestandteile des „DEN basic service“. Das DEN-Management sorgt für das entsprechende Format und die Semantik der DENM. Jede Version des DENM-Formates hat dabei eine entsprechende Protokollversionsnummer. Um die entsprechenden Informationen bezüglich eines Ereignisses zu sammeln, stellt das DEN-Management Schnittstellen zu anderen Einrichtungen zur Verfügung [ETSI2010b].

Zusätzlich werden Verwaltungsfunktionen bereitgestellt. Diese Funktionen beinhalten das Löschen von DENMs, falls diese veraltet sind, sowie das Versenden von Informationen an andere Einrichtungen zur weiteren Verarbeitung [ETSI2010b]. Die LDM stellt eine Datenbank dar, die durch den Empfang einer DENM aktualisiert wird.

RHW-Anwendungen haben die Aufgabe, eine DENM zu starten. Verschiedene Informationen werden von den RHW-Anwendungen an die Facility-Schicht bereitgestellt. Hierfür ist jedem Ereignis ein Ereignistyp und eine Ereignisposition zugeordnet. Die Ereignisposition gibt die Position des Events an, der Ereignistyp wird durch einen Ursachencode weiter beschrieben [ETSI2010b].

Ortsbezogene Informationen und Zeitinformationen zu dem entsprechenden Vorgang werden weitergegeben. Auch Angaben zur Übertragungsfrequenz der Nachricht sowie Informationen über das geografische Gebiet werden übermittelt. Angaben zu dem voraussicht-

lichen Zeitpunkt der Beendigung des Ereignisses sind ebenfalls enthalten [ETSI2010b].

Optional kann der „DEN basic service“ die sogenannte „Keep Alive Forwarding“ (KAF) Funktionalität bereitstellen. Deren Hauptziel besteht darin, eine empfangene DENM zu speichern und bei Bedarf an andere ITS-S weiterzuleiten [ETSI2014e]. Die „Keep Alive Forwarding“ Funktionalität kommt hier zum Tragen. Sie ist in der Lage, die Verbreitung einer DENM vor Ablauf der Gültigkeitsdauer bereit zu stellen, selbst wenn die ursprüngliche ITS-Station nicht mehr im Stande ist, die DENM selbst zu übertragen [ETSI2014e]. Ein Beispiel hierfür wäre, wenn die ursprüngliche ITS-Station eine Panne hat und dadurch der Betrieb der ITS-Station ausfällt. Die KAF-Funktion einer ITS-S, welche die DENM zuvor empfangen hat, könnte nun die Übertragung fortsetzen [ETSI2014e].

Allgemeiner Ablauf eines Anwendungsfalls

Erkennt eine ITS-Station ein Ereignis, sendet sie eine DENM, um die Informationen an andere Stationen innerhalb des relevanten Bereiches zu verteilen. Die Verbreitung einer DENM wird immer durch eine Applikation ausgelöst. Über APIs werden Informationen zwischen dem „DEN basic service“ und den ITS-S Anwendungen ausgetauscht [ETSI2014e]. Dabei sendet eine Anwendung eine Anfrage an den „DEN basic service“, um die Erstellung einer DENM zu starten. Es wird zwischen drei verschiedenen Anwendungsanfragen unterschieden, dem App-DENM_trigger, dem AppDENM_update und der AppDENM_termination [ETSI2014e].

Je nach Anfrage wird eine bestimmte DENM vom „DEN basic service“ generiert und zwar entweder eine „New DENM“, eine „Update DENM“ oder eine „Cancellation“ bzw. „Negation DENM“ [ETSI2014e].

Die Übertragung einer DENM wird von einer Anwendung auf der Anwendungsschicht gestartet und kann auch wieder durch eine Anwendung beendet werden [ETSI2014e]. Sie kann so lange wiederholt werden wie das Ereignis selbst andauert [ETSI2014e]. Eine DENM kann außerdem durch andere ITS-Stationen weitergeleitet werden. Ist die erhaltene Information relevant, können diese Informationen bzw. Warnungen an den Fahrer weitergegeben werden.

Eine mögliche Technologie für die DENM-Verbreitung ist ITS-G5 [Lin2015, Seite 142]. Für die Verbreitung wird das Geobroadcast Protokoll der GN Funktionalität verwendet [Lin2015, Seite 142]. Falls das entdeckte Event eine sofortige Handlung erfordert, um beispielsweise potentielle Kollisionen zu vermeiden, wird die „traffic class“ der DENM auf die höchste Priorität gesetzt.

Die Terminierung einer DENM kann entweder durch eine vordefinierte Verfallszeit erfolgen oder durch die Erzeugung einer DENM, die über die Beendigung des Ereignisses berichtet [ETSI2014e].

Die verschiedenen DENM-Typen werden im Folgenden erläutert.

New DENM

Diese DENM wird erstellt, wenn eine Station ein neues Ereignis erkennt. Eine Anwendung sendet eine Anfrage des Typs AppDENM_trigger an den „DEN basic service“. Daraufhin wird eine New DENM generiert [ETSI2014e]. Jede neue DENM bekommt eine eigene ActionID zugewiesen [ETSI2014e]

Update DENM

Bei einer Update DENM wird die Information zu einem bestehenden Ereignis aktualisiert. Die aktualisierten Informationen werden dem „DEN basic service“ über die Anwendungsanforderung AppDENM_update zur Verfügung gestellt [ETSI2014e]. Die Update DENM wird von genau der Station übertragen, die zu dem entsprechenden Ereignis die New DENM gesendet hat [ETSI2014e].

Cancellation DENM

Diese DENM sendet die Information zur Beendigung eines speziellen Events. Die Nachricht muss von der ITS-S gesendet werden, die die New DENM für das gleiche Ereignis erzeugt hat [ETSI2014e].

Die Wiederholung einer DENM wird gestoppt, wenn deren Wiederholungsdauer beendet wird. Wie schon erwähnt, kann die Wiederholungsdauer auch von einer Anwendung aktualisiert werden [ETSI2014e].

Außerdem ist es möglich, dass die Quell ITS-Station die Terminierung des Events erkennt, bevor die Gültigkeitsdauer des Events abgelaufen ist [ETSI2014e]. In solch einem Fall wird eine Cancellation DENM generiert.

Negation DENM

Auch durch diese DENM kann die Beendigung eines Ereignisses erfolgen. Die Station, die die New DENM gesendet hat muss allerdings nicht die Station sein, die die Negation DENM sendet. Es kann sich auch um eine Station handeln, die zuvor eine DENM über das entsprechende Ereignis erhalten hat und diese jetzt negiert, da das Event abgeschlossen ist [ETSI2010b].

Es ist möglich, dass sich ein Fahrzeug, welches eine New DENM gesendet hat, nicht mehr im Umfeld des Ereignisses befindet [ETSI2014e]. Hier sendet die Anwendung der ITS-Station eine Anfrage der Art AppDENM_termination an den „DEN basic service“.

Daraufhin generiert dieser eine Negation DENM [ETSI2014e]. Bei der Erzeugung einer Negation DENM wird die actionID auf die actionID gesetzt, auf den sich das Event bezieht [ETSI2014e].

Aufbau der DENM

Die DENM besteht aus einem *ITS-PDU Header* und mehreren Containern, die den Payload der DENM bilden. Der DENM Payload besteht aus dem *Management-Container*, dem *Situation Container*, dem *Location-Container* und dem *à la carte Container*. Dabei sind der *Header* und der *Management Container* in jeder DENM enthalten. Die anderen Container hingegen sind optional. Bei einer negation und cancellation DENM fallen der *Situation Container*, der *Location Container* und der *à la carte Container* weg [ETSI2014e]. Der Aufbau einer DENM ist in Abbildung 1.18 zu sehen.

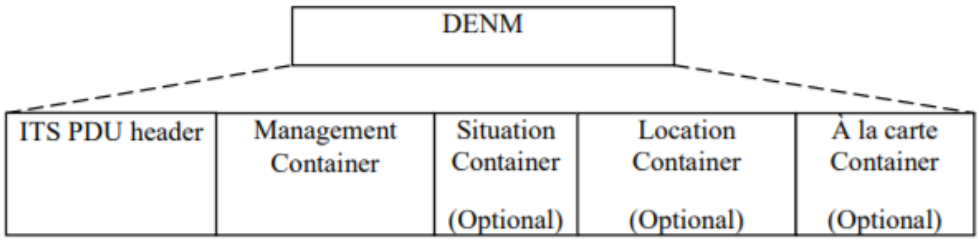

Abbildung 1.18: DENM-Aufbau [ETSI2014e]

DENM PDU Header

Der *PDU-Header* enthält Informationen über die Version des Protokolls, den Nachrichtentyp und die ID der entsprechenden Station [ETSI2014e]. Diese sind in folgender Abbildung dargestellt.

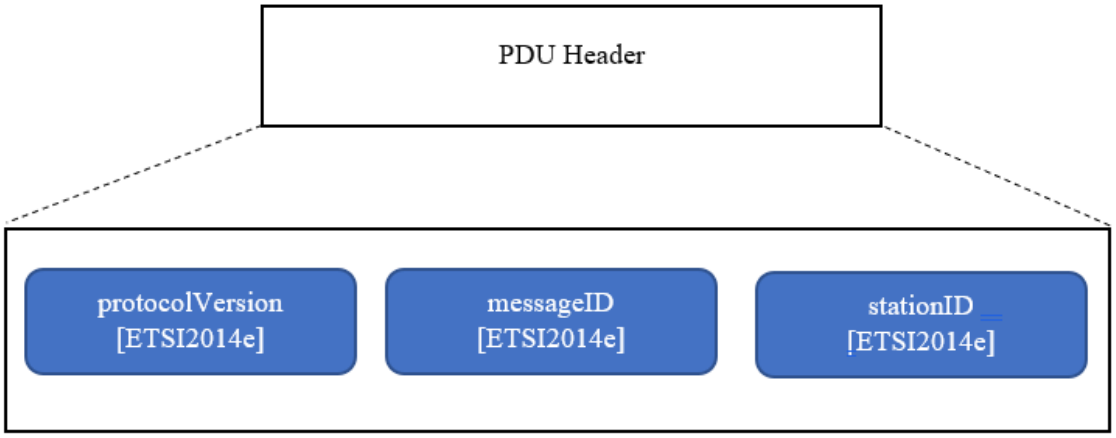

Abbildung 1.19: DENM-Header. Quelle [eigene Darstellung]

Die Felder werden in folgender Tabelle beschrieben.

Tabelle 1.7: DENM PDU Header. Quelle [eigene Darstellung]

DENM-Feldname	**Feldbeschreibung**
protocolVersion	Auswahl eines geeigneten Protokolldekoders an der ITS-Station des Empfängers [ETSI2010b].
messageID	Typ der Nachricht [ETSI2010b]
stationID	Identifiziert eine ITS-Station. Diese kann sich im Laufe der Zeit ändern [ETSI2014e].

Management Container

Der *Management Container* enthält Informationen über das DENM-Management und das Protokoll [ETSI2014e]. Die zugehörigen Felder sind in der folgenden Abbildung zu sehen.

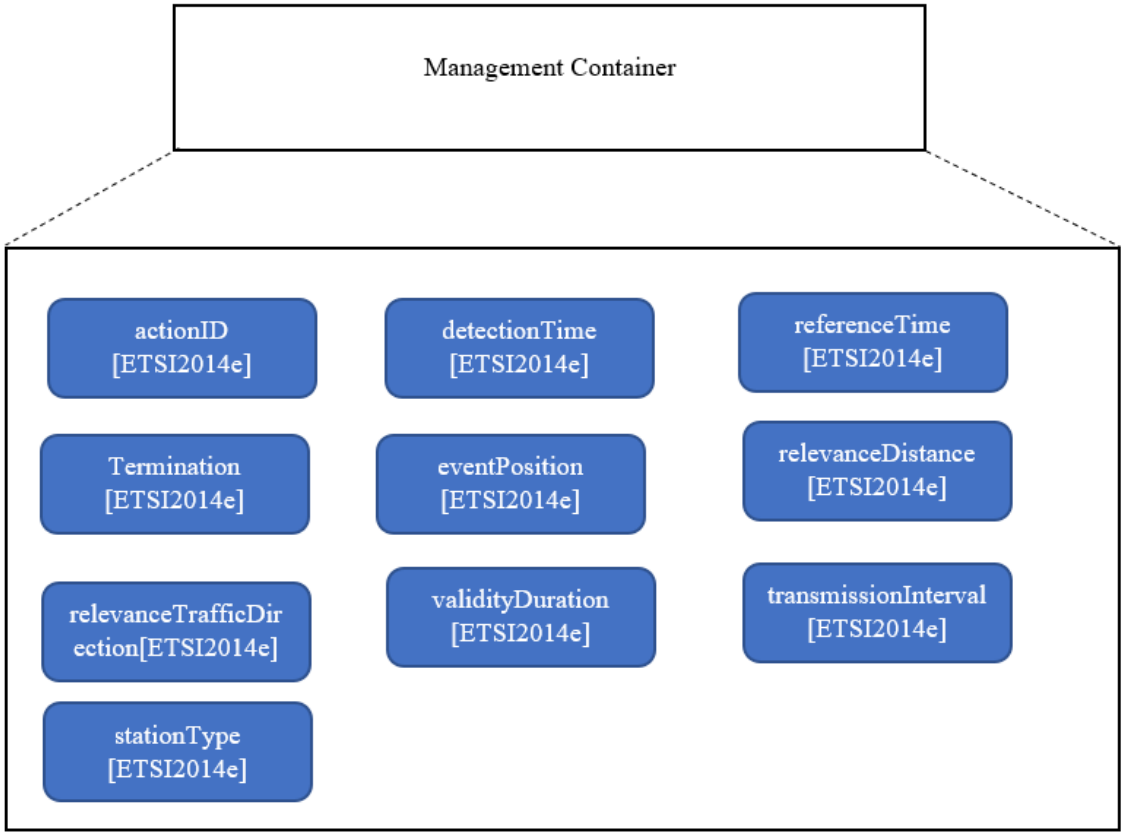

Abbildung 1.20: Management Container. Quelle [eigene Darstellung]

Die Beschreibung der in dem *Management Container* enthaltenen Felder sind in Tabelle 1.8 dargestellt.

