Hochschule Reutlingen
Reutlingen University

INF
Informatik

Uwe Kloos, Natividad Martínez, Gabriela Tullius (Hrsg.)

Informatics Inside
Digital Future

Informatik-Konferenz an der Hochschule Reutlingen
10. Mai 2017

ISBN 978-3-00-056455-0

Impressum

Anschrift:
Hochschule Reutlingen / Reutlingen University
Fakultät Informatik
Human-Centered Computing
Alteburgstraße 150
D-72762 Reutlingen

Telefon: +49 7121 / 271-4002
Telefax: +49 7121 / 271-4042

E-Mail: infoinside@reutlingen-university.de
Internet: http://www.infoinside.reutlingen-university.de

Organisationskomitee:
Prof. Dr. Gabriela Tullius, Hochschule Reutlingen
Prof. Dr. Natividad Martínez, Hochschule Reutlingen
Prof. Dr. Uwe Kloos, Hochschule Reutlingen

Lukas Brand
Heiko Brumme
Tobias Fleischer
Gamze Gök
Isabel Hagen
Denise Junger
Mücahit Karabulut
Dina Kurbanismailova
Arjana Mehmeti
Armin Müller
Iana Preuß
Marc Roswag
Anastasia Schmieder
David Schneider
Oliver Streicher
Benjamin Weinert

Hochschule Reutlingen
Reutlingen University

Herstellung und Verlag: Hochschule Reutlingen
ISBN 978-3-00-056455-0

Inhaltsverzeichnis

Longpaper

Sicherheitsinfrastruktur in einem VANET – Architektur und Schwachstellen

Marc Roswag
Reutlingen University
Marc.roswag@Student.
Reutlingen-University.DE

Abstract
Das Ziel dieser Arbeit ist die Infrastruktur einer modernen Fahrzeug-zu-Fahrzeug Kommunikation auf ihre Sicherheit zu prüfen. Dazu werden die Sicherheitsstandards für die Funkkommunikation genauer beschrieben und anschließend mit möglichen Angriffsmodellen geprüft. Mit dem erläuterten Wissen der VANET Architektur werden verschiedene Angriffe verständlicher. Dadurch werden die Schwachstellen offengelegt und Gegenmaßnahmen an passenden Punkten in der Architektur verdeutlicht.

Schlüsselwörter
IT-Security, VANET, 802.11p, C2C, V2X

CR-Kategorien
B.4.1 Data Communications Devices, B.4.2 Input/Output Devices, D.4.6 Security and Protection, C.2.0 Security and protection

1 Einleitung

Das Fahrzeuge immer mehr über eine kabellose Verbindung in ein gemeinsames Netzwerk integriert werden sollen, ist in der Automobil Branche deutlich ersichtlich. Sobald ein Gerät kabellos in ein Netzwerk integriert wird, besteht eine deutlich höhere Gefährdung durch Cyber Angriffe auf ein solches Gerät. Die Motivation ein Fahrzeug über ein solches Netzwerk anzugreifen sind trivial. Es besteht durch das hohe Risiko, welches sich daraus ergibt, ein hoher Bedarf an Gegenmaßnahmen. Das dies bereits im Gange ist und auch durchaus nie mit Sicherheit vermieden werden kann zeigt der Angriff von den Sicherheitsforschern Charlie Miller und Chris Valasek, den es offenbar gelungen ist über ein Uconnect-Infotainmentsystem von Fiat Chrysler Kontrolle über das Internet von der Ferne aus über ein Fahrzeug gelangen konnten. [17] Es konnten sogar über den CAN-Bus das Bremsen und Beschleunigen des Fahrzeuges betätigt werden, ohne dass der Fahrer Einfluss darauf hatte. [17]

Für die Sicherheit eines solchen Netzwerkes haben sich sechs bedeutende europäische Automobilhersteller zusammengeschlossen, um einen Sicherheitsstandard für die Fahrzeug-zu-Fahrzeug Kommunikation zu bestimmen. Dieser Zusammenschluss nennt sich Car-to-Car Communication Consortium C2C CC. [13]

Im folgenden Abschnitt wird der Begriff V2X Kommunikation eingeführt und anhand dessen das Themengebiet VANET

Betreuer Hochschule: Prof. Dr.-Ing. Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
13.03.2017 Hochschule Reutlingen

verdeutlicht. Dabei wird auch auf die übertragenden Informationen eingegangen, um ein Verständnis darüber zu erlangen, wie wichtig die Sicherheit eines solchen Netzwerkes ist.

Anschließend wird der Standard 802.11p beschrieben, welcher speziell für VANETs konzipiert wurde. Dabei werden auch Sicherheitsstandards beschrieben.

In Kapitel 4 wird die Architektur mit allen wichtigen Komponenten in einem VANET beschrieben. Anhand dieser Komponenten wird der Ablauf des Systems offengelegt, um daran Schwachstellen der Architektur zu verdeutlichen.

Abschließend werden verschiedene bekannte Angriffe vorgestellt, welche ein VANET gefährden. Für diese Angriffe werden auch Schutzmaßnahmen angesprochen.