Tabelle 1.8: Management Container. Quelle [eigene Darstellung]

DENM-Feldname	**Feldbeschreibung**
actionID	Wird generiert, wenn eine ITS-Station ein Ereignis entdeckt. Setzt sich aus stationID und Sequenznummer zusammen [ETSI2010b]
detectionTime	Gibt den Zeitpunkt an, zu dem das Event von der ITS-Station erkannt wurde [ETSI2014e]. Bei einem Update ist dies der Zeitpunkt, an dem das Update erkannt wurde [ETSI2014e]

referenceTime	Zeitpunkt, an dem New DENM, Update DENM oder Cancellation DENM erzeugt wurde [ETSI2014e]
Termination	Gibt an, ob es sich um eine Cancellation oder eine Negation DENM handelt. Feld optional. Bei Cancellation DENM=termination auf isCancellation, Negation DENM=termination auf isNegation [ETSI2014e]
eventPosition	Geografische Position des Events [ETSI2014e]
relevanceDistance	Entfernung, in der die Ereignisinformation für die empfangene ITS-Station relevant ist, ausgehend von der Ereignisposition [ETSI2014e]. Feld optional. 0=weniger als 50 m, 1=weniger als 100 m, 2=weniger als 200 m, 3=weniger als 500 m, 4=weniger als 1000 m, 5=weniger als 5 km, 6=weniger als 10 km, 7=Distanz über 10 km [ETSI2014a]
relevanceTrafficDirection	Verkehrsrichtung, in der die Ereignisinformation für die empfangenen ITS-Stationen relevant sind. Optional [ETSI2014e]
validityDuration	Gültigkeitsdauer einer DENM. Wird von der Quell-ITS-Station angegeben. Schätzung wie lange das Event andauern könnte. Dauer über die die DENM im „DEN basic service“ auf der empfangenen ITS-Station bestehen bleiben soll [ETSI2014e] Feld optional.
transmissionInterval	Informiert die ITS-Stationen, die die DENM erhalten haben, über das geplante Sendeintervall von zwei aufeinanderfolgenden DENMs [ETSI2014e] Feld optional
stationType	Gibt den Typ der ITS-Station an. 0=unbekannt, 1=Fußgänger, 2=Fahrrad, 3=Moped, 4=Motorrad 5=PKW, 6=Bus, 7=leicher LKW, 9= Anhänger, 10=spezielles Fahrzeug 11=Tram, 15=RSU [ETSI2014a]

Situation Container

Der *Situation Container* enthält Informationen bezüglich des detektierten Ereignisses [ETSI2014e].

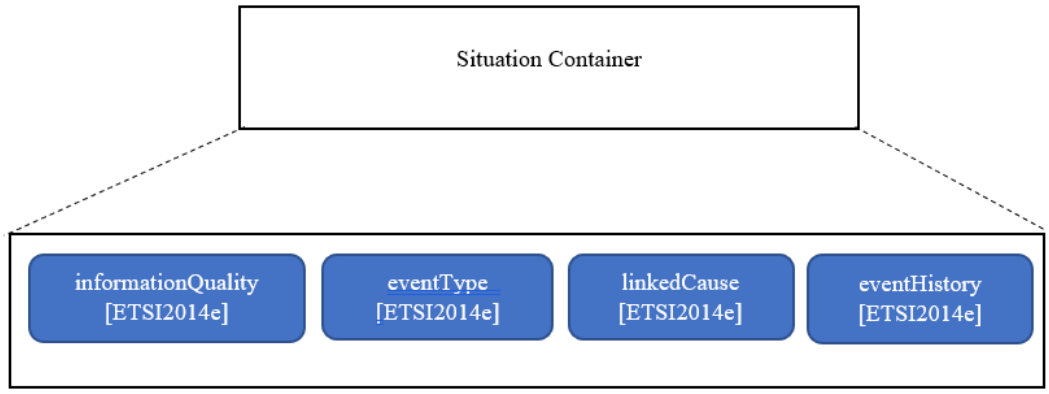

Abbildung 1.21: Situation Container. Quelle [eigene Darstellung]

In der folgenden Tabelle findet sich eine genaue Erläuterung zu den einzelnen Feldern.

Tabelle 1.9: Situation Container. Quelle [eigene Darstellung]

DENM-Feldname	**Feldbeschreibung**
informationQuality	Gibt die Qualität der Information an, die von der Quell-ITS-Station bereitgestellt wurde [ETSI2014e]. Der niedrigste Wert, den dieses Feld annehmen kann ist 1, der höchste 7
eventType	Beschreibt das Event. Er setzt sich aus einem CauseCode und dem SubCauseCode zusammen [ETSI2014e]
linkedCause	Beschreibt ein Ereignis, welches mit dem Ereignistyp verknüpft wird z.B. Unfall durch schlechte Wetterbedingungen [ETSI2014e]. Feld optional
eventHistory	Liste von Ereignispunkten, die den Umfang des Ereignisses darstellen. Dabei sind bis zu 40 Eventpunkte möglich [ETSI2014e]. Feld optional

Location Container

Der *Location Container* enthält Informationen über den Ort des Ereignisses [ETSI2014e].

Der Aufbau des Containers ist in folgender Abbildung dargestellt.

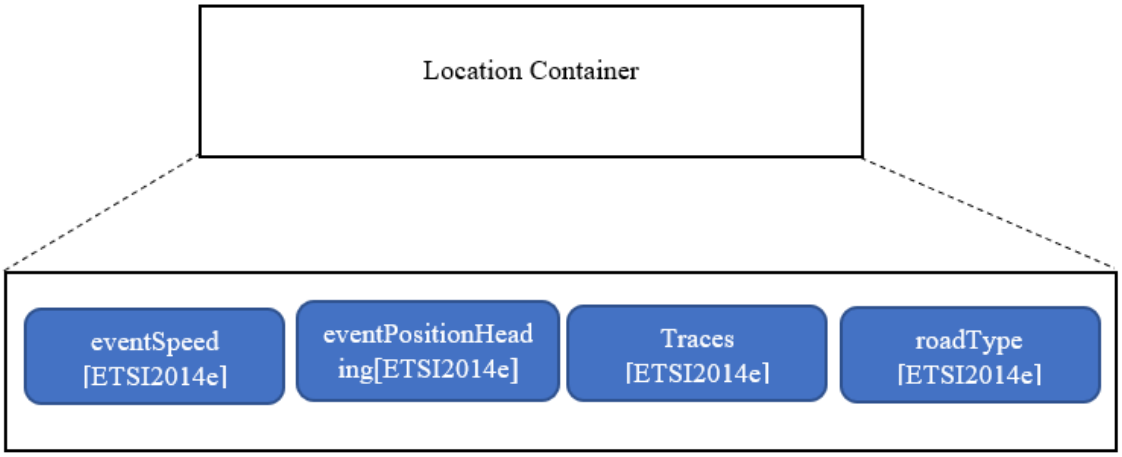

Abbildung 1.22: Location Container. Quelle [eigene Darstellung]

Die Erläuterung der einzelnen Felder ist in folgender Tabelle aufgezeigt.

Tabelle 1.10: Location Container. Quelle [eigene Darstellung]

DENM-Feldname	**Feldbeschreibung**
eventSpeed	Geschwindigkeit des Ereignisses [ETSI2014e]. Feld ist optional
eventPositionHeading	Gibt Kursrichtung des Ereignisses an [ETSI2014e]. Feld ist optional.
Traces	Standortbezogene Information des Events. Jede „trace“ besteht aus einer Liste von Wegpunkten, die einen Pfad aufbauen, der sich der Ereignisposition nähert. Dies ermöglicht es dem Empfänger die Relevanz der Events abzuschätzen, indem er seinen eigenen Pfad mit dem Pfad vergleicht, der in der erhaltenen DENM angegeben ist [Lin2015, Seite 145]
roadType	Information über die Straßensegmente [ETSI2014a]

À la carte Container

Der *à la carte Container* enthält zusätzliche Informationen, die von den anderen Containern nicht bereitgestellt werden. Es besteht die Möglichkeit für ITS-S Anwendungen, spezifische Informationen unterzubringen [ETSI2014e].

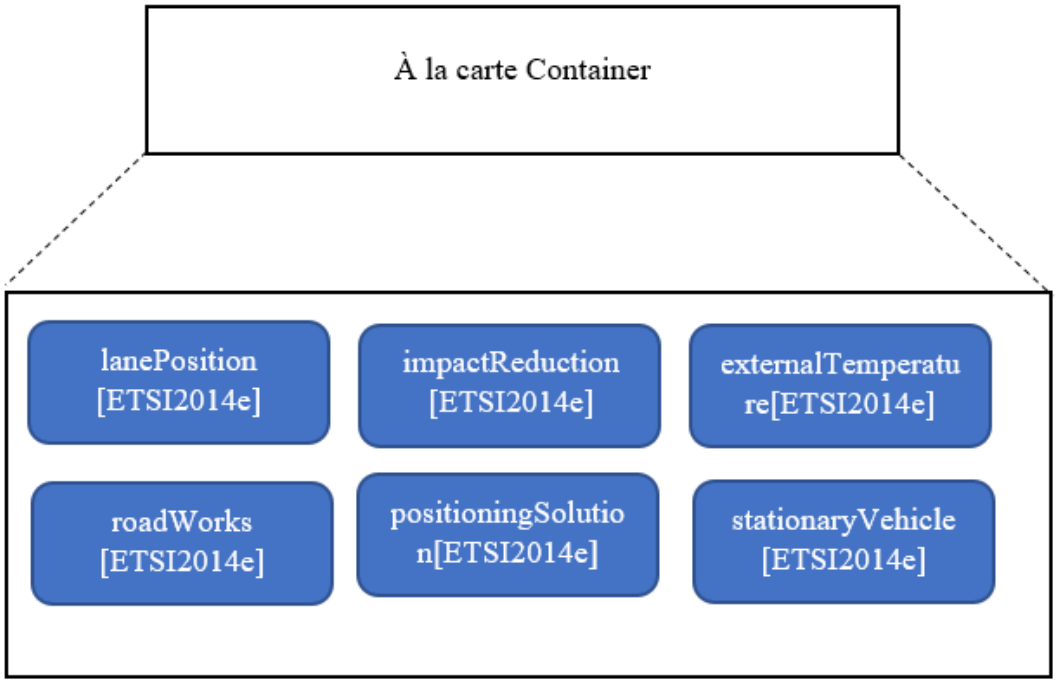

Abbildung 1.23: À la carte Container. Quelle [eigene Darstellung]

Die Felder werden in der folgenden Tabelle erläutert.

Tabelle 1.11: À la carte Container. Quelle [eigene Darstellung]

DENM-Feldname	**Feldbeschreibung**
lanePosition	Gibt die Fahrspur des Ereignisses an. Dabei gibt z.B. der Wert 0 die Standspur an [ETSI2014a]
impactReduction	Dieser Container wird hinzugefügt, wenn eine mögliche Kollision erkannt wird. Er enthält Daten für die Milderung der Kollision [ETSI2014e]. Optional.
externalTemperature	Informationen über ungünstige Wetterbedingungen [ETSI2014e]

roadWorks	Dieser Container wird bei Baustellen/Straßenarbeiten hinzugefügt. Enthält Informationen über die Baustelle und deren Zugang [ETSI2014e]
positioningSolution	Technologie, die verwendet wird, um die geografische Position zu bestimmen [ETSI2014a]. Feld optional.
stationaryVehicle	Dieser Container enthält Informationen über ein stehendes Auto [ETSI2014e]. Optional.

1.6.3 Signal Phase and Timing Message (SPAT)

SPAT ist für die Bereitstellung der Ampelphasen und Zeitinformationen verantwortlich. Diese werden von RSUs an die Fahrzeuge übertragen. Die empfangende ITS-S verarbeitet die Informationen zusammen mit den entsprechenden Daten der Kreuzungstopologie. Dies ermöglicht die Zuordnung der Ampelinformationen zu dem entsprechenden Straßensegment [Lin2015, Seite 156]. Informationen bezüglich der Kreuzungstopologie können von der RSU durch eine MAP-Nachricht zur Verfügung gestellt werden. Um Ampelphasen und Zeitinformationen zu erhalten, ist eine Verbindung der RSU mit dem Ampelsteuerungssystem notwendig [ETSI2013b]. Die Standardisierungsarbeiten für SPAT- und MAP-Nachrichten sind noch nicht abgeschlossen [Lin2015, Seite 156].

SPAT Format

Eine SPAT Nachricht enthält den Ampelstatus einer oder mehrere Kreuzungen. Jede bildet ein „Intersectionstate data frame“. Jeder „data frame“ setzt sich aus verschiedenen Informationskategorien zusammen, die der Beschreibung der Kreuzung dienen [Lin2015, Seite 157].

Zu den sogenannten *message management data* gehören allgemeine Informationen der Nachricht einschließlich der Erzeugungszeit einer Nachricht.

Intersection data enthalten allgemeine Informationen über die Kreuzung sowie eine jeweilige ID der Kreuzung. Außerdem beinhalten sie Informationen über allgemeine Statusinformationen sowie eine Fahrspurliste. Dies Liste kann sich im Laufe der Zeit ändern. Ein Beispiel wäre eine Spur, die nur zu einer bestimmten Zeit am Tag für den Verkehr geöffnet ist [Lin2015, Seite 158].

Die Statusdaten zeigen den Steuerstatus der Ampel der entsprechenden Kreuzung an. Außerdem kann der Status einer Kreuzung auch den Status des SPAT- und MAP - Über-

tragungssystems anzeigen [Lin2015, Seite 158].

Traffic light status data beschreibt den Ampelstatus der Kreuzung, der als Bewegungsstatus bezeichnet wird. Jeder Bewegungsstatus bezieht sich auf bestimmte Fahrzeugspuren innerhalb der Kreuzung. Diesem wird eine ID zugeteilt, die innerhalb der Kreuzung eindeutig ist [Lin2015, Seite 158]. Der Bewegungsstatus kann bei einem Bewegungsereignis die geschätzte Phasenwechselzeit, den Phasentyp sowie eine empfohlene Geschwindigkeit liefern [Lin2015, Seite 158].

Maneuvering assistance data unterstützt ein Fahrzeug beim Verlassen der Kreuzung. Dabei können Informationen wie beispielsweise die Schätzung der Warteschlangenlänge sowie Informationen über Fußgänger, vorausgesetzt solche Informationen werden von den Sensoren zur Verfügung gestellt, enthalten sein [Lin2015, Seite 158].

Other data fassen Informationen für regionale Erweiterungen zusammen [Lin2015, Seite 158].

1.6.4 MAP

MAP-Nachrichten liefern Informationen über die Straßentopologie und Straßengeometrie. Eine solche Nachricht wird von einer RSU an die Fahrzeuge gebroadcastet. Die MAP-Nachricht kann von verschiedenen Anwendungen verwendet werden und mit anderen SPAT-Nachrichten verarbeitet werden [Lin2015, Seite 158]. Der Inhalt von MAP-Nachrichten umfasst folgende Daten:

Die *message management data* enthält allgemeine Informationen der Nachricht inklusive Nachrichten ID [Lin2015, Seite 159].

Die *Map Meta Data* enthalten die Metadaten des MAP-Inhaltes inklusive des Straßentopologietypes, wie zum Beispiel Kreuzung, Kurve, Parkplatz oder Begrenzungsinformationen, falls die Straße auf bestimmte Nutzer begrenzt ist [Lin2015, Seite 159].

Die *Intersection geometry* enthält die Beschreibung einer oder mehrere Kreuzungen. Für eine bestimmte Kreuzung werden die Fahrspuren nacheinander beschrieben. Jede Bahnform wird durch eine Liste von Attributen beschrieben [Lin2015, Seite 159]. Dabei sind auch Attribute der Bahn selbst enthalten, wie beispielsweise die ID, die Breite der Spur sowie eine geografische Beschreibung der Spur usw. Falls MAP zur Unterstützung der SPAT-Nachricht verwendet werden soll, kann eine Spur einer Gruppe von Spuren zugeordnet werden. Jede Gruppe entspricht einem Ampelbewegungszustand [Lin2015, Seite 159].

Die *Road segment geometry* dient der Beschreibung von Straßensegmenten. Hier wer-

den Informationen durch Fahrspuren innerhalb der entsprechenden Straße bereitgestellt [Lin2015, Seite 160].

Other data dienen auch hier der regionalen Erweiterung [Lin2015, Seite 160].

1.6.5 In-Vehicle Information (IVI)

IVI steht für „In-Vehicle Information“. Die IVI-Nachricht liefert Verkehrszeicheninformationen an die jeweiligen Verkehrsteilnehmer [Lin2015, Seite 151]. Empfängt eine ITS-Station solche Daten, werden diese Daten verarbeitet und die Relevanz der Informationen für den Fahrer eingeschätzt. Handelt es sich um wichtige Informationen, können diese dem Fahrer als Warnung oder Information zur Verfügung gestellt werden [Lin2015, Seite 151].

Überblick der Nachricht

Die Struktur der IVI-Nachricht lässt sich von der der DENM ableiten. Die Nachricht wird von einer RSU übertragen, welche in Verbindung mit einem Rechenzentrum steht und die Information bereitstellt [Lin2015, Seite 152-153]. Auch die Entwicklung der IVI-Nachricht ist noch nicht abgeschlossen.

Es gibt verschiedene Gebiete, die für die IVI-Anwendung von Bedeutung sind. Die *Minimum Dissemination Area* gibt das Gebiet an, in dem die Nachricht verbreitet wird. Die *Detection Zone* zeigt das Gebiet an, in dem die entsprechende ITS-Station die empfangene Nachricht verarbeiten soll. Die Fahrzeuge, die sich in einer solchen Zone aufhalten, werden durch IVI auf entsprechende Straßenschilder aufmerksam gemacht [Lin2015, Seite 153].

Die *Driver Awareness Zone* wird durch die ITS-Station bestimmt, die die Nachricht empfängt. Die Daten werden dem Fahrer innerhalb einer Mindestzeit zur Verfügung gestellt, bevor er in die Relevanzzone eintritt [Lin2015, Seite 153]. Bei der Mindestzeit spielen Faktoren wie die Fahrgeschwindigkeit und die Fahrroute eine Rolle.

Die sogenannte *Relevance Zone* ist die Zone, für die ein bestimmtes Zeichen gilt. Ein Beispiel hierfür ist die Geschwindigkeitsbegrenzung, die in einem bestimmten Bereich gilt, wie in Abbildung 1.24 zu sehen ist [Lin2015, Seite 154].

Die *Reference Position* schließlich ist der Ausgangspunkt für die Beschreibung der verschiedenen Zonen [Lin2015, Seite 154]. Dabei wird die Referenzposition von allen Zonen abgedeckt. Dies ist in Abbildung 1.24 veranschaulicht. Die Referenzposition entspricht nicht immer der Position der Verkehrsschilder [Lin2015, Seite 154].

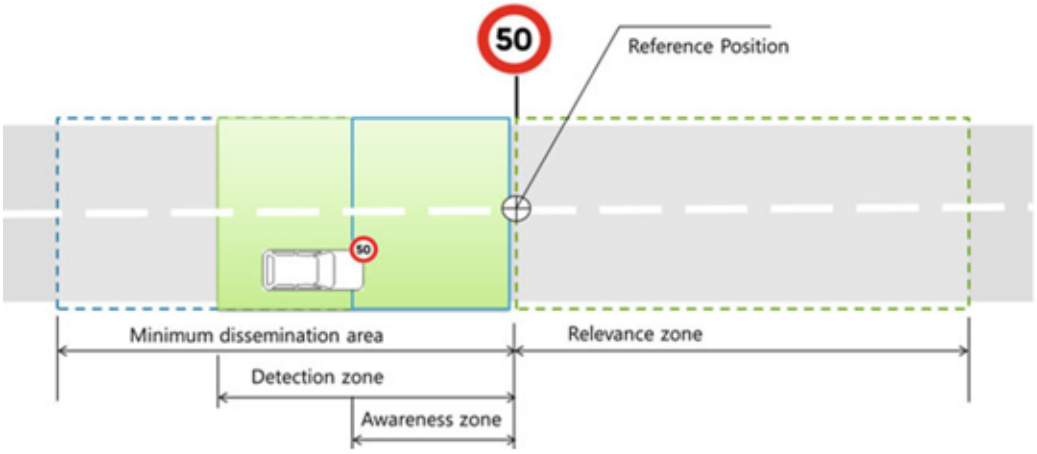

Abbildung 1.24: Übersicht der unterschiedlichen IVI Gebiete [Lin2015, Seite 153]

Format

Diese Nachricht besteht aus einer Struktur, die auf Containern basiert [Lin2015, Seite 154]. Jede IVI besteht aus mindestens einem *management Container* und optional einem oder mehreren *location container* und *application container*.

Der *management Container* enthält Verwaltungsinformationen der Nachricht.

Der *location Container* bietet Beschreibungsinformationen für eine oder mehrere Zonen sowie eine oder mehrere Referenzpositionen [Lin2015, Seite 155]. Dabei kann eine Zone durch geografische Punkte und Abstandattribute, welche von der Referenzposition ausgehen, beschrieben werden [Lin2015, Seite 155].

Der *Application Container* enthält Anwendungsdaten. Momentan kann zwischen drei verschiedenen Anwendungscontainern unterschieden werden. Es gibt den sogenannten *IVI General Container*, den *IVI Text Container* und den *IVI Layout Container* [Lin2015, Seite 155]. Der *IVI general Container* liefert Informationen zum Inhalt und Typ des Schildes. Jedes Schild ist mit einer oder mehreren Zonen verbunden, welche in dem *Location Container* beschrieben werden [Lin2015, Seite 155].

Der *Text Container* bietet dem Nutzer die Möglichkeit Textinformationen zur Verfügung zu stellen.

Der *Layout Container* definiert Layout Informationen für Verkehrszeichen [Lin2015, Seite 155]. Ziel ist es, die Verkehrszeichen im Fahrzeug so anzuordnen, wie sie am Straßenrand angeordnet sind [Lin2015, Seite 155].

Für die Sicherheit der IVI-Nachricht sieht der aktuelle Entwurf eine SSP vor, die angibt, ob die sendende ITS-Station berechtigt ist, den entsprechenden Inhalt zur Unterstützung der betreffenden Anwendung bereitzustellen [Lin2015, Seite 155].

Abbildung 1.25: IVI Nachricht [Lin2015, Seite 154]

1.7 Schutzziele

Authentizität

Ein Ziel in der V2X-Kommunikation besteht darin, bei einer Kommunikation nur legitimierte Fahrzeuge teilnehmen zu lassen [Fuchs2015, Seite 530]. „Authentizität wird auch als Echtheit des Absenders oder der Information bezeichnet“ [Baier2016]. Dies ist ein essentiell wichtiges Merkmal für die Sicherheit.

Integrität

Ein zweiter Aspekt besteht in der Integrität der Nachrichten. Versendete Informationen dürfen nicht verändert werden, dies ist insbesondere für sicherheitsrelevante Nachrichten wichtig [Moalla2011].

Vertraulichkeit

Manche Anwendungen erfordern, dass der Inhalt einer Nachricht nur für Sender und Empfänger Zugang bietet [Moalla2011].

Privatsphäre

Anonymität alleine ist für den Schutz der Privatsphäre ungeeignet, da ein Hauptanliegen darin besteht, die ITS-Stationen zu beobachten, um die Sicherheit zu erhöhen [ETSI2012b]. Somit dienen die Pseudonymität und die Unverkettbarkeit dem angemessenen Schutz der Privatsphäre. Die Pseudonymität stellt sicher, dass man einen Service nutzen

kann, ohne dabei seine Identität zu enthüllen, gleichzeitig verantwortet man sich jedoch für dessen Nutzung [ETSI2012b]. Die Unverkettbarkeit sorgt dafür, dass man Ressourcen und Services häufiger nutzen kann, ohne dass dadurch jemand eine Verbindung herstellen kann [ETSI2012b].

1.8 Public Key Infrastructure (PKI)

Zur Gewährleistung der Sicherheit innerhalb der V2X-Kommunikation wird eine „Public Key Infrastructur“ implementiert. Diese besteht aus einer *Root CA* (RCA), einer *Enrolement Authority* (EA) und einer *Authorization Authority* (AA). Die EA wird auch „long term CA“ genannt und die AA ist ebenfalls unter dem Begriff „Pseudonym CA“ bekannt [Fuchs2015, Seite 530].

Die *Root CA* stellt Zertifikate für die AAs und die EAs aus. Die *Root CA* ist für die Verwaltung der „Certificate Revocation List“ und der „Trust-service Status List“ zuständig. Die „Certificate Revocation List“ beinhaltet die widerrufenen CAs, während die „Trust-service Status List“ die vertrauenswürdigen CAs auflistet [Pierpaolo2016]. Falls es mehrere *Root CAs* gibt, kann durch Cross-Zertifizierung Vertrauen zwischen diesen hergestellt werden. Somit gilt die *Root-CA* als Vertrauensanker dieses Systems [Bißmeyer2011].

RCAs werden beispielsweise von Regierungen oder Fahrzeugherstellern betrieben, AAs und EAs von verschiedenen Behörden oder auch Fahrzeugherstellern [Lonc2016]. Es gibt also mehrere solcher *Enrolement* und *Authorization Authoritys*.

Eine zentrale Root CA vereinfacht den Prozess der Registrierung neuer EAs und AAs [Bißmeyer2011].

Die EA stellt ein sogenanntes „Enrolement Certificate“ (EC) aus während die AA sogenannte „Authorization Tickets“ (AT) erstellt [Fuchs2015, Seite 531]. Bei dem EC handelt es sich um ein langfristiges Zertifikat, während es sich bei dem AT um ein kurzfristiges Zertifikat handelt [Pierpaolo2016].

Damit ein Fahrzeug an der V2X Kommunikation teilnehmen kann, muss es zunächst in den Besitz eines EC kommen. Durch die Registrierung bei solch einer EA erhält das Fahrzeug ein EC. Mithilfe dieses Zertifikates kann nun ein Pseudonymzertifikat bei der AA angefordert werden. Bei solch einer Anfrage wird die jeweilige Identität der ITS-Station verschlüsselt übertragen, zusammen mit dem entsprechenden Zertifikat und der Kennzeichnung des EA [Pierpaolo2016]. Die AA liest die Kennzeichnung der EA und überprüft diese in der entsprechenden TSL. Nach Überprüfung wird die EA aufgefordert, die Anfrage zu validieren oder eben nicht. Falls die Anfrage validiert wird, kann das Pseudonymzertifikat an die jeweilige Station gesendet werden [Pierpaolo2016]. Ein

häufiger Wechsel der Pseudonymzertifikate soll die Privatsphäre der ITS-S gewährleisten. Dieser Vorgang ist in Abbildung 1.26 veranschaulicht.