Abgeschlossen wird diese Arbeit mit einer kurzen Zusammenfassung der Fakten und einen Ausblick, welcher die Gegenmaßnahmen gegen einige Angriffe nochmals aufgreift.

2 V2X Kommunikation

V2X Kommunikation ist ein allgemeiner Begriff für den Austausch von Informationen zwischen Fahrzeugen selbst oder mit dessen Umgebung (Die Umgebung bildet sich aus der Architektur, welche in Kapitel 4 genauer beschrieben wird). V2X Kommunikation unterteilt sich in zwei Bereiche, welche in den folgenden Abschnitten genauer beschrieben werden. Zum einen geht es um den Austausch zwischen einem Fahrzeug und einer Infrastruktur (V2I), welche Straßenbaken [1] oder umliegenden Tankstellen und ähnliches bestehen kann. Diese senden einem Fahrzeug in der Nähe Informationen über den aktuellen Verkehrsstand und den Straßenzustand. Zum anderen gibt es den Bereich Fahrzeug-zu-Fahrzeug Kommunikation (V2V), bei welchem sich Fahrzeuge in der Nähe untereinander Informationen senden können. Bei dieser Technik verhält sich jedes Fahrzeug ähnlich wie ein Router, welcher Informationen entgegennehmen kann und diese auch weiterleiten kann. So können also auch Informationen über eine größere Distanz versendet werden, als es die Reichweite eines einzelnen Routers auf einer bestimmten Frequenz zulässt. [2]

2.1 V2I

Bei V2I Kommunikation, handelt es sich ausschließlich um den Nachrichtenaustausch zwischen einem Fahrzeug und einer statischen Instanz. Diese statischen Instanzen können am Straßenrand oder Tankstellen installierte Geräte sein, welche das Fahrzeug mit Informationen für den umliegenden Streckenbereich versorgen. [1] In dieser Arbeit wird jedoch der Schwerpunkt auf die im folgenden beschriebene V2V Kommunikation gelegt.

2.2 V2V

Es gibt für die Fahrzeug-zu-Fahrzeug Kommunikation viele ähnliche Abkürzungen, welche ähnliches oder sogar das gleiche bedeuten. Beispielsweise C2C (Car-to-Car) oder auch VANET, welches sich spezifischer auf die Technologie dahinter bezieht.[3]

2.2.1 Technische Probleme

V2V nutzt eine WLAN Technik, welche im Ad-Hoc Modus fungiert. Das bedeutet, dass dabei Daten direkt zwischen den Clients übertragen werden. Alle Clients sind dabei gleichberechtigt und können ohne Umwege mit einander kommunizieren. Direkt bedeutet in diesem Sinne ohne über einen Router bzw. Access-Point als Nachrichtenübermittler Daten auszutauschen. [4] Vergleicht man jedoch ein V2V Ad-Hoc Netzwerk mit einem alltäglichen WLAN, welches im Ad-Hoc Modus ohne zusätzliche Infrastruktur agiert, gibt es entscheidende Unterschiede.

Die herausstechenden Anforderungen an das Ad-Hoc Netzwerk bei V2V sind kurz gesagt die folgenden:

- Schnell wechselnde Kommunikationspartner
- Stark schwankende Kommunikationsdichte
- Schneller Informationsaustausch ohne Verzögerung
- Sicherheit

Bei der Fahrzeug-zu-Fahrzeug Kommunikation wechseln beispielsweise die Kommunikationspartner ständig. Nachdem ein Fahrzeug an einer Kreuzung abbiegt, wechseln Kommunikationspartner sehr schnell. Hinzu kommt, dass die stark wechselnde Anzahl an Kommunikationspartnern und die dabei entstehenden Nachrichten. Auf einer Autobahn mit viel Verkehr und sehr vielen weiteren Fahrzeugen, wird es viel Kommunikation geben, welche redundante Informationen beinhalten und die zur Verfügung stehenden Kanäle belegen. Dagegen kann es auch sein, dass bei Nacht auf einer großen Straße keine Kommunikationspartner vorhanden sein können. Zusammenfassend lässt sich feststellen, dass eine stark schwankende Kommunikationsdichte eine Herausforderung an das Ad-Hoc Netzwerk bei der V2V Kommunikation darstellt. [3] Außerdem wird eine Anforderung sein, dass Informationen ohne Verzögerungen übertragen werden. Bei großen Geschwindigkeiten beim aneinander Vorbeifahren auf einer Autobahn in entgegengesetzter Richtung müssen Informationen schnell ausgetauscht werden können. [1,3]

2.2.2 Sicherheitsaspekte

Ein weiterer sehr relevanter Aspekt und Großteil in dieser Ausarbeitung ist die IT-Sicherheit bei einer V2X Kommunikation. Die Sicherheit zielt in diesem Feld weniger auf die Verschlüsselung von Daten hin, welches im Normalfall bei IT-Sicherheit eine große Rolle spielt und als *Confidentiality* bekannt ist, sondern viel mehr auf die Zuverlässigkeit, Echtheit von Daten und die Anonymität der Fahrer. Dafür werden in der IT-Sicherheit allgemein die Begriffe *Integrity*, für eine unveränderliche Nachricht und *Authority*, für das Authentifizieren eines Netzwerkteilnehmers verwendet. Es werden Sicherheitsmechanismen eingesetzt, welche verhindern sollen, dass gefälschte Warnnachrichten versendet werden können. Durch eine solche Manipulation des Systems wird die Sicherheit, worauf V2X hinzielt, viel mehr gefährdet als geschaffen. [1]