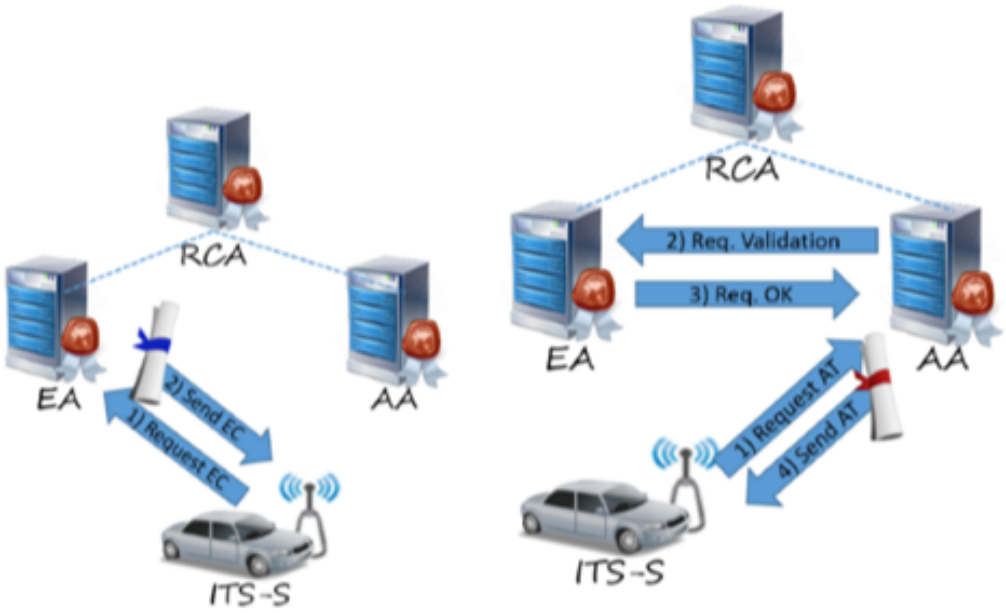

Abbildung 1.26: Public Key Infrastructure [Pierpaolo2016]

Mit Hilfe dieses Konzeptes wird die Privatsphäre der ITS-Station geschützt. Die AA kennt die Identität der jeweiligen ITS-Station nicht und vertraut auf die EA, die überprüft, ob die ITS-Station berechtigt ist ein AT zu erhalten oder nicht. Die EA hingegen kennt zwar die Identität der ITS-Station, weiß aber nicht, welches Pseudonymzertifikat von dieser Station benutzt wird [Pierpaolo2016].

Zudem wird der Schutz der Privatsphäre durch die Verhinderung eines eindeutigen Identifikators in den Nachrichten verhindert [Strubbe2017].

Der Sender signiert seine Nachrichten mit dem privaten Schlüssel eines gültigen Pseudonyms. Als Signaturalgorithmus wird ECDSA verwendet [Ullmann2016]. Die Nachricht kann anschließend mit angehängter Signatur und Zertifikat gesendet werden [Bißmeyer2011]. Auf Empfängerseite wird die Integrität der Nachricht nun mit Hilfe des öffentlichen Schlüssels in dem angehängten Zertifikat überprüft [Bißmeyer2011]. Anschließend wird festgestellt, ob das AT gültig und die entsprechende AA vertrauenswürdig ist.

Zu erwähnen ist außerdem, dass eine ITS-Station anstelle des kompletten Zertifikates auch einen 8 Byte Hashwert des Zertifikates angeben kann [Bittl2015b, Seite 73]. Dadurch wird die Nachricht gekürzt, mit dem Ziel, Bandbreite auf dem Funkkanal zu sparen [Bittl2015b, Seite 73].

Falls dem Empfänger die AA unbekannt ist, muss er im weiteren Schritt das Zertifikat, welches von der *Root CA* signiert wurde, prüfen [Fuchs2015, Seite 531]. Dieses Verfahren stellt die Integrität und die Authentizität der Nachricht sicher [Khodaei2015].

2 Methodenteil

Die im folgenden Methodenteil recherchierten Angriffe zeigen eine Auswahl von Angriffsmöglichkeiten im VANET. Der Überblick erfolgt in Bezug auf Themenfelder der Einleitung dieser Bachelorarbeit. Alle Szenarien haben Einfluss auf die Sicherheit der V2X-Kommunikation.

Sybil-Angriff

Bei einem Sybil-Angriff verwendet der Angreifer mehrere Identitäten gleichzeitig. Somit werden mehrere ITS-Stationen simuliert [ETSI2018]. Dies ist möglich, wenn ein Fahrzeug mehrere Pseudonyme gleichzeitig besitzt.

Ein Angreifer kann beispielsweise anderen Fahrzeugen und der Infrastruktur vortäuschen, dass es zu einem Stau kommt [ETSI2018].

Die Stärke eines Sybil-Angriffs hängt von der Anzahl der gültigen Pseudonyme ab [ETSI2018]. Je mehr zur Verfügung stehen, desto größer der Angriff [ETSI2018].

Denial-of-Service Angriff

Solch ein Angriff zielt auf die Verfügbarkeit eines Systems ab. In einem VANET könnte ein Angreifer zum Beispiel versuchen, durch einen DOS-Angriff die Kommunikation zwischen den Fahrzeugen und der Infrastruktur zu unterbinden [Sakiz2017].

Flooding-Angriffe beispielsweise fluten das Netzwerk, um dessen Ressourcen zu erschöpfen und auszulasten [Sakiz2017]. Folge dieses Angriffs ist, dass legitimierte Nutzer diese Ressourcen nicht mehr nutzen können [Sakiz2017]. Dies kann beispielsweise zu Unfällen führen, wenn sicherheitsrelevante Nachrichten dadurch nicht rechtzeitig empfangen werden können [Hamida2015].

Ein Distributed Denial of Service (DDOS) Angriff wird von verschiedenen Orten aus gestartet [Sakiz2017].

Ein Beispiel für einen Flooding-Angriff im VANET wäre der aus dem OSI-Schichtenmodell bekannte SYN-Flooding Angriff. Eine TCP Verbindung wird durch einen sogenannten „three way handshake“ aufgebaut. Bei einem Angriff wird eine große Anzahl an SYN-Anfragen an den Opferknoten gesendet [Mokhtar2015]. Daraufhin sendet der Opferknoten als Bestätigung eine SYN-ACK Nachricht an die gespoofte Adresse [Nema2014]. Daraufhin bekommt der Opferknoten jedoch kein ACK-Paket mehr zurück, wie es im Normalfall vorgesehen ist [Nema2014]. Durch die Menge an empfangenen

SYN-Paketen wird enorm viel Speicher reserviert. Ist der Ressourcenverbrauch zu hoch, kann das System dadurch für eine gewisse Zeit außer Betrieb gesetzt werden [Mokhtar2015, Nema2014].

GPS-Spoofing

Ein Angreifer kann mit einem GPS-Simulator falsche Informationen an Fahrzeuge schicken. Ein GPS-Simulator ist dabei in der Lage, stärkere Signale als das ursprüngliche GPS-Signal zu erzeugen [Sakiz2017]. Somit kann der Angreifer falsche Zeit- und Ortsinformationen bei dem Opfer-Fahrzeug erzeugen.

Malware Angriff

Solch ein Angriff kann beispielsweise durch Viren oder Würmer erfolgen, die das Netzwerk oder die Softwarekomponenten der ITS-S angreifen [Hamida2015].

Passive eavesdropping attack

Dieser Angriff gefährdet die Privatsphäre eines Knotens im VANET. Bei dem Angriff geht es darum, das Netzwerk zu überwachen und die Bewegungen einzelner Fahrzeuge zu verfolgen. Es handelt sich hierbei um einen passiven Angriff, er ist auch als „traffic analysis attack“ bekannt [Sakiz2017].

Sensor Tampering

Bei diesem Angriff versucht man die Sensoren eines Fahrzeuges zu täuschen, damit daraus falsche Ergebnisse resultieren [Sakiz2017]. Solche Angriffe sind wahrscheinlich, da diese intern nicht erkannt werden [Sakiz2017].

Bogus Information Attack

Im VANET stellen Fahrzeuge anderen Fahrzeugen Informationen zur Verfügung. Diese Informationen müssen jedoch nicht immer der Wahrheit entsprechen [Sakiz2017]. Ein „böswilliger“ Knoten könnte falsche Informationen an andere Knoten senden. Bei solch einem Angriff zielt der Angreifer darauf ab, andere Fahrzeuge zu manipulieren [Sakiz2017].

3 Ergebnisteil

In dieser Arbeit wurden die sicherheitsrelevanten Aspekte für die V2X Kommunikation analysiert.

Aufgabe der „Public Key Infrastructure“ ist es, Integrität, Authentizität und Privatsphäre zu gewährleisten. Eine sichere Kommunikation zwischen den Teilnehmern des Netzwerkes ist das Ziel.

Die Recherchen haben ergeben, dass sowohl Angriffe, die schon aus dem OSI-Schichtenmodell bekannt sind, als auch neue Angriffe, die nur das VANET betreffen, möglich sind. Der DOS-Angriff ist ein Beispiel, von dem beide Netzwerke betroffen sein können.

Mittels eines GPS-Spoofing-Angriffs können Zeitinformationen, die in jeder Nachricht enthalten sind, verfälscht werden. Diese Art Falschinformationen können auch durch Manipulation eines Sensors erzeugt werden.

Der Sybil-Angriff macht sich die Tatsache zunutze, dass die Implementierung der PKI, und insbesondere der Pseudonymzertifikate, Fahrzeugen die gleichzeitige Verwaltung mehrerer Identitäten ermöglicht. Das Vortäuschen falscher Identitäten im Straßenverkehr stellt so eine Angriffsmöglichkeit dar.

Insgesamt ist festzuhalten, dass es auch in diesem Netzwerk Schwachstellen gibt, die es angreifbar machen.

4 Diskussion

Die Car Forensik ist ein sehr breit gefächertes Gebiet, welches unter anderem die Frage von Sicherheitslücken aufwirft und für Software- und Hardwarehersteller in der Automobilbranche eine enorme Herausforderung darstellt. In den USA beispielsweise ist der Eingriff in das Fahrzeugsteuerungssystem über das Internet bereits gelungen [Käfer2015, Seite 48]. Durch einen Implementierungsfehler einer Unterhaltungseinheit konnte man die Bremsen und den Antrieb eines Jeeps Cherokee kontrollieren [Käfer2015, Seite 48]. Der Angriff war durch die IP-Adresse des Fahrzeuges über das Internet möglich [Käfer2015, Seite 48].

Sicherheitsexperten in den USA gelang es mittels eines Adapters auf dem OBD Port über WLAN eine Verbindung zum Computer aufzubauen und somit Kontrolle über das Auto zu erlangen [Käfer2015, Seite 47]. Die Angreifer waren in der Lage die Lenkung des Fahrzeugs zu kontrollieren [Käfer2015, Seite 47]. Um den Angriff durchführen zu können, braucht man vorher Zugriff zum Inneren des Fahrzeuges.

Ein anderes Beispiel wäre BMW „ConnectedDrive“, welche es Fahrzeugen ermöglicht, sich mit der Infrastruktur zu vernetzten [Käfer2015, Seite 141]. Über die Applikation „Remote“ kann man über das Smartphone bestimmte Funktionen des Fahrzeuges abrufen, wenn dies mit „ConnectedDrive“ ausgestattet ist [Käfer2015, Seite 145]. Mit dieser App ist es möglich, das Fahrzeug zu orten und ähnliches. Startet man die App zum ersten Mal, muss man zunächst Sicherheitsfragen beantworten, die vorher im BMW-Portal eingestellt wurden. Gelingt es einem Angreifer nun in den Besitz des Handys zu gelangen und erhält er dadurch entsprechende Daten, kann er die Zugangsdaten für das Portal ändern und hat somit auch die Möglichkeit, das Fahrzeug zu orten [Käfer2015, Seite 148].

In dieser Diskussion werden verschiedene Angriffsmöglichkeiten auf die V2X-Kommunikation und das Netzwerk analysiert und mögliche Verhinderungsmaßnahmen vorgestellt.

Angriffe auf Zeit- und Ortsinformationen

In der Einleitung wurden bereits Mechanismen zur Gewährleistung der Sicherheit von Kommunikation dargelegt. Im Rahmen dieser Bachelorarbeit wird ein Schwerpunkt auf die Absicherung der Kommunikation durch Zertifikate gelegt. Diese weisen ihre Gültigkeit durch Zeitstempel auf. Neben dem Gültigkeitsnachweis kann auch die Aktualität der Nachricht durch den Empfänger geprüft werden.

Manipuliert man die Zeitstempel, könnten sicherheitsrelevante Nachrichten wie CAMs oder DENMs verfälscht werden. Eine Möglichkeit die Zeitstempel zu verändern bietet

das GPS-Spoofing, dessen Anwendbarkeit im folgenden Paper untersucht wird.

Das Paper “Emerging Attacks on VANET Security based on GPS Time Spoofing“ befasst sich mit der Auswertung verschiedener Angriffe. Zu diesem Zweck werden unterschiedliche Szenarien getestet.

GPS-Spoofing macht es dem Angreifer möglich, GPS-Signale zu verfälschen. Die entsprechende ITS-Station empfängt dadurch verfälschte Orts- und Zeitinformationen [Bittl-2015a]. Wird das GPS-Signal so manipuliert, dass das entsprechende ITS-System dadurch einen Zeitstempel erhält, der in der Zukunft liegt, kann sogar die Verfügbarkeit eines Systems verletzt werden. Der Zeitstempel kann so weit in die Zukunft gesetzt werden, dass die entsprechende ITS-Station für diesen Zeitraum keine gültigen Zertifikate besitzt.

Folge eines solchen Angriffes ist, dass alle erhaltenen Nachrichten als ungültig angesehen werden, da diese einen Zeitstempel aufweisen, der für die angegriffene ITS-Station als abgelaufen erscheint, da er in der Vergangenheit liegt [Bittl2015a].

Es besteht zwar die Möglichkeit für die Kommunikation in einen unsicheren Modus zu wechseln, allerdings würden die anderen ITS-Systeme diese Meldungen vermutlich ignorieren, da sie als nicht vertrauenswürdig angesehen würden [Bittl2015a].

In einer Versuchsumgebung haben Forscher die GPS-Spoofing-Methode getestet. Verwendet wird eine ITS-S Hardware der Firma Cohda. Das Gerät hat eine drahtlose Verbindung zu einem GPS-Gerät und wird als DUA (Device under attack) bezeichnet, weil es das zu attackierende Gerät darstellt [Bittl2015a].

In der Testumgebung wird der DUA zunächst ein gefälschtes GPS-Signal von Beginn des Betriebes an zur Verfügung gestellt.

In dem ersten Szenario besitzt die DUA Pseudonymzertifikate, die in dem Zeitraum des erhaltenen GPS-Signals gültig sind [Bittl2015a]. Es wird überprüft, ob die DUA Nachrichten generiert, die den gleichen Zeitstempel wie das gefälschte GPS-Signal aufweist [Bittl2015a].

In einem zweiten Szenario enthält die DUA Pseudonymzertifikate, die nicht in dem Zeitraum des erhaltenen GPS-Signals gültig sind [Bittl2015a].

Die Ergebnisse zeigen, dass es in dem ersten Szenario zur Generierung von Nachrichten mit falschen Zeitstempeln gekommen ist. In dem zweiten Szenario wurden keine Nachrichten versendet und somit war der DOS-Angriff erfolgreich [Bittl2015a].

Die Durchführung der Versuche haben gezeigt, dass der im Methodenteil beschriebe-

ne Angriff des GPS-Spoofings möglich ist. Weiter wurde festgestellt, dass man durch ein verfälschtes GPS-Signal einen DoS-Angriff bewirken kann.

Die Ergebnisse verdeutlichen, dass ein DOS-Angriff wie beschrieben eine Bedrohung für die Verkehrssicherheit ist. Ist ein Fahrzeug durch verfälschte Zeitstempel von der Kommunikation ausgeschlossen, kann es keine Statusinformationen von anderen Verkehrsteilnehmern erhalten und somit ist der kooperative Informationsaustausch im Straßenverkehr nicht möglich.

Allerdings ist gerade dies eines der Ziele, die in Zukunft durch die Kommunikation von Fahrzeugen miteinander erreicht werden sollen, da dies maßgeblich zur Sicherheit beiträgt. Betrifft ein DOS-Angriff mehr als ein Fahrzeug, kann dies deutlich größere Auswirkungen haben und den positiven Effekt der V2X-Kommunikation, nämlich der erhöhten Sicherheit und Effizienz, trüben.

Sybil-Angriff

In der Zukunft liegenden Zeitstempel können einen Sybil-Angriff ermöglichen [Bittl-2015a]. Bei diesem hat der Täter die Möglichkeit, mehrere Identitäten gleichzeitig anzunehmen und so die Illusion von weiteren Verkehrsteilnehmern zu erzeugen [Bißmeyer2014]. Dieser Angriff ist möglich, wenn ein Fahrzeug mit einem Satz von Pseudonymzertifikaten ausgestattet ist, die sich in ihrer Gültigkeit überlappen [Bißmeyer2014]. Als Resultat kann der Angreifer mehrere Pseudonymzertifikate parallel nutzen. Die Knoten, die aufgrund der verschiedenen Pseudonyme erstellt werden, können dazu beitragen, die Quantität gefälschter Nachrichten zu erhöhen [Gu2016].

In dem Paper “Emerging Attacks on VANET Security based on GPS Time Spoofing“ soll der Sybil-Angriff durch die Generierung von zukünftigen Zeitstempeln verursacht werden. Verschiedene Ansätze beschreiben, wie man an einen zukünftigen Zeitstempel gelangen kann. Das Hinzufügen einer festen Zeitkonstante zu dem empfangenen GPS-Signal oder aber die Erzeugung von GPS-Nachrichten mit willkürlicher Zeit- und Positionsinformation sind Beispiele hierfür [Bittl2015a].

Das Gelingen des Angriffes ist wahrscheinlicher, wenn dieser vor dem Start des Fahrzeuges stattfindet [Bittl2015a]. Ist der Neustart des Autos für den Angriff essentiell, kann sich der Angreifer Gebiete, wie zum Beispiel Parkplätze aussuchen, bei denen solch eine Aktion wahrscheinlich ist [Bittl2015a].

Der Versuchsaufbau des Sybil-Angriffes ist der gleiche wie bei dem DOS-Angriff im vorherigen Abschnitt. Auch hier wird eine ITS-Hardware der Firma Cohda verwendet.

Im Test wird dem DUA das gleiche GPS-Signal mehrfach zur Verfügung gestellt. Bevor das GPS-Signal neu zur Verfügung gestellt wird, wird die DUA zurückgesetzt [Bittl-

2015a]. Mittels dieses Tests soll geprüft werden, ob die DUA mehrere Nachrichten mit unterschiedlichen Pseudonymzertifikaten für die gleiche Zeitspanne signiert hat [Bittl-2015a].

Die Ergebnisse des Versuches zeigen, dass die CAMs mit unterschiedlichen Pseudonymzertifikaten signiert wurden und somit ein Sybil-Angriff möglich ist [Bittl2015a].

Die Versuche haben verdeutlicht, dass durch mehrfachen Besitz von Pseudonymzertifikaten die Gefahr der Illusion von Fahrzeugen entsteht [Bittl2015a]. Durch die beschriebenen Angriffe auf die Zeit- und Positionsinformationen ist anzumerken, dass dadurch die Zuverlässigkeit dieser Informationen in Frage gestellt werden kann.

Lösungsvorschläge gegen Angriffe auf Zeit- und Ortsinformationen

Es wurden verschiedene Lösungsvorschläge entwickelt, um zukünftige Zeitstempel zu verhindern, die im Folgenden diskutiert werden [Bittl2015a].

Zeitsynchronisationssysteme, wie beispielsweise ntpd, folgen dem Prinzip, dass ein Zeitsprung nur in eine Richtung möglich ist, nämlich in die Zukunft. Damit wird sichergestellt, dass die Zeit monoton steigend ist. Hierfür muss nur der höchste Wert gespeichert werden [Bittl2015a]. Der Nachteil dieser Methode besteht darin, dass dies zu einem permanenten DOS-Angriff führen kann. Ist der Angreifer einmal in der Lage, die Zeitbasis einer OBU zu manipulieren und somit die Zeit in die Zukunft zu setzten, kann dadurch ein Fahrzeug von der Kommunikation ausgeschlossen werden [Bittl2015a]. Deshalb eignet sich diese Methode eher weniger für eine Angriffsabwehr.

Ein weiterer Ansatz besteht darin, die Lebensdauer von Pseudonymzertifikaten zu begrenzen. Diese Zertifikate sollen nur eine recht kurze Zeitspanne gültig sein [Bittl2015a]. Im Idealfall wird ein neues Zertifikat ausgeliefert, bevor die Lebenszeit des Vorgängers abgelaufen ist [Bittl2015a].

Privatheit durch Pseudonyme

Nachrichten werden unverschlüsselt übertragen und können von jedem Verkehrsteilnehmer in Reichweite mitgelesen werden. Dies birgt die Gefahr in sich, dass ein Angreifer verschiedene Ortsinformationen eines Fahrzeuges sammeln könnte, um dieses anschließend zu tracken. Eine Lösung dieses Problems könnte die Verwendung von verschiedenen Pseudonymen darstellen, die in der Einleitung bereits beschrieben wurden, und die die Privatsphäre des Fahrzeuges schützen sollen. Mit Hilfe der Pseudonyme soll das Tracken anderer Verkehrsteilnehmer erschwert bzw. verhindert werden. Nichtsdestotrotz stellt sich die Frage, ob durch den häufigen Austausch von Statusmeldungen zwischen den Fahrzeugen und den darin enthaltenen Orts- und Zeitinformationen die Möglichkeit besteht, die Pseudonyme miteinander zu verbinden [Wiedersheim2010]. Genau dieser

Ansatz wurde in dem Paper „Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough“ untersucht.

Das Paper geht von einem Angreifer aus, der perfekte Abhörmöglichkeiten besitzt [Wiedersheim2010]. Er soll, nachdem er bestimmte Positionsinformationen gesammelt hat, den Multiple Hypothesis Tracking (MHT) - Algorithmus benutzen, um diese Samples zu Positionsprofilen zu verbinden [Wiedersheim2010]. Allgemein bewegen sich mehrere Ziele im Raum, die periodisch abgetastet werden [Wiedersheim2010]. Diesen Zielen werden Positionsmessungen zugeordnet, um eine Spur zu bilden.

Der MHT-Algorithmus generiert jedes Mal, wenn eine Reihe von Messungen auftritt, eine Hypothese bezüglich der Datenzuordnung [Wiedersheim2010]. Die Hypothese stellt die Möglichkeit der Zuordnung zum Ziel dar [Wiedersheim2010]. Für jede Hypothese wird die Wahrscheinlichkeit berechnet und diejenige mit der höchsten Wahrscheinlichkeit wird gewählt. MHT verwendet den Kalman Filter, um die Zustandsgrößen, also Position und Geschwindigkeit des Ziels, zu schätzen [Wiedersheim2010]. Zur Optimierung wird der Zero-Scan Algorithmus verwendet, da die Anzahl der Hypothesen sehr schnell wachsen kann. Der Zero-Scan Algorithmus folgt dabei nur der Hypothese mit der größten Wahrscheinlichkeit und verwirft alle anderen [Wiedersheim2010].

Für die Erstellung einer solchen Simulation wird der JiST/SWANS Ad-hoc Netzwerksimulator in Kombination mit STRAW verwendet [Wiedersheim2010]. STRAW ist für die Simulierung von Fahrzeugbewegungen zuständig [Wiedersheim2010]. Zunächst wird überprüft, inwieweit die Trackingrate von der Nachrichtenrate abhängt. Für jede neue Nachricht wird ein anderes Pseudonym verwendet [Wiedersheim2010].

Es stellt sich heraus, dass bei einer geringen Fahrzeugdichte und bei einer hohen Nachrichtenrate die Trackingdauer ca. 800 Sekunden oder mehr beträgt. Im Durchschnitt ist eine Verfolgung von 800 bis 1000 Sekunden möglich [Wiedersheim2010]. Allerdings sinkt der Erfolg bei einer höheren Fahrzeugdichte. Zu erkennen ist außerdem, dass die meisten Fehler an einer Kreuzung auftreten. Bei einer niedrigen Nachrichtenrate ist die Verfolgung von Spuren weniger gut möglich [Wiedersheim2010].

Insgesamt ist anzumerken, dass dieses Paper von einem globalen Angreifer ausgeht, der perfekte Abhörmöglichkeiten hat. In der Realität ist es eher unwahrscheinlich, dass ein Hacker in der Lage ist, alle gesendeten Nachrichten abzufangen. Insofern sind die Ergebnisse tendenziell als unrealistisch einzustufen. Auch im Paper selbst wird angemerkt, dass ein Täter, der nicht alle Nachrichten abhören kann, deutlich schwächer wäre.

Betrachtet man die Felder in einer CAM, lässt sich feststellen, dass einige Felder Daten enthalten, die sich nicht ändern, wie beispielsweise die Länge und Breite eines Fahrzeuges sowie die Protokollversion etc. Durch die unverschlüsselte Nachrichtenübertragung sind diese Daten für einen Angreifer verfügbar. Fragwürdig ist daher, ob ein Wechsel der

Pseudonyme sinnvoll sein kann, wenn die Nachricht konstante Datenfelder enthält, die sich auch bei einem Wechsel der Pseudonyme nicht ändern. Mit genau dieser Untersuchung hat sich Sebastian Bittl in seiner Doktorarbeit beschäftigt [Bittl2017].

Für seine Untersuchung verwendet Sebastian Bittl die Metrik „Vehicle Uniqueness“ (VU). VU ist ein Maß für Zusatzinformationen, sprich konstanten Daten [Bittl2017]. Um VU zu berechnen wird ein Vektor e_i definiert, der alle konstanten Daten enthält, die für ein Fahrzeug zur Verfügung stehen [Bittl2017]. I stellt eine Gruppe von Knoten dar, die während eines Pseudonymwechsels kooperieren. VU gibt die Wahrscheinlichkeit an, dass es einen Knoten in I gibt, der einen bestimmten Vektor e_i aufweist [Bittl2017]. Knoten, die einen gleichen Vektor aufweisen, sind für den Angreifer nicht unterscheidbar. Solche Knoten bilden ein Anonymitätsset [Bittl2017]. Die Verteilung des Anonymitätssets wird durch eine kumulierte Verteilungsfunktion dargestellt (CDF) [Bittl2017].

Die Simulation wird mit dem ezCar2X Framework durchgeführt. Dieses stellt den ETSI Protokollstapel zur Verfügung [Bittl2017]. Der ezCar2X Protokollstapel wird in ns-3 eingebettet und über die TraCI-Schnittstelle mit SUMO verbunden [Bittl2017]. Die Verkehrsdichte variiert.