3 Der 802.11p Standard für V2X Kommunikation

Für die Architektur eines VANET, hat das Institute of Electrical and Electronics Engineers IEEE einen neuen Standard für 802.11 Wireless Verbindungen definiert. Dieser Standard nennt sich 802.11p. Für diesen Standard wird die Dedicated Short Range Communication DSRC verwendet, welche für eine Kommunikation auf kurze Reichweiten und sehr geringe Latenzzeiten verantwortlich ist. [8]

Dafür wurde ein Frequenzband im 5,9 GHz Spektrum reserviert. USA hat ein 75 MHz Band (von 5,850 GHz – 5,925 GHz) dafür vorgesehen und Europa ein 30 MHz Band. [16] In folgender Abbildung ist zu erkennen, dass Europa das Frequenzband in dem höheren Frequenzbereich erweitern kann bei Bedarf. Der Frequenzraum ist in 7 Kanäle unterteilt. [2]

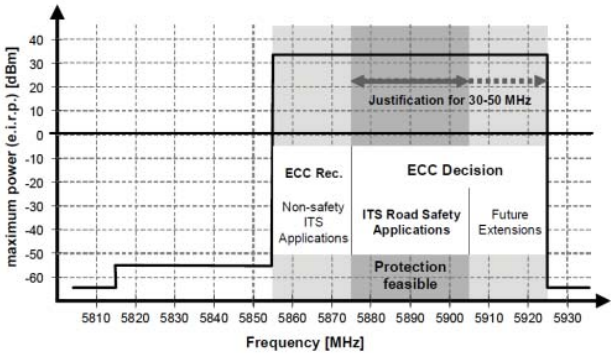

Abbildung 1: Genutzer Frequenzbereich für 802.11p in Europa [2]

Die Arbeitsgruppe 802.11p ist aus den Aktivitäten von 802.11a und 802.11g entstanden und nutzt die hohe Datenrate von 54 Mbit/s für die Fahrzeugkommunikation. Mit der 802.11p-Technik wird eine zuverlässige Schnittstelle für intelligente Transportsysteme (ITS) etabliert.

Die Randbedingungen für diesen Standard sehen eine Fahrgeschwindigkeit von bis zu 200 km/h, einen Entfernungsbereich von 1 km und eine Datentransferrate zwischen 4 ms und 50 ms und eine äußerst geringe Latenzzeit von 4 ms vor. [2]

Für den 802.11p Standard ist das Widerrufen von Zertifikaten eine Kernfunktion, um die Sicherheit zu gewährleisten. [13] In folgender Abbildung ist die Sicherheitsinfrastruktur beschrieben. Dabei ist A der Sender und B der Empfänger.

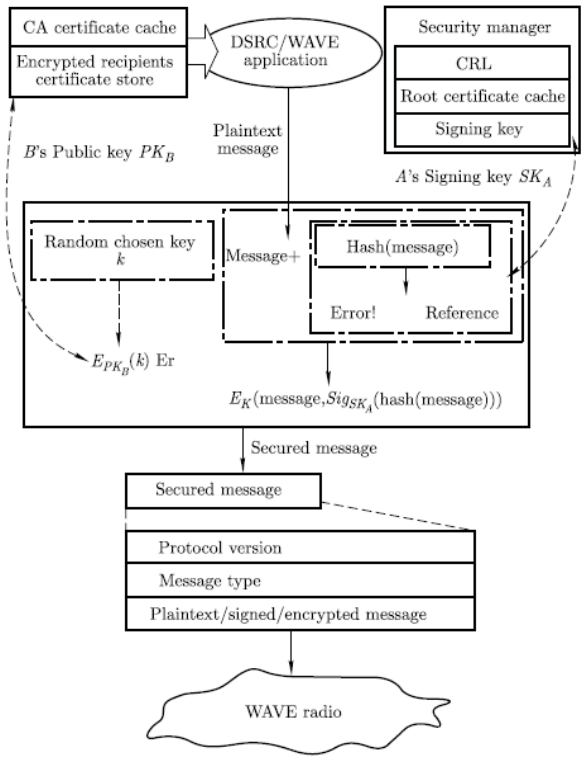

Abbildung 2: Sicherheitsinfrastruktur nach dem 802.11p Standard [13]

Es ist zu erkennen, dass es einen Zertifikatspeicher gibt, welches mit dem PK_b verschlüsselt wird. Dieses wird zusammen mit der eigentlichen Nachricht mit Hilfe einer Hashfunktion zusammen in ein Paket verpackt und dann als sichere Nachricht versendet. Daraus entsteht eine WAVE-Nachricht. So ist die Nachricht am Ende durch das Zertifikat und den öffentlichen Schlüssel signiert und verschlüsselt.