In der ersten Versuchsreihe werden in dem Vektor e_i drei konstante Datenfelder berücksichtigt, nämlich die Identifizierung der Authorization Authority sowie die Länge und die Breite des Fahrzeugs. Die Ergebnisse dieses Versuches zeigen, dass ein Angreifer in der Lage ist, die Fahrzeuge zu tracken, trotz eines Pseudonymwechsels [Bittl2017].

Um den Möglichkeiten der Fahrzeugverfolgung entgegenzuwirken, wird im nächsten Versuchsdurchlauf eine gemeinsame AA für alle Fahrzeuge verwendet. Somit enthält der e_i Vektor nur noch zwei Felder, nämlich die Länge und die Breite eines Fahrzeugs [Bittl2017]. Im Vergleich zum vorherigen Versuch haben sich im Ergebnis die Anonymitätssets verringert. Folglich hat sich die Privatsphäre der Knoten verbessert. Trotzdem ist die Anzahl der Anonymitätssets hoch und es gibt viele Sets, die nur eine geringe Anzahl der Gesamtmenge ausmachen [Bittl2017].

In einer dritten Versuchsreihe soll die Genauigkeit der Dimensionsangaben, sprich der Länge und der Breite eines Fahrzeuges, reduziert werden, um die VU zu verringern [Bittl2017]. Auch hier zeigen die Resultate, dass die Anzahl der Anonymitätssets reduziert werden kann und somit die Privatsphäre verbessert wird [Bittl2017]. Aber auch hier ist eine Verfolgung der Knoten möglich [Bittl2017].

Der im Methodenteil erwähnte Angriff des „Passive eavesdropping“ kommt den im Paper beschriebenen Angriffen gleich. Es handelt sich sowohl um einen passiven Angriff als auch um das Belauschen der Kommunikationen zwischen den Fahrzeugen.

Vergleicht man die beiden Vorgehensweisen der Arbeiten miteinander, ergibt sich, dass in

der ersten Arbeit die Geschwindigkeits- und Positionsdaten in Betracht gezogen wurden, während im zweiten Ansatz der Fokus auf den konstanten Datenfeldern einer Nachricht lag. Im ersten Paper hat der Trackingversuch bei hoher Verkehrsdichte keine guten Ergebnisse erzielt, dies war im zweiten Paper anders. Hier versucht Sebastian Bittl außerdem herauszufinden, ob sich die Ergebnisse durch Streichen bestimmter konstanter Daten verbessern lassen. Im ersten Paper werden keine Lösungsmöglichkeiten aufgezeigt.

Evaluierung sicherheitsrelevanter Nachrichten bei hoher Verkehrsdichte

Ein wichtiger sicherheitsrelevanter Aspekt in der Carforensik ist die verzögerungsfreie Übermittlung von Nachrichten. Die Frage, die sich dabei stellt ist, ob das MAC-Protokoll, welches von dem Standard ETSI verwendet wird, zuverlässig ist. Um dieser Frage nachzugehen haben verschiedene Paper Simulationsumgebungen entwickelt, die die Performance des MAC-Protokolls bei hoher und niedriger Fahrzeugdichte beschreiben.

Im Paper „An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications“ wird der Fokus der Untersuchung auf die Performance von MAC gelegt, insbesondere werden Sicherheitsanwendungen berücksichtigt [Kloiber2010]. Für die Modellierung des Verkehrs auf der Autobahn wird ein stochastischer Ansatz verwendet [Kloiber2010].

Die Fahrzeuge sind mit Kommunikationseinheiten ausgestattet, um Nachrichten periodisch versenden zu können [Kloiber2010]. Fahrzeuge werden außerdem mit einer Geschwindigkeit von 20 m/s (72 km/h) auf der äußeren Spur und bis 40 m/s (144 km/h)auf der inneren Spur erzeugt [Kloiber2010]. Zudem wird eine Datenrate von 6Mbit/s und eine Kanalbreite von 10 MHz verwendet.

Um die Anwendbarkeit zu testen, ist eine Metrik für die Performance notwendig [Kloiber2010]. Das sogenannte „update delay“ wird in der „Complementary Cumulative Distribution Function“ (CCDF) repräsentiert. Die update delay Verteilung wird verwendet, um die Performance des MAC-Protokolls zu analysieren [Kloiber2010]. „Update delay“ stellt eine Metrik dar, die auf der Seite des Nachrichtenempfängers verwendet wird. Sie bildet die Zeitdifferenz zwischen zwei aufeinanderfolgenden Nachrichten ab, die vom gleichen Sender versendet werden [Kloiber2010]. Auf dieser Grundlage baut die Empfängerseite ein Histogramm aus den akkumulierten „update delays“ auf. Ist die Simulation abgeschlossen, wird das Histogramm verwendet, um die CCDF abzuleiten [Kloiber2010].

Wie aus der Einleitung bekannt ist, wird CAM benutzt, um Statusinformationen eines Fahrzeugs an die Umgebung zu verteilen. Je nachdem wann man die letzte CAM erhalten hat, sind die Informationen aktuell oder weniger aktuell [Kloiber2010]. Die Metrik „update delay“ stellt die Aktualität der Informationen beim Empfang dar, welches eine Voraussetzung von Sicherheitsanwendungen ist [Kloiber2010].

Für die Performanceanalyse wird die Open Source event-basierte Simulationsumgebung ns-3 verwendet [Kloiber2010]. Die Nachrichtenrate wird bei verschiedenen Simulationsdurchläufen variiert. Die Nachrichtengrößer beträgt 500 Byte [Kloiber2010]. Die Simulationszeit wird auf 10 Minuten pro Lauf gesetzt.

Die Variation in der Simulation wird durch zwei Parameter geregelt, von der „Mean Time Ahead Distance“ (MTDA) zwischen aufeinanderfolgenden Fahrzeugen und von der jeweiligen Nachrichtenfrequenz [Kloiber2010].

Die Ergebnisse des Versuchs sind in der folgenden Abbildung dargestellt.

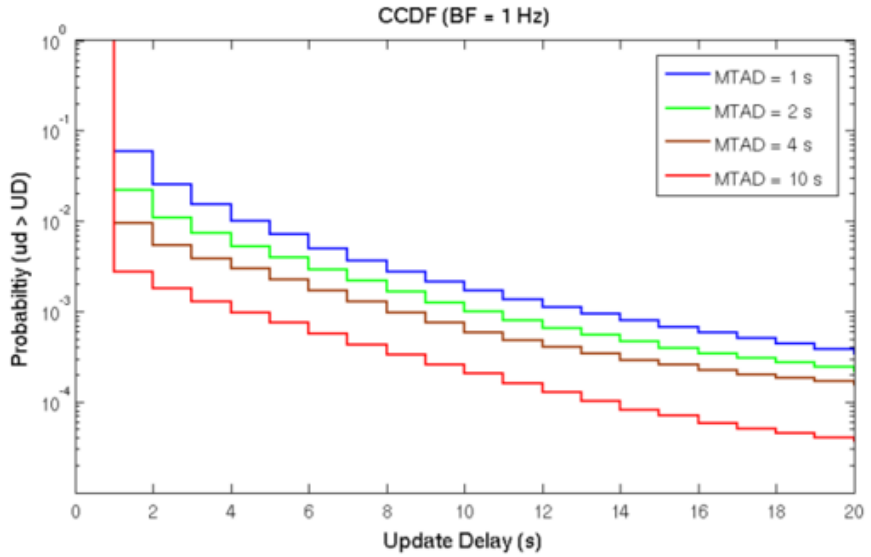

Abbildung 4.1: Update Delay Verteilung für eine Frequenz von 1 Hz und verschiedenen MTDAs [Kloiber2010]

Man kann nun eine Kurve auswählen und daraus einen Zuverlässigkeitswert ableiten [Kloiber2010]. Wählt man beispielsweise die rote Kurve, die eine sehr geringe Dichte an Fahrzeugen darstellt, kann man dazu eine maximale „update delay“ wählen. CCDF wird verwendet, um die Zuverlässigkeit einer Sicherheitsanwendung zu bestimmen, indem man die Wahrscheinlichkeit von 1 abzieht [Kloiber2010]. Somit gibt die y-Achse die Wahrscheinlichkeit an, dass ein „update delay“ größer als ein bestimmter Wert auf der x-Achse ist. Das Paper hat bei einem MTAD Wert von 10 s und einem update Delay Wert von 5 s eine Berechnung der Zuverlässigkeit durchgeführt (rote Kurve). Es konnte eine Zuverlässigkeit von 99,925 % ermittelt werden [Kloiber2010]. Bei einem MTAD von 1 s und einem update delay Wert von 5 s ergab die Auswertung eine Zuverlässigkeit von 99,3 % [Kloiber2010].

Daraus resultiert, dass bei einer höheren Verkehrsdichte die Wahrscheinlichkeit größer

ist, das maximale „update delay“ zu überschreiten. Bezüglich der physikalischen Schicht gelten Sicherheitskommunikationssysteme als zuverlässig, wenn maximal eine Fehlerrate von 10^{-8} erreicht wird [Kloiber2010]. Es ist jedoch erkennbar, dass die meisten Sicherheitsanwendungen bei einer Frequenz von 1 Hz eine Ausfallwahrscheinlichkeit von 10^{-3} aufweisen [Kloiber2010]. Insgesamt lässt sich festhalten, dass die Zuverlässigkeit bei höherer Verkehrsdichte sinkt.

Ein weiteres Paper hat sich mit der Auswirkung der eingeführten Sicherheitsprozesse auf zeitkritische Anwendungen beschäftigt.

Wie schon in der Einleitung erwähnt, werden Sicherheitsmechanismen integriert, um die Authentizität, die Integrität und die Privatsphäre zu schützen, Wie bereits bekannt ist, wird hierfür eine „Public Key Infrastructure “ implementiert. Die Nachricht wird auf der Senderseite signiert und auf der Empfängerseite wiederum verifiziert [Brahim2015]. Es stellt sich die Frage, inwieweit diese Prozesse die Kommunikationseffizienz beeinflussen. Genau mit dieser Analyse hat sich das Paper „Performance Impact of Security on Cooperative Awareness in Dense Urban Vehicular Networks“ beschäftigt [Brahim2015].

Für diese Versuchsreihe wurde der ns-3 Netzwerksimulator verwendet. Verschiedene Szenarien werden dargestellt, die sich in der Verkehrsdichte unterscheiden [Brahim2015]. SUMO wird für die Mobilitätsspuren verwendet [Brahim2015]. In dem Szenario mit niedriger Dichte werden 50 Fahrzeuge pro Quadratkilometer gewählt, für die mittlere Dichte 100 Fahrzeuge und für die hohe Dichte 200 Fahrzeuge pro Quadratkilometer [Brahim2015].

Es sei bemerkt, dass sich diese Arbeit auf die oberen Schichten (Sicherheit und Anwendungen) konzentriert [Brahim2015]. Deshalb wird DCC für die Kanalsteuerung auf der MAC-Schicht vernachlässigt [Brahim2015].

Die Ergebnisse der Versuche zeigen, dass die Verzögerungen der CAMs mit der Verkehrsdichte korreliert. Weiter wurde in Erfahrung gebracht, dass bei nahe liegenden Nachbarn etwa 75% der Paketlieferung erreicht wurden, sowohl bei hoher als auch bei niedriger Netzwerkdichte. Für Knoten, die weiter entfernt waren, pendelte sich die Paketlieferungsrate bei einem dichten Netzwerk auf weniger als 30 % ein, bei einem spärlichen Netz auf weniger als 50 % ab ca. 300 m Entfernung [Brahim2015]. Ist die Paketrate hoch, kann es bei nahe aneinander liegenden Knoten aufgrund der Sicherheitsmaßnahmen zu zusätzlichen Verzögerungen kommen [Brahim2015].

Vergleicht man die beiden Vorgehensweisen miteinander, lässt sich feststellen, dass beide Paper auf den ns-3 Simulator zurückgreifen. Das zweite Paper verwendet zusätzlich den SUMO Simulator. In dem Paper „An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications“ werden Sicherheitsaspekte in die CAM integriert. Auch in dem Paper „Performance Impact of Security on Cooperative Awareness in Den-

se Urban Vehicular Networks“ werden die Sicherheitsmechanismen integriert. Zusätzlich wird bei der Paketlieferung die Distanz betrachtet, was in dem anderen Paper nicht der Fall ist.

Resultat des ersten Papers: Erhöht sich die Fahrzeugdichte, erhöht sich auch die Wahrscheinlichkeit den „Update Delay“ Wert zu überschreiten. Mit anderen Worten, der Pakettransport zweier aufeinanderfolgender CAMs dauert länger.

Resultat des zweiten Papers: Bei hohem Netzwerkverkehr nimmt die Paketlieferrate bei weiterem Abstand zwischen den Knoten ab.

Beide kommen zu dem Schluss, dass die Paketlieferrate mit der Netzwerkdichte korreliert.

Flooding

Der Keep Alive Forwarding (KAF) Algorithmus wird, wie bereits in der Einleitung erklärt, verwendet, um DENMs zwischenzuspeichern und später eventuell weiterzuleiten [Tubbene2015].

In der Arbeit „Performance Evaluation of V2V and V2I Messages in C-ITS“ werden Vor- und Nachteile dieses Algorithmus erörtert. KAF erlaubt es Fahrzeugen, diejenigen DENMs immer wieder zu senden, welche diese bereits weitergeleitet haben [Tubbene2015]. Der Autor beschreibt in seiner Arbeit das Risiko eines zusätzlichen Verkehrsoverheads durch die zuvor beschriebenen Wiederholungen von Nachrichtensendungen [Tubbene2015].

Es ist durchaus wahrscheinlich, dass sich im Straßenverkehr unterschiedliche DENMs verschiedener Sender auf das gleiche Event beziehen [Tubbene2015]. Somit ist es sehr gut möglich, dass DENMs, die für das gleiche Event zwischengespeichert sind auch für das gleiche Event wieder ausgestrahlt werden [Tubbene2015]. Dieses „re-broadcasting“ führt zu einem erhöhten Datenverkehr.

Durchführung eines Flooding-Angriffes

Die Arbeit „Abusing Keep-Alive Forwarding to flood a VANET“ beschäftigt sich ebenfalls mit dem KAF-Algorithmus und untersucht, ob es möglich ist, mit Hilfe dieses Algorithmus und den DENMs ein Netzwerk zu fluten. Zur Untersuchung werden einige Tests durchgeführt [Billman2016].

Mit Hilfe von Veins wird eine Simulationsumgebung aufgebaut. Veins ist ein Simulator, der eine Interaktion zwischen dem Netzwerksimulator OMNeT++ und dem Verkehrssimulator SUMO ermöglicht [Billman2016]. Die Mobilitätsmuster der Knoten, die

durch OMNeT++ erstellt werden, werden statisch berechnet und somit nicht von realen Verkehrsbeobachtungen beeinflusst [Billman2016]. SUMO verwendet Dateien von Livemessungen und kann OMNeT++ ergänzen. Die Simulationen laufen parallel über das „Traffic Control Interface“ ab, der die Kommunikation zwischen OMNeT++ und SUMO ermöglicht [Billman2016].

Es werden insgesamt 40 Simulationen durchgeführt, 20 davon stellen einen Angriff dar. Jeder Durchgang dauert 75 Sekunden [Billman2016]. 32 Fahrzeuge fahren hier in beide Richtungen [Billman2016]. Um nachher Rückschlüsse ziehen zu können, testet man zunächst, wie sich die DENM normalerweise verhält. Deshalb wird erst einmal eine Situation simuliert, in der ein Fahrzeug ein Problem hat und daraufhin eine DENM versendet. Diese kann in dem KAF-Cache der Fahrzeuge, die sich innerhalb der Relevanzdistanz befinden, gespeichert werden [Billman2016]. Um die Situation so realistisch wie möglich zu gestalten, werden CAMs von jedem Fahrzeug zehn Mal pro Sekunde versendet [Billman2016].

In einem zweiten Szenario wird der Versuch unternommen, ein Netzwerk zu fluten, indem ein Fahrzeug kontinuierlich DENMs mit einer eindeutigen ActionID versendet. Diese sorgen dafür, dass die DENMs jeweils einen Eintrag und Timer (Gültigkeit, Weiterleitung) in der KAF erhalten [Billman2016]. Insgesamt werden 307 einzigartige DENMs erzeugt. Um die Weiterleitung der DENMs durch andere Fahrzeuge auszulösen, wird das „transmissionInterval“ auf einen niedrigen Wert gesetzt (2 Millisekunden), die Relevanzdistanz hingegen auf einen hohen Wert. Die Gültigkeitsdauer wird mit einem willkürlichen Wert versehen, der länger als die Simulation andauert [Billman2016].

Die Resultate der Versuche zeigen, dass während eines Angriffs 17,5% der Fahrzeuge keine DENM von dem Auto erhalten haben, das ein Problem hatte (Auto aus Szenario 1). Als kein Angriff stattfand, haben hingegen alle Fahrzeuge die entsprechende DENM erhalten [Billman2016]. Durch den Angriff fand außerdem eine starke Nachrichtenverzögerung statt. Nach einer Sekunde erreichte die reale DENM aus Szenario 1 nur fünf Autos [Billman2016]. Die anderen Fahrzeuge erhielten die Nachricht mit einer Verzögerung von mehr als zehn Sekunden [Billman2016]. Außerdem gehen während des Angriffs 60 % der Pakete der rechtmäßigen DENM verloren [Billman2016].

Die Versuche zeigen, dass man den KAF-Algorithmus missbrauchen kann, um das Netzwerk zu fluten. Dies stellt ein Sicherheitsrisiko für die V2X - Kommunikation dar, da man sich in solch einem Fall nicht mehr auf das Netzwerk verlassen kann. Außerdem widerspricht dies den in der Einleitung herausgearbeiteten Sicherheitsanforderungen, nämlich einer zuverlässigen Datenübertragung. Die Informationen in der V2X-Kommunikation sind zeitsensitiv. Jegliche Zeitverzögerung kann verursachen, dass versendete Informationen den Empfänger in der risikorelevanten Zeit nicht mehr erreichen.

Die Ergebnisse zeigen außerdem, dass sich auch die Vermutung des erhöhten Daten-

verkehrs aus dem Paper „Performance Evaluation of V2V and V2I Messages in C-ITS“ bestätigt.

Adressierung des Problems der mehrfachen Einträge zu einem Event

Die Arbeit „Performance Evaluation of V2V and V2I Messages in C-ITS“ adressiert das Problem, dass möglicherweise mehrere DENMs das gleiche Event beschreiben. Diese werden jedoch weder von der Logical dynamic map noch von KAF als solche erkannt.

Auch das Paper „Efficient and Unique Identifier for V2X Events Aggregation in the Logical Dynamic Map“ beschäftigt sich mit dem Problem, dass das gleiche Ereignis, an welchem unterschiedliche Fahrzeuge teilnehmen, mehrmals in der LDM zu finden ist.

Die Lösung, welche das Paper vorschlägt, besteht in der Aggregierung der DENMs bzw. der Einträge in der LDM, die das gleiche Ereignis beschreiben [Menouar2011]. Um dies so effizient wie möglich zu gestalten, muss der Ort des Ereignisses, die ActionID sowie die „Natur des Ereignisses“ berücksichtigt werden [Menouar2011]. Zunächst werden alle Ereignisse mit dem gleichen Typ in einer Gruppe zusammengefasst [Menouar2011]. Anschließend werden Ereignisse aggregiert, die sich am gleichen Ort befinden. Die Distanz zwischen den Orten der Ereignisse muss unterhalb eines vordefinierten Schwellwertes liegen [Menouar2011].

Bogus Information

Ein weiteres Paper hat sich mit der Möglichkeit der Verbreitung falscher Informationen beschäftigt.

Das Paper „Short Paper: Experimental Analysis of Misbehavior Detection and Prevention in VANETs“ untersucht die Weitergabe falscher Informationen, die durch die Installation einer Malware ausgelöst werden. Anschließend werden Gegenmaßnahmen vorgeschlagen [Bißmeyer2013].

Für die Durchführung des Angriffes wird die EEBL-Funktion eines Fahrzeuges missbraucht. Kommt es bei einem Auto zu einer Notbremsung, sendet es daraufhin eine DENM, um die Nachbarn zu informieren. Nach dem Empfang einer DENM berechnet die EEBL-Anwendung, ob sich das bremsende Fahrzeug im Relevanzbereich befindet. Ist dies der Fall, wird dem Fahrer eine Warnung angezeigt [Bißmeyer2013].

Für den Test des Angriffes werden drei Autos verwendet, die jeweils mit einem V2X Kommunikationssystem ausgestattet sind [Bißmeyer2013]. Bei einem dieser Fahrzeuge wird Malware auf die AU installiert, bei den andere beiden Fahrzeugen werden keine Veränderungen vorgenommen [Bißmeyer2013].

Das Opfer-Fahrzeug bewegt sich mit einer konstanten Geschwindigkeit von 14 m/s (50,4 km/h). Zu Beginn des Tests fährt das Fahrzeug des Angreifers (Fahrzeug A), auf dem die Malware installiert ist, im Abstand von 350 m hinter dem Opfer [Bißmeyer2013]. Nachdem Fahrzeug A in der Kommunikationsreichweite des Opfers ist, entdeckt die Malware das Opfer-Fahrzeug und führt einen EEBL-Angriff (Emergency Electronic Brake Light) aus, indem ein „Ghost Vehicle“ erstellt wird [Bißmeyer2013].

Der Angreifer generiert CAMs für A1 (Ghost Vehicle) bevor diese eine EEBL Warnung broadcastet. Diese EEBL-DENM wird anschließend vom Opfer empfangen und in dessen Fahrzeug angezeigt [Bißmeyer2013].

Überholt das Opfer A1 wird dies von der Malware erkannt und eine neues „Ghost“ Fahrzeug vor dem Opferfahrzeug platziert [Bißmeyer2013]. Dieser Angriff wird solange wiederholt bis der Angreifer die Kommunikationsreichweite des Opfers verlässt [Bißmeyer2013].

Als Gegenmaßnahme wird eine Plausibilitätsprüfung auf der Anwendungsschicht vorgeschlagen [Bißmeyer2013]. Das gleiche Szenario, welches zuvor beschrieben wurde, wird auch hier angewandt. Das Ergebnis zeigt, dass dem Fahrer anhand der Plausibilitätsprüfung keine gefälschte Warnung angezeigt wird [Bißmeyer2013].

Im Methodenteil wurde bereits der „Malware-Angriff“ und die „Bogus Information Attack“ beschrieben. Das Paper zeigt im Vergleich dazu die Kombination der beiden Angriffe und deren Auswirkungen.

4.1 Fazit und Ausblick

Zusammenfassend kann zu dieser Arbeit gesagt werden, dass die sicherheitsrelevanten Aspekte in Car2X Protokollen erfolgreich dargelegt werden konnten. Zunächst wurde die zukünftige Kommunikation zwischen Fahrzeugen untereinander sowie zwischen Fahrzeugen und Infrastruktur beschrieben. Es konnte aufgezeigt werden, dass die Sicherheit des Nachrichtenaustausches durch die „Public Key Infrastructure“ gewährleistet wird. Weiterhin wurde festgestellt, dass durch Zertifikate die Integrität, die Authentizität und die Privatsphäre des Nutzers bzw. des Fahrers geschützt wird.

Trotz der implementierten Sicherheitsmechanismen stellte sich heraus, dass es verschiedene Angriffspunkte gibt. Diese Bachelorarbeit zeigt auf, dass das VANET für Angriffe anfällig ist, die ebenfalls im OSI-Schichtenmodell zu Problemen führen. Ein Beispiel hierfür ist der DOS-Angriff, welcher auf die Verletzung der Verfügbarkeit eines Systems abzielt.

Neben den durch das OSI-Schichtenmodell bekannten Angriffen, kam diese Arbeit außerdem zu dem Ergebnis, dass auch neue Angriffsmöglichkeiten entwickelt wurden, die eine Bedrohung für die Netzwerkteilnehmer darstellen. Es können demnach durch Manipulation von GPS-Signalen Nachrichten mit verfälschten Informationen erzeugt werden. Eine Folge dessen wäre, dass ein Fahrzeug nicht mehr in der Lage ist mit anderen Verkehrsteilnehmern zu kommunizieren.

Des Weiteren wurde herausgefunden, dass es trotz der Verteilung von Pseudonymzertifikaten möglich ist, mittels im Klartext übertragener Daten ein Fahrzeug zu verfolgen.

Für alle vorab beschriebenen Sicherheitslücken wurden anschließend verschiedene Lösungsvorschläge analysiert.

Es besteht auch in Zukunft durchaus Bedarf sich mit Sicherheitslücken im Bereich der V2X Kommunikation auseinanderzusetzen.

Man könnte beispielsweise das Injizieren falscher Nachrichten, die von einem virtuellen Fahrzeug ausgehen, weiter untersuchen. Neben der Authentifizierung des Senders könnten noch Mechanismen zur Erkennung eines nicht existierenden Verkehrsteilnehmers implementiert werden.

Verschiedene Paper haben sich bereits mit der Evaluierung von Erkennungsmechanismen beschäftigt. Ein Beispiel hierfür ist das Paper [Bißmeyer2013] welches eine Plausibilitätsüberprüfung vorgeschlagen und getestet hat, um virtuelle Fahrzeuge zu erkennen. In Zukunft ist es vorstellbar zu prüfen, ob und wie eine Integration solcher Systeme in die ETSI-Referenzarchitektur möglich ist.

Auch die Umsetzung einer sicheren Zeitsynchronisation in VANET, um Angriffe wie GPS-Spoofing zu verhindern, wäre ein interessantes Thema für künftige Untersuchungen.

Literaturverzeichnis

[Almalag2013] Almalag, Mohammad S.; Weigle, Michele C.; Olariu, Stephan (2013): MAC Protocols for VANET. In: Stefano Basagni (Hg.): Mobile ad hoc networking. Cutting edge directions, Bd. 44. Second edition. Hoboken, New Jersey: Wiley (IEEE series on digital & mobile communication), S. 599–618.

[Autolitano2013] Autolitano, Alessia; Campolo, Claudia; Molinaro, Antonella; Scopigno, Riccardo M.; Vesco, Andrea (2013): An insight into Decentralized Congestion Control techniques for VANETs from ETSI TS 102 687 V1.1.1. In: 2013 IFIP Wireless Days (WD). Valencia, Spain, 13.11.2013 - 15.11.2013: IEEE, S. 1–6.

[Baier2016] Baier, Harald Prof. Dr.; Magraf, Marian Prof. Dr.; Edelkamp, Stefan Prof. Dr.; Gärtner, Sebastian; Ossenbühl, Sven (2016): IT-Sicherheit. Hochschule Darmstadt.

[Billman2016] Billman, Johan; Hellström, Victor (2016): Abusing Keep-Alive Forwarding to flood a VANET. When safety messages become a safety risk. Linköping University.

[Bittl2015a] Bittl, Sebastian; Gonzalez, Arturo A.; Myrtus, Matthias; Beckmann, Hanno; Sailer, Stefan; Eissfeller, Bernd (2015): Emerging attacks on VANET security based on GPS Time Spoofing. In: 2015 IEEE Conference on Communications and Network Security (CNS). Florence, Italy, 28.09.2015 - 30.09.2015: IEEE, S. 344–352.