4 VANET

VANET (engl. Vehicular ad-hoc network) ist ein wichtiges Thema im Bereich der V2V Kommunikation. Es handelt sich dabei um ein eine besondere Form von MANET (engl. Mobile ad-hoc network), welches jedoch eigene technische Ansprüche stellt, wegen der bereits erwähnten technischen Anforderungen bei V2V Kommunikation aus Kapitel 2.2. [6] Da es sich bei VANET um ein Ad-Hoc Netz handelt, lässt sich sagen, dass ohne eine feste Infrastruktur zwischen den Fahrzeugen kommuniziert wird. Es bilden sich dynamische vermaschte Netze, zwischen denen Nachrichten entweder Broadcast oder Multicast gesendet werden können. [4] Bei Broadcast Nachrichten, ist allgemein zu beachten, dass es für einen Angreifer erstmal möglich ist diese Nachrichten abzufangen. Dies wird bei einigen Angriffen aus Kapitel 5 ausgenutzt.

4.1 Architektur

Die allgemeine Architektur für die V2V Kommunikation wurde vom „Car 2 Car Communication Consortium“ vorgeschlagen. Bei der Architektur wird zwischen 3 Kommunikationsbereichen Unterschieden. [4]

- Inter-vehicle communication
- Vehicle-to-roadside communication
- Inter-roadside comunication

Der erste Bereich „Inter-vehicle communication“ bezeichnet die Kommunikation zwischen den Fahrzeugen. De zweite Bereich „Vehicle-to-Roadside“ bezeichnet die Kommunikation zwischen Fahrzeug und den Straßenbaken. Der Dritte Bereich „Inter-roadside communication“

bezeichnet die Kommunikation zwischen den Straßenbaken selbst. [6]

Die Infrastruktur am Straßenrand, wie es hauptsächlich in den USA und Japan genutzt wird [3], werden als sogenannte RSUs (engl. road-side unit) bereitgestellt. [6] Das C2C CC gibt auch die vorausgesetzte Hardware in einem Fahrzeug vor. Es wird erwartet, dass jedes Fahrzeug über eine OBU (engl. On-board unit) und eine AU (engl. application unit) besitzt. [6] Die folgende Abbildung 4 zeigt die daraus entstehende Architektur für VANETs.

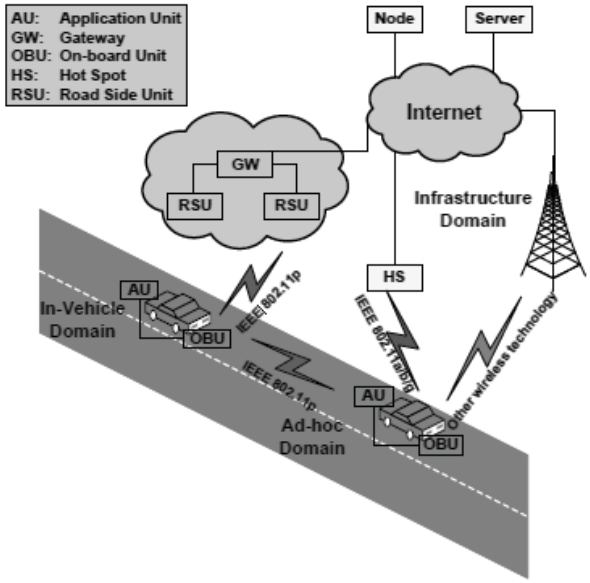

Abbildung 3: VANET Architektur nach den Vorgaben von C2C CC [6]

4.1.1 Die Road-Side Unit

RSUs sind Geräte, welche an festen Positionen am Fahrbahnrand befestigt sind. Im Laufe dieser Arbeit wurde diese bereits als Straßenbaken bezeichnet. Sie enthalten mindestens eine Kommunikationseinheit, um die Kommunikation mit Fahrzeugen (der OBU) oder anderen RSU ermöglicht. RSUs bilden die Infrastruktur für ein VANET Netzwerk. [6] Zusätzlich zu der Kommunikationseinheit, welche für den Datenaustausch mit Fahrzeugen und umliegenden RSUs zuständig ist, haben RSUs weitere Kommunikationseinheiten installiert, welche, wie in Abbildung 3 zuerkennen, über das Internet die Infrastruktur für den Informationsaustausch erweitern.

4.1.2 Die On-Board Unit

Jedes Fahrzeug empfängt und sendet Nachrichten über die On-Board Unit (OBU). [7] Diese Sendeleistung dieser OBU ist so dimensioniert, dass sie über kurze Reichweiten schnell eine hohe Datenrate übertragen kann. Diese basiert auf dem 802.11p Standard, welche in einem hohen Frequenzbereich Daten überträgt. Durch diese Eigenschaft, wird die V2V Kommunikation zu einem hochdynamischen mobilen Ad Hoc Netzwerk (VANET), welches kleine Cluster von Fahrzeugen erzeugt, die wiederum miteinander kommunizieren können. [10]

Die Forschung beabsichtigt OBUs auf einen Authentifizierungsplan basierend zu konstruieren, bei welchem die Fahrzeuge selbst zertifizierende Schlüsselpaare erzeugen.[7] Ein Schlüsselpaar besteht wie bei asymmetrischen Kryptoverfahren üblich aus einem öffentlichen und einem privaten Schlüssel. Die selbst Zertifizierung soll mit Hilfe eines Prüfwertes bei der *Trusted Authority* TA initialisiert und geprüft werden bei der Registrierung in ein VANET. [7] TAs gehören wie RSUs zu den statischen Komponenten in einem VANET. Das heißt sie sind festinstallierte Geräte am Straßenrand. Der Prüfwert wird durch eine Einweg-Hashfunktion berechnet. Dieser Wert wird darauf hin an mehrere Fahrzeuge in der Umgebung gesendet, damit diese Nachrichten ebenfalls überprüfen können. [7]

4.1.3. Die Application Unit

Application Units (AUs) können sich als einfach Anwendungen definieren lassen, welche mit der OBU kommunizieren und darüber die eigentliche Kommunikation bei VANET einleiten. [9] AUs lassen sich in zwei Kategorien unterteilen. Zum einen die Unterhaltungsanwendungen, welche beispielsweise das Chatten mit umliegenden Fahrzeugen erlauben.[6] Wichtiger für diese Arbeit ist jedoch die andere Kategorie,

welche sich auf die sicherheitsrelevanten Anwendungen bezieht. [6]Diese überwachen den Datenverkehr. Beispielsweise welche Daten vertraulich sind und auch welche Datenrelevant sind, um das VANET nicht zu überlasten.

Außerdem kann man auch unterscheiden zwischen festinstallierten AUs und portable AUs. Sicherheitsrelevante AUs sind oft auch festinstalliert. Die Architektur gibt jedoch auch die Möglichkeit, Geräte über eine drahtlose Verbindung mit der OBU zu verbinden. Das können zum Beispiel Smartphones sein. [6] AUs haben zum einen die Möglichkeit die Kommunikation über das VANET zu nutzen, können jedoch auch auf viele Sensoren wie GPS, welche ein Fahrzeug zur Verfügung stellt, zugreifen. [6] An dieser Stelle ist bereits zu erkennen, dass die Sicherheit nicht unterschätzt werden sollte, da über diesen Eingang schnell in das System eingedrungen werden kann. Die Anzahl an AUs, welche einem Fahrzeug hinzugefügt werden können ist derzeit noch nicht beschränkt. [6]

Bei der V2X Kommunikation sind schon verschiedene Anwendungen in Überlegung. Besonders für den sicherheitsrelevanten Bereich, welcher durch V2X erreicht werden soll. Dazu gehören Anwendungen, welche V2V Kommunikation nutzen, um Fahrzeuge zu warnen vor Unfallstellen oder auch die Verbindung mit einem Rettungswagen, welcher seine Route an umliegende Fahrzeuge weitergibt, damit eine Rettungsschleuse schnell entstehen kann. [6] Außerdem soll auch die V2I Kommunikation für Rettungseinsätze genutzt werden, damit ein Rettungswagen eine Ampelschaltung beeinflussen kann, so dass dieser schneller und sicherer zu einem Unfallort gelangen kann. [6] Auch an dieser Stelle, ist die bösartige Absicht eines Angreifers keineswegs auszuschließen und es muss in einem VANET durch entsprechende Sicherheitsmaßnahmen entgegengewirkt werden.

4.1.4 Sicherheitskomponenten

Event Data Recorder EDR:

Die EDR ist vergleichbar mit einer Black-Box in einem Flugzeug, welche für das mitschreiben von Daten während der Fahrt verantwortlich ist. Es werden hier Daten gespeichert wie beispielsweise GPS Daten, Geschwindigkeit, Zeit und empfangene Nachrichten. Dies hilft besonders bei der Nachprüfung bei einem Unfall. [11]

Trusted Component TC oder auch Tramper Proof Device TPD:

Die TC ist für den Schutz der kryptografischen Materialien verantwortlich. Es handelt sich hierbei um eine Hardware, welche Schlüssel speichert und Verschlüsselungsoperationen ausführt. [11] Diese Hardware nutzt eine eigene Stromversorgung, welche sich gelegentlich mit Hilfe der Fahrzeugelektronik wieder auflädt. [7] In dieser wird auch ein sogenanntes *Wurzelzertifikat* des Landes gespeichert, bei der Herstellung eines Fahrzeuges. [18]

Electronic Licence Plate ELP:

Bei ELP handelt es sich um eine elektronische Lizenz, welche ähnlich wie das Nummernschild eines Fahrzeuges für die einzigartige Identität eines Fahrzeug steht. So kann bei einem Diebstahl geprüft werden, ob es sich um das korrekte Auto handelt. [12]

Vehicular Public Key Infrastructure VPKI:

Es gibt eine sehr große Anzahl an Fahrzeugen, welche aus verschiedenen Ländern und Regionen kommen und weite Strecken zurücklegen. Dabei ist ein robustes, internationales und skalierbares Schlüssel-Management sehr wichtig. VPKI steht für eine solche Infrastruktur, welche sich aus den verschiedenen Trustet Authoritys TAs und den Fahrzeugen bildet. TAs können hierbei auch durch zertifizierte Fahrzeuge bereitgestellt werden. [7]

Authentification:

Um das Einmischen von Dritten in den Datenverkehr oder gefälschten Daten im Netzwerk vorzubeugen, ist eine Authentifizierung der Pakete erforderlich, bei der sich der Sender in gewisser Hinsicht ausweißt. Bei V2X Kommunikation wird hier für derzeit das *elliptic curve cryptography EEC* Verfahren verwendet. [11] Dies ist ein sehr komplexes asymmetrisches Kryptoverfahren, welches der Nachfolger des *Rivest, Shamir and Adleman RSA* Verfahrens darstellt. Bei asymmetrischen Verschlüsselungsverfahren entsteht durch die Komplexität der Berechnungsfunktionen ein hoher Grad an Overhead. Dies könnte weiterhin reduziert werden, in dem nur kritische Nachrichten signiert werden. [7]

Privatsphäre:

Privatsphäre ist ein wichtiger Faktor für die Akzeptanz von VANETS bei der Bevölkerung und ist demnach auch für den Erfolg und die Durchsetzung sehr relevant. Die Gefährdung der Geheimhaltung wird besonders durch den großen Overhead und dem Datenverkehr zwischen den Fahrzeugen beeinflusst. Dabei werden Informationen über die Zeit, der Position und der Identität übermittelt, welche präzise den Sender ermitteln lassen. [13] Es ist jedoch für die Authentifizierung Voraussetzung, dass sich ein Teilnehmer in einem Netzwerk identifizieren kann um autorisiert zu werden. Ein Nummernschild an einem Fahrzeug ist gewissermaßen nichts anderes als die Identität eines Fahrzeuges. Man kann bei der Identität zwischen Personen gebundener Identität und Fahrzeug gebundener Identität unterscheiden. [14,15] Es ist in einem VANET sinnvoll, ein Fahrzeug von dem falsche Nachrichten ausgehen zu identifizieren, da der Fahrer nicht in jedem Fall dafür verantwortlich ist. Es können Fehler in der Software vorliegen, durch Implementierungsfehler oder durch absichtliche bösartige Manipulation von Dritte. Für die Identifizierung eines Fahrzeugs kann in der Nachricht einfach gehalten die ELP mitgesendet werden.

Die Gesetzeslage steht jedoch derzeit dem gegenüber und macht grundsätzlich den Fahrzeughalter für derartige bösartige Gefährdung des Straßenverkehres verantwortlich. (§7 StVG) [14]

Sichere Positionierung:

Ein Fahrzeug könnte eine gefälschte GPS Position senden, um beispielsweise in einem Haftungsfall zu flüchten oder benachbarte Fahrzeuge zu täuschen. Dafür ist eine Prüfung der Positionsdaten durch mehrere Instanzen notwendig. [7] Es wird die Position von mehreren Fahrzeugen geprüft, welche sich in der Nähe des betroffenen Fahrzeuges befinden. Dies wird außerdem von einer Basis-Station vorgenommen. [7]

4.1.5 CA – Zertifizierungsinstanz

Als zentrale und vertrauenswürdige Instanz für die Erstellung von Zertifikaten, ist die CA verantwortlich. Von dieser Instanz werden VANET-Identitäten als gültige Netzwerkteilnehmer zertifiziert. Dafür sendet ein Teilnehmer Informationen zur seiner Identität an die CA, welche diese mit ihrem privaten Schlüssel verschlüsselt und so eine Identität zertifiziert. Die CA sollte daher einen sehr hohen Grad an Sicherheit genießen, da der private Schlüssel einer solchen Instanz ein primäres Ziel eines Angreifers ist. Wenn ein Angreifer diesen Schlüssel bekommen würde, könnte dieser selbst Zertifikate erstellen, welche nicht von echten Zertifikaten zu unterscheiden wären. [15] Zudem wird eine CA-Hierarchie gebildet, in welcher sich CAs gegenseitig Zertifizieren können.

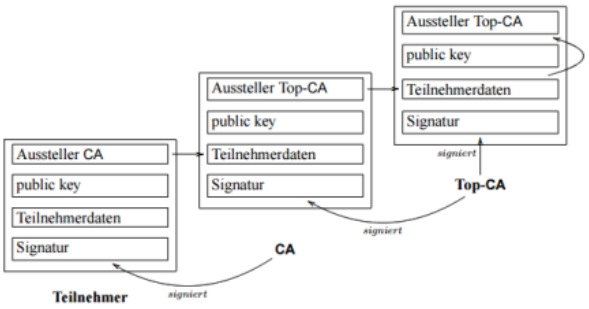

Abbildung 4 Zertifizierung- Hierarchie [15]

5 Angriffe auf ein VANET

Sobald ein Risikomanagement im Bereich Verkehrskommunikation über VANET zum Einsatz kommt, wird schnell deutlich, dass es einen sehr hohen Bedarf an Gegenmaßnahmen vor Angriffen verlangt. Dies ergibt sich aus einmal dem Grad der Wahrscheinlichkeit, dass es potenzielle Angreifer gibt und die Auswirkungen, welche dadurch entstehen können. Dass die Motivation von Angreifern in diesem Bereich gegeben ist, wurde bereits zu Beginn dieser Arbeit gezeigt. Auch die Auswirkungen sind teilweise vorgestellt worden. Verkehrsteilnehmer können statt unterstützt, verwirrt werden durch falsche Nachrichten. Dadurch würde sich das Risiko für einen Unfall stark erhöhen. Die genaue Auswirkung, müsste im Einzelfall betrachtet werden. Es muss dabei die Art eines Angriffes klar sein. Im Folgenden werden einige verschiedene Angriffsmöglichkeiten vorgestellt und die Auswirkungen und mögliche Gegenmaßnahmen untersucht.