[Bittl2015b] Bittl, Sebastian; Aydinli, Berke; Roscher, Karsten (2015): Effective Certificate Distribution in ETSI ITS VANETs Using Implicit and Explicit Requests. In: Mohamed Kassab, Marion Berbineau, Alexey Vinel, Magnus Jonsson, Fabien Garcia und José Soler (Hg.): Communication Technologies for Vehicles, Bd. 9066. Cham: Springer International Publishing (Lecture Notes in Computer Science), S. 72–83.

[Bittl2017] Bittl, Sebastian (2017): Efficient Secure Communication in VANETs under the Presence of new Requirements Emerging from Advanced Attacks. Humboldt-Universität zu Berlin.

[Bißmeyer2011] Bißmeyer, Norbert; Stübing, Hagen; Schoch, Elmar; Götz, Stefan; Stotz, Jan Peter; Lonc, Brigitte (2011): A generic public key infrastructure for securing car-to-x communication.

[Bißmeyer2013] Bißmeyer, Norbert; Schröder, Klaus Henrik; Petit, Jonathan; Mauthofer, Sebastian; Bayarou, Kpatcha M. (2013): Short paper: Experimental analysis of misbehavior detection and prevention in VANETs. In: 2013 IEEE Vehicular Networking Conference. Boston, MA, USA, 16.12.2013 - 18.12.2013: IEEE, S. 198–201.

[Bißmeyer2014] Bißmeyer, Norbert (2014): Misbehavior Detection and Attacker Identification in Vehicular Ad-hoc Networks. Technische Universität Darmstadt.

[Brahim2015] Brahim, Mohamed Ben; Hamida, Elyes Ben; Filali, Fethi; Hamdi, Noureddine (2015): Performance impact of security on cooperative awareness in dense urban vehicular networks. In: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Abu Dhabi, United Arab Emirates, 19.10.2015 - 21.10.2015: IEEE, S. 268–274.

[CAR2007] CAR 2 CAR Communication Consortium Manifesto. Overview of the C2C-CC System (2007).

[Chen2014] Chen, Lei; Englund, Cristofer (2014): Cooperative ITS — EU standards to accelerate cooperative mobility. In: 2014 International Conference on Connected Vehicles and Expo (ICCVE). Vienna, Austria, 03.11.2014 - 07.11.2014: IEEE, S. 681–686.

[Dreßler2013] Dreßler, Patrick (2013): Funksysteme, Protokolle und Anwendungen der Car-to-X-Kommunikation. Technische Universität Ilmenau.

[ETSI2009a] ETSI TR 102 638 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions (2009).

[ETSI2009b] ETSI ES 202 663 - V1.1.0 - Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band (2009).

[ETSI2010a] ETSI TS 102 636-3 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture (2010).

[ETSI2010b] ETSI TS 102 637-3 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service (2010).

[ETSI2010c] ETSI EN 302 665 - V1.1.1 - Intelligent Transport Systems (ITS); Communications Architecture (2010).

[ETSI2011a] ETSI TS 102 636-5-1 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol (2011).

[ETSI2011b] ETSI TS 102 637-2 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (2011).

[ETSI2011c] ETSI TR 102 863 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization (2011).

[ETSI2012a] ETSI TS 102 940 - V1.1.1 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management (2012).

[ETSI2012b] ETSI TS 102 941 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management (2012).

[ETSI2012c] ETSI EN 302 663 - V1.2.0 - Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band (2012).

[ETSI2013a] ETSI TS 101 539-1 - V1.1.1 - Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification (2013).

[ETSI2013b] ETSI TS 102 894-1 - V1.1.1 - Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications (2013).

[ETSI2013c] ETSI TS 102 894-2 - V1.1.1 - Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary (2013).

[ETSI2013d] ETSI EN 302 636-2 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios (2013).

[ETSI2014a] ETSI TS 102 894-2 - V1.2.1 - Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary (2014).

[ETSI2014b] ETSI EN 302 636-3 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture (2014).

[ETSI2014c] ETSI EN 302 636-4-1 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality (2014).

[ETSI2014d] EN 302 637-2 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (2014).

[ETSI2014e] ETSI EN 302 637-3 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service (2014).

[ETSI2016] ETSI TS 103 248 - V1.1.1 - Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP) (2016).

[ETSI2018] ETSI TR 103 415 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management (2018).

[Festag2014] Festag, Andreas (2014): Cooperative intelligent transport systems standards in europe. In: IEEE Commun. Mag. 52 (12), S. 166–172. DOI: 10.1109/MCOM.2014.6979970.

[Fuchs2015] Fuchs, Hendrik; Hofmann, Frank; Löhr, Hans; Schaaf, Gunther (2015): Car-2-X. In: Hermann Winner, Stephan Hakuli, Felix Lotz und Christina Singer (Hg.): Handbuch Fahrerassistenzsysteme. Wiesbaden: Springer Fachmedien Wiesbaden, S. 525–540.

[Gramaglia2012] Gramaglia, Marco; Bernardos, Carlos J.; Soto, Ignacio; Calderon, Maria; Baldessari, Roberto (2012): IPv6 address autoconfiguration in geonetworking-enabled VANETs: characterization and evaluation of the ETSI solution. In: J Wireless Com Network 2012 (1), S. 1538. DOI: 10.1186/1687-1499-2012-19.

[Gu2016] Gu, Pengwenlong; Khatoun, Rida; Begriche, Youcef; Serhrouchni, Ahmed (2016): Vehicle Driving Pattern Based Sybil Attack Detection. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Sydney, Australia, 12.12.2016 - 14.12.2016: IEEE, S. 1282–1288.

[Hamida2015] Hamida, Elyes; Noura, Hassan; Znaidi, Wassim (2015): Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. In: Electronics 4 (3), S. 380–423. DOI: 10.3390/electronics4030380.

[Hobert2015] Hobert, Laurens; Festag, Andreas; Llatser, Ignacio; Altomare, Luciano; Visintainer, Filippo; Kovacs, Andras (2015): Enhancements of V2X communication in support of cooperative autonomous driving. In: IEEE Commun. Mag. 53 (12), S. 64–70. DOI: 10.1109/MCOM.2015.7355568.

[IEEE2012] LAN/MAN Standards Committee of the IEEE Computer Society: IEEE Std 802.11™-2012, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: WLAN MAC and PHY specifications.

[Käfer2015] Käfer, Thomas (2015): Car-Forensics 4.0. Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung. Norderstedt: Books on Demand.

[Khodaei2015] Khodaei, Mohammad; Papadimitratos, Panos (2015): The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems. In: IEEE Veh. Technol. Mag. 10 (4), S. 63–69. DOI: 10.1109/MVT.2015.2479367.

[Kloiber2010] Bernhard Kloiber, Thomas Strang, Fabian de Ponte-Müller, Cristina Rico Garcia und Matthias Röckl (2010): An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications. 35th Australian Conference on Optical Fibre Technology (ACOFT 2010). Melbourne, VIC, 05.12.2010 - 09.12.2010: IEEE.

[Lin2015] Lin, Lan; Misener, James A. (2015): Message Sets for Vehicular Communications. In: Antonella Molinaro, Riccardo Scopigno und Claudia Campolo (Hg.): Vehicular ad hoc networks. Standards, solutions, and research. Cham, Switzerland: Springer, S. 123–163.

[Lonc2016] Lonc, Brigitte; Cincilla, Pierpaolo (2016): Cooperative ITS security framework: Standards and implementations progress in Europe. In: 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Coimbra, Portugal, 21.06.2016 - 24.06.2016: IEEE, S. 1–6.

[Menouar2011] Menouar, Hamid; Filali, Fethi; Abu-Dayya, Adnan (2011): Efficient and unique identifier for V2X events aggregation in the Local Dynamic Map. In: 2011 11th International Conference on ITS Telecommunications. St. Petersburg, Russia, 23.08.2011 - 25.08.2011: IEEE, S. 369–374.

[Moalla2011] Moalla, Rim; Lonc, Brigitte; Labiod, Houda; Simoni, Noemie (2012): How to secure ITS applications? In: 2012 The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net). Ayia Napa, Cyprus, 19.06.2012 - 22.06.2012: IEEE, S. 113–118.

[Mokhtar2015] Mokhtar, Bassem; Azab, Mohamed (2015): Survey on Security Issues in Vehicular Ad Hoc Networks. In: Alexandria Engineering Journal 54 (4), S. 1115–1126. DOI: 10.1016/j.aej.2015.07.011.

[Nasrallah2016] Nasrallah, Yamen Y.; Al-Anbagi, Irfan; Mouftah, Hussein T. (2016): Adaptive Backoff Algorithm for EDCA in the IEEE 802.11p protocol. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC). Paphos, Cyprus, 05.09.2016 - 09.09.2016: IEEE, S. 800–805.

[Nema2014] Nema, Megha; Stalin, Shalini Prof.; Lokhande, Vijay Prof. (2014): Analysis of Attacks and Challenges in VANET. In: International Journal of Emerging Technology and Advanced Engineering.

[Payerl2013] Payerl, Christian; BSc (2013): Integration von Car-to-X Kommunikation in die E/E-Architektur von Fahrzeugen. Technische Universitat Graz.

[Pierpaolo2016] Pierpaolo, Cincilla; Omar, Hicham; Benoit, Charles (2016): Vehicular PKI scalability-consistency tradeoffs in large scale distributed scenarios. In: 2016 IEEE Vehicular Networking Conference (VNC). Columbus, OH, USA, 08.12.2016 - 10.12.2016: IEEE, S. 1–8

[Popescu-Zeletin2010] Popescu-Zeletin, Radu; Radusch, Ilja; Rigani, Mihai Adrian (2010): Vehicular-2-X Communication. State-of-the-Art and Research in Mobile Vehicular Ad hoc Networks: Springer.

[Sakiz2017] Sakiz, Fatih; Sen, Sevil (2017): A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. In: Ad Hoc Networks 61, S. 33–50. DOI: 10.1016/j.adhoc.2017.03.006.

[Sandonis2016] Sandonis, Victor; Soto, Ignacio; Calderon, Maria; Urueña, Manuel (2016): Vehicle to Internet communications using the ETSI ITS GeoNetworking protocol. In: Trans. Emerging Tel. Tech. (3), S. 1–16. DOI: 10.1002/ett.2895.

[Schmidt2008] Schmidt, Robert K.; Leinmüller, Tim; Böddeker, Bert (2008): V2X-Kommunikation. Eching.

[Schröder2013] Schröder, Henrik (2013): Analysis of Attack Methods on Car-to-X Communication Using Practical Tests. Master-Thesis. Technische Universität Darmstadt.

[Schumacher2012] Schumacher, Henrik; Tchouankem, Hugues; Nuckelt, Jörg; Kürner, Thomas; Zinchenko, Tetiana; Leschke, Andre; Wolf, Lars (2012): Vehicle-to-Vehicle IEEE 802.11p performance measurements at urban intersections. In: 2012 IEEE International Conference on Communications (ICC). Ottawa, ON, Canada, 10.06.2012 - 15.06.2012: IEEE, S. 7131–7135.

[Sjöberg2013] Sjöberg, Katrin (2013): Medium access control for vehicular ad hoc networks. Zugl.: Göteborg, Univ., Diss., 2013. Göteborg: Chalmers Univ. of Technology (Doktorsavhandlingar vid Chalmers Tekniska Högskola, N.S., 3513).

[Strubbe2017] Strubbe, Thomas; Thenée, Nicolas; Wieschebrink, Christian (2017): IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen. In: Datenschutz Datensicherheit - DuD 41 (4), S. 223–226. DOI: 10.1007/s11623-017-0762-7.

[Tanuja2015] Tanuja, K; Sushma, T M; Bharathi, M; Arun, K H (2015): A Survey on Vanet Technologies. In: IJCA 121 (18), S. 1–9. DOI: 10.5120/21637-4965.

[Tubbene2015] Tubbene, Halvard (2015): Performance Evaluation of V2V and V2I Messages in C-ITS. Norwegian University of Science and Technology.

[Ullmann2016] Ullmann, Markus; Thomas Strubbe; Christian Wieschebrink (2016): Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication. In: InfoWare 2016, November 13-17, 2016 - Barcelona, Spain, Tfv3, InfoWare, 2016, Seville, gnd/115543370X. - [Wilmington, Del.] : IARIA.

[URL_1] Development of accident figures in Germany since 1970. Online verfügbar unter https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTgM_4GgeWVNoE7cYQoJnYRK-LU2uKPH-bEiMgl9Ypmf9Tj0H-y-g, zuletzt geprüft am 04.09.2018.

[Wang2012] Wang, Qing; Fan, Pingyi; Letaief, Khaled Ben (2012): On the Joint V2I and V2V Scheduling for Cooperative VANETs With Network Coding. In: IEEE Trans. Veh. Technol. 61 (1), S. 62–73. DOI: 10.1109/TVT.2011.2167249.

[Wiedersheim2010] Wiedersheim, Bjorn; Ma, Zhendong; Kargl, Frank; Papadimitratos, Panos (2010): Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In: 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS). Kranjska Gora, 03.02.2010 - 05.02.2010: IEEE, S. 176–183.

[Wu2014] Wu, Qiong; Zheng, Jun (2014): Performance modeling of the IEEE 802.11p EDCA mechanism for VANET. In: 2014 IEEE Global Communications Conference. Austin, TX, USA, 08.12.2014 - 12.12.2014: IEEE, S. 57–63.

[Yang2009] Yang, Yanbin; Wei, Yulin (2009): A MAC Scheme with QoS Guarantee for MANETs. In: IJCNS 02 (08), S. 759–763. DOI: 10.4236/ijcns.2009.28088.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Mittweida, 24.09.2018