- Eavesdropping / Sniffing

Bei Eavesdropping oder auch Sniffing handelt es sich um das Abhören von Datenpaketen. Dies ist nur Hilfreich für den Angreifer, wenn die Pakete unverschlüsselt sind. Diese Art von Angiffen ist auch für Angreifer mit wenig Knowhow und Ressourcen einfach durchzuführen. In Erinnerung an Kapitel 4.1.4 im Abschnitt Authentifikation, wird klar, dass dieser Angriff durch die Verschlüsselung mit einem modernen asymmetrischen Verfahren verhindert wird.

- Spoofing / Masquerading

Bei diesem Angriff versucht ein Angreifer die Identität eines anderen Netzteilnehmers anzunehmen oder zumindest seine eigene Identität zu fälschen. Der Angreifer muss dafür seine Hardware Adresse ändern können. Die Quelladeresse einer Nachricht sollte in einem VANET ebenfalls auf ihre Korrektheit und Gültigkeit geprüft werden.

- Replay Attack

Hierbei wird eine Nachricht kopiert und wiederholt gesendet, um eine gültige Signatur nachzuahmen. Mit Hilfe von Zufallszahlen in einem Paket (Nonces) kann ein solcher Angriff unterbunden werden.

- Cheating with positioning information

Der Angreifer versucht seine GPS-Informationen zu fälschen. Auch hier sollten Nachrichten verglichen werden und so auf ihre Korrektheit überprüft werden. [15]

- Movement patterns

Bei dieser Art von Angriff, versucht der Angreifer nach mehrmaligem Abhören von Nachrichten und dessen Position ein Bewegungsmodell eines oder mehrerer Teilnehmer zu erstellen. Hierbei sollte das Abhören der Nachrichten unterbunden werden. Auch die Quelladresse sollte verschlüsselt sein. [15]

- Denial of service

Einer der bekanntesten und oft auch effektivsten Angriffe. Hier bei versucht ein oder mehrere Angreifer sehr viele Nachrichten in das Netz einzuschleusen, um das System außerbetrieb zu nehmen. Nachrichten von anderen Teilnehmern werden durch Nachrichtenstau blockiert oder Router (Fahrzeuge) durch den Nachrichtenstau überlastet. Es ist schwierig sich von dieser Art von Angriffen effektiv zu schützen, jedoch gibt es verschiedene Ansätze. Einer wäre, frühzeitig ungewöhnliches Verhalten von Netzteilnehmern zu entdecken und Nachrichten von diesen Teilnehmern sofort zu verwerfen bzw. zu blockieren. [6]

- Sinkhole Attackes /selective forwarding

Hierbei werden vereinzelnd Pakete verworfen, um ein gezieltes Verhalten eines Verkehrsteilnehmers zu erzeugen oder zu unterbinden. Möglich ist dies beispielsweise durch einen Man-in-the-Middle Angriff. Dies ist in einem Ad-Hoc Netzwerk wie ein VANET, jedoch nur schwer möglich, da Nachrichten auf direktem Wege gesendet werden. Es müssten dafür die Routing-Tabelle eines Netzwerkteilnehmers manipuliert werden, was durch

entsprechende Gegenmaßnahmen zu unterbinden ist.[15]

- Sybil attackes

Bei diesem Angriff versucht ein Angreifer mehrere Netzwerkteilnehmer zu erstellen, um dadurch die Kooperation zwischen den Netzwerkteilnehmern zu untergraben. Dies ist durch Identitätsüberprüfung bei der Registrierung in ein VANET zu unterbinden. Es sollten hier nur gültige Teilnehmer zugelassen werden. [15]

- Worm hole

Dieser Angriff ist nach dem Prinzip eines Wurmloches zwischen zwei Galaxien aufgebaut. Zwei Angreifer arbeiten dabei zusammen und versuchen Nachrichten von Netzteilnehmern zu kopieren und an einem anderen Ort im Netz einzuspeisen. Beispielsweise steht Angreifer 1 in einem Stau und sendet alle Nachrichten weiter an Angreifer 2, welcher sich weit weg auf einer wenig befahrenden Straße befindet. Angreifer 2 speist die Nachriten in seinem Gebiet ein, um so falsch Informationen zu verbreiten - *Bogus Information*. [vgl. 18]

Anhand dieser Angriffe erkennt man, dass ein Großteil durch die Verschlüsselung der beschriebenen PKI unterbunden wird. Die gesamte Infrastruktur eines VANET sollte für die IT-Sicherheit jedoch noch einige weitere Sicherheitsmechanismen aktivieren, um einen hohen Grad an Sicherheit zu gewährleisten. Durch die Verhaltensanalyse von Netzwerkteilnehmern können Angriffe frühzeitig erkannt werden und entsprechende Gegenmaßnahmen *(siehe Kapitel 4 – sichere Positionierung)* eingeleitet werden.

6 Literaturverzeichnis

[1] Robert K. Schmidt, Tim Leinmüller, Bert Böddeker, V2X Communication https://www.tu-ilmenau.de/fileadmin/media/telematik/schmidt/080718_V2X-Kommunikation.pdf, 2008, letzter Zugriff: 27.02.2017

[2] Andreas Lübke, The current status of Car-to-X communication, Volkswagen AG, Wolfsburg, Deutschland, https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/Personalhomepages/Personalhomepages-IuI/luebke/VDE_2008_Luebke_Paper.pdf, 2008, letzter Zugriff: 27.02.2017

[3] Benjamin Schinzel, V2V Vehicle-to-Vehicle Communication, https://www.cs.hs-rm.de/~linn/fachsem0809/V2V_Komm/V2V_Fachseminar_Schinzel.pdf, Fachhochschule Wiesbaden, 2009, letzter Zugriff: 15.02.2017

[4] Jogendra Majhi, Optimized Collision Warning Protocol in VANET, http://ethesis.nitrkl.ac.in/6800/1/Optimized_Majhi_2015.pdf, 2015, letzter Zugriff: 06.03.2017

[5] Michael Meincke, Peter Tondl, María Dolores Pérez Guirao, Klaus Jobmann, Wireless Adhoc Networks for Inter-Vehicle Communication https://www.ikt.uni-hannover.de/uploads/tx_tkpublikationen/MTP2002.pdf, 2002, letzter Zugriff: 08.03.2017

[6] Lars Klein, Herausforderungen in Fahrzeug-Ad-hoc Netzwerken, Communciation and Networked Systems (ComSys), https://www.uni-muenster.de/imperia/md/content/comsys/lehre/ws1516/seminar/klein-kfzfunkkommunikation.pdf, Institute of Computer Science, 2016, letzter Zugriff: 23.02.2017

[7] Saroj Kumar Biswal, On Board Unit Based Authentication for V2V Communication in VANET, http://ethesis.nitrkl.ac.in/6244/1/E-8.pdf, Department of Computer Science and Engineering National

Institute of Technology, 2014, letzter Zugriff: 27.02.2017

[8] D. Jiang and L. Delgrossi, Towards an International
Standard for Wireless Access in Vehicular Environments," in Vehicular Technology Conference, "IEEE 802.11p, 2008. VTC Spring 2008. IEEE,
ISBN: 978-1-4244-1644-8

[9] Mrunmayi S Sahasrabudhe, Meenu Chawla, Survey of Applications based on Vehicular Ad-Hoc Network (VANET) Framework, ISSN: 0975-9646
https://pdfs.semanticscholar.org/ff5b/25e0ab35547460118fd53bd3af1ab9ecce23.pdf, 2014, letzter Zugriff: 08.04.2017

[10] Bernhard Wiegel, Quality of Service in Fahrzeug-Fahrzeug-Netzen – dezentrale und schichtübergreifende Steuerung des Nachrichtenaufkommens,
https://oparu.uni-ulm.de/xmlui/bitstream/handle/123456789/2553/vts_8887_13294.pdf?sequence=1&isAllowed=y, 2013, letzter Zugriff: 03.03.2017

[11] Raya Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. "Securing vehicular communications." IEEE Wireless Communications 13, no. 5, 2006

[12] Raya Maxim, Daniel Jungels, Panos Papadimitratos, Imad Aad, and Jean-Pierre Hubaux.
"Certificate revocation in vehicular networks." Laboratory for computer Communications
and Applications (LCA) School of Computer and Communication Sciences, EPFL,
Switzerland, 2006

[13] Weidong, Security in Vehicular Ad Hoc Networks (VANETs),
https://www.researchgate.net/file.PostFileLoader.html%3Fid%3D55b40f1c5e9d9748938b457d%26assetKey%3DAS%253A273819204292614%254014422,
94993693+&cd=1&hl=de&ct=clnk&gl=de, 2013

[14] Klaus Plößl, Hannes Federath, Vorschlag für eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks,
http://svs.informatik.uni-hamburg.de/publications/2006/PlFe2006AutomotiveVanetSecInfra.pdf,
Universität Regensburg, 2006

[15] Manuel Reil, Entwurf einer Sicherheitsinfrastruktur für Vehicular Ad-hoc Networks (VANETs),
http://manuel.reil.co/Sicherheitsinfrastruktur_vanet.pdf, 2006, letzter Zugriff: 27.03.2017

[16] Ram Shringar Raw , Manish Kumar , Nanhay Singh, Security challenges, issues and their solutions for VANET,
http://airccse.org/journal/nsa/5513nsa08.pdf, 2013, letzter Zugriff: 25.02.2017

[17] Ronals Eikenberg, Hacker steuern Jeep Cherokee fern, Heise Security,
https://heise.de/-2756331, 2015, letzter Zugriff: 05.04.2017

[18] Ram Shringar Raw , Manish Kumar, Nanhay Singh, Security challanges, issues and their solutions for VANET,
http://airccse.org/journal/nsa/5513nsa08.pdf , 2013, letzter Zugriff: 26.02.2